

ROAR

Manual de Formação:

Apoio Especializado a Vítimas de Cibercrime

.

Training Manual:

Specialised Support to Victims of Cybercrime

.

Manual de Formare:

Asistență Specializată pentru Victimele
Criminalității Informatice



ROAR
empowering
victims of
cybercrime

APAV
Asociația Pentru
Apărarea Victimei
Apoio a Vitima



This Manual was funded by the
European Union's Internal
Security Fund – Police

Promoted by:

Associação Portuguesa de Apoio à Vítima (APAV) | Portugal

Partners:

Ministério da Administração Interna (MAI) | Portugal

Procuradoria-Geral da República (PGR) | Portugal

PT Portugal | Portugal

Weisser Ring | Germany

ACTEDO | Romania

ISBN: 978-989-54855-8-1

Legal Deposit:

Title:

Training Manual: Specialised Support to Victims of Cybercrime.

Author:

2021 © APAV – Associação Portuguesa de Apoio à Vítima

Address:

APAV – Associação Portuguesa de Apoio à Vítima

Rua José Estêvão, 135 A

1150-201 Lisboa

Portugal

Tel.: +351 213 587 900

Email: apav.sede@apav.pt

Website: www.apav.pt

Facebook: www.facebook.com/APAV.Portugal

INDEX

| | |
|---|--------|
| Introducing the Training Course | 5 |
| a.1. Outcomes | 7 |
| a.2 Outline | 7 |
| a.3 Duration | 9 |
| a.4 Trainers | 9 |
| a.5. Assessment and Certification | 9 |
| Organising the Training Course | 11 |
| b.1. Resources | 11 |
| b.2 Trainer Notes | 12 |
| ANNEXES | 15 |
| PART 1 - UNDERSTANDING CYBERCRIME | 37 |
| MODULE 1 - UNDERSTANDING CYBERCRIME PHENOMENA | 37 |
| Typologies of cybercrime | 37 |
| Concepts and definitions | 37 |
| Risk factors and related behavioural vulnerabilities related to cyber-victimisation | 40 |
| MODULE 2 - LEGAL FRAMEWORK OF CYBERCRIME | 45 |
| Cybercrime in International Law and in the European Union acquis | 45 |
| National legal framework of cybercrime | 45 |
| Investigation and law enforcement main challenges | 46 |
| MODULE 3 - VICTIMOLOGY AND IMPACT OF CYBERCRIME | 53 |
| Prevalence of cybercrime | 53 |
| Impact on individual victims | 53 |
| • Physical, psychological and emotional health consequences | 54 |
| • Financial impact | 54 |
| • Fear of cybercrime and perceptions of cybersecurity | 54 |
| PART 2 - SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME | 61 |
| MODULE 4 - KEY ASPECTS OF SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME | 61 |
| Structuring specialised support to victims of cybercrime | 61 |
| • Empathy, communication techniques and emotional support | 61 |
| • Collection of information | 62 |
| • Risk assessment and development of protection plans | 62 |
| • Identification of support needs | 63 |
| • Crisis intervention | 64 |
| MODULE 5 - SPECIALISED SUPPORT TO VICTIMS OF CYBER-DEPENDENT CRIMES | 71 |
| Modi operandi and nature of the crime | 71 |
| Prevention strategies | 72 |
| Intervention strategies | 73 |
| • Strategies for preserving digital evidence | 73 |
| • To whom and how to report | 73 |
| • Strategies to overcome victimisation and its impacts | 73 |
| MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD | 81 |
| Types, modi operandi and nature of the crimes | 81 |
| • Online shopping (ecommerce) fraud | 81 |
| • Bank fraud | 81 |
| • Scams in intimate relationships (romance and dating scams) | 82 |
| Prevention strategies | 83 |
| Intervention strategies | 83 |
| • Strategies for preserving digital evidence | 83 |
| • To whom and how to report | 84 |
| • Strategies to overcome victimisation and its impacts | 84 |

| | |
|---|-----|
| MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT | 97 |
| Modi operandi and nature of the crime | 97 |
| Prevention strategies | 99 |
| Intervention strategies | 99 |
| • Strategies for preserving digital evidence | 99 |
| • To whom and how to report | 99 |
| • Strategies to overcome victimisation and its impacts | 100 |
| MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE | 109 |
| Types, modi operandi and nature of the crimes | 109 |
| • Dissemination of child sexual abuse material (CSAM) | 109 |
| • Child sexual abuse material generated online | 109 |
| • Self-generated content | 110 |
| • Live streaming of child sexual abuse | 110 |
| • Online grooming | 110 |
| • Grooming via social networks and online video games | 110 |
| Prevention strategies | 111 |
| Intervention strategies | 111 |
| • Strategies for preserving digital evidence | 111 |
| • To whom and how to report | 112 |
| • Strategies to overcome victimisation and its impacts | 112 |
| MODULE 9 - SPECIALISED SUPPORT TO VICTIMS OF CYBERBULLYING | 123 |
| Modi operandi and nature of the crime | 123 |
| Prevention strategies | 124 |
| Intervention strategies | 124 |
| • Strategies for preserving digital evidence | 124 |
| • To whom and how to report | 124 |
| • Strategies to overcome victimisation and its impacts | 125 |
| MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES | 135 |
| Types, modi operandi and nature of the crime | 135 |
| • Cyberstalking | 135 |
| • Non-consensual image sharing | 135 |
| Prevention strategies | 136 |
| Intervention strategies | 136 |
| • Strategies for preserving digital evidence | 136 |
| • To whom and how to report | 137 |
| • Strategies to overcome victimisation and its impacts | 137 |

INTRODUCTION

ABOUT THE MANUAL

Nowadays approximately 90% of EU citizens have access to the Internet¹, and the daily Internet use is rising.² In an increasingly globalised world, where physical and virtual borders are becoming blurred, the risks associated with Internet use have risen substantially. It is therefore not surprising that victimisation by data theft or fraud constitutes the sixth highest global risk, followed by victimisation by any other type of cyber attack as the seventh most likely victimisation risk.³

Cybercrime has spread to all areas of crime, with attacks being directed not only against people and property but also against States, affecting critical structures, the economy and, above all, safety and social cohesion.

Children are a particularly vulnerable group to cyber-victimisation, given their naturally limited cyber resilience abilities and their low awareness of the risks associated with internet use, combined with their increasingly earlier access to the internet due to the massification of access to smartphones and tablets.⁴ Attention should therefore be paid to the emergence of self-generated explicit sexual material, i.e. created by children or young people themselves. On the other hand, crimes related to child sexual abuse and exploitation material and to solicitation of minors to perform sexual acts have a greater likelihood of success when using the internet.⁵

Similarly, people over 55 years of age have also been associated with increased exposure to the risks of using the Internet: being less informed of these risks, they are less likely to take personal digital protection measures.⁶

The European Parliament resolution of 3 October 2017 on combating cybercrime (2017/2068(INI))⁷ contains important considerations on the impact on people's safety, integrity of their personal data as well as on the protection of privacy and fundamental freedoms, due to the significant increase in ransomware attacks, botnets and illegal system interference. This highlights the need to harmonise legal provisions relating to cybercrime and online child sexual abuse and exploitation in different Member States. To this end, strengthening cooperation among all stakeholders and between States is essential.

Victims of cybercrime must benefit fully from all their rights⁸, and Member States must focus on prevention, promoting awareness and specialist support of victimisation.

There is, therefore, an urgent need to improve understanding of cybercrime, particularly by the general population, professionals and policy-makers, and to promote aligned responses in the fight against cybercrime. To this end, the need for joined efforts and expertise of States, industry, criminal police, judicial authorities, media and civil society organisations is stressed in order to ensure effective investigations and enable a victims' rights-based approach.

Following from this position and aiming at creating useful tools for raising awareness and training in the fight against cybercrime from the victims' perspective, we developed the **"ROAR - Training Manual: Specialised Support to Victims of Cybercrime"**. This covers a set of procedures and specialised training for the support and capacity development of the victims of cybercrime. The Manual is one of the outputs of the ROAR Project, which is coordinated by APAV (Associação Portuguesa de Apoio à Vítima / Portuguese Association for Victim Support), in partnership with the Guarda Nacional Republicana (National Republican Guard), the Portuguese Attorney General's Office (Procuradoria-Geral da República) and Altice Portugal, and with the international partners: Weisser Ring (Germany) and *Equality and Human Rights Action Centre* (Romania). This Project, co-sponsored by the Internal Security Fund - Police of the European Union, seeks to raise awareness of this type of crime among civil society in general, and potential victims in particular, and to contribute to increasing cyber-resilience, the number of cybercrimes reported to the authorities and the demand for specialised support services.

¹ EUROSTAT, <https://ec.europa.eu/eurostat/databrowser/view/tin00134/default/bar?lang=en>

² In the European context, see *Special Eurobarometer 499 Report - Europeans' attitudes towards cyber security*, European Commission, pp. 9-14.

³ Global Risks Report 2020, World Economic Forum http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

⁴ *Internet Organised Crime Threat Assessment (IOCTA) Report 2019*, Europol, pp. 32-33. See also *Special Eurobarometer 499 Report - Europeans' attitudes towards cyber security*, European Commission, pp. 15-21.

⁵ *IOCTA Report 2019*, Europol, pp. 29-34.

⁶ *Special Eurobarometer 499 Report - Europeans' attitudes towards cyber security*, European Commission, pp. 46-47. See also *APAV / INTERCAMPUS Barometer, People's Perception of Cyber-security*, March 2020, pp. 11-12.

⁷ P8_TA(2017)0366, European Parliament resolution of 3 October 2017 on combating cybercrime (2017/2068(INI)).

⁸ enshrined in Directive 2012/29/EU.

INTRODUCTION

This Training Manual sets out a series of training recommendations for a specific audience who is key in supporting victims of cybercrimes, the victim support officer (VSO). The Manual also focuses on preventing and fighting cybercrime, offering useful, pragmatic and up-to-date examples and materials adapted to the European reality.

This is not a comprehensive Training Manual, rather, it offers guidelines for organising training activities for support professionals. In addition to suggesting procedures for better and more effective support to victims of cybercrime, it also seeks to promote shared reflection among the training participants on key concepts such as victims of crime, cybercrime, cyber-security or cyber-resilience.

The Course "**Specialised Support to Victims of Cybercrime**" is organised as follows:

- a. Introducing the training course
- b. Organising the training course
- c. Developing the training course
- d. Training sessions
- e. Teaching resources

INTRODUCTION

a. Introducing the training course

This Training Course "Specialised Support to Victims of Cybercrime" is targeted at victim support officers (VSOs) and is aimed at promoting their knowledge on cybercrime and associated realities such as impact on victims, legal framework and develop their skills on important aspects in communicating and interacting with victims of these crimes.

It is intended that the VSOs understand the specific characteristics of cybercrime and of its impact on victims, in order to understand better the victims' specific needs for information and support, and consequently improve the way they support and communicate with these victims.

This Training Course is also aiming at promoting awareness and empowerment of victims of cybercrime, namely by enabling the creation of cyber-resilience mechanisms and an increase in the reporting of these crimes, and at ensuring that the responses of the criminal justice system and victim support services are adequate, adapted and centered on the victim and their specific needs.

OUTCOMES

Upon completion of the training, the participants should be able to correctly recognise the different typologies and concepts associated with cybercrime, as well as other matters equally important for intervention with victims of cybercrime: the cybercrime legal framework; risk factors and the impact of cybercrime on victims; the key aspects of specialised support to cybercrime victims; specialised support to victims of different types of cybercrime, namely *modi operandi*, specific intervention and prevention strategies.

OUTLINE

| | INTRODUCTION | DURATION |
|----------|---|------------|
| | Welcome and trainer introduction Introduction of participants Training objectives and contents overview | 5 Minutes |
| | PART 1 - UNDERSTANDING CYBERCRIME | |
| Module 1 | Understanding cybercrime phenomena Typologies of cybercrime Concepts and definitions Risk factors and behavioural vulnerabilities related to cyber-victimisation | 30 Minutes |
| Module 2 | Legal framework of cybercrime Cybercrime in International Law and in the European Union acquis National legal frameworks of cybercrime Investigation and law enforcement main challenges | 45 Minutes |
| Module 3 | Victimology and impact of cybercrime Prevalence of cybercrime Impact on individual victims Physical, psychological and emotional health consequences Financial impact Fear of cybercrime and perceptions of cybersecurity | 20 Minutes |
| | PART 2 - SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME | |
| Module 4 | Key aspects of specialised support to victims of cybercrime Structuring specialised support to victims of cybercrime Empathy, communication techniques and emotional support Collection of information Risk assessment and development of protection plans Identification of support needs Crisis intervention | 80 Minutes |

INTRODUCTION

a. Introducing the training course

Module 5 Specialised support to victims of cyber-dependent crimes

Modi operandi and nature of the crimes
Prevention strategies
Intervention strategies
 Strategies for preserving digital evidence
 To whom and how to report
 Strategies to overcome victimisation and its impacts

40 Minutes

Module 6 Specialised support to victims of online fraud

Types, modi operandi and nature of the crimes
 Online shopping (ecommerce) fraud
 Bank fraud
 Scams in intimate relationships (romance and dating scams)
Prevention strategies
Intervention strategies
 Strategies for preserving digital evidence
 To whom and how to report
 Strategies to overcome victimisation and its impacts

40 Minutes

Module 7 Specialised support to victims of online identity theft

Modi operandi and nature of the crime
Prevention strategies
Intervention strategies
 Strategies for preserving digital evidence
 To whom and how to report
 Strategies to overcome victimisation and its impacts

40 Minutes

Module 8 Specialised support to children and young people victims of online sexual abuse

Types, modi operandi and nature of the crimes
 Dissemination of child sexual abuse material (CSAM)
 Child sexual abuse material generated online
 Self-generated content
 Live streaming of child sexual abuse
 Online grooming
 Grooming via social networks and online video games
Prevention strategies
Intervention strategies
 Strategies for preserving digital evidence
 To whom and how to report
 Strategies to overcome victimisation and its impacts

40 Minutes

Module 9 Specialised support to victims of cyberbullying

Modi operandi and nature of the crime
Prevention strategies
Intervention strategies
 Strategies for preserving digital evidence
 To whom and how to report
 Strategies to overcome victimisation and its impacts

40 Minutes

Module 10 Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual image sharing

Types, modi operandi and nature of the crimes
 Cyberstalking
 Non-consensual image sharing
Prevention strategies
Intervention strategies
 Strategies for preserving digital evidence
 To whom and how to report
 Strategies to overcome victimisation and its impacts

40 Minutes

INTRODUCTION

a. Introducing the training course

Each module is initially presented with a **brief theoretical/conceptual introduction** followed by a **session plan**, organised as follows:

- Topic
- Participants
- Session duration
- General objective
- Specific objectives
- Content
- Methods
- Teaching resources
- Assessment | Activities
- Observations

TOTAL DURATION OF THE TRAINING

The total duration of this Training Course is 7 hours (420 minutes).

The course should be delivered in one single day.

TRAINERS

Trainers should have a pedagogical qualification, such as a teaching certificate (*Certificado de Competências Pedagógicas* in Portugal – CCP, formerly CAP), and a background in social sciences and humanities.

ASSESSMENT AND CERTIFICATION

Training Assessment

The outcomes of the training are assessed:

- By the trainers using the Participants' Individual Training Assessment Form (see template in annex);
- By the participants using the Training Feedback Form (see template in annex).

Certification of the participants includes:

- Issuing a Vocational Training Certificate - document issued by the training entity that proves that the participant attended the training course (see certificate's template in annex);
- Assessing the participants using a continuous and interactive system, focusing on the observation of their performance in response to the activities proposed.

INTRODUCTION

b. Organising the training course

This Manual includes activities, materials for delivering the course contents, such as PowerPoint slides and handouts that support interaction during the training sessions.

Resources

To organise and deliver this Training Course, it is necessary to take into consideration the range of resources described below.

Training room and materials

The training room and the materials play an essential role when organising a training course. The trainer should consider beforehand where the course will take place, the resources needed and the list of materials required. The number of participants per course should ideally be between 10 and 18.

We suggest the use of the following checklist:

CRITERIA

CHECKLIST

- The room has appropriate acoustics and lighting
 - The room is in perfect hygiene and cleanliness conditions
 - There are enough power outlets
 - The condition and layout of the tables and chairs are appropriate
 - There is a computer with the required software (Office PowerPoint)
 - There is a datashow, speakers and a projection screen
 - There is paper and pens to distribute to the participants
 - There are teaching materials to distribute to the participants
 - There is a whiteboard and markers
-

The participants should be informed about logistics, for example: where they can have their meals during the course and the location of public transport links, such as bus stops, underground stations and nearby taxi stands.

INTRODUÇÃO

b. Organização da formação

TRAINER NOTES

PREPARING FOR THE TRAINING COURSE

- Read and understand the *ROAR - Training Manual: Specialised support to victims of cybercrime*.
- Become familiar with the resources available in this Manual, including the proposed visual aids (PowerPoint slides), activities and handouts
- Complement the reading of this Training Manual with the contents of the *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*
- Know the objectives and programme of the training course
- Prepare all documents [outline, registration forms, teaching materials, etc.] and in sufficient number to be distributed to the participants
- Set aside enough paper and pens to distribute to the participants
- Ensure you have the Attendance sheet, the Training Feedback forms and the Participants' Individual Training Assessment form
- Check the room conditions, taking into account the number of participants
- Check the room logistics: computer and data projection software and hardware

AT THE BEGINNING OF THE TRAINING COURSE

- Provide the participants with a warm welcome
- Highlight the importance of the course and the expected outcomes
- Introduce the training course objectives and outline

DURING THE TRAINING COURSE

- Interact and communicate with the participants and promote closeness
- Collect feedback on the training at different points, to enable corrections or changes to the training approach
- Validate and reinforce messages
- Ask whether there are any doubts/questions

AT THE END OF THE TRAINING COURSE

- Complete the Participants' Individual Training Assessment form
- Assess participants' experience with the course by distributing the Training Feedback forms

The PowerPoint slides are offered as a guide and support for the development of this Training Course. The trainer should not simply read them out loud, but complement them with additional information orally to enrich the presentation's content.

When presenting the slides, attention should be paid to the projected display and ensure that it is focused, centred and can be seen from anywhere in the training room. The image's brightness should be adjusted so that the participants can read the slides without darkening them.

The trainer should be aware of their delivery, and should therefore consider aspects such as:

- Tone of voice;
- Gestures;
- Body language;
- Facial expressions;
- Naming the participants;
- Images;

INTRODUÇÃO

b. Organização da formação

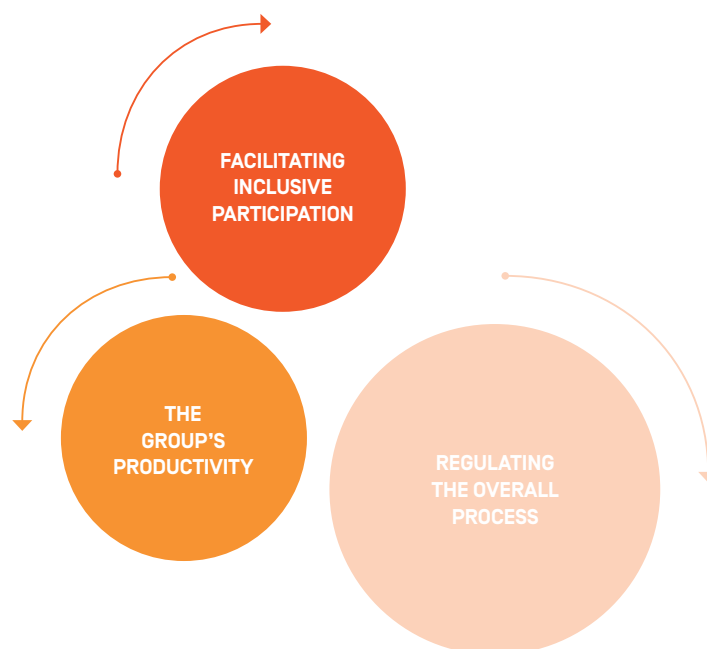
- Examples;
- Sense of humour;
- Use of analogies.

The trainer should also be mindful of how they promote participation and how they use audiovisual aids to explain, demonstrate and exemplify.

The trainer should also keep in mind the flow of the whole presentation:



The trainer should also remember that they are responsible for:



During the training, the trainer should seek to:

- Gather the facts;
- Select and demonstrate their value;
- Ensure the group's understanding;
- Take a range of roles: organising, guiding, directing, informing, interpreting, reformulating, animating, stimulating, referring, moderating and reconciling where necessary. It must do so without the participants being aware, which implies:
 - Demonstrating competency and being tactful;
 - Being able to think clearly and quickly;
 - Being able to express oneself easily;
 - Remaining impartial;
 - Being analytical;
 - Ability to resist being influenced;
 - Have self-control;
 - Be patient.

INTRODUÇÃO

b. Organização da formação

The trainer should facilitate the training course by:

- Rephrasing individual opinions, which facilitates expression of opinions, gives importance to those who express them and encourages other participants to listen to the ideas expressed, stimulating interactions;
- Summarising, which is of fundamental importance and should be done when, for example, paraphrasing and summarising a longer intervention or synthesizing two or more opinions:
 - Summarise in a sentence;
 - Partial summary after each section of the session plan;
 - Final summary.

The trainer should use a range of techniques:

| | |
|--|--|
| TEST QUESTION | Used to define a word or a concept that participants use with different connotations. It is also used to define an unknown word that a participant has used. |
| ASKING DIRECTLY FOR PARTICIPATION | Used to promote sharing/participation by a participant who for a long time has remained silent, or to give the floor to a participant who expresses their interest in participating. |
| ECHO/REVERSE QUESTION | Question put to the trainer by a participant and returned in the same form, asking the participant to share their own answer. |
| RELAY QUESTION | Repeating the question put to the trainer by one participant to another participant. |
| MIRROR QUESTION | Repeating the question put to the trainer by a participant, returning it to the group. |
| RELAUNCH QUESTION | Repeating a question asked earlier and still not answered by the group. |

In addition to these techniques, the trainer can make the training more engaging by sharing their own ideas in the form of questions, rather than making statements.

The conclusion of the session/module and/or the training day is an extremely important moment. A good wrap-up is fundamental; therefore, the trainer should:

- Be brief;
- Highlight the most important stages and/or concepts and significant key points;
- Promote the sharing of views and feedback from the participants;
- Sum up.

ANNEXES

- Course Specifications
- Timetable
- Registration Form
- Attendance Sheet
- Record of Issues and Withdrawals
- Training Feedback Form - internal participant
- Training Feedback Form - external participant
- Participants' Individual Training Assessment Form
- Final Mark Sheet

ANNEXES • Course Specifications

| DATE/S | REF. CODE | | TRAINING AREA |
|---------------------------------|--|----------------------|----------------------|
| ORGANISATIONAL TYPE OF TRAINING | INTERNAL | INTER-ORGANISATIONAL | INTRA-ORGANISATIONAL |
| TRAINING TITLE | Specialised Support to Victims of Cybercrime | | |
| TRAINERS | | | |
| TIMETABLE | TOT. TRAINING HOURS | | 7 Hours |
| VENUE | | | |
| PRE-REQUISITES | Working directly or indirectly with victims of cybercrime[s]. | | |
| TARGET AUDIENCE | Victim Support Officers [VSO]. | | |
| TYPE OF TRAINING | Other vocational training | MODE OF DELIVERY | In person |
| METHODS OF DELIVERY | Expository, interrogative and active. | | |
| GENERAL OBJECTIVE | By completing the training, the participants should be able to correctly identify the different typologies and concepts associated with cybercrime, and to acquire knowledge on other matters equally important in the intervention with victims of cybercrime, namely: the legal framework of cybercrime; risk factors and the impact of cybercrime; key aspects of specialised support to victims of cybercrime; specialised support to victims of different types of cybercrime, particularly modi operandi, specific intervention and prevention strategies. | | |

| | |
|-----------------------|---|
| OBJETIVOS ESPECÍFICOS | <p>Upon completion of the training, the trainees should be able to correctly:</p> <ul style="list-style-type: none"> • Distinguish cyber-dependent crimes from crimes enabled by the Internet and ICT; • Recognise different concepts and definitions associated with cybercrime, including types of cybercrime; • Identify sociodemographic risk factors of cyber-victimisation; • Remember the behavioural vulnerabilities related to cyber-victimisation, namely the risk factors related to Internet and ICT usage behaviours; • Recognize the legal framework of cybercrime, both under international and national legal frameworks; • Identify at least half of the challenges discussed during the course in relation to cybercrime investigation and law enforcement; • Recognise the impact of cybercrime on different areas of the lives of victims of cybercrime; • Identify the consequences of cybercrime on perceptions of cybersecurity and fear of cybercrime; • List all aspects and central steps in structuring specialised support to victims of cybercrime; • Distinguish the nature and modi operandi of different types of cybercrime; • List intervention strategies for specialised support to victims of different types of cybercrime; • Recognise the re-victimisation prevention strategies proposed for the intervention with victims of different types of cybercrime. |
|-----------------------|---|

| Course Outline | Duration | Trainers |
|---|------------|----------|
| INTRODUCTION <ul style="list-style-type: none"> • Welcome and trainer introduction • Introduction of participants • Objectives and contents of the training overview | 5 Minutes | |
| PART 1 - UNDERSTANDING CYBERCRIME | | |
| Module 1 - Understanding cybercrime phenomena <ul style="list-style-type: none"> • Typologies of cybercrime • Concepts and definitions • Risk factors and behavioural vulnerabilities related to cyber-victimisation | 30 Minutes | |
| Module 2 - Legal framework of cybercrime <ul style="list-style-type: none"> • Cybercrime in International Law and in the European Union acquis • National legal framework of cybercrime • Investigation and law enforcement main challenges | 45 Minutes | |
| Module 3 - Victimology and impact of cybercrime <ul style="list-style-type: none"> • Prevalence of cybercrime • Impact on individual victims <ul style="list-style-type: none"> • Physical, psychological and emotional health consequences • Financial impact • Fear of cybercrime and perceptions of cybersecurity | 20 Minutes | |

PART 2 - SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

Module 4 - Key aspects of specialised support to victims of cybercrime 80 Minutes

- Structuring specialised support to victims of cybercrime
 - Empathy, communication techniques and emotional support
 - Collection of information
 - Risk assessment and development of protection plans
 - Identification of support needs
 - Crisis intervention

Module 5 - Specialist support to victims of cyber-dependent crime 40 Minutes

- Modi operandi and nature of the crimes
- Prevention strategies
- Intervention strategies
 - Strategies for preserving digital evidence
 - To whom and how to report
 - Strategies to overcome victimisation and its impacts

Module 6 - Specialised support to victims of online fraud 40 Minutes

- Types, modi operandi and nature of the crimes
 - Online shopping (ecommerce) fraud
 - Bank fraud
 - Scams in intimate relationships [romance and dating scams]
- Prevention strategies
- Intervention strategies
 - Strategies for preserving digital evidence
 - To whom and how to report
 - Strategies to overcome victimisation and its impacts

Module 7 - Specialised support to victims of online identity theft 40 Minutes

- Modi operandi and nature of the crime
- Prevention strategies
- Intervention strategies
 - Strategies for preserving digital evidence
 - To whom and how to report
 - Strategies to overcome victimisation and its impacts

Module 8 - Specialised support to children and young people victims of online sexual abuse 40 Minutes

- Types, modi operandi and nature of the crimes
 - Dissemination of child sexual abuse material (CSAM)
 - Child sexual abuse material generated online
 - Self-generated content
 - Live streaming of child sexual abuse
 - Online Grooming
 - Grooming via social networks and online video games
- Prevention strategies
- Intervention strategies
 - Strategies for preserving digital evidence
 - To whom and how to report
 - Strategies to overcome victimisation and its impacts

Module 9 - Specialised support to victims of cyberbullying 40 Minutes

- Modi operandi and nature of the crime
- Prevention strategies
- Intervention strategies
 - Strategies for preserving digital evidence
 - To whom and how to report
 - Strategies to overcome victimisation and its impacts

Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images 40 Minutes

- Types, modi operandi and nature of the crimes
 - Cyberstalking
 - Non-consensual image sharing
- Prevention strategies
- Intervention strategies
 - Strategies for preserving digital evidence
 - To whom and how to report
 - Strategies to overcome victimisation and its impacts

ANNEXES • Course Specifications

EDUCATIONAL RESOURCES AND EQUIPMENT

Computer with Office software (PowerPoint) and Media Player (or other similar software) installed, overhead projector| Datashow, speakers, TV or screen, chairs, PowerPoint presentation.

SUPPORTING BIBLIOGRAPHY

APAV (2021). *RQAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*. Lisbon: APAV.

KNOWLEDGE ASSESSMENT

Diagnostic assessment by surveying the participants' expectations and level of knowledge on the subject.

Formative/summative assessment using practical activities and verification of objectives being met.

CERTIFICATION

Upon successful completion of the course a Vocational Training Certificate will be issued through the SIGO platform (Sistema de Informação e Gestão da Oferta Educativa e Formativa / Information and Management System of Educational and Training Offer) based on the following criteria:

- Course attendance of 80% or above;
- Whether the participant engaged in the activities proposed during the course ;

There are costs for issuing second copies of certificates..

ANNEXES • Timetable

COURSE: Specialised Support to Victims of Cybercrime

VENUE:

START/END TIME:

START DATE:

END DATE:

MONTH

DATE 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

MORNING

AFTERNOON

Modules

Topics

Trainer

1. Understanding cybercrime phenomena
2. Legal framework of cybercrime
3. Victimology and impact of cybercrime
4. Key aspects of specialised support to victims of cybercrime
5. Specialised support to victims of cyber-dependent crimes
6. Specialised support to victims of online fraud
7. Specialised support to victims of online identity theft
8. Specialised support to children and young people victims of online sexual abuse
9. Specialised support to victims of cyberbullying
10. Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual image sharing

ANNEXES • Registration Form

IDENTIFICATION OF THE PARTICIPANT

Full Name [*]:

Address [*]:

Postal Code [*]:

Locality [*]:

Nationality [*]:

Gender [*]:

Country of origin [*]:

Date of birth [*]:

Birth Place - Municipality[*]:

Place of birth - County [*]:

Mobile phone [*]:

E-mail [*]:

Type of identity document [*]:

☐ Residence permit
☐ Civil identification [citizen card/ID card]

☐ Military
☐ Passport

Identification document number[*]:

Valid until [*]:

Tax identification number [*]:

ACADEMIC QUALIFICATIONS

Academic qualifications [*]:

Other qualifications:

PROFESSIONAL SITUATION

Labour status [*]:

☐ 1. Employed:
☐ 2. Unemployed:
☐ 3. Other. Please specify:
☐ 4. Looking for the first job

☐ 1.1. Employee
☐ 1.2. Self-employed
☐ 2.1. Unemployed [< 12 months]
☐ 2.2. Long-term unemployed [> 12 months]

PROFESSIONAL DATA

Company [*]:

Activity sector [*]:

Position/Function [*]:

BILLING DATA

Address:

Tax identification number:

TRAINING COURSE

Training course name [*]:

Date/s [*]:

Venue [*]:

ANNEXES • Registration Form

Have you been informed and do you accept the conditions for registration and attendance of this training course and the general training rules defined in the Training Regulations? If yes, please mark X in the box.

☐

In accordance with the National Personal Data Protection Standard, the data here included can only be disclosed for the purposes of monitoring and evaluating this training. In addition to the situations mentioned above, do you authorise your personal data to be used for the communication of initiatives and information of a professional nature by APAV - Associação Portuguesa de Apoio à Vítima? If so, please mark X in the box.

☐

NOTE: Selection criteria for the applications received are:

1. Order of arrival of the application, if the number of participants exceeds the available quota
2. Maximum limit of participants planned for each training course
3. Compliance with each training course pre-defined requirements
4. Submission of the application by the registration deadline
5. Complete registration form

I declare, on my word of honour, that all the elements contained in this form are true.

Date: / /

Signature of the participant:

ANNEXES • Attendance Sheet

AÇÃO DE FORMAÇÃO

Designação da ação de formação [*]:

Data/s [*]:

Local de realização [*]:

PROFESSIONAL DATA

DATE

REF. CODE

TRAINING AREA

TRAINING TITLE Specialised Support to Victims of Cybercrime

TRAINERS

SESSION TIMES

| | | SIGNATURE | | TRAINING COORDINATION TEAM | |
|----|-----------|-----------|-----------|----------------------------|-------------|
| Nº | FULL NAME | MORNING | AFTERNOON | TIMES AND TYPE OF ABSENCE | |
| | | | | JUSTIFIED | UNJUSTIFIED |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| 6 | | | | | |
| 7 | | | | | |
| 8 | | | | | |
| 9 | | | | | |
| 10 | | | | | |
| 11 | | | | | |
| 12 | | | | | |
| 13 | | | | | |
| 14 | | | | | |
| 15 | | | | | |
| 16 | | | | | |
| 17 | | | | | |
| 18 | | | | | |
| 19 | | | | | |
| 20 | | | | | |

SUMMARY

TRAINER(S) SIGNATURE:

PEDAGOGICAL COORDINATION TEAM SIGNATURE:

ANNEXES • Record of Issues and Withdrawals

RECORD OF ISSUES AND WITHDRAWALS

TRAINING TITLE

TRAINING AREA

REF. CODE

TRAINER

DATE

SESSION TIMES

VENUE

PARTICIPANT

CONTACTS

Issues (tick X)

- ☐ Change of schedule
- ☐ Change of trainer
- ☐ Equipment failure
- ☐ Logistics problems
- ☐ Participant withdrawal
- ☐ Issue with the participants
- ☐ Issue with the trainer
- ☐ Issue with the training support staff
- ☐ Other. Which?

☐ No issues and withdrawals to be recorded

* Reason for the participant's withdrawal (mark with X)

- ☐ Health reasons
- ☐ Personal reasons
- ☐ Professional reasons
- ☐ Issue with the training provider
- ☐ Other. Which?

DESCRIPTION

DATE:

PEDAGOGICAL COORDINATION TEAM SIGNATURE:

ANNEXES • Record of Issues and Withdrawals

TO BE COMPLETED BY THE TRAINING MANAGEMENT

Categorisation of the Severity of the Issue/Complaint (mark with X)

NOT THAT SERIOUS

- ☐ Little impact on the training
- ☐ First time

SERIOUS

- ☐ Impacted on the training
- ☐ Reincident (2nd time)
- ☐ Possibility of more than 2 people affected

VERY SERIOUS

- ☐ High impact on the training
- ☐ Re-occurrence (more than 2 times)
- ☐ High number of associated complaints
- ☐ Requires intervention from the coordination team

Complaint Resolution

Resolution Date

Solution Description

Date

Executive Coordinator Signature

Communication to the interested parties

Communication mode

Date

ANNEXES • Training Feedback Form - Internal Participant

TRAINING FEEDBACK FORM - INTERNAL PARTICIPANT

DATE

REF. CODE

TRAINING AREA

COURSE/MODULE TITLE

Specialised Support to Victims of Cybercrime

TRAINERS

VENUE

DURATION

Your feedback is very important for the improvement of the quality of APAV's training. We appreciate your sincere opinion to help us improve. Please feedback using the following assessment scale:

- 1 = **Poor** (rating between 0 and 4 points);
- 2 = **Unsatisfactory** (rating between 5 and 9 points);
- 3 = **Satisfactory** (rating between 10 and 13 points);
- 4 = **Good** (rating between 14 and 17 points);
- 5 = **Very Good** (rating between 18 and 20 points).

1. Organisation of the training

- Duration of the course/module
- Room conditions (equipment/comfort)
- Pedagogical coordination

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |
| | | | | |
| | | | | |

2. Trainer

- Punctuality
- Clarity of interventions
- Content expertise (topics)
- Answers to questions/doubts
- Methods and techniques used
- Delivery of the programme
- Support materials (documentation, exercises)

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

3. Content

- Relevance of the content for the objectives and expectations
- Relevant content for your work
- Impact of the content on your professional/personal development
- Potential application of the content within 3 months

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |
| | | | | |
| | | | | |

4. Overall assessment

- of the course/module

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |

COMMENTS AND SUGGESTIONS FOR IMPROVEMENT

PLEASE SUGGEST OTHER COURSES YOU WOULD LIKE TO ATTEND

Participant Name:

ANNEXES • Training Feedback Form - External Participant

TRAINING FEEDBACK FORM - EXTERNAL PARTICIPANT

| | | |
|---|-----------|-----------------------------|
| DATE | REF. CODE | EDUCATION AND TRAINING AREA |
| COURSE/MODULE TITLE Specialised Support to Victims of Cybercrime | | |
| TRAINERS | | |
| VENUE | | DURATION |

Your feedback is very important for the improvement of the quality of APAV's training. We appreciate your sincere opinion to help us improve. Please feedback using the following assessment scale:

- 1 = **Poor** (rating between 0 and 4 points);
- 2 = **Unsatisfactory** (rating between 5 and 9 points);
- 3 = **Satisfactory** (rating between 10 and 13 points);
- 4 = **Good** (rating between 14 and 17 points);
- 5 = **Very Good** (rating between 18 and 20 points).

1. Organisation of the training

- Duration of the course/module
- Room conditions (equipment/comfort)
- Pedagogical coordination
- Value for money

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

2. Trainer

- Punctuality
- Clarity of interventions
- Content expertise (themes)
- Answers to questions/doubts
- Methods and techniques used
- Delivery of the content
- Support materials (documentation, activities)

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

3. Conteúdos

- Relevance of the content to the objectives and expectations
- Relevant content for your work
- Impact of content on your professional/personal development
- Potential use of content within 3 months

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

4. Overall assessment

- of the course/module

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |

COMMENTS AND SUGGESTIONS FOR IMPROVEMENT

PLEASE SUGGEST OTHER COURSES YOU WOULD LIKE TO ATTEND

Participant Name:

ANNEXES • Final Mark Sheet

FINAL MARK SHEET

DATE

REF. CODE

TRAINING AREA

COURSE/MODULE TITLE

Specialised Support to Victims of Cybercrime

TRAINERS

VENUE

DURATION

Your feedback is very important for the improvement of the quality of APAV's training. We appreciate your sincere opinion to help us improve. Please feedback using the following assessment scale:

- 1 = **Poor** (rating between 0 and 4 points);
- 2 = **Unsatisfactory** (rating between 5 and 9 points);
- 3 = **Satisfactory** (rating between 10 and 13 points);
- 4 = **Good** (rating between 14 and 17 points);
- 5 = **Very Good** (rating between 18 and 20 points).

Participant's full name

Final Grade

OBSERVATIONS

Trainer

Pedagogical coordination team

PARTE
PART
PARTEA

1

**COMPREENDER
O CIBERCRIME**

**UNDERSTANDING
CYBERCRIME**

**SĂ ÎNȚELEGEM
CRIMINALITATEA
INFORMATICĂ**

MOD. 1

PART 1 - UNDERSTANDING CYBERCRIME

MODULE 1 - UNDERSTANDING CYBERCRIME PHENOMENA

INTRODUCTION

Typologies of cybercrime

This Module presents definitions for the concept of cybercrime. We use different typologies and categorisations to demonstrate this phenomenon's complexity and the range of forms or types of acts included.

As these definitions and typologies are developed in Chapter 1 - Part I of the *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*, this Manual will only present a summary of this content, with emphasis on key concepts.

The trainer should point out that cybercrime can be categorised into:

- **Cyber-dependent crimes** – these are associated with new forms of crime, whose occurrence depends on the existence and use of ICT, computers and computer networks (Leukfeldt, Notté & Malsch, 2020; Maimon & Louderback, 2019). They are designated cybercrimes *stricto sensu* as their practice depends on a computer system and their aim is to attack the availability, access, integrity, authenticity, confidentiality, conservation and security of information.
- **Cyber-enabled crimes** - traditional forms of crime in which ICT plays an important role, and which include not only financially motivated crime, but also forms of interpersonal violence and sex crimes. Examples are cyberstalking or Internet scams (Leukfeldt et al., 2020).

In the latter case, the different forms of cybercrime that are made possible or enabled by the Internet and ICT can be further subdivided into:

- Financially motivated cybercrimes (e.g. phishing⁹ and romance and dating scams¹⁰);
- Cybercrimes in interpersonal relationships (e.g. cyberstalking¹¹);
- Sexual cybercrimes (e.g., revenge porn¹²).

Concepts and definitions

Let us then begin by defining the most common **cyber-dependent crimes**, also known as cybercrime *stricto sensu*, which are the focus of this Module. From Module 5 of this Training Course onwards, we will further our understanding of this type of cybercrimes by deconstructing them and presenting specific proposals for intervention and prevention.

Hacking or cracking are commonly defined as **unauthorised access to computer systems with criminal intent** (Grabosky, 2016 *cit in* Maimon & Louderback, 2019). They are associated with cyber-trespassing, which involves the unauthorised crossing of invisible boundaries of the online environment (Wall, 2001 *cit in* Maimon & Louderback, 2019).

Hacking includes a number of behaviours, such as redesigning hardware or software systems to change their intended function, as well as participating in the hacker subculture (Bachmann, 2010, Holt, 2007, Steinmetz, 2015 *cit in* Maimon & Louderback, 2019).

Spamming or SPAM, the acronym for 'Sending and Posting Advertisement in Mass', refers to the **sending of data and mass distribution** of e-mails advertising products, services or investment schemes, which may be fraudulent and even contain malware or other executable file attachment (Rathi & Pareek, 2013).

⁹ This phenomenon is addressed in Module 5 of this Training Course.

¹⁰ This phenomenon is addressed in Module 6 of this Training Course.

¹¹ This phenomenon is addressed in Module 10 of this Training Course.

¹² This phenomenon is addressed in Module 10 of this Training Course.

PART 1 - UNDERSTANDING CYBERCRIME

MODULE 1 - UNDERSTANDING CYBERCRIME PHENOMENA

Malware refers to a variety of hostile or intrusive software (e.g. computer viruses, worms¹³, ransomware¹⁴, spyware¹⁵, adware¹⁶, scareware¹⁷, etc.). This is **software intended to infiltrate equipment illicitly** in order to cause damage, alterations or theft of information. Malware can also take the form of executable code, scripts, active content and other software (Aycock, 2006 *cit in* Reep-van den Bergh & Junger, 2018).

One of the most used schemes concerns publishing content with titles that arouse curiosity or call for some kind of 'urgent' action, as well as invitations to download games or suggestions to visit new profiles.

Phishing is the mass sending of e-mails - spamming - usually with a link to a web page, which the recipients are persuaded to access, appealing to urgent causes or actions. As a rule, these e-mails request or highlight the importance of the recipients 'updating', 'validating' or 'confirming' their banking details.

These e-mails (and the pages to which they refer) are fake and constitute an approximate reproduction of the original communications made by banks, credit institutions or others that allow online payments. When accessing such pages, the user is usually asked to enter banking information, enabling the criminal to capture and misuse it.

The **distributed denial of service (DDoS) attack**, in turn, concerns an intentional attempt to overload a particular computer system, with the purpose of making it unusable (Overvest & Straathof, 2015).

Regarding **cyber-enabled crimes**, the most common are online fraud, identity theft and crimes related to child sexual abuse and exploitation.

Online fraud can take many forms:

- Online shopping (or ecommerce) fraud;
- Bank fraud;
- Scams in intimate relationships (online romance and dating scams).

Online shopping fraud presents different degrees of complexity, including simple schemes in which the seller promises to send the buyer a certain item after a bank transfer is made, but that does not happen and the buyer ends up by not receiving the item.

In **bank fraud**, we can include phishing scams used to gain access to the victim's banking information, as well as credit card fraud. Credit card fraud refers to the use of another person's credit card for personal use, without the card owner's and issuer's knowledge (Patel & Singh, 2013).

Scams in intimate relationships occur when the perpetrator seeks to establish a relationship of trust and intimacy, through the Internet and ICT, with a certain target, as a prelude to obtaining personal benefit, namely financial and patrimonial benefit.

Online identity theft includes the following cumulative acts:

- Obtaining personal and/or confidential information about another person without their knowledge;
- Possession or transfer of such data and being aware that they will be used for illicit purposes;
- Use of previously obtained data for committing crimes.

Crimes related to sexual abuse and exploitation of children and young people via the internet include:

- **Online sexual abuse**, as a wide-range concept, can be defined as encompassing **any form of child sexual**

¹³ Worms are malicious codes that spread through a network, with or without human assistance (Kienzie & Elder, 2003).

¹⁴ Ransomware is malware inserted into the system by download and creates an 'exe' file to run. The goal may include the extortion of the victim by encrypting their personal information (Kansagra, Kumhar & Jha, 2016).

¹⁵ Spyware is an automatic program that collects information about the user and their Internet usage habits and transmits this information to an external entity, without the user's knowledge and consent.

¹⁶ Adware is software that automatically displays or downloads (usually unwanted) advertising material when the user is online (Gao, Li, Kong, Bissyandé & Klein, 2019).

¹⁷ Scareware is a form of malware that misleads the user into believing that their computer is infected when in fact the system is working (Seifert, Stokes, Lu, Heckerman, Colcernian, Parthasarathy & Santhanam, 2015).

abuse in an online context. This broad concept includes different manifestations of abuse and exploitation, from non-contact sexual abuse such as harassment and grooming facilitated by ICT and the internet, social networks or other platforms, , to sharing image and/or audio content in the darkweb showing sexual abuse and exploitation of children, using previously taken photographs or video.

- **Live online child sexual abuse:** the practice of sexual acts with children and their live transmission, through live streaming services, enabling others to watch.
- **Online grooming**, which can be defined as a **process of manipulation** and a **form of solicitation** of children. It usually starts with a non-sexual approach, through the internet and ICT, including online games and social networks, in order to establish a relationship of trust with the child and persuade the child to meet face-to-face, so that the perpetrator can consummate the sexual abuse. Establishing a relationship of trust with the child, mediated by the internet and ICT, can also aim at **persuading the child to produce and share sexual content**.
- As a result of sexual abuse and exploitation, the offender can threaten or blackmail the child with the **dissemination or sharing of the self-generated sexual content**, with the aim of obtaining sexual favours, money or other benefits. This is called **child sexual extortion**.

In exploring the concepts and phenomena of child sexual abuse and exploitation online, this Module also addresses an important terminological issue:

- The expressions **child sexual abuse material (CSAM)** and **child sexual exploitation material (CSEM)** seek to replace, at least in non-legal contexts, the concept of child pornography (terminology still featuring in national and international legislation).

In the context of online aggressions in interpersonal relationships, we outline the most common cases, namely cyberbullying, cyberstalking and non-consensual sharing of images.

Cyberbullying is a form of online aggression using ICT and the internet and its associated behaviours include: the dissemination of negative/false information intended to defame the victim (by using phone calls, text messages, video messages, e-mail, chat room, websites, social networks); the victim's harassment (using the same means just mentioned) (APAV, 2011; Jahankhani et al., 2014). We also want to draw attention to sexual cyberbullying, which includes behaviours such as online sharing of rumours or lies about the victim's sexual behaviour or online sharing of information regarding the victim's intimacy, in a non-consensual manner.

Cyberbullying differs from more conventional forms of bullying as:

- it can be done at any time of the day, regardless of the need for direct contact between victim and aggressor;
- the aggressor can remain anonymous;
- it has a high potential for 'advertising' and audience reach;
- it is difficult to remove the content created (Stopbullying. Gov, 2017).

Cyberstalking can be defined as a form of stalking which, while sharing characteristics of persecution and persistent harassment such as being intrusive, repetitive, persistent and causing fear to the victim, is practised using the Internet and ICT, with the aim of threatening and harassing the victim (Maran & Begotti, 2019).

Cyberstalking practices can include different predatory behaviours: making various unwanted attempts to contact the victim via telephone, e-mail and social networks; installing spyware on the victim's computer; accessing the victim's e-mail and/or social network account without the victim's permission, to monitor private information and the victim's daily life and/or to act using their identities (Martellozzo & Jane, 2017).

Still in the field of online violence in the context of interpersonal relationships, we can add the **non-consensual sharing of images and videos** to cyberbullying and cyberstalking.

Motivations for disseminating this content can include:

- **Sexual extortion or coercion of the victim.**
- **Revenge**, often referred to as revenge porn, involving the non-consensual disclosure of intimate images of a partner, usually after the relationship has ended, as a form of retaliation.

Risk factors and behavioural vulnerabilities related to cyber-victimisation

Risk factors relate to characteristics, conditions or variables associated with a particular person that increase the probability of negative or undesirable outcomes (Reppold et al., 2002 *cit in* Maia et al., 2016).

Thus, the **risk factors associated with cyber-victimisation** are characteristics or conditions that can increase a person's probability or vulnerability to cybercrime.

In the case of cybercrime, individual characteristics may not be so significant for the occurrence of victimisation, since cybercrime involves a minimal (or even non-existent) direct interaction between victim and perpetrator. For example, in the case of malware, it is difficult to determine who the actual victim of the malicious software infection will be, since any computer can potentially be infected, regardless of the users' individual characteristics (Ngo & Paternoster, 2011).

Research is not particularly extensive in this field, as in many others areas associated with cybercrime. Nevertheless, the following risk factors have been identified:

- **Risk factors associated with socio-demographic characteristics**

The characteristics **gender**, **age** and level of **education** are addressed in this Module. *The ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*, Chapter 3 - Part I, explores more fully the results and conclusions of some studies addressing cybercrime victimisation risk factors and/or measuring these variables, aiming at defining the sociodemographic profile of the victims of different forms of cybercrime.

- **Risk factors associated with the use of the Internet and ICT**

Factors such as technological literacy and the disinhibition effect, and their contribution to the increase or reduction of vulnerability to cyber-victimisation are explored in this Module:

- **Technological literacy** refers to the awareness, knowledge and skills that enable a person to use effectively the Internet, ICT and associated equipment and tools, and also to navigate digital environments (Holt & Bossler, 2013 *cit in* Maimon & Louderback, 2019). Technological literacy appears to reduce the risk of cyber-victimisation (Holt & Bossler, 2008).
- The **disinhibition effect** refers to the process or effect that results from how physical distance affects interaction or communication through ICT, which includes the absence of direct contact in the communication process, a greater anonymity and the perception of greater control over the interaction process. The disinhibition effect can contribute to exposure to situations and/or to the adoption of online behaviours that increase vulnerability to cyber-victimisation (Agustina, 2015).

In addition to the above, this Module also explores other risk factors of cyber-victimisation, such as the **levels of use** of the Internet and ICT and the **type of activities conducted** on the Internet or through the Internet and ICT.

As mentioned in relation to the socio-demographic risk factors, the *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*, Chapter 3 - Part I, also addresses, in greater depth, each of these **cybercrime risk factors associated with the behaviour of Internet and ICT users**.

In order to gain a greater understanding of the contents covered in this Module, we suggest, in addition to carefully studying its content (above key concepts and supporting PowerPoint slides), consulting the *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*, in particular Chapters 1 and 3 - Part I.

PART 1 - UNDERSTANDING CYBERCRIME

MODULE 1 - UNDERSTANDING CYBERCRIME PHENOMENA

VSO Training - Specialised Support to Victims of Cybercrime



Specialised Support to Victims of Cybercrime

PART I – UNDERSTANDING CYBERCRIME

Module 1 – Understanding Cybercrime Phenomena



1. Understanding cybercrime phenomena

Cybercrime - Definition

Cybercrime encompasses two distinct types of crime:



1. Cyber-dependent crimes / computer crimes / Cybercrime stricto sensu

2. Cyber-enabled crimes / Cybercrime lato sensu



1. Understanding cybercrime phenomena

Typologies of cybercrime

Cyber-dependent crimes - the occurrence of these crimes depends on the existence and use of information and communications technology (ICT), computers and computer networks. Their practice depends on a computer system and their aim is to attack the availability, access, integrity, authenticity, confidentiality, conservation and security of information.

Cyber-enabled crimes – traditional forms of crime which are made possible, facilitated or enabled by the internet and ICT.



Cybercrime - Definition

1. Computer Crimes:

In cybercrime, not all crimes are computer crimes. Computer crimes are those in which information and communications technology is a means and end for the crime to be practiced and that affects one or more requirements for the operationalisation of the security of the information: **confidentiality, integrity, availability and authenticity of the information**. The practice of these crimes is punishable by the Cybercrime Law (Portugal).



Cybercrime - Definition

2. Cybercrime lato sensu:

Traditional forms of crime enabled by the use of information and communications technology. E.g.: Causing offense to someone over social networks. In these situations, unlike the previous type of crime, the computer system is not compromised in what concerns **confidentiality, integrity, availability or authenticity**.



PART 1 – UNDERSTANDING CYBERCRIME

MODULE 1 – UNDERSTANDING CYBERCRIME PHENOMENA

1. Understanding cybercrime phenomena

Concepts and definitions

Cyber-dependent crimes:

- Hacking or cracking: unauthorised access to computer systems with criminal intent
- Spamming or SPAM;
- Malware (e.g., computer virus, worms, ransomware, spyware, adware, scareware, etc.)
- Phishing
- DDoS

Cyber-enabled crimes:

- Different types of online fraud (Online shopping (e-commerce) fraud; Bank fraud; Scams in intimate relationships (online romance and dating scams).
- Online identity theft



1. Understanding cybercrime phenomena

Concepts and definitions

Cyber-enabled crimes (continuation)

- Crimes related to sexual abuse and exploitation of children and young people via the Internet
 - oAny form of online abuse
 - oOnline grooming
 - oThreat and blackmail to disseminate or share self-generated sexual content
 - oChild sexual abuse and exploitation material → differences and connection with the concept of child pornography?
 - Self-generated content
- Crimes related with online aggression
 - oCyberbullying
 - oCyberstalking
- oNon-consensual sharing of images and videos
 - E.g. revenge porn



1. Understanding cybercrime phenomena

Risk factors and behavioural vulnerabilities related with cybervictimisation

Individual characteristics do not seem to be that significant for the occurrence of victimisation - cybercrime involves a minimal (or even non-existent) direct interaction between the victim and the perpetrator

Risk factors associated with socio-demographic characteristics - **gender, age** and level of **education**

Risk factors associated with the use of the Internet and ICT

- Technological literacy
- Disinhibition effect
- Levels of use of the internet and ICT
- Type of activities conducted

Additional information: ROAR Handbook – from understanding and preventing cybercrime to supporting and empowering victims, namely Chapters 1 and 3 – Part I



PART 1 - UNDERSTANDING CYBERCRIME

MODULE 1 - UNDERSTANDING CYBERCRIME PHENOMENA

SESSION PLAN 1

1. Training

Training Title Training Course Specialised Support to Victims of Cybercrime

Modules/Topics Introduction
Understanding cybercrime phenomena

Date of Session **Time** **Total Duration** 35 minutes

Trainers

2. Specific Objectives By the end of the session, the participants should be able to correctly:

- Identify the other participants and the trainer;
- Identify the training course objectives and content ;
- Distinguish cyber-dependent crimes and cyber-enabled crimes;
- Recognise different concepts and definitions associated with cybercrime, namely types of cybercrime;
- Identify cyber-victimisation risk factors related to sociodemographic characteristics;
- List behavioural vulnerabilities related to cyber-victimisation.

3. Session Plan

| | Content | Methods | Resources | Assessment Activities | Duration (minutes) |
|--------------|---|-----------------------|--|----------------------------|-----------------------|
| Introduction | Introduction and overview: Introductions and survey of expectations Introduction of the trainer Introductions of the participants Presentation of the objectives and content of the training course | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| | Typologies of cybercrime: • Cyber-dependent crimes vs. cyber-enabled crimes | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| Development | Concepts and definitions: • Concepts and definitions: • Hacking, spamming, malware, phishing and DDoS (distributed denial of service) attack • Online fraud: online shopping (e-commerce) fraud, bank fraud and intimate relationship scams (online romance and dating scams) • Online identity theft • Online child sexual abuse and exploitation: online live child sexual abuse, online grooming and child sexual abuse material • Cyberbullying • Cyberstalking and non-consensual image sharing | Expository and active | Computer: Datashow and projection screen | Observation | 10 |
| | Risk factors and behavioural vulnerabilities related to cyber-victimisation: • Risk factors associated with socio-demographic characteristics • Risk factors associated with the use of the Internet and ICT | Expository and active | Computer: Datashow and projection screen | Observation | 10 |
| Conclusion | Concluding summary and clarification of doubts | Expository and active | Computer: Datashow and projection screen | Observation | 5 |

OBSERVATIONS

Participants:

Victim Support Officers (VSO)

Date: / /

Trainer:

PART 1 - UNDERSTANDING CYBERCRIME

MODULE 1 - UNDERSTANDING CYBERCRIME PHENOMENA

INSTRUCTIONS AND KEY INFORMATION FOR THE TRAINER

CONTENT MATCHING

Session Plan *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*

| | PART | CHAPTER |
|---|---|------------------|
| Introduction | No correspondence | |
| | Use Training Course Outline (see Annexes) | |
| Typologies of cybercrime | Part I – Understanding | Chapter 1 - 1.2. |
| Concepts and definitions | Part I – Understanding | Chapter 1 - 1.3. |
| Risk factors and behavioural vulnerabilities related to cyber-victimisation | Part I – Understanding | Chapter 3 - 3.2. |
| Concluding summary and clarification of doubts | No correspondence | |

MOD. 2

PART 1 - UNDERSTANDING CYBERCRIME

MODULE 2 - LEGAL FRAMEWORK OF CYBERCRIME

INTRODUCTION

In this Module, the trainer presents, in line with Chapter 2 - Part I of the *ROAR Handbook - from the understanding and prevention of cybercrime to the support and empowerment of victims*, the cybercrime legal framework .

Using mainly an expository teaching method, the trainer presents cybercrime in the context of **international law and in the European Union acquis**, covering:

- The Council of Europe Convention on Cybercrime of 23 November 2001¹⁸;
- The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, known as the Lanzarote Convention¹⁹;
- The Cybersecurity Strategy of the European Union²⁰;
- The European Parliament resolution on the fight against cybercrime of 3 October 2017²¹.

In this Module, some European Union Directives are also outlined:

- Directive 2011/92/EU - on combating the sexual abuse, sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA²²;
- Directive 2013/40/EU - on attacks against information systems and replacing Council Framework Decision 2005/222/JHA²³;
- Directive (EU) 2019/713 - on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA²⁴;
- Directive 2000/31/EC - on electronic commerce²⁵;
- Regulation 2016/679 - Implementing general data protection regulation (GDPR)²⁶.

This Module also presents some European and international level initiatives to fight cybercrime, including those by the INHOPE Association²⁷.

The Module continues with the presentation of the **national legal framework of cybercrime**.

The case of Portugal

The Portuguese case starts with a presentation of Law 109/2009 of 15 September 2009, the *Lei do Cibercrime* (LC), Cybercrime Law, which transposes Framework Decision 2005/222/JHA (replaced by Directive 2013/40/EU) and adapts domestic law to the Budapest Convention (CCCE).

In the Portuguese legal system, in addition to the LC, it is also possible to find provisions for crimes that can be committed by electronic means, although not exclusively, also called cyber-enabled offenses. Therefore, this Module also explores the Portuguese Penal Code and provisions on Cybercrime.

¹⁸ Council of Europe Convention on Cybercrime, Budapest, 2001. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>.

¹⁹ Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, <https://rm.coe.int/protection-of-children-against-sexual-exploitation-and-sexual-abuse/1680794e97>.

²⁰ Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; Cybersecurity Strategy of the European Union: An Open, Safe And Secure Cyberspace, Brussels, 7.2.2013, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN>.

²¹ European Parliament Resolution of 3 October 2017 on the Fight Against Cybercrime [2017/2068 (INI)], <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0366&from=EN>.

²² Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse, sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN>.

²³ Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN>.

²⁴ Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&from=EN>.

²⁵ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market [Directive on electronic commerce], <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN>.

²⁶ Regulation 2016/679, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504>.

²⁷ See <https://www.inhope.org/EN>.

The case of Romania

The Romanian legal system has no specific law on cybercrime.

Thus, the legal provisions for incrimination are provided for in the Romanian Penal Code, which is analysed in this Module, as well as other legal commitments and developments in Romania in the fight against cybercrime.

This Module concludes with a presentation and reflection on the **main challenges in cybercrime investigation and law enforcement**:

- The main challenges in cybercrime investigation and law enforcement are transversal to all European states, and are particularly felt by criminal police and prosecutors:
 - The fast circulation of online content, the anonymity offered by some platforms and encryption techniques²⁸ make it difficult or even impossible to trace the origin of online illegal content;
 - The difficulty in harmonising mechanisms for blocking illegal content makes it possible for the same content to reappear in sites situated in other countries;
 - The complexity of tools and instruments capable of processing large amounts of data in a short time;
 - The tight deadlines for preservation of evidence by Internet Service Providers (ISPs);
 - Cooperation with third countries hosting illegal content;
 - The dilemma between privacy and the provision of secretive methods of investigation.

²⁸ See, for example, Modules 8, 9 and 10 of this Training Course, where end-to-end encryption is discussed.

PART 1 - UNDERSTANDING CYBERCRIME

MODULE 2 - LEGAL FRAMEWORK OF CYBERCRIME

Specialised Support to Victims of Cybercrime

PART I – UNDERSTANDING CYBERCRIME

Module 2 – Legal Framework



2. Legal Framework of Cybercrime

- International Law and the European Union Acquis;
- Cybercrime Law, in Portugal: *Lei do Cibercrime*;
- Cybercrime in the Portuguese Penal Code: *Código Penal Português*;
- Other Legislation.

Additional information: Chapter 2 - Part I ROAR Handbook – from understanding and preventing cybercrime to supporting and empowering victims, legal Framework of cybercrime.



2. Legal Framework of Cybercrime

Internacional Law and the European Union Acquis

The Council of Europe Convention on Cybercrime of 23 November 2001;
The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, known as the Lanzarote Convention;

Directive 2011/93/EU - on combating the sexual abuse, sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA;
Directive 2013/40/EU - on attacks against information systems and replacing Council Framework Decision 2005/222/JHA;
Directive (EU) 2019/713 - on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA;
Directive 2000/31/EC - on electronic commerce;
Regulation 2016/679 - Implementing general data protection regulation (GDPR).



2. Legal Framework of Cybercrime

Internacional Law and the European Union Acquis

The most important legal instrument for cybercrime, the **Council of Europe Convention on Cybercrime, of 23 November 2001**, is aimed at «the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation», in order to «make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence».



2. Legal Framework of Cybercrime

International Law and the European Union Acquis

The Convention imposes on the State Parties an obligation to align their national substantive criminal and procedural laws to the specificities of cybercrimes, with the objective of harmonising legislation, including adequate instruments for criminal investigations and proceedings, and simplifying international cooperation, facilitating and expediting the detection, investigation, collection of evidence and location of suspects.



2. Legal Framework of Cybercrime

Lei do Cibercrime – Cybercrime Law (Portugal)

In the Portuguese legal system, the cybercrime legal Framework is mainly regulated by **Law 109/2009 of 15 September, Lei do Cibercrime (LC)**, Cybercrime Law, which transposes Framework Decision 2005/222/JAI and adapts domestic law to the Budapest Convention (CCCE).

The legal types of crimes covered by the Lei do Cibercrime are described in articles 3 to 8 of this law.



PART 1 - UNDERSTANDING CYBERCRIME

MODULE 2 - LEGAL FRAMEWORK OF CYBERCRIME

2. Legal Framework of Cybercrime

A Lei do Cibercrime – Cybercrime Law (Portugal)

Article 3 – Computer forgery

The crime of Computer Forgery takes place when, whoever, "enters, modifies, deletes or suppresses computer data or otherwise interferes with computer data". For the crime to take place it also requires that **information or documents that are not genuine are produced with the intent to cause deception in legal relations**. These conditions distinguish it from the crime of computer damage – article 4 (LQ).

Example of Computer Forgery: Josefa creates, in her computer, a document that looks like the proof of a bank transfer and sends it to mobile shop, to show that she paid the agreed price.



2. Legal Framework of Cybercrime

A Lei do Cibercrime – Cybercrime Law (Portugal)

Article 4 – Computer damage

Any person who without legal permission or without being authorised to do so, deletes, alters, destroys, in whole or in part, damages, removes or renders unusable or inaccessible programs or other computer data of others or in any way affects their ability to use, shall be punished.

The penalty is only for illegal actions. This excludes from security tests to a system, as long as they have been authorised by the owner of the system.

The legal good being protected in this type of crime is the integrity and reliability of the data and that the computer programs work correctly. Unlike the crime of Damage (article 212 Penal Code), this article not only protects property, the computer damage, beyond the patrimonial integrity of the computer data as property of the lawful owner, it also covers the functional integrity of the data in what concerns the availability and efficient use of the computer data.

Example: João's computer is infected by a virus which codifies/encrypts all data stored, which disables him from accessing it.



2. Legal Framework of Cybercrime

A Lei do Cibercrime – Cybercrime Law (Portugal)

Article 5 – Computer Sabotage

Distinguishing between computer damage and computer sabotage is not easy. In the case of computer damage, what is punished is the acts related to the computer data, while in the case of the computer sabotage, what matters is the disturbance in the operation of the computer systems or in data communication.

This legal concept also punishes the dissemination of virus and other malware, intended to cause computer sabotage (article 5, paragraph 2, LQ). In these cases there is an advance of the criminal jurisdiction to the phase of preparatory actions for the crime of sabotage.

Example: The setting up of botnets with the purpose of allowing malware to control networks: a collection of zombie computers is used for malicious activities such as DoS and DDoS attacks.



2. Legal Framework of Cybercrime

A Lei do Cibercrime – Cybercrime Law (Portugal)

Article 6 – Illegal access

The crime of illegal access seeks to protect the security of the computer system, its confidentiality. It is a crime dealing with abstract danger, intended to function as a barrier to avoid the practice of other more serious illicit activity. Therefore, for the crime to take place it is sufficient that there is access without legal permission or authorisation.

Example: The crime of illegal access is committed by someone who, without permission/authorisation to do so, accesses a private group on the social network WhatsApp created by Year 7 students, and there shares links for the sale of fake money.



2. Legal Framework of Cybercrime

A Lei do Cibercrime – Cybercrime Law (Portugal)

Article 7 – Unlawful Interception

It is a crime to intercept electronic transmissions of data via phone, fax, email or files. For the crime to take place it is not necessary that the information is actually obtained, it is enough to attempt to gain that information.

The expression 'non-public', which is used in the CCCE (article 3) in relation to illegal interception, refers to the nature of transmissions and not to the nature of the computer data. The data communicated can be information made available publicly, but the parties may wish to communicate confidentially. Alternatively, the data may be secret, for commercial purposes, until the service is paid for. Therefore, the expression 'non-public' does not exclude public networks.

Example: Pedro installs software in Maria's phone to allow him to access all her phone conversations.



2. Legal Framework of Cybercrime

A Lei do Cibercrime – Cybercrime Law (Portugal)

Article 8 – Illegal reproduction of protect program

Although the protected good is a private right, the law assumes the existence of an essential right of the State to protect intellectual property holders and this justifies an interest of the State in putting in place criminal protection measures against their violation.

Therefore, this crime does not depend on a complaint, it is a public crime.



PART 1 - UNDERSTANDING CYBERCRIME

MODULE 2 - LEGAL FRAMEWORK OF CYBERCRIME

2. Legal Framework of Cybercrime

Cybercrime in the Código Penal Português – Portuguese Penal Code

The Portuguese Penal Code and provisions on Cybercrime

Cybercrime stricto sensu is also provided for in the Portuguese Penal Code (PC). Here provision is made for crimes that affect the availability, access, integrity, authenticity, preservation and security of the information such as :

- **Article 193 - Intrusion by means of ICT**
- **Article 194 - Breach of correspondence or telecommunications**
- **Artigo 221.º - Computer fraud and communications fraud**



2. Legal Framework of Cybercrime

Cybercrime in the Código Penal Português – Portuguese Penal Code

Besides cybercrime, other common crimes can be committed and their effects enhanced by the use of technology. In this type of crime, the constitutive element of the crime is not the use of technology.

Examples:

Crimes against honour committed by displaying insulting expressions or accusations in online pages, blogs or circulated over email. The relevance of the technology regards only the use of the electronic means for the dissemination of the insulting or defaming expression and the higher potential for damage of the legal good protected (cf. Article 183/1 a) Penal Code: offense committed through means that facilitate its dissemination; and in paragraph 3 of the same article: social media, i.e. social networks).



2. Legal Framework of Cybercrime

Cybercrime in the Código Penal Português – Portuguese Penal Code

❖ **Illicit recordings and photographs** (article 199 PC) – The right to your own image covers two autonomous rights: the right not to be photographed and the right not to have that photo disseminated. The person may authorised or give consent to have their photo taken and may not authorised that the photo is used or disseminated. A person cannot be photographed or have their photo used against their will. Someone that posts the photo of another person on Facebook, against that person's wishes, even if they had legitimately taken the photo, could be accused of the crime of Illicit Recordings and Photographs, article 199 paragraph 2, of the Penal Code. (Ac. TRP de 5-06-2015)



2. Legal Framework of Cybercrime

Cybercrime in the Código Penal Português – Portuguese Penal Code

❖ **Privacy intrusion** (articles 192 and 197 PC)

❖ **Discrimination and incitement to hatred and violence** (article 240 PC)

❖ **Extortion** (article 223 PC). Normally associated with ransomware. A large amount of money, usually paid in Bitcoins, is demanded to restore a system that was compromised by a cyber attack that encrypted the data stored or the operating files.



2. Legal Framework of Cybercrime

Cybercrime no Código Penal Português – Portuguese Penal Code

❖ **Pornography of minors** (article 176 PC)

❖ **Grooming of minors** (article 176-A PC) In this case the offender (who needs to be over 18 years of age) who, using information and communications technology, grooms a minor (under 18 years of age) for a meeting aiming at the practice of sexual abuse acts of relevance (absolute or qualified) or to use a minor in a pornographic show, film or recording, is punished with a sentence of imprisonment from 1 month to 1 year. However, the sentences for this crime can be aggravated by one third, in their lower and upper limits, if the crime is jointly committed by one or more people.



2. Legal Framework of Cybercrime

Cybercrime in the Código Penal Português – Portuguese Penal Code

❖ **Domestic Violence** (article 152, paragraph 2, sub-paragraph b of the PC) – precept introduced by Law 44/2018 aiming at protecting specifically personal data (namely image or sound, which includes videos, films, photos) about intimacy (namely sexual) and the privacy of any victim (sensitive private data), when disseminated (posted/spread) through the Internet or other means of widespread public dissemination (such as through social networks), without the consent of the victim.

❖ **Stalking** (154-A PC)



PART 1 - UNDERSTANDING CYBERCRIME

MODULE 2 - LEGAL FRAMEWORK OF CYBERCRIME

2. Legal Framework of Cybercrime

A Lei do Cibercrime – Cybercrime Law (Portugal)

Article 3 – Computer forgery

The crime of Computer Forgery takes place when, whoever, "enters, modifies, deletes or suppresses computer data or otherwise interferes with computer data". For the crime to take place it also requires that **information or documents that are not genuine are produced with the intent to cause deception in legal relations**. These conditions distinguish it from the crime of computer damage – article 4 (LC).

Example of Computer Forgery: Josefa creates, in her computer, a document that looks like the proof of a bank transfer and sends it to mobile shop, to show that she paid the agreed price.



2. Legal Framework of Cybercrime

A Lei do Cibercrime – Cybercrime Law (Portugal)

Article 4 – Computer damage

Any person who without legal permission or without being authorised to do so, deletes, alters, destroys, in whole or in part, damages, removes or renders unusable or inaccessible programs or other computer data of others or in any way affects their ability to use, shall be punished.

The penalty is only for illegal actions. This excludes from security tests to a system, as long as they have been authorised by the owner of the system.

The legal good being protected in this type of crime is the integrity and reliability of the data and that the computer programs work correctly. Unlike the crime of Damage (article 212 Penal Code), this article not only protects property, the computer damage, beyond the patrimonial integrity of the computer data as property of the lawful owner, it also covers the functional integrity of the data in what concerns the availability and efficient use of the computer data.

Example: João's computer is infected by a virus which codifies/encrypts all data stored, which disables him from accessing it.



2. Legal Framework of Cybercrime

A Lei do Cibercrime – Cybercrime Law (Portugal)

Article 5 – Computer Sabotage

Distinguishing between computer damage and computer sabotage is not easy. In the case of computer damage, what is punished is the acts related to the computer data, while in the case of the computer sabotage, what matters is the disturbance in the operation of the computer systems or in data communication.

This legal concept also punishes the dissemination of virus and other malware, intended to cause computer sabotage (article 5, paragraph 2, LC). In these cases there is an advance of the criminal jurisdiction to the phase of preparatory actions for the crime of sabotage.

Example: The setting up of botnets with the purpose of allowing malware to control networks: a collection of zombie computers is used for malicious activities such as DoS and DDoS attacks.



2. Legal Framework of Cybercrime

A Lei do Cibercrime – Cybercrime Law (Portugal)

Article 6 – Illegal access

The crime of illegal access seeks to protect the security of the computer system, its confidentiality. It is a crime dealing with abstract danger, intended to function as a barrier to avoid the practice of other more serious illicit activity. Therefore, for the crime to take place it is sufficient that there is access without legal permission or authorisation.

Example: The crime of illegal access is committed by someone who, without permission/authorisation to do so, accesses a private group on the social network WhatsApp created by Year 7 students, and there shares links for the sale of fake money.



2. Legal Framework of Cybercrime

A Lei do Cibercrime – Cybercrime Law (Portugal)

Article 7 – Unlawful Interception

It is a crime to intercept electronic transmissions of data via phone, fax, email or files. For the crime to take place it is not necessary that the information is actually obtained, it is enough to attempt to gain that information.

The expression 'non-public', which is used in the CCCE (article 3) in relation to illegal interception, refers to the nature of transmissions and not to the nature of the computer data. The data communicated can be information made available publicly, but the parties may wish to communicate confidentially. Alternatively, the data may be secret, for commercial purposes, until the service is paid for. Therefore, the expression 'non-public' does not exclude public networks.

Example: Pedro installs software in Maria's phone to allow him to access all her phone conversations.



2. Legal Framework of Cybercrime

A Lei do Cibercrime – Cybercrime Law (Portugal)

Article 8 – Illegal reproduction of protect program

Although the protected good is a private right, the law assumes the existence of an essential right of the State to protect intellectual property holders and this justifies an interest of the State in putting in place criminal protection measures against their violation.

Therefore, this crime does not depend on a complaint, it is a public crime.



PART 1 - UNDERSTANDING CYBERCRIME

MODULE 2 - LEGAL FRAMEWORK OF CYBERCRIME

SESSION PLAN 2

1. Training

Training Title Training Course Specialised Support of Victims of Cybercrime

Modules/Topics Legal framework of cybercrime

Date of Session **Time** **Total Duration** 45 minutes

Trainers

2. Specific Objectives By the end of the session, the participants should be able to correctly:

- Identify the international cybercrime legal framework ;
- Identify the national cybercrime legal framework;
- Identify at least half of the challenges addressed in the training concerning cybercrime investigation and law enforcement.

3. Session Plan

| | Content | Methods | Resources | Assessment Activities | Duration (minutes) |
|--------------|--|-----------------------|--|-------------------------|--------------------|
| Introduction | Cybercrime in International Law and in the European Union acquis | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| | Cybercrime in International Law and in the European Union acquis: <ul style="list-style-type: none"> • Cybercrime in International Law and in the European Union acquis: • Council of Europe Convention on Cybercrime • Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse • Cybersecurity Strategy of the EU • European Parliament resolution on the fight against cybercrime • Directive 2011/92/EU - on combating the sexual abuse, sexual exploitation of children and child pornography • Directive 2013/40/EU - on attacks against information systems • Directive (EU) 2019/713 - on combating fraud and counterfeiting of non-cash means of payment • Directive 2000/31/EC - on electronic commerce • Regulation 2016/679 - general data protection regulation (GDPR) | Expository and active | Computer: Datashow and projection screen | Observation | 15 |
| Development | National legal framework of cybercrime | Expository and active | Computer: Datashow and projection screen | Observation | 20 |
| | Investigation and law enforcement main challenges | Expository and active | Computer: Datashow and projection screen | Observation | 3 |
| Conclusion | Concluding summary and clarification of doubts | Expository and active | Computer: Datashow and projection screen | Observation | 2 |

OBSERVATIONS

Participants:

Victim Support Officers (VSO)

Date: / /

Trainer:

PART 1 - UNDERSTANDING CYBERCRIME

MODULE 2 - LEGAL FRAMEWORK OF CYBERCRIME

INSTRUCTIONS AND KEY INFORMATION FOR THE TRAINER

CONTENT MATCHING

Session Plan *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*

| | PART | CHAPTER |
|--|-------------------------|---------------------------|
| Cybercrime in International Law and in the European Union acquis | Part I - Understanding | Chapter 2 - 2.1. and 2.2. |
| National legal framework of cybercrime | Part I - Understanding | Chapter 2 - 2.3. |
| Investigation and law enforcement main challenges | No correspondence | |
| | See Module Introduction | |
| Concluding summary and clarification of doubts | No correspondence | |

MOD. 3

PART 1 - UNDERSTANDING CYBERCRIME

MODULE 3 - VICTIMOLOGY AND IMPACT OF CYBERCRIME

INTRODUCTION

Prevalence of cybercrime

Despite the growing knowledge about diversity of cybercriminality, **information about the real scale of victimisation by different types of cybercrime is still incipient**, and therefore the real prevalence rates in the population are unknown (Reep-van den Bergh & Junger, 2018).

Despite not covered by this Course, we suggest that you read about *The dark figures of cybercrime in the ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims* (Chapter 1 - Part I), which explores the reasons and difficulties associated with knowing the real dimension of the different cybercrimes.

Next, we present some statistics analysed in the supporting PowerPoint of this Module, which show the scale of different types of cybercrime in Portugal:

- In the Portuguese context, phishing and malware infection (including ransomware) were the most registered types of incidents in 2019 by CERT.PT and RNCSIRT (National Computer Security Incident Response Team and National Computer Security Incident Response Teams Network²⁹, respectively)³⁰;
- The most frequent crimes recorded by the Safer Internet Line³¹ in 2019 were fraud, identity theft and phishing (APAV, 2019);
- Between 2009 and 2018, according to the Portuguese Directorate General for Justice Policy³², there was a steady increase in the percentage of computer crimes, crimes of intrusion by ICT and computer and communications fraud, among all crimes recorded in the country;
- Some relevant socio-demographic characteristics concerning cybersecurity incidents in Portugal in 2019 are:
 - Gender - No relevant gender differences;
 - Age - Individuals aged 25-34 are more likely to acknowledge having suffered cybersecurity incidents (35%) than individuals aged 65-74 (18%);
 - Education - In general, individuals aged between 25 and 64 and with a higher level of formal education, tend to report having been the victim of more cybersecurity incidents (40%) than those in the same age group with a lower level of formal education (17%);

We also suggest consulting Chapter 1 - Part I of the *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*, which refers, to studies, surveys and reports analysing the prevalence or incidence of these phenomena in the HIGHLIGHT | STATISTICS IN FOCUS sections.

Impact on individual victims

In this section we explore the content of Chapter 4 - Part I of the *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*. We advise reading this chapter for improving knowledge on the consequences of different types of cybercrime.

These consequences will be revisited in Modules 5 to 10 of this Training Course, which covers *strategies to overcome victimisation and its impacts*, this time analysed according to the type of cybercrime.

As stated in the ROAR Handbook, it is considered generally that the consequences experienced by victims of cybercrime are not significantly different from the consequences experienced by victims of *traditional* crimes.

It should be noted that the impact of cybercrime on the victim is very variable, being aggravated or attenuated according to a set of variables:

- **Individual variables**, namely socio-demographic characteristics and Internet usage skills and behaviour;

²⁹ Original Portuguese title: Equipa de Resposta a Incidentes de Segurança Informática Nacional and Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática, respectively.

³⁰ Report Cibersegurança em Portugal, Riscos e Conflitos, June 2020, Observatório de Cibersegurança.

³¹ Linha Internet Segura, in Portuguese.

³² In Portuguese, Direção-Geral da Política de Justiça. See detailed information at <https://estatisticas.justica.gov.pt/sites/siej/pt-pt>

PART 1 - UNDERSTANDING CYBERCRIME

MODULE 3 - VICTIMOLOGY AND IMPACT OF CYBERCRIME

- **Variables associated with the cybercrime** itself, including: the type of cybercrime, the duration of cybervictimisation, the level of publicity of the cybervictimisation and, where applicable, the relationship with the cybercrime perpetrator;
- **Variables associated with the formal and informal support network.**

Physical, psychological and emotional health consequences

To start with, it should be noted that the emotional and psychological consequences of cybercrime are largely underestimated - cybercrime is viewed as a low-impact crime (Button, Lewis, & Tapley, 2014a cit in Jansen & Leukfeldt, 2018).

Some of the consequences and reactions often pointed out are (Leukfeldt et al., 2019; Cross et al., 2016; De Kimpe et al., 2020; Jansen & Leukfeldt, 2018; Cross et al., 2016):

- loss of confidence;
- guilt;
- shame;
- anger and frustration;
- anxiety and re-experience of incidents;
- fear and sadness;
- anguish;
- feelings of insecurity, powerlessness and disappointment;
- decline in levels of self-confidence and levels of trust towards others;
- social isolation;
- depression and suicidal ideation;
- decrease in productivity;
- physical symptoms such as sleep disorders, excessive tiredness or weakness, appetite problems, headaches and nausea.

Financial impact

The financial consequences of cybercrime may include (Leukfeldt et al., 2019):

- costs incurred by the victims as a consequence of the act they were subjected to, including increased expenses with health, travel, telecommunications costs and/or the need to replace equipment;
- waste of time and loss of work hours and possible subsequent loss of income;
- additional costs associated with the need to change their routines and lifestyle, including the adoption of protection measures and the implementation of more effective cybersecurity mechanisms, moving house and/or changing place of work/study, or other.

Fear of cybercrime and perceptions of cybersecurity

With regard to the impact of cybercrime on individual victims, the *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims* also explores the fear of cybercrime and the perceived risk of cybercrime. This topic is covered in this Module. You should therefore consult Chapter 4 - Part I of the Handbook and consider the following key concepts:

- **Fear of crime** can be defined as an emotional reaction to crime and/or to symbols associated with it.
- **Perceived risk** constitutes a cognitive judgment through which people assess their own risk or probability of victimisation, based on their personal experiences, social context and circumstances, which in turn is reflected in fear of crime (Ferraro, 1995, Rontree, 1998 cit in Yucedal, 2010).

Thus:

PART 1 - UNDERSTANDING CYBERCRIME

MODULE 3 - VICTIMOLOGY AND IMPACT OF CYBERCRIME

The **perceived risk of cyber-victimisation**, as a result of cognitive processes that include analysis of personal experiences of previous cyber-victimisation (if that is the case) and of victimisation/crime clues arising from online lifestyle, can lead to **behavioural responses aimed at greater protection**. This can include setting cybersecurity measures/mechanisms and changing Internet and ICT usage behaviours (Yucedal, 2010).

There are some studies devoted to measuring the fear of cybercrime³³.

³³ See the case of Special Eurobarometer 423: *Cyber security*, available at https://www.europeandataportal.eu/data/datasets/s2019_82_2_423_eng?locale=en

PART 1 - UNDERSTANDING CYBERCRIME

MODULE 3 - VICTIMOLOGY AND IMPACT OF CYBERCRIME

Specialised Support to Victims of Cybercrime

PART I - UNDERSTANDING CYBERCRIME

Modulo 3 – Victimology and Impact of Cybercrime



3. Victimology and impact of Cybercrime

Prevalence of Cybercrime in PT

- Phishing, malware and ransomware
- Fraud
- Identity theft
- Crime of intrusion by means of ICT

2019 data; CERT.PT, RNCISRT, Linha Internet Segura/Safe Internet Line



3. Victimology and impact of Cybercrime

Impact on individual victims

It is generally considered that the consequences experienced by victims of cybercrime are not significantly different from the consequences experienced by victims of traditional crimes.

The impact of cybercrime may vary according to:

- **Individual variables:** socio-demographic characteristics, Internet usage skills and behaviour;
- **Variables associated with the cybercrime itself,** including: the type of cybercrime, the duration of cybervictimisation, the level of publicity of the cybervictimisation and, where applicable, the relationship with the cybercrime perpetrator;
- **Variables associated with the support network,** formal and informal.

To learn more about the needs of victims of cybercrime, refer to Chapter 4 - Part I do ROAR Handbook – from understanding and preventing cybercrime to supporting and empowering victims.



3. Victimology and impact of Cybercrime

Impact on individual victims

- **Physical, psychological and emotional health consequences:** loss of confidence; guilt; shame; anger and frustration; anxiety and re-experience of incidents; fear and sadness; anguish; feelings of insecurity, powerlessness and disappointment; decline in levels of self-confidence and levels of trust towards others; social isolation; depression and suicidal ideation; decrease in productivity; physical symptoms such as sleep disorders, excessive tiredness or weakness, appetite problems, headaches and nausea.
- **Financial Impact:** costs incurred by the victims as a consequence of the criminal act, waste of time and loss of work hours and possible subsequent loss of income, additional costs associated with the need to change their routines and life style.
- **Fear of cybercrime and perceptions of cybersecurity:** can lead to behavioural responses aimed at greater protection. At the same time, **personal experiences of victimisation** can increase the perceived risk of re-victimisation and, consequently, the fear of crime.



PART 1 - UNDERSTANDING CYBERCRIME

MODULE 3 - VICTIMOLOGY AND IMPACT OF CYBERCRIME

SESSION PLAN 3

1. Training

Training Title Training Course Specialised Support to Victims of Cybercrime

Modules/Topics Victimology and impact of cybercrime

Date of Session **Time** **Total Duration** 20 minutes

Trainers

2. Specific Objectives By the end of the session, the participants should be able to correctly:

- Recognise the impact of cybercrime on different areas of cybercrime victims' lives ;
- Identify the consequences of cybercrime on perceptions of cybersecurity and fear of cybercrime.

3. Session Plan

| | Content | Methods | Resources | Assessment Activities | Duration (minutes) |
|--------------|--|-----------------------|--|----------------------------|-----------------------|
| Introduction | Prevalence of cybercrime | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| | Impact on individual victims: <ul style="list-style-type: none"> • Physical, psychological and emotional health consequences • Financial impact • Fear of cybercrime and perceptions of cybersecurity | Expository and active | Computer: Datashow and projection screen | Observation | 13 |
| Development | | | | | |
| Conclusion | Concluding summary and clarification of doubts | Expository and active | Computer: Datashow and projection screen | Observation | 2 |
| | | | | | |

OBSERVATIONS

Participants:

Victim Support Officers (VSO)

Date: / /

Trainer:

PART 1 - UNDERSTANDING CYBERCRIME

MODULE 3 - VICTIMOLOGY AND IMPACT OF CYBERCRIME

INSTRUCTIONS AND KEY INFORMATION FOR THE TRAINER

CONTENT MATCHING

Session Plan

ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims

| | PART | CHAPTER |
|--|------------------------|---|
| Prevalence of cybercrime | Part I - Understanding | Chapter 1 - 1.3. See text boxes HIGHLIGHTS STATISTICS IN FOCUS |
| Impact on individuals victims | Part I - Understanding | Chapter 4 - 4.1. |
| Concluding summary and clarification of doubts | No correspondence | |

PARTE
PART
PARTEA

2

**APOIO
ESPECIALIZADO
A VÍTIMAS DE
CIBERCRIME**

**SPECIALISED
SUPPORT TO
VICTIMS OF
CYBERCRIME**

**ASISTENȚĂ
SPECIALIZATĂ
PENTRU VICTIME**

MOD. 4

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 4 - KEY ASPECTS IN SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

INTRODUCTION

Structuring specialised support to victims of cybercrime

This Module introduces a care and support approach to victims of cybercrime. It presents a set of key guidelines and core areas to consider when intervening with cybercrime victims, regardless of the type of cybercrime to which the victim has been subjected. Subsequent Modules will aim at deepening the participants' understanding of prevention and intervention strategies specific to each type of cybercrime (from cyber-dependent crimes to cyber-enabled crimes), with a view to supporting the victim to overcome the experience of cybercrime and its impacts.

Therefore, this Module addresses the following topics:

- Key personal and technical competencies for a support professional, a Victim Support Officer (VSO), namely empathy and communication skills;
- Emotional support;
- Collection of information;
- Risk assessment of re-victimisation and the development of protection plans;
- Identification of support needs;
- Crisis intervention.

This module includes a summary of the contents of Chapters 1, 2 and 3 - Part II of the *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*. In order to improve understanding of the topics covered, we suggest a careful reading of those chapters.

Empathy, communication techniques and emotional support

Supporting victims of cybercrime requires that the support professional (VSO) develops a set of key competencies and skills:

- **Empathy:** refers to the ability to see things from the victim's perspective, to be sensitive to the situation experienced by the victim and to sense and understand the victim's feelings and meanings attributed to the crime; it is a fundamental competence for establishing a supportive and trusting relationship.
- **Other personal competencies and skills are:**
 - Vocation;
 - Capacity for emotional self-management and establishing positive interpersonal relationships;
 - Positive stress management and capacity for the peaceful resolution of interpersonal and/or interinstitutional problems;
 - Respect for human dignity and tolerance and respect for cultural values and differences.

Regarding **technical competences**, in addition to the need for specific training on how to support cybercrime victims and in technological literacy³⁴, **communication skills** when contacting and supporting cybercrime victims are also essential, particularly, knowing how to listen, ability to transmit clear and easy-to-understand information and messages (Person et al., 2011).

Communication and empathy are fundamental throughout the intervention and support process with the victim of cybercrime, in particular emotional support.

Succinctly, the **emotional support** to a victim of cybercrime is underpinned by the approach and attitudes of the support professional (VSO):

- **Empathetic communication** and active listening;
- **Non-verbal language;**

³⁴ See the analysis of this concept in Module 1 of this Training Course.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 4 - KEY ASPECTS IN SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

- **Acknowledging the complaint** and **respecting the victim's pace** when sharing their experience;
- Encouraging the **victim's emotional expression and validating** their experience of cybervictimisation.

Collection of information

Collecting information is central for the support and intervention process.

The first contact with the victim will be dedicated to this process of collecting information, which entails circular and constant steps as they regularly feed into any process of support and intervention with the victim.

In summary, the process of collecting information seeks to cover 3 areas:

1. Personal and pre-victimisation history;
2. Experience of cyber-victimisation;
3. Post-victimisation history.

Asking the cybercrime victim's collaboration in this process will make it possible to:

- Obtain information on the cybercrime situation experienced;
- Measure impacts and consequences;
- Assess the risk and define protection measures;
- Identify the victim's needs;
- Deploy the most appropriate resources and services to meet those needs.

Risk assessment and development of protection plans

Assessing the risk level will inform on the **likelihood of further cyber-victimisation against the victim**.

The risk assessment process is based on:

- **Information shared by the victim** regarding their experience of cyber-victimisation;
- Use of that information to **identify (in a more or less structured way) the re-victimization risk factors** present in each case (and which will be given particular attention in planning the intervention, personal online protection behaviours and cyber-security measures, in order to prevent revictimisation);
- **The supporting professional's (VSO) experience and professional judgement.**

In general, we can say that assessing the revictimisation risk should focus on **three risk areas**:

1. The victim's characteristics;
2. The cybercrime's specific characteristics and dynamics;
3. The perpetrator's characteristics.

In this Module, we explore some **variables and risk factors associated with each of the above risk areas** which should be considered by the professional (VSO) in their intervention. The *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*, in Chapter 3 - Part I and Chapter 3 - Part II, details the risk factors to be considered.

This Module also aims to make professionals/participants in the training aware of the need for the mechanisms and strategies for the victim's risk assessment to be accompanied by the development of **protection plans**:

- Strategies for the prevention of re-victimisation should be defined and agreed between the victim and the professional (VSO), and should include protection measures and behaviours against new crime situations, as well as strategies and practical instructions for dealing with and acting in the face of the possible reoccurrence of cybervictimisation.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 4 - KEY ASPECTS IN SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

Identification of support needs

Following the collection of information with the victim, and considering the results of the revictimisation risk assessment, it is important that the professional (VSO) identifies the **support needs of the cybercrime victim**.

In general, the needs of victims of cybercrime are relatively similar to the needs of victims of other more *traditional* forms of crime (Leukfeldt et al., 2020).

As such, these needs can be summarised as (Cross et al., 2016; Leukfeldt et al., 2020):

- **Emotional and psychological needs**, with emphasis on being recognised as a victim of crime and having their experience of cybervictimisation valued and validated, and having access to support and recovery/reparation for the consequences of the crime suffered;
- **Criminal proceedings and information related needs**, in particular information on existing support services, rights, complaints procedures and on the development of the criminal proceedings;
- **Practical and financial needs**, such as support in removing online content, liaising with entities and seeking financial compensation.

Detailed information enabling a better understanding of the needs identified with (and by) victims of cybercrime is provided in Chapter 4 - Part I of the *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*.

In the specific case of **needs relating to rights and criminal proceedings**, it is essential to ensure that, at any stage of the criminal proceedings, the victim has access to information about their rights so that they can exercise them:

- The support professional (VSO) must be familiar with the cybercrime legal framework presented in Module 2 of this Training Course;
- The support professional (VSO) should also have a good level of knowledge about the criminal procedure stages and the legal rights of the victims of crime, in order to help victims understand and exercise these rights:
 - Right to information;
 - Right to receive proof of complaint;
 - Right to translation;
 - Right of access to victim support services;
 - Right to be heard;
 - Rights when the defendant is not accused;
 - Right to mediation services;
 - Right to information or legal protection;
 - Right to compensation for participating in the proceedings and reimbursement of expenses;
 - Right to restitution of property;
 - Right to compensation;
 - Right to protection;
 - Rights of victims with special protection needs;
 - Right to be forgotten³⁵.

These rights are presented in more detail in the *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*, Chapter 3 - Part II. See also the full text of Directive 2012/29/EU³⁶.

Refer also to Chapter 3 - Part II of the same Handbook for strategies to help identifying support needs during the intervention process.

Following the identification of support, information and protection needs, it may be necessary to **(internally or externally) refer** the victim of cybercrime to specialised services/responses, particularly legal, psychological and social or other services.

³⁵ This right, unlike the previous ones, is not part of Directive 2012/29/EU. It is included in Article 17 of the General Personal Data Protection Regulation.

³⁶ Available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0029>

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 4 - KEY ASPECTS IN SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

In this Module, **secondary victimisation** is also discussed and defined: this is a second form of victimisation, caused by an inadequate response by the institutional systems and structures responsible for meeting the victims' needs and the discrepancy between their response and the interests, needs and rights of those victims.

Crisis intervention

The experience of cybervictimisation can potentially also lead the victim to experience a **crisis** situation, which can be observed, for example, through intense psychological reactions.

Crisis intervention (or psychological first aid) is an **intensive, focused and time-limited action**, oriented towards solving current problems and responding to specific objectives. It is a response providing initial support and practical, non-invasive care, in crisis or emergency situations.

This Module explores the objectives and stages of crisis intervention, which can be summarised in the following key aspects:

- Assessing the victim's safety and their (personal and social) resources to respond adequately to the situation;
- How to implement the intervention tasks aimed at the victim's recovery and reorganization.

The crisis intervention stages are discussed in detail in the *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*, Chapter 3 - Part II.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 4 - KEY ASPECTS IN SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

Specialised Support to Victims of Cybercrime

PART II – SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

Module 4 – Key aspects of specialised support to victims of cybercrime



4. Key aspects of specialised support to victims of cybercrime

Structuring specialised support to victims of cybercrime

This module addresses the following topics:

- Key competencies of a support professional – Victim Support Officer (VSO): personal and technical competencies such as empathy and communication skills;
- Collection of information;
- Assessment of the risk of re-victimisation;
- Identification of support needs;
- Crisis intervention.



4. Key aspects of specialised support to victims of cybercrime

Structuring specialised support to victims of cybercrime

a. Key personal competencies of the VSO:

- Empathy;
- Vocation;
- Capacity for emotional self-management and establishing positive interpersonal relationships;
- Positive stress management and capacity for the peaceful resolution of interpersonal and/or interinstitutional problems;
- Respect for human dignity and tolerance and respect for cultural values and differences.

Key technical competencies for a VSO: specific training on victim support, technological literacy, communication skills for contacting and supporting victims of cybercrime



4. Key aspects of specialised support to victims of cybercrime

Structuring specialised support to victims of cybercrime

a. Competencies of the VSO

The emotional support to a victim is underpinned by the approach and attitudes of the VSO, e.g.:

- Empathetic communication and active listening;
- Non-verbal language;
- Acknowledging the complaint and respecting the victim's pace when sharing their experience;
- Encouraging the victim's emotional expression and validating their experience of cybervictimisation.



4. Key aspects of specialised support to victims of cybercrime

Structuring specialised support to victims of cybercrime

b. Collection of information

Personal and pre-victimisation history;
Experience of cybervictimisation;
Post-victimisation history.

This will enable:

- Obtaining information on the cybercrime situation experienced;
- Measuring impacts and consequences;
- Assessing the risk and defining protection measures;
- Identifying the victim's needs;
- Deploying the most appropriate resources and services to meet those needs.



4. Key aspects of specialised support to victims of cybercrime

Structuring specialised support to victims of cybercrime

c. Risk assessment and development of protection plans

Seeking to establish the likelihood of further cyber-victimisation against the victim.

Through:

Information shared by the victim regarding their experience of cybervictimisation;

Use of that information to identify (in a more or less structured way) the re-victimisation risk factors present in each case (and which will be given particular attention in planning the intervention, personal online protection behaviours and cyber-security measures, in order to prevent revictimisation);

The supporting professional's (VSO) experience and judgement.



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 4 - KEY ASPECTS IN SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

4. Key aspects of specialised support to victims of cybercrime

Structuring specialised support to victims of cybercrime

c. Risk assessment and development of protection plans

Risk assessment should be accompanied by the development of **protection plans**:

Strategies for the prevention of re-victimisation, agreed and defined between the victim and the professional (VSO), that include protection measures and behaviours against new crime situations, as well as strategies and practical instructions for leading with and acting in the face of the possible recurrence of cybervictimisation.



4. Key aspects of specialised support to victims of cybercrime

Structuring specialised support to victims of cybercrime

d. Identification of support needs

Emotional and psychological needs, with emphasis on being recognised as a victim of crime and having their experience of cybervictimisation valued and validated, and having access to support and recovery/reparation for the consequences of the crime suffered;

Criminal proceedings and information related needs, namely information on existing support services, rights, complaints procedures and on the development of the criminal proceedings;

Practical and financial needs, such as support in removing online content, liaising with entities and seeking financial compensation.



4. Key aspects of specialised support to victims of cybercrime

Structuring specialised support to victims of cybercrime

d. Identification of support needs

In the case of **needs relating to rights and criminal proceedings**, it is essential to ensure that, at any stage of the criminal proceedings, the victim has access to information about their rights.

Therefore:

- ✓The VSO must be familiar with the cybercrime legal framework, presented in Module 2 of this training course;
- ✓The VSO should also know the criminal procedure stages and the legal rights of the victims of crime, in order to help victims understand and exercise these rights, namely: Right to information; Right to receive proof of complaint; Right to translation; Right of access to victim support services; Right to be heard; Rights when the defendant is not accused; Right to mediation services; Right to information or legal protection; Right to compensation for participating in the proceedings and reimbursement of expenses; Right to restitution of property; Right to compensation; Right to protection; Rights of victims with special protection needs; Right to be forgotten.



4. Key aspects of specialised support to victims of cybercrime

Structuring specialised support to victims of cybercrime

d. Identification of support needs

Special attention should be given to the phenomenon of **secondary victimisation**, caused by the inadequate response by the institutional systems and structures and the discrepancy between their response and the interests, needs and rights of those victims.

If needed, the victim of cybercrime should be (**internally or externally**) referred to specialised services/responses, namely legal, psychological and social or other services.



4. Key aspects of specialised support to victims of cybercrime

Structuring specialised support to victims of cybercrime

e. Crisis intervention

The experience of cybervictimisation can lead the victim to experience intense psychological reactions.

Crisis intervention = psychological first aid = is an **intensive, focused and time-limited action**, oriented towards solving current problems and responding to specific objectives. It is a response providing initial support and practical, non-invasive care, in crisis or emergency situations.

Stages:

Assessing the victim's safety and their (personal and social) resources to respond adequately to a situation;

Implementing the intervention aimed at the recovery and reorganisation of the victim.



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 4 - KEY ASPECTS IN SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

SESSION PLAN 4

1. Training

Training Title Training Course Specialised Support to Victims of Cybercrime

Modules/Topics Key aspects of specialised support to victims of cybercrime

Date of Session **Time** **Total Duration** 80 minutes

Trainers

2. Specific Objectives

By the end of the session, the participants should be able to correctly list all aspects and key steps in structuring specialised support to victims of cybercrime, such as:

- Empathy and communication techniques;
- Emotional support;
- Collecting information;
- Risk assessment and development of protection plans;
- Identifying support needs;
- Crisis intervention.

3. Session Plan

| | Content | Methods | Resources | Assessment Activities | Duration (minutes) |
|--------------|---|-----------------------|--|----------------------------|-----------------------|
| Introduction | Structuring specialised support to victims of cybercrime | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| | Structuring specialised support to victims of cybercrime: <ul style="list-style-type: none"> • Empathy, communication techniques and emotional support • Collection of information • Risk assessment and development of protection plans • Identification of support needs • Crisis intervention | Expository and active | Computer: Datashow and projection screen | Observation | 60 |
| Development | Activity 1 | Active | White board/flipchart, markers and Guidance for Activity 1 | Observation | 10 |
| | Concluding summary and clarification of doubts | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| Conclusion | | | | | |

OBSERVATIONS

Participants:

Victim Support Officers (VSO)

Date: / /

Trainer:

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 4 - KEY ASPECTS IN SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

INSTRUCTIONS AND KEY INFORMATION FOR THE TRAINER

CONTENT MATCHING

Session Plan *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*

| | PART | CHAPTER |
|--|-----------------------------|--|
| Structuring specialised support to victims of cybercrime | | |
| Empathy, communication techniques and emotional support | Part II - Proceeding | Chapter 1 - 1.1. and 1.2. Chapter 2 - 2.1. and 2.2. |
| Collection information | Part II - Proceeding | Chapter 2 - 2.3. |
| Risk assessment and development of protection plans | Part I - Understanding | Chapter 3 - 3.2. |
| Identification of support needs | Part II - Proceeding | Chapter 3 - 3.2. |
| | Part I - Understanding | Chapter 4 - 4.2. |
| Crisis intervention | Part II - Proceeding | Chapter 3 - 3.3. |
| | Part II - Proceeding | Chapter 3 - 3.1. |
| Activity 1 | No correspondence | |
| | See Guidance for Activity 1 | |
| Concluding summary and clarification of doubts | No correspondence | |

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 4 - KEY ASPECTS IN SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

GUIDANCE FOR ACTIVITY 1

| Module/Topic | Key aspects in specialised support to victims of cybercrime | REF. CODE | TRAINING AREA |
|-------------------|---|-----------|---------------|
| Objectives | This activity aims to consolidate the key aspects to be considered in the specialised support to victims of cybercrime. It seeks in particular to promote the participants' reflection on a set of practices and attitudes by the support professional (VSO) that can benefit or hinder the intervention and support provided to a victim. | | |
| Delivery | <p>Having as a starting point Table 3 [available in Chapter 2 - Part II of the <i>ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims</i>], the trainer should write on the board/flipchart available in the training room a set of attitudes and practices that can be identified when contacting victims of cybercrime.</p> <p>These practices and attitudes can be positive or negative for the intervention success.</p> <p>In addition to the practices listed in Table 3, we also suggest the group reflects on the following attitudes:</p> <ul style="list-style-type: none"> a) <i>Minimising the problem or the impact of the cyber-victimisation experience reported by the victim.</i> b) <i>Offering solutions to the problem presented by the victim or as an answer to the identified needs.</i> c) <i>Promising the victim to solve the problem presented or to meet the identified needs.</i> d) <i>Encouraging the victim to share their experience of cyber-victimisation, as well as their thoughts, feelings and reactions.</i> e) <i>Sharing personal experiences or similar situations concerning cyber-victimisation with the victim.</i> <p>Once written on the board/flipchart, and for each statement, the trainer should ask the group to what extent each of the attitudes/practices may or may not be appropriate, seeking to promote the participants' reflection.</p> <p>The discussion about each statement should be guided towards the following outcomes:</p> <ul style="list-style-type: none"> a) Unsuitable practice/attitude. It is important to recognise and validate the victim and their experience as a form of crime and victimisation. As such, it is important to explain to the victim that, in the context of the support intervention, their account and experience matter and that the professional (VSO) believes in what is being said. It is also important to explain that there are other people experiencing similar situations, thus breaking the notion of theirs being a 'unique case', and framing possible reactions, emotions, feelings and thoughts within the lived cyber-victimisation experience. b) Unsuitable practice/attitude. Respecting the decisions and the autonomy of the victim is fundamental. Although possible solutions can be explored jointly between victim and professional (VSO), they should not replace the victim in the decision-making process or offer solutions to the victim without their involvement in the decision-making process. Instead, the VSO should present and explore the advantages and disadvantages of each possible decision, so that the victim can make informed decisions. c) Unsuitable practice/attitude. Providing the victim with a false sense of security and/or promoting unrealistic expectations as to their role and/or the resolution of the situation and/or the satisfaction of their needs can be counterproductive and can lead to a breakdown in the relationship of trust between professional (VSO) and the victim and/or to the victim's frustration with the failure/dissatisfaction in how their needs are being met. d) Proper practice/attitude. However, it is important to ensure that the victim's timings and wishes are respected. The victim should not be forced to share information if they are not ready or able to do so. e) Unsuitable practice/attitude. The professional should not share their personal information and experiences as a means of developing a rapport with the victim. This may be counterproductive and may lead to a breakdown of the professional relationship between victim and professional (VSO). Deconstructing beliefs of unique vulnerability should instead be done by presenting factual information, such as the prevalence associated with the type of cybercrime suffered by the victim or the number of supported victims who have suffered similar victimisation situations. | | |
| Notes | See Chapter 2 [point 2.1.] of Part II of the <i>ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims</i> . | | |

MOD. 5

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 5 - SPECIALISED SUPPORT TO VICTIMS OF CYBER-DEPENDENT CRIMES

INTRODUCTION

Key concepts associated with cyber-dependent crimes are covered in Module 1 of this Training Course. The current Module builds up on that and on the previous module, which covered general good practice and key aspects of interventions with victims of cybercrime. To promote knowledge of specific interventions in cyber-dependent crime situations, this module explores intervention strategies and prevention of re-victimisation, as well as the *modi operandi* and nature of the crimes.

Modi operandi and nature of the crime

Cyber-dependent crimes can be defined as any crime that **can only be committed through computers, computer networks or other forms of ICT**. As already mentioned, they are crimes that could not be committed without the Internet.

Thus, they include activities such as the creation and dissemination of **malware** and **hacking** to steal confidential personal or industrial data and/or **distributed denial-of-service (DDoS) attacks** to cause financial and/or reputational damage.

Victims of this type of crime include:

- legal persons (such as companies and organisations);
- natural persons (i.e. any citizen).

Several types of attacks are used to commit these crimes, of which we will highlight **ransomware, theft of confidential information** (data compromise) and distributed denial-of-service (DDoS) attacks.

Ransomware is a type of malicious software, or malware, designed to **deny access to a computer system or data until a ransom is paid**. Ransomware is usually spread by phishing emails or when visiting an infected website.

The most common way of carrying out ransomware attacks continues to be through **social engineering** and by **sending phishing emails**, often already directed to a person or company (**spear phishing**), as a way of accessing the individual victim's or organisation's computers or computer networks and then encrypting the data.

Another type of attack pertains to the **exploitation of vulnerabilities in the computers' remote access protocols**: in these cases, the attacker tries to exploit vulnerabilities in the software itself in order to have remote access to the computer.

Ransomware, as well as other types of attacks analysed, constitute a crime, and its definition and punishment are covered in the Portuguese Cybercrime Law. The **crime of computer damage** pertains to infecting someone else's computer and preventing the victim accessing certain files.

Online personal information theft is also another common type of cybercrime. It is mainly related to illegally obtaining financial information, such as credit card details, bank details or crypto-currency wallets. Access to this information is very valuable as it can be sold or used to steal the victims' assets.

There are other types of high-value personal information beyond financial information. In this sense, access to victims' personal information allows the attacker to create phishing emails specifically targeted at those victims (spear phishing). One advantage is that this attack is more precise and therefore the victim will likely find it more credible since the email will contain their personal data. Some examples of crimes that use this *modus operandi* are **online fraud** and **unlawful access**.

The theft of online personal information can be characterised by three phases:

- 1) **Research**: The cybercriminal looks for vulnerabilities; these vulnerabilities may focus on the person, network infrastructures or electronic devices;
- 2) **Attack**: Once weaknesses have been identified, the cybercriminal starts their attack:

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 5 - SPECIALISED SUPPORT TO VICTIMS OF CYBER-DEPENDENT CRIMES

- against the electronic devices, by exploiting their vulnerabilities in order to gain access.
- through social engineering, in which people are the vulnerability focus, being deceived by attackers and led to reveal information that will allow access to electronic devices or the network.

3) Data exfiltration: Once the attacker has gained access to the electronic devices, they can search for the data they want to transfer. If these devices are connected in a network, the cybercriminal can infiltrate the network and attack other devices.

Distributed denial-of-service (DDoS) attacks aim at **degrading online services** such as **websites, email** and **DNS** (Domain Name System) **services**. To achieve these goals, the cybercriminal can use several **forms of attacks**:

- Use multiple computers to direct large volumes of traffic to online services, in order to make these services temporarily unavailable;
- Diverting a company's online services (e.g. website) in an attempt to redirect users to another website.

Because of its characteristics, this type of criminal practice affects mainly legal persons, but individuals can be indirect victims as the attack prevents their access to these services.

Distributed denial-of-service attacks are also defined and punished by the Portuguese Cybercrime Law, under the provision of **computer sabotage**.

Prevention strategies

To prevent **ransomware attacks and theft of confidential information**, the following strategies can be used:

- Enabling strong spam filters to prevent phishing emails. It is also recommended to use email authentication mechanisms with Sender Policy Framework (SPF), Domain Message Authentication Reporting and Compliance (DMARC) and Domain Keys Identified Mail (DKIM) to prevent email spoofing;
- Use of mechanisms to analyse executable files from the sent or received email folders, preventing users from receiving them;
- Configuring the firewall to block access to IPs (Internet Protocol) already known to be a threat;
- Configuring antivirus and anti-malware programs on all computers and configuring them to perform regular checks;
- Implementing training and awareness-raising activities on online risks, mainly among company staff as they can be targets of these types of attacks;
- Applying the 'Principle of Least Privilege' in companies/organisations: no user should be granted administrative access beyond what is strictly necessary for the exercise of their activity.

Because **distributed denial-of-service (DDoS) attacks** occur mainly in online services provided by corporate entities, organisations must ensure that their online services remain active, even in the event of an attack. For this purpose, the following prevention mechanisms can be implemented:

- Determine what level of service is appropriate and should be maintained at all times;
- Define which online service functionalities can be provided in the event of an attack;
- Identify, by engaging the organisation's IT (Information Technology) team or Webhost contracted to host the online services, which cyber-attack protection measures are currently implemented, namely:
 - What is the resilience capacity to a distributed denial-of-service attack;
 - What are the costs (if any) of suffering this type of attack;
 - What is the traffic limit beyond which the Webhost is required to or should notify the organisation that their servers should be shut down;
 - Which measures provided by the Webhost and the IT team are automatically triggered when such attacks occur.
- Protect the organisation's domains by using domain registration blocking³⁷ and confirming that the domain

³⁷ REGISTRAR-LOCK is a status code that can be defined in an Internet domain name by the sponsoring registrar of the domain name. It is usually done to prevent unauthorised, unwanted or accidental changes to the domain name.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 5 - SPECIALISED SUPPORT TO VICTIMS OF CYBER-DEPENDENT CRIMES

- registration details are correct;
- Check who are the contact persons responsible for sharing information between the organisation and the Webhost, and whether it is a 24/7 contact network, i.e. whether these contact persons are available every day of the week and at any time of the day;
- Establish a contact network outside the current network in case the latter fails;
- Implement real-time monitoring mechanisms for distributed denial-of-service attacks;
- Conduct a segmentation of the different critical services (e.g. email) from other services that can be more easily attacked (e.g. webhosting services);
- Provide an alternative version of the website with the essential information

Intervention strategies

Strategies for preserving digital evidence

In this type of cybercrime, in addition to the measures that can be taken to preserve evidence, it is essential to adopt strategies to mitigate an attack and report it to entities that can provide technical support and criminal investigation expertise.

Regarding **ransomware** attacks or any other attack aimed at interfering or sabotaging a computer system, the following measures should be taken:

- Place all systems offline immediately;
- Ensure that backups are malware free;
- Contact immediately the National Cybersecurity Centre (in Portugal, the Centro Nacional de Cibersegurança)³⁸ to request support and report the computer attack to the police authorities;
- If possible and where applicable, collect and secure the part of the data not infected by the virus;
- If possible, change the passwords for the network and all online accounts after the attack. After removing the virus, change the access data of all accounts again;
- Delete registry data and files that prevent the virus from loading;

Many of these measures also apply to situations/attacks that involve the **online theft of confidential information**.

In the case of a malware attack on the devices or network, all devices must be placed offline, and then all access data (username and password) must be changed. The source of the information leak must also be identified and its vulnerabilities corrected. Finally, the computer attack must be reported to the competent authorities.

Regarding **distributed denial-of-service attacks**, the following measures can be taken:

- Transfer of online services to a cloud service with high traffic capacity and the ability to host a non-dynamic website;
- Hiring a company/service that offers mechanisms to fight distributed denial-of-service attacks or developing in-house solutions involving specialised technicians responsible for implementing these measures;
- Deactivate services that allow a distributed denial-of-service attack to be effective (e.g. having a version of the website ready for upload).

To whom and how to report

In order to report this type of attack, the competent criminal investigation authorities (the Polícia Judiciária in Portugal) should be contacted.

Strategies to overcome victimisation and its impacts

It is very important that the victim support officer/professional (VSO) understands the dynamics, impact and

³⁸ See <https://www.cnscs.gov.pt/>

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 5 - SPECIALISED SUPPORT TO VICTIMS OF CYBER-DEPENDENT CRIMES

consequences associated with cyber-victimisation experiences in order to be able to assist the victim in overcoming the crime experience.

In this context, in addition to Module 3, it is important to read Chapters 3 and 4 - Part I of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*.

As already mentioned in Module 3, existing studies on the impact and consequences of cyber-victimisation are scarce and, in generic terms, it is considered that the consequences experienced by victims of cybercrime are not significantly different from those experienced by victims of other types of crimes.

In the specific case of cyber-dependent crimes, beyond the health consequences, the financial impact and the fear of cybercrime for the individual victims, we also need to consider how the cybercriminal used the victim's illegitimately accessed data.

To elaborate on the strategies to help victims overcome cybercrime, this Module explores key aspects already addressed in the previous Module. We also recommend, for an in-depth approach to this matter, to consult Chapter 2 - Part II *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*.

Among the objectives of support and intervention with cybercrime victims, the following stand out:

- To positively acknowledge the complaint/demand for support and to validate that experience;
- To provide information on crime and its prevalence.
- To prevent new crimes e.g. by developing protection plans with the victim.

PART 2 – SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 5 – SPECIALISED SUPPORT TO VICTIMS OF CYBER-DEPENDENT CRIMES

Specialised Support to Victims of Cybercrime

PART II – SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

Module 5 – Specialised support to victims of cyber-dependent crimes



5. Specialised support to victims of cyber-dependent crimes

a. Modi operandi and nature of the crime

Cyber-dependent crimes – can only be committed through computers, computer networks or other forms of ICT, so could not be committed without the Internet

Malware and Hacking – usually used to steal personal information
Distributed denial-of-service (DDoS) attacks – intended to cause damage to online services such as websites, e-mail and DNS services → financial and/or reputational damage (crime of computer sabotage)

Ransomware – type of malware designed to deny access to a computer system or data until a ransom is paid (crime of computer damage)



5. Specialised support to victims of cyber-dependent crimes

a. Modi operandi and nature of the crime

Theft of confidential information

Phishing, spear phishing – emails with malicious links

Exploiting of software vulnerabilities to gain remote access to the computer

Theft of online personal information – financial information, bank details, wallets, etc.

Research

Attack

Data exfiltration



5. Specialised support to victims of cyber-dependent crimes

b. Prevention strategies

-Ransomware attacks and theft of confidential information

Enabling strong spam filters; using email authentication mechanisms with Sender Policy Framework (SPF), Domain Message Authentication Reporting and Compliance (DMARC) and Domain Keys Identified Mail (DKIM) to prevent email spoofing;

Using of mechanisms to analyse executable files from the sent or received email folders, preventing users from receiving them;

Configuring the firewall to block access to IPs (Internet Protocol) already known to be a threat;



5. Specialised support to victims of cyber-dependent crimes

b. Prevention strategies

Ransom attacks and theft of confidential information

Configuring antivirus and anti-malware programs on all computers and configuring them to perform regular checks;

Implementing training and awareness-raising activities on online risks, mainly among company staff as they can be targets of these types of attacks;

Applying the 'Principle of Least Privilege' in companies/organisations: no user should be granted administrative access beyond what is strictly necessary for the exercise of their activity.



5. Specialised support to victims of cyber-dependent crimes

b. Prevention strategies

-Distributed denial-of-service (DDoS) attacks

Determine what level of service is appropriate and should be maintained at all times;

Define which online service functionalities the organisation can choose to not provide in the event of an attack (e.g. if the organisation's website is suffering a cyber-attack during the pandemic, then access to all the website content can be stopped, except contact details in order to mitigate network overload);

• Protect the organisation's domains by using domain registration blocking and confirming that the domain registration details (e.g. contact details) are correct;



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 5 - SPECIALISED SUPPORT TO VICTIMS OF CYBER-DEPENDENT CRIMES

5. Specialised support to victims of cyber-dependent crimes

b. Prevention strategies

-Distributed denial-of-service (DDoS) attacks

Identify, by engaging the organisation's IT (Information Technology) team or Webhost contracted to host the online services, which cyber-attack protection measures are currently implemented, namely:

- What is the resilience capacity to a distributed denial-of-service attack;
- What are the costs (if any) of suffering this type of attack;
- What is the traffic limit beyond which the Webhost is required to or should notify the organisation that their servers should be shut down;
- Which measures provided by the Webhost and the IT team are automatically triggered when such attacks occur.



5. Specialised support to victims of cyber-dependent crimes

b. Prevention strategies

-Distributed denial-of-service (DDoS) attacks

Check who are the contact persons responsible for sharing information between the organisation and the Webhost, and whether it is a 24/7 contact network, i.e. whether these contact points are available every day of the week and at any time of the day;

Establish a contact network outside the current network (e.g. have a list of telephone contact details and consider also using email addresses outside the organisation for exchanging information) in case the current network fails;

Implement real-time monitoring mechanisms for distributed denial-of-service attacks;

Conduct a segmentation of the different critical services (e.g. email) from other services that can be more easily attacked (e.g. webhosting services);

Provide an alternative version of the website with the essential information.



5. Specialised support to victims of cyber-dependent crimes

c. Intervention strategies

i. Preserving digital evidence

Ransomware, online theft of confidential information, malware,

Place all systems offline immediately;

Ensure that backups are malware free;

If possible and where applicable, collect and secure the part of the data not infected by the virus;

If possible, change the passwords for the network and all online accounts after the attack. After removing the virus, change the access data of all accounts again;

Delete registry data and files that prevent the virus from loading;

Identify the source of the information leak correct its vulnerabilities;

- Contact immediately the National Cybersecurity Centre to request support and report the computer attack to the police authorities; <https://www.cncs.gov.pt/>



5. Specialised support to victims of cyber-dependent crimes

c. Intervention strategies

i. Preserving digital evidence

Distributed denial-of-service (DDoS) attacks:

Transfer of online services to a cloud service with high traffic capacity and the ability to host a non-dynamic website;

Hiring a company/service that offers mechanisms to fight distributed denial-of-service attacks or developing in-house solutions involving specialised technicians responsible for implementing these measures;

Deactivate services that allow a distributed denial-of-service attack to be effective (e.g. having a version of the website ready for upload that does not include a content search mechanism, dynamic content, or large files increasing too much internet traffic).



5. Specialised support to victims of cyber-dependent crimes

c. Intervention strategies

ii. To whom and how to report

Judiciary Police in Portugal.

iii. Strategies to overcome victimisation and its impacts

In addition to Module 3, it is important to read Chapters 3 and 4 - Part I of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*.

Among the objectives of support and intervention with cybercrime victims, the following stand out:

- To positively acknowledge the complaint/demand for support and to validate that experience.

To provide information on crime and its prevalence.

Prevent new crimes e.g. by developing protection plans with the victim.



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 5 - SPECIALISED SUPPORT TO VICTIMS OF CYBER-DEPENDENT CRIMES

SESSION PLAN 5

1. Training

Training Title Training Course on Specialised Support to Victims of Cybercrime

Modules/Topics Specialised support to victims of cyber-dependent crimes

Date of Session **Time** **Total Duration** 40 minutes

Trainers

2. Specific Objectives

By the end of the session, the participants should be able to correctly:

- Distinguish the nature and modi operandi of cyber-dependent crimes;
- List proposed intervention strategies for specialised support to victims of cyber-dependent crime;
- Recognise proposed strategies for the prevention of re-victimisation with victims of cyber-dependent crime.

3. Session Plan

| | Contents | Methods | Resources | Assessment Activities | Duration (minutes) |
|--------------|--|-----------------------|--|----------------------------|-----------------------|
| Introduction | Activity 2 | Active | Guidance for Activity 2, Activity 2 Sheet and pens | Observation | 5 |
| | Modi operandi and nature of the crimes | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| Development | Prevention strategies | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| | Intervention strategies: <ul style="list-style-type: none"> • Strategies for preserving digital evidence • To whom and how to report • Strategies to overcome victimisation and its impacts | Expository and active | Computer: Datashow and projection screen | Observation | 20 |
| Conclusion | Concluding summary and clarification of issues | Expository and active | Computer: Datashow and projection screen | Observation | 5 |

OBSERVATIONS

Participants:

Victim Support Officers (VSO)

Date: / /

Trainer:

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 5 - SPECIALISED SUPPORT TO VICTIMS OF CYBER-DEPENDENT CRIMES

GUIDELINES AND KEY INFORMATION FOR THE TRAINER

CONTENT MATCHING

| | | |
|--|--|------------------|
| Session Plan | <i>ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims</i> | |
| | PART | CHAPTER |
| Activity 2 | No correspondence | |
| | See Guidance for Activity 2 | |
| Modi operandi and nature of the crimes | No correspondence | |
| | See Module Introduction | |
| Prevention strategies | No correspondence | |
| | See Module Introduction | |
| Intervention strategies | | |
| Strategies for preserving digital evidence | No correspondence | |
| | See Module Introduction | |
| To whom and how to report | No correspondence | |
| | See Module Introduction | |
| Strategies to overcome victimisation and its impacts | Part II - Proceeding | Chapter 2 - 2.1. |
| | See Module Introduction | |
| Síntese conclusiva e esclarecimento de questões | No correspondence | |

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 5 - SPECIALISED SUPPORT TO VICTIMS OF CYBER-DEPENDENT CRIMES

GUIDANCE FOR ACTIVITY 2

| Module/Topic | Specialised support to victims of cyber-dependent crime | REF. CODE | TRAINING AREA |
|--------------|--|-----------|---------------|
| Objectives | The aim of this activity is, by using a short and playful exercise, to review some key concepts covered in Module 1 (relating to phenomena and cyber-attacks associated with cyber-dependent crime) and to introduce Module 5 topics on support to victims of cyber-dependent crimes. | | |
| Delivery | <p>The trainer should give the participants the Activity Sheet, explaining that for each (total or partial) definition presented in Column A there is a correspondent phenomenon/concept in Column B. The participants have 60 seconds to make the links between definitions/Column A and phenomena/Column B.</p> <p>Then, the trainer must check the correct answers with the group of participants, clarifying doubts, if any.</p> <p>The phenomena/concepts (Column B) and their definitions/phrases (Column A) are as follows:</p> <p>Hacking: It involves unauthorised access to computer systems.</p> <p>Spamming: It concerns sending and publishing mass advertising.</p> <p>Malware: It is hostile or intrusive software.</p> <p>Cyber-dependent crime: It refers to cybercrime stricto sensu.</p> <p>Phishing: It is used for unlawful access to confidential information.</p> <p>Distributed denial of service (DDoS) attack: It concerns the overload of a system.</p> | | |
| Notes | See Module Introduction | | |

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 5 - SPECIALISED SUPPORT TO VICTIMS OF CYBER-DEPENDENT CRIMES

ACTIVITY 2 SHEET

Link each definition in Column A to the corresponding phenomenon in Column B.

COLUMN A

It is hostile or intrusive software

It refers to cybercrime stricto sensu.

It involves unauthorised access to computer systems

It concerns the overload of a system

It is used for unlawful access to confidential information

It concerns sending and publishing mass advertising

COLUMN B

Hacking

Spamming

Malware

Cyber-dependent crime

Phishing

Distributed denial of service attack

MOD. 6

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

INTRODUCTION

In Portugal, two types of fraud can be distinguished: the crime of fraud, provided for and punished in Article 217 of the Criminal Code, and the crime of computer fraud, provided for and punished in Article 221 of the Criminal Code:

- **Fraud** – the key element in the crime of fraud concerns deceiving someone, and obtaining their collaboration to act in an attempt to gain a benefit.
- **Computer fraud** – here there is a direct attack on property carried out via a computer. The computer is the perpetrator's instrument, so it is not in itself an element of deception. Unlike the crime of fraud, it is not necessary that the perpetrator has a financial gain, their intent to financial gain is sufficient. That being the case, it is also not required that there is an intention to mislead someone. To be considered a crime, it is sufficient to incorrectly set up, totally or partially, a computer programme configuration, which can add, modify or suppress stages in the program and/or the introduce new instructions.

This Module will explore the most statistically frequent types of online fraud and those that cause the most damage to their victims:

- Online shopping (ecommerce) fraud;
- Bank fraud;
- Scams in intimate relationships (romance and dating scams).

These phenomena are also explored in Chapter 1 - Part I of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*.

Types, modi operandi and nature of the crime

Online shopping [ecommerce] fraud

Online shopping fraud presents different degrees of complexity:

- from simple schemes, in which the seller promises to send the buyer a certain item after a bank transfer is made, and the buyer does not receive the item;
- to more elaborate schemes, that may involve falsifying documents, such as proofs of bank transfer, exploiting vulnerabilities in online shopping websites that store users' bank details (credit or debit cards), which are accessed and sold by cyber-criminals on the darkweb or used for bank transactions without the victim's knowledge (card not present fraud).

Internet auction fraud is another example of online shopping fraud that occurs when the purchased items are fake or illicitly obtained or when the seller advertises non-existent items or makes them available for sale (Jahankhani et al., 2014).

Bank fraud

Bank fraud often takes the shape of **phishing** attacks against individual victims or collective entities (such as corporations and organisations). The way phishing works has already been described:

- As a general rule, by receiving emails or SMS, the victim is led to click on a link that they think is from their bank, and are directed to a website resembling their bank website. This website design uses a technique called pharming, the term used for an attack based on the DNS cache poisoning technique, which consists of corrupting the Domain Name System (DNS) in a network of computers, causing a website's Uniform Resource Locator (URL) to be directed to a different server rather than the original server.

Credit card fraud refers to the use of another person's credit card for personal use, without the card owner's and the issuer's knowledge (Patel & Singh, 2013). There are several cyber-dependent methods/crimes that can be used to gain access to cards and their details, such as phishing, spamming or hacking (Jahankhani et al., 2014).

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

Also noteworthy is **skimming fraud**, which consists in copying the magnetic strip of a payment card, without the cardholder's knowledge or consent, when they use the card at an ATM (automated teller machine) or at a till point terminal.

Recently there have been other types of attacks, notably on ATM machines, in a process known as **jackpotting**, through which the criminal gives the command for the ATM machines to dispense cash. The attack to ATM machines can occur through the introduction of malware in the equipment/ATM's computer system or through hardware connection, called 'Black-Box'.

Scams in intimate relationships [romance and dating scams]

Scams in intimate relationships occur when the perpetrator seeks to establish a relationship of trust and intimacy, specifically through the Internet and ICT, with a certain target, as a prelude to obtaining personal benefit, namely financial and patrimonial benefit. Fraudulent acts may include access to the victim's money, bank accounts, credit cards, passports, email accounts or national identification numbers, or even coercing the victim to commit crimes in the perpetrator's name.

In this Module, we will explore the *modi operandi* of these three types of fraud, as well as prevention and intervention strategies that the course participant, as a victim support officer/professional (VSO), should consider when providing support to victims of online fraud.

Regarding **ecommerce** fraud, particularly the most common scams - which are not associated with the user's data exfiltration - take place on online sales platforms where individuals buy and sell goods.

When the perpetrator of the fraud presents themselves as the seller:

- They publish fake adverts in platforms used for buying and selling various items - rental properties, pets, used cars, boats, bicycles, etc..
- The advert may include photos and other details - usually copied from a genuine seller's advert - and may also publicise the sale of that item at a low price;
- When the victim shows interest in the item, the perpetrator may claim, for example, that they are travelling or have moved to another location, which is why a courier company will deliver the goods after receipt of payment. After payment, the victim may receive a false receipt via email, even though they will not receive the purchased item and will not be able to contact the seller;
- In the case of real estate, the perpetrator will act as the owner or landlord of a property for purchase or rent. When the victim shows interest in the property, the perpetrator will make up excuses for not showing the property to the buyer in person, for example by claiming that they are outside the country/town. If the victim maintains an interest in acquiring the property or renting it, a deposit will be requested..

When the perpetrator of the fraud presents themselves as the buyer:

- The seller publishes an advertisement on an ecommerce platform and receives an email or message from a person potentially interested in buying the item, apparently from another country (taking into account the spelling and grammatical errors that the text contains);
- The person concerned requests the seller's bank details (bank identification number or *Paypal*® payment details) in order to make the payment, and informs that they will contact a delivery company to collect the item;
- The buyer then contacts the seller again, informing that they are unable to make payment to the carrier and that they have transferred to the seller's account the value of the item plus the cost of delivery;
- The buyer asks the seller to pay the delivery company by sending money, providing the necessary details (name and address of the supposed delivery company). Normally, in order to increase the credibility of the scheme, the buyer attaches to this email a (fake) proof of the supposed transfer made to the seller.

In **bank fraud**, the most used *modus operandi* is the sending of phishing emails. See the example used in the slides section for this Module (*PowerPoint*):

- A typical example of a phishing email contains a copy of the image and lettering of a communication made by a bank;
- As a rule, this type of email invites the recipient to download a file or to click on a link that redirects them to a

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

- website where they are asked to enter their personal data;
- These websites are designed to be very similar to genuine banking websites (see method explained in Module 5).

In **romance and dating scams**, we can identify the following *modi operandi*:

- Setting up of false profiles on social networks, dating sites or other chat and social interaction platforms;
- Establishing contact with apparently more vulnerable targets, namely people with public profiles (privacy settings);
- Developing an emotional link with the previously identified target, gathering as much information as possible about them;
- Developing a narrative aimed at extorting personal/financial assets from the target.

Prevention strategies

At this point in the delivery of the Module, the trainer should inform the course participants about the following strategies which they, as victim support officers/professionals (VSO), can use when supporting the victim in order to **prevent ecommerce or bank frauds**:

- Do not purchase goods over unsecured Wi-Fi networks (public Wi-Fi or networks where no password is required).
- Select well-known and reliable online shopping platforms and websites that offer secure payment methods.
- Check and recognise secure websites:
 - The website should display a lock symbol on the left-hand side immediately before the website address;
 - The website URL must contain the certificate - 'https://'; containing the 's' of 'secure' added to the 'http', and check the URL, namely when the addresses are shared by message or email;
- Do not provide personal information or personal data requested through unsolicited emails, messages, calls, websites;
- Check the name of the sender of the email - typos or other errors mean that the sender of the email is not who they say they are or who they say they represent.

For the **prevention of scams in intimate relationships**, the trainer should transmit to the course participants the following strategies which they, as support professionals (VSO), can use in their intervention with the supported victim:

- Check the profile picture (e.g. through the Tin Eye or Google Chrome image search engines by clicking on the mouse's right button and choosing the 'Google picture search' option);
- Perform Google® search by copying paragraphs from messages received via chat or email in order to understand whether this is an approach/communication already known and reported by others;
- Check for spelling mistakes indicating that the person is not using their native language;
- Check whether the perpetrator makes multiple requests to communicate through chat platforms such as Facebook®, WhatsApp®, Kik®, SMS, Messenger® or Skype®.

Intervention strategies

Strategies for preserving digital evidence

This Module also covers the evidence preservation strategies that the support professionals can explain to the victims being supported. Some of these strategies are presented below according to type of online fraud.

How to preserve evidence, in case of **ecommerce and bank frauds**:

- If there is transfer of assets, keep records of such transfers and contact the bank;
- File criminal complaints with the competent authorities;
- Request support from victim support entities to deal with the emotional suffering caused by the victimisation situation and ensure follow-up throughout the criminal process.

In addition to the above strategies, in the event of **scam in an intimate relationship**, the victim should:

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

- Keep records of all communications with the perpetrator;
- Report the perpetrator's profile to the website, social network or online dating platform.

It is important that the support professional (VSO) remains available to **support and/or accompany** the victim when delivering these strategies.

To whom and how to report

In Portugal, **computer frauds** must be reported to the competent police authorities (Polícia Judiciária) or public prosecutor's office (Ministério Público). **Fraud** can be reported to any criminal police body with generic jurisdiction (PSP and GNR), provided it is not an **aggravated fraud**. In the latter case, the competent criminal police body is the Polícia Judiciária. For all intents and purposes, the crime can always be reported to the Ministério Público, whatever its nature.

Strategies to overcome victimisation and its impacts

The **insecurity** generated by the loss of financial stability has a negative impact on victims of online frauds. In addition to **financial loss**, the victim can manifest a diverse set of **symptoms and consequences** arising from the experience of victimisation, which are common to all victims of crime:

- **Flashbacks**: constant thoughts about what happened;
- **Anxiety**, which can also be associated with concentration difficulties;
- **Difficulty sleeping and nightmares**;
- **Feeling of guilt**, which can be further reinforced by the possible reactions of those closest to the victim after the victim discloses their cyber-victimisation experience;
- **Anger**, sometimes associated with thoughts of revenge;
- **Fear** of becoming a victim of crime again;
- **Mood swings**;
- **Physical disorders** such as eating disorders, chest pains, dizziness, headaches, back and neck pains, digestive problems or sweating.

Regarding guidelines to help victims overcome a cybercrime experience, this Module will explore the key aspects already addressed in Module 4 concerning intervention and support for victims of cybercrime. For an in-depth approach to this topic, consult also Chapter 2 - Part II *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*.

In addition to the central guidelines for intervention outlined in Module 4, the following **emotional support strategies** are considered particularly important when supporting victims of online fraud:

- Listening empathically, demonstrating that you are actively listening, understanding what is being said and valuing the reactions, emotions/sentiments, behaviours, thoughts and meanings attributed by the victim to their experience of online fraud;
- Demonstrating that you believe what the victim is telling you about what happened without being judgmental;
- Normalising the reactions presented, framing/contextualizing the victim's reactions in the emotional context of the situation experienced;
- Making available to the victim the services provided by the organisation, explaining how they can help..

Other support strategies should also be highlighted at this point in the Module:

- Informing in a simple, succinct and clear way, transmitting essential information to the victim about what happened and the next steps to take, using language adjusted to the victim's characteristics;
- Refraining from promoting unrealistic expectations regarding the role of the support professional (VSO) and/or the resolution of the situation;
- Not making decisions for the victim and respecting their choices;

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

- Informing about the possibility of re-victimisation, exploring possible scenarios that the victim may be faced with;
- Defining an economic recovery plan with the victim in order to provide strategies for the victim to regain control over their life;
- Prevent new crime by raising awareness about the importance of adopting the prevention strategies already described in this Module.

The specific case of victims of scams in intimate relationships [romance and dating scams]

At this point in the Module, the trainer should also explore the specific case of intervention with victims of scams in intimate relationships. Start with Activity 3 (see Session Plan), which details the emotional and psychological reactions and consequences of this form of victimisation:

- Intense guilt;
- Feeling of injustice and widespread distrust of others;
- Shame for being scammed;
- Reluctance to report the crime to the police authorities, especially if they have found out that the perpetrator is someone close to and trusted by them, like a relative or a friend;
- Social isolation.

In addition to the above strategies, the trainer should also explore the following strategies:

- Recommend the progressive resumption of activities, including internet and ICT usage habits;
- Encourage greater involvement in previously enjoyable activities, including offline activities;
- Mobilise social support and, if the victim so wishes and with their permission, involve family and/or friends in the recovery process, requesting their help in preventing avoidance and isolation, for example;
- Avoid overprotection by family and friends (without neglecting the safety of the victim).

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

Specialised Support to Victims of Cybercrime

PART II – SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

Module 6 – Specialised support to victims of online fraud



6. Specialised support to victims of online fraud

In Portugal, there is a difference between...

Fraud, article 217 of the Criminal Code - deceiving someone, and obtaining their collaboration to act in an attempt to gain a benefit

Computer fraud, article 221 of the Criminal Code - direct attack on property carried out via a computer; the computer is the means through each the crime takes place, thus it is not in itself an element of deception, the perpetrator's intent to financial gain is sufficient.

In this Module - the most statistically frequent types of online fraud and those that cause the most damage to their victims:

1. **Online shopping (ecommerce) fraud;**
2. **Bank fraud;**
3. **Scams in intimate relationships (romance and dating scams).**



6. Specialised support to victims of online fraud

a. Types and Modi operandi

1. Online shopping (ecommerce) fraud

Simple schemes: paying for a certain item but not receiving it
More elaborate schemes: falsifying documents, such as proofs of bank transfer, exploiting vulnerabilities in online shopping websites that store users' bank details (credit or debit cards), which are accessed and sold by cyber-criminals on the darkweb or used for bank transactions without the victim's knowledge (card not present fraud)

e.g. Internet auction fraud, online selling platforms, fake adverts, etc.



6. Specialised support to victims of online fraud

a. Types and Modi operandi

2. Bank fraud

Mainly via **phishing** attacks – text message or email with a malicious link – directing to a page resembling the bank website

E.g.:

MBWAY fraud

Credit card fraud – using someone's credit card without the card owner's and the issuer's knowledge

Skimming fraud – copying a card's magnetic strip (when used at an ATM or at a till)
Jackpotting – the ATM dispenses cash following the criminals's installing malware or using a black-box



6. Specialised support to victims of online fraud

a. *Modi operandi*

Common computer fraud methods: SPAM

The term SPAM can be an acronym derived from the English expression "Sending and Posting Advertisement in Mass" or meaning also Stupid Pointless Annoying Messages.



Fonte: Data Technical



6. Specialised support to victims of online fraud

a. *Modi operandi*

Common computer fraud methods: Phishing

Phishing owes its name to the English word "fishing". It uses technology that leads the user to reveal personal and/or confidential information.



Fonte: Data Technical



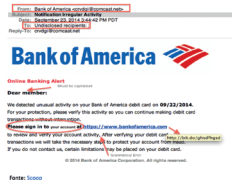
PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

6. Specialised support to victims of online fraud

a. Modi operandi

Phishing email example



Email attempting to copy a legitimate entity's image and lettering (e.g. bank, online streaming services, government organisations, etc.)

It leads the user to download a file or click on a link, which will redirect the user to a site where they are asked to enter their personal data.



6. Specialised support to victims of online fraud

a. Modi operandi

Common computer fraud methods: Pharming

In computing, Pharming is a term for an attack using the DNS cache poisoning technique, which damages the DNS (Domain Name System) in a computer network and redirects a site's URL (Uniform Resource Locator) to a different server.



Activity:

Rio da Realidade | Não caias na armadilha

https://beinternetawesome.withgoogle.com/pt-br_br/interland/rio-realidade



6. Specialised support to victims of online fraud

a. Modi operandi

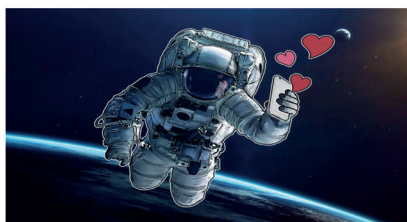
3. Scams in intimate relationships (romance and dating scams)

The agent seeks to establish a relationship of trust and intimacy, specifically through the Internet and ICT, with a certain target, as a prelude to obtaining personal benefit, namely financial and patrimonial benefit.

Fraudulent acts: access to the victim's money, bank accounts, credit cards, passports, email accounts or national identification numbers, or even coercing the victim to commit crimes in the perpetrator's name.



Online Relationships



Source: <https://www.kaspersky.com/blog/online-dating-scams/>



6. Specialised support to victims of online fraud

a. Modi operandi

3. Scams in intimate relationships (romance and dating scams)

Setting up of false profiles on social networks, dating sites or other chat and social interaction platforms;

Establishing contact with apparently more vulnerable targets, namely people with public profiles (privacy settings);

Developing an emotional link with the previously identified target, gathering as much information as possible about them;

Developing a narrative aimed at extorting personal/financial assets from the target.



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

6. Specialised support to victims of online fraud

Online Relationships

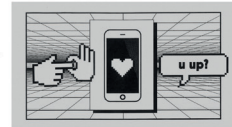
What are some of the Risks of Online Relationships?



6. Specialised support to victims of online fraud

Example: Sexting

Results from combining the words 'sex' and 'texting' and involves exchanging erotic messages, with or without photos, via mobile phones, chats or social networks.



6. Specialised support to victims of online fraud

a. Tipos e Modi operandi Risks of Online Relationships

❑ Non-Consensual Sharing of Images and Videos: (covered in Module 10)

- Sextortion
- Revenge Porn
- Grooming

❑ Online Sexual Harrassment:

- Threats and Coercion
- Sexual Bullying
- Unwanted Sexualisation



6. Specialised support to victims of online fraud

a. Types and Modi operandi Risks of Online Relationships

Online Sexual Harrassment

Online Sexual Harrassment can take many forms, such as:

- Threats and Coercion;
- Sexual Bullying;
- Unwanted Sexualisation



6. Specialised support to victims of online fraud

a. Types and Modi operandi Risks of Online Relationships

Threats and Coercion

In these cases the victim is threatened, coerced into online sexual behaviour or blackmailed with sexual content.

It includes behaviours such as:

- ❑ Harass or pressure someone to share sexual images or engage in sexual behaviour online (or offline);
- ❑ Threaten with the publication of sexual content (images, videos, rumours) to threaten, coerce or blackmail someone ('sextortion');
- ❑ Online sexual threats (for example, threats of rape);
- ❑ Inciting other people to commit online sexual violence;
- ❑ Encourage someone to engage in sexual behaviour and then share images or videos showing it.



6. Specialised support to victims of online fraud

a. Types and Modi operandi Risks of Online Relationships

Sexual Bullying

Someone who is systematically excluded from a group or community by the use of humiliating, disturbing or discriminatory sexual content.

It includes behaviours such as:

- ❑ Sharing online rumours or lies about the victim's sexual behaviour;
- ❑ Online use of offensive or discriminatory sexual language against the victim;
- ❑ Stealing the victim's identity and subsequently sharing sexual content involving the victim or sexually harassing others;
- ❑ Sharing information online about someone's intimacy without their consent to promote sexual harassment against that person;
- ❑ Being bullied because of gender identity or sexual orientation;
- ❑ Body shaming - sharing derisive comments on the victim's physical appearance;
- ❑ Outing - When someone discloses publicly information about another person's sexual orientation or gender identity without this person's knowledge or authorisation.



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

6. Specialised support to victims of online fraud

a. Types and Modi operandi

Risks of Online Relationships

Unwanted Sexualisation

When one receives unwanted sexual solicitations, comments or content.

It includes behaviours such as:

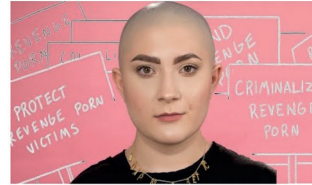
- ☐ Sexualised comments (for example, about photos published in social networks);
- ☐ Viral sex challenges that pressure people to participate;
- ☐ Sending sexual content to someone (images, emojis, messages) without this person's consent;
- ☐ Unwanted sexual advances or requests for sexual favours;
- ☐ Sex jokes;
- ☐ Rating peers in terms of their attractiveness/ sexual activity;
- ☐ Editing images of a person to change them into images with sexual content.



Activity – Discussion

"A Victim Of Revenge Porn Tells Their Story" (2018)

<https://www.youtube.com/watch?v=Gw2-K97EweI>



6. Specialised support to victims of online fraud

b. Prevention strategies

Preventing ecommerce or bank fraud:

- Do not purchase goods over unsecured Wi-Fi networks (public Wi-Fi or networks where no password is required).
- Select well-known and reliable online shopping platforms and websites that offer secure payment methods.
- Do not provide personal information or personal data requested through unsolicited emails, messages, calls, websites;
- Check the name of the sender of the email - typos or other errors mean that the sender of the email is not who they say they are or who they say they represent.

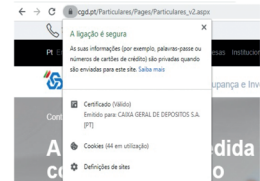


6. Specialised support to victims of online fraud

b. Prevention strategies

Preventing ecommerce or bank fraud:

- Check and recognise secure websites :
 - The website should display a lock symbol on the left-hand side immediately before the website address;
 - The website URL must contain the certificate - 'https://'; containing the 's' of 'secure' added to the 'http', and check the URL, namely when the addresses are shared by message or email;



6. Specialised support to victims of online fraud

b. Prevention strategies

Preventing scams in intimate relationships:

- Check the profile picture (e.g. through the Tin Eye or Google Chrome image search engines by clicking on the mouse's right button and choosing the "Google picture search" option);
- Perform Google® search by copying paragraphs from messages received via chat or email in order to understand whether this is an approach/communication already known and reported by others;
- Check for spelling mistakes indicating that the person is not using their native language;
- Check whether the perpetrator makes multiple requests to communicate through chat platforms such as Facebook®, WhatsApp®, Kik®, SMS, Messenger® or Skype®.



6. Specialised support to victims of online fraud

c. Intervention strategies

i. Preserving digital evidence

In the case of ecommerce and bank fraud:

- If there is transfer of assets, keep records of such transfers and contact the bank;
- File criminal complaints with the competent authorities;
- Request support from victim support entities to deal with the emotional suffering caused by the victimisation situation and ensure follow-up throughout the criminal process.



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

6. Specialised support to victims of online fraud

c. Intervention strategies

i. Preserving digital evidence

In the event of **scam in an intimate relationship**, the victim should:

- Keep records of all communications with the perpetrator;
- Report the perpetrator's profile to the website, social network or online dating platform.

It is important that the support professional (VSO) remains available to **support and/or accompany** the victim when delivering these strategies.



6. Specialised support to victims of online fraud

c. Intervention strategies

ii. To whom and how to report

Computer frauds – competent police authorities or public prosecutor's office

Fraud - any criminal police body with generic jurisdiction (PSP and GNR in Portugal)

Aggravated fraud - Polícia Judiciária in Portugal.

For all intents and purposes, the crime can always be **reported to the Public Prosecutor's Office**, whatever its nature.



6. Specialised support to victims of online fraud

c. Intervention strategies

ii. Strategies to overcome victimisation and its impacts

We recommend reading Module 5 on intervention and support with cybercrime victims and also, for an in-depth approach to this topic, to consult Chapter 2 - Part II ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims

Consider also:

Emotional support strategies:

- Listening empathically, demonstrating that you are actively listening, understanding what is being said and valuing the reactions, emotions/sentiments, behaviours, thoughts and meanings attributed by the victim to their experience of online fraud;
- Demonstrating that you believe what the victim is telling you about what happened without being judgmental;
- Normalising the reactions presented, framing/contextualizing the victim's reactions in the emotional context of the situation experienced;
- Making available to the victim the services provided by the organisation, explaining how they can help.



6. Specialised support to victims of online fraud

c. Intervention strategies

ii. Strategies to overcome victimisation and its impacts

Other support strategies should also be considered:

- Informing, in a simple, succinct and clear way, transmitting essential information to the victim about what happened and the next steps to take, using language adjusted to the victim's characteristics;
- Refraining from promoting unrealistic expectations regarding the role of the support professional (VSO) and/or the resolution of the situation;
- Not making decisions for the victim and respecting their choices;
- Informing about the possibility of re-victimisation, exploring possible scenarios that the victim may be faced with;
- Defining an economic recovery plan with the victim in order to provide strategies for the victim to regain control over their life;
- Prevent new crime by raising awareness about the importance of adopting the prevention strategies already described in this Module.



6. Specialised support to victims of online fraud

c. Intervention strategies

ii. Strategies to overcome victimisation and its impacts

Regarding scams in intimate relationships, in addition to the above strategies, the trainer should also explore the following strategies:

- Recommend the progressive resumption of activities, including internet and ICT usage habits;
- Encourage greater involvement in previously enjoyable activities, including offline activities;
- Mobilise social support and, if the victim so wishes and with their permission, involve family and/or friends in the recovery process, requesting their help in preventing avoidance and isolation, for example;
- Avoid overprotection by family and friends (without neglecting the safety of the victim).



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

SESSION PLAN 6

1. Training

Training Title Training Course Specialised Support to Victims of Cybercrime

Modules/Topics Specialised support to victims of online fraud

Date of Session **Time** **Total Duration** 40 minutes

Trainers

2. Specific Objectives

By the end of the session, the course participants should be able to correctly:

- Distinguish correctly the nature and modi operandi of online fraud, including fraud in e-commerce, bank fraud and scams in intimate relationships;
- List correctly proposed intervention strategies for specialised support to victims of online fraud;
- Recognise correctly strategies to prevent re-victimisation for intervention with victims of online fraud.

3 Session Plan

| | Content | Methods | Resources | Assessment Activities | Duration [minutes] |
|--------------|--|-----------------------|--|-------------------------|--------------------|
| Introduction | Types of online fraud: <ul style="list-style-type: none"> • Online (ecommerce) fraud • Bank fraud • Scams in intimate relationships | Expository and active | Computer: Datashow and projection screen | Observation | 2 |
| | Modi operandi and nature of the crimes | Expository and active | Computer: Datashow and projection screen | Observation | 10 |
| Development | Prevention strategies | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| | Intervention strategies: <ul style="list-style-type: none"> • Strategies for preserving digital evidence • To whom and how to report • Strategies to overcome victimisation and its impacts | Expository and active | Computer: Datashow and projection screen | Observation | 15 |
| Conclusion | Activity 3 | Active | Guidance for Activity 3 and Case of Activity 3 | Observation | 5 |
| | Concluding summary and clarification of issues | Expository and active | Computer: Datashow and projection screen | Observation | 3 |

OBSERVATIONS

Participants:

Victim Support Officers (VSO)

Date: / /

Trainer:

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

INSTRUCTIONS AND KEY INFORMATION FOR THE TRAINER

CONTENT MATCHING

| Session Plan | <i>ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims</i> | |
|--|--|------------------|
| | PART | CHAPTER |
| Types of online fraud | Part I - Understanding | Chapter 1 - 1.3. |
| | See Module Introduction | |
| Modi operandi and nature of the crimes | No correspondence | |
| | See Module Introduction | |
| Prevention strategies | No correspondence | |
| | See Module Introduction | |
| Intervention strategies | | |
| Strategies for preserving digital evidence | No correspondence | |
| | See Module Introduction | |
| To whom and how to report | No correspondence | |
| | See Module Introduction | |
| Strategies to overcome victimisation and its impacts | Part II - Proceeding | Chapter 2 - 2.1. |
| | See Module Introduction | |
| Activity 3 | No correspondence | |
| | See Guidance for Activity 3 | |
| Concluding summary and clarification of issues | No correspondence | |

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

GUIDANCE FOR ACTIVITY 3

| Module/Topic | Module 6 - Specialised support to victims of online fraud | REF. CODE | TRAINING AREA |
|--------------|--|-----------|---------------|
| Objectives | To consolidate the information and content addressed in this module, particularly the nature of online fraud and strategies to prevent re-victimisation and intervention. | | |
| Delivery | <p>The trainer should read the Activity 3 Case for Discussion (or ask any of the participants present to read it aloud).</p> <p>We suggest that this case is either distributed in a handout or projected on a screen so participants can read it.</p> <p>Afterwards, the trainer can present the following questions to the group:</p> <ol style="list-style-type: none">1. What type of fraud do you identify in this case?2. What are the consequences of the victimisation displayed by the victim of this case?3. What should the VSO include in the intervention/support to the victim? <p>During the group's participation, the trainer should bear in mind the following points:</p> <ol style="list-style-type: none">1. Lucinda's account fits in with a situation of scam in intimate relationships.2. In the situation reported by Lucinda, feelings of guilt, shame, distrust of other people's intentions and isolation/avoidance of social interactions/relationships are evident, in line with the consequences and reactions expressed by victims of romance and dating scams. It is also evident the victim's resistance to reporting the crime due to a close (friendly) relationship with the perpetrator.3. Key aspects of the intervention should be highlighted: listening empathetically; showing that you believe in the situation reported; framing reactions in the context of the situation experienced by the victim; recommending resumption of activities and involvement in enjoyed activities (particularly offline); mobilising people from the significant network (if the victim shows willingness for them to be involved); preventing further crime by informing on safety/cybersecurity measures; presenting the advantages and disadvantages associated with reporting. See information provided in the Module Introduction. | | |
| Notes | See Module Introduction | | |

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD

ACTIVITY 3: CASE FOR DISCUSSION

Lucinda, 55, widow, mother of three children, all of them of legal age. The youngest is 23 and left home last year. At the first support session, she said the following:

"I know it was my fault, it was all my fault, I'm not young enough for this anymore... But it's just that I feel so lonely since my youngest son left home... And this friend of mine, or that I thought of as being a friend, Adelaide... came to me with this story that I'm still young, that I could find someone to keep me company, that she had a colleague who also found a boyfriend on Facebook. Well, by chance - I thought at the time, dumb! - only a few days later, I have a Facebook friend request from a gentleman named José, very well presented. He is 60 years old, divorced for a long time, with grown up children. He started talking with me and treated me so well... I hadn't been paid that much attention for so long... I felt I was 20 again! He told me that he lived in the United States, but that he was thinking of coming back to Portugal. I believed everything he said, I even looked for plane tickets to go to see him... Anyway... Soon afterwards he starts saying that one of his children was very sick and that he needed to send money to his son. Only he wasn't able to make transfers from the United States to Portugal - he explained why but, frankly, I didn't even pay attention to the explanation, because all I wanted was to be able to help him, on something as distressing as a son's illness... - and he asked me to make these transfers myself. And I did, I did... I transferred more than 5,000 euros... And now I find out that all this was a scam by Adelaide... There was never any José... [crying...] How could I have been so dumb?! How embarrassing... It was all my fault for wanting to have someone... I'm fine on my own, I don't want any friends or anything! Look, I just wanted to get my money back, but I don't want to report it. I can't, I don't want anything bad to happen to her, she's got little kids, you know..."

MOD. 7

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT

INTRODUCTION

Identity theft covers the unauthorised obtaining of personal and/or confidential data from a specific victim, and its possession or transfer and use in committing a crime.

These acts correspond to **online identity theft** when the victim's personal and/or confidential data are obtained via the internet and/or when the data obtained, by whatever means, are transferred via the internet, and/or used to commit a crime via the internet.

If the crime is categorised under only one of the acts described below, then its associated behaviours - obtaining, possession or use - have to take place over the Internet for the crime to be classified as online identity theft.

We can identify **three distinct acts**:

1. Obtaining personal data [via the Internet];
2. Possessing or transferring data [via the internet], knowing that they will be used for illicit purposes;
3. Using the data for committing crimes [over the Internet].

We can also identify **three types of identity theft**:

- Crimes not directly related to the victim but committed by using their identity;
- Crimes aimed at the enrichment of the offender or others and causing direct harm to the victim;
- Crimes aimed at defaming the victim.

In this Module, we explore the *modi operandi* used in online identity theft, as well as prevention and intervention strategies that the course participant, as a victim support officer/professional (VSO), should consider when providing support to victims of this type of cybercrime.

Modi operandi and nature of the crime

In Portugal, identity theft in itself is not, a crime; rather, it concerns unauthorised obtaining of personal data with a view to committing a criminal activity. Therefore, when we speak of identity theft, we can refer to a multiplicity of crimes provided for and punished in the Portuguese Penal Code.

This Course Module starts with an Activity (see Session Plan) illustrating different legally defined crimes that can be associated with online identity theft, such as: crime of forgery of documents (art. 256, nr. 1, al. a) of the Portuguese Penal Code); crime of unlawful access (art. 6, nr. 1 of the Cybercrime Law); crime of computer fraud (art. 221, nr. 1 of the Portuguese Penal Code).

Regarding the identity theft *modi operandi*, we can identify two methods:

- A **less technological** one, using so-called **social engineering** to obtain personal information from victims;
- A **more technological** one, in which the interaction with the victim is not a fundamental element for committing this crime.

Regarding the **social engineering** methods in identity theft, the following can be identified:

- Exploitation of the human factor as an element of vulnerability for cybersecurity;
- An act of psychological manipulation aimed at causing someone to act in a certain way or to disclose confidential information;

Less technological methods may be easier to use than more technological ones (such as malware or hacking), especially for cybercriminals whose low technical skills prevent them using certain tools and/or acquiring them in the darkweb.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT

Examples:

- Vishing (obtaining data through phone calls - more and more cybercriminals resort to native speakers);
- Romance and dating scams;
- Sextortion;
- Online child grooming;
- Going through the rubbish;
- Intercepting mail;
- Stealing documents containing the victim's personal or financial information;
- Pretending to be a person who can ask for such data/information;
- Obtaining information from people close to the victim;
- Contacting the victim under false pretences to obtain privileged information;
- Buying this information;
- Observing the victim as they use the information;
- Theft of hardware or mobile phone containing the victim's personal or confidential information.

As for the **more technological methods** for obtaining personal data, the following should be highlighted:

1. Identity theft through phishing:

- Massive email delivery with a shortcut to a webpage;
- The victim provides the perpetrator with personal information/passwords/access codes by accessing this website;
- The perpetrator of the crime accesses the real page of the bank, entering the victim's details and withdrawing money from the account;
- Money laundering: the process by which the perpetrators of some criminal activities conceal the origin of the goods and income (advantages) obtained illicitly, transforming the liquidity from these activities into legally reusable capital, by concealing the origin or real owner of the funds.

2. Identity theft through the use of malware:

- Malware, software that can be disseminated in various ways to illicitly infiltrate equipment, computers and networks for the purpose of stealing information, altering information or causing damage:
 - Through a link or file received via email;
 - When downloading movies or games;
 - Access to compromised websites;
 - Installing compromised apps, etc.

An example of **identity theft that combines social engineering and technological methods** is **spear phishing**: creating phishing emails using social engineering techniques to customise messages and websites, enhancing the credibility of the information and misleading the victim into providing information.

The most common situations of online identity theft are:

1. Phishing para obtenção de acesso à conta de e-mail:

- Once the victim's personal and confidential data has been obtained, using any of the more sophisticated methods mentioned above, the criminal can obtain access to the victim's email account. This will allow the perpetrator to become aware of the mailbox contents, to establish contact with the victim's bank - normally with the account manager - to carry out banking operations or to use that mailbox for sending email messages, which will normally be requests for financial aid.

2. Phishing para obtenção de acesso à conta bancária:

- Bulk emailing (spamming);
- The messages contain a link to a fake bank page;
- On the fake page, the user is asked to fill in/send confidential data.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT

3. Defamation on social networks:

- There are situations of identity theft aimed at defaming the victim on a social network, usually occurring within a friendship or dating relationships:
 - Creating a fake profile;
 - Using the victim's real profile, using their access credentials:
 - The victim themselves provide data to the perpetrator;
 - The perpetrator obtains these data by other means.

Prevention strategies

At this point in the Module, the trainer should cover the following strategies which can be used by the course participants in the intervention with the victim to **prevent online identity theft**:

- Configuring antivirus and anti-malware programs on their devices and configuring them to perform regular checks;
- Activating spam filters;
- Protecting devices by using authentication methods with biometric data or, alternatively, lock codes and installation of antivirus software;
- Checking and recognising secure websites (See information in Module 6 on this topic);
- Refraining from providing personal information or personal data requested through emails, messages, calls, unsolicited websites;
- Checking the name of the sender of the email - typos or other errors mean that the sender of the email is not/ representative of who they say they are;
- Checking for spelling mistakes indicating that the person is not communicating in their native language.

Intervention strategies

Strategies for preserving digital evidence

In this Module, the trainer should also present strategies to preserve digital evidence that can be explained to the victims during the supporting process. Since identity theft can have a multiplicity of criminal purposes, some generic strategies are presented below:

- Preserving the evidence on social networks by copying the URL of illegal content and screenshots of such content (See Module 10 for additional information on copying the URL);
- If there are asset transfers, keeping records of such transfers and contact the bank;
- Filing criminal complaints with the competent authorities;
- Requesting support from victim support entities to deal with the emotional suffering caused by the victimisation situation and ensure follow-up throughout the criminal process.

It is important that the support professional (VSO) remains available to **assist and/or accompany** the victim in the process of implementing the above strategies.

To whom and how to report

In Portugal, identity theft in itself is not a crime. However, it can be a means to commit a multitude of crimes provided for and punished in the Portuguese Criminal Code and the Cybercrime Law. In such cases, the facts must be reported to any criminal police body with generic jurisdiction (PSP and GNR), to the Polícia Judiciária or the Ministério Público (Public Prosecutor's Office), depending on the crime. For all purposes, the crime can always be reported to the Ministério Público, regardless of its nature.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT

Strategies to overcome victimisation and its impacts

Identity theft is a serious inconvenience for the victim and a great deal of time is spent repairing the consequences of the crime. In addition to the **time spent**, a consequence often pointed out by victims, the **emotional impact** of identity theft is described as being similar to the reactions of victims of violent crime. Many victims feel their privacy violated, feel helpless, fearful that the crime will be repeated and suspicious of the intentions of those around them. If victim identity theft is used for defamation on social networks, the impact that the **publicity/audience** adds to the crime committed exacerbates symptoms of emotional and psychological ill being.

In addition to the central guidelines for intervention given in Module 4 of this Training Course, the following **support strategies** are considered to be particularly relevant when supporting victims of online identity theft:

- Providing emotional support to the victim by listening, validating their experience and normalizing/framing reactions;
- Explaining to the victim that there are other people living situations similar to their own, breaking the idea of 'unique case';
- Informing in a simple, succinct and clear way, transmitting essential information to the victim about what happened and the next steps to take, through language adjusted to the victim's characteristics;
- Explaining the various types of support provided, conveying the message that the victim is not alone throughout this process;
- Refraining from promoting unrealistic expectations as to how the situation will be resolved;
- Explaining to the victim that, by the very nature of identity theft, other crimes can be committed against them, strengthening the professional's availability to support the victim;
- Preventing new crimes by raising awareness of the importance of adopting the prevention strategies described above in this Module.

Whenever possible, the presentation of these strategies (as well as the following ones) should be accompanied by concrete examples of how they work, aiming at making the course participants familiar with the language and form of communication to be used with the victim throughout the support. These examples are available in the slides section (*PowerPoint*).

Victims of identity theft may be **reluctant to report their crime to the police authorities**, especially if they have found out that the perpetrator is someone close to and trusted by them, such as a relative or a friend. In these cases, in addition to the above strategies, it is important that the support professional (VSO):

- Reinforces the victim's determination in seeking support and revealing their personal experience of cyber-victimisation;
- Assists the victim in their decision to report the crime (without taking decisions on behalf of the victim and/or influencing the process) by showing them the advantages and disadvantages of each option, for an informed decision;
- Passes on essential information to victims about their rights after they have lodged a complaint, reaffirming that support is independent of that.

Victims of online identity theft sometimes feel **wronged**, need to prove their innocence or feel **disappointed/frustrated** with the outcome of the criminal process. The support professional (VSO) should be aware of and act on these thoughts by:

- Reinforcing that they believe in the victim's account;
- Validating the experience and recognising the effects caused by the victimisation situation at various levels (psychologically and emotionally, socially and in other areas impacted);
- Valuing previous attempts at protection/resolution;
- Preventing blaming;
- Suggesting the sharing of feelings and fears with people trusted by the victim, recommending that these people keep their willingness to listen, without pressing for sharing;
- Explaining that recovery from victimisation is independent of the outcome of the criminal proceedings;
- Providing psychological support.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT

Specialised Support to Victims of Cybercrime

PART II – SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

Module 7 – Specialised support to victims of online identity theft



7 - Specialised support to victims of online identity theft

Identity theft

Identity theft covers the unauthorised obtaining of personal and/or confidential data from a specific victim, and its possession or transfer and use in committing a crime.

These acts correspond to **online identity theft** when the victim's personal and/or confidential data are obtained via the internet

We can identify **three distinct acts**:

- Obtaining personal data [via the Internet];
- Possessing or transferring data [via the Internet], knowing that they will be used for illicit purposes;
- Using the data for committing crimes [over the Internet].



7 - Specialised support to victims of online identity theft

a. Types and Modi operandi

Identity theft

We can also identify **three types of identity theft**:

- Crimes not directly related to the victim but committed by using their identity;
- Crimes aimed at the enrichment of the offender or others and causing direct harm to the victim;
- Crimes aimed at defaming the victim.



7 - Specialised support to victims of online identity theft

a. Modi operandi

Regarding the identity theft modi operandi, we can identify two methods:

- A **less technological** one, using so-called **social engineering** to obtain personal information from victims;
- A **more technological** one, in which the interaction with the victim is not a fundamental element for committing this crime.

Regarding the **social engineering** methods in identity theft, the following two forms can be identified:

- Exploitation of the human factor as an element of vulnerability for cybersecurity;
- An act of psychological manipulation aimed at causing someone to act in a certain way or to disclose confidential information;



7 - Specialised support to victims of online identity theft

a. Modi operandi

Less technological methods may be easier to use than more technological ones (such as malware or hacking), especially for cybercriminals whose low technical skills prevent them using certain tools and/or acquiring them in the darkweb.

Examples:

- Vishing (obtaining data through phone calls - more and more cybercriminals resort to native speakers);
- Romance and dating scams; Sextortion;
- Online child grooming;
- Going through the rubbish;
- Intercepting mail;
- Stealing documents containing the victim's personal or financial information;
- Pretending to be a person who can ask for such data/information;
- Obtaining information from people close to the victim;
- Contacting the victim under false pretences to obtain privileged information;
- Buying this information;
- Observing the victim as they use the information;
- Theft of hardware or mobile phone containing the victim's personal or confidential information.



7 - Specialised support to victims of online identity theft

a. Modi operandi

As for the **more technological methods** for obtaining personal data, the following should be highlighted:

Identity theft through phishing:

- Massive email delivery with a shortcut to a webpage;
- The victim provides the perpetrator with personal information/passwords/access codes by accessing this website;
- The perpetrator of the crime accesses the real page of the bank, entering the victim's details and withdrawing money from the account;
- Money laundering: the process by which the perpetrators of some criminal activities conceal the origin of the goods and income (advantages) obtained illicitly, transforming the liquidity from these activities into legally reusable capital, by concealing the origin or real owner of the funds.



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT

7 - Specialised support to victims of online identity theft

a. *Modi operandi*

Still in relation to the **more technological methods** for obtaining personal data:

Identity theft through the use of malware :

- Malware, software that can be disseminated in various ways to illicitly infiltrate equipment, computers and networks for the purpose of stealing information, altering information or causing damage :
- Through a link or file received via email;
- When downloading movies or games;
- Access to compromised websites;
- Installing compromised apps, etc.

An example of **identity theft that combines social engineering and technological methods is spear phishing**: creating phishing emails using social engineering techniques to customise messages and websites, enhancing the credibility of the information and misleading the victim into providing information.



7 - Specialised support to victims of online identity theft

a. *Modi operandi*

Most common situations of online identity theft:

1) Phishing for access to an email account:

Once the victim's personal and confidential data has been obtained, using any of the more sophisticated methods mentioned above, the criminal can obtain access to the victim's email account. This will allow the perpetrator to establish contact with the victim's bank - normally with the account manager - to carry out banking operations or to use that mailbox for sending email messages, which will normally be requests for financial aid

2) Phishing for bank account access:

Through bulk emailing (spamming). These messages contain a link to a fake bank page. On this fake page, the user is asked to fill in/send confidential data.



7 - Specialised support to victims of online identity theft

a. *Modi operandi*

Most common situations of online identity theft:

3) Defamation on social networks:

There are two situations of identity theft aimed at defaming the victim on a social network, usually occurring within friendship or dating relationships:

- Creating a fake profile;
- Using the victim's real profile, using their access credentials:
 - o The victim themselves provide data to the perpetrator;
 - o The perpetrator obtains these data by other means.



7 - Specialised support to victims of online identity theft

b. *Prevention strategies*

- Configuring antivirus and anti-malware programs on their devices and configuring them to perform regular checks;
- Activating of spam filters;
- Protecting devices by using authentication methods with biometric data or, alternatively, lock codes and installation of antivirus software;
- Checking and recognising secure websites:
 - o The website should display a lock symbol on the left-hand side immediately before the website address;
 - o The website URL must contain the certificate - 'https://'; containing the 's' of 'secure' added to the 'http', and check the URL, namely when the addresses are shared by message or email;
- Refraining from providing personal information or personal data requested through emails, messages, calls, unsolicited websites;
- Checking the name of the sender of the email - typos or other errors mean that the sender of the email is not/representative of who they say they are;
- Checking for spelling mistakes indicating that the person is not communicating in their native language.



7 - Specialised support to victims of online identity theft

c. *Intervention strategies*

i. *Preserving digital evidence*

- Preserving the evidence on social networks by copying the URL of illegal content and screenshots of such content;
- If there are asset transfers, keeping records of such transfers and contact the bank;
- Filing criminal complaints with the competent authorities;
- Requesting support from victim support entities to deal with the emotional suffering caused by the victimisation situation and ensure follow-up throughout the criminal process.

It is important that the support professional (VSO) remains available to **assist and/or accompany** the victim.



7 - Specialised support to victims of online identity theft

c. *Intervention strategies*

ii. *To whom and how to report*

Identity theft in itself is not a crime. However, it can be a means to commit a multitude of crimes provided for and punished in the Portuguese Criminal Code and the Cybercrime Law.

In Portugal, facts should be reported to:

- Any criminal police body with generic jurisdiction (PSP e GNR);
- Polícia Judiciária;

Or to, depending on the crime,

- Ministério Público / Public Prosecutor's Office (all crimes are under their competence, regardless of the nature of the crime).



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT

7 - Specialised support to victims of online identity theft

c. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

Support strategies: (In addition to the central guidelines for intervention – Module 4)

- Providing emotional support to the victim by listening, validating their experience and normalizing/framing reactions;
- Explaining to the victim that there are other people living situations similar to their own, breaking the idea of 'unique case';
- Informing, in a simple, succinct and clear way, transmitting essential information to the victim about what happened and the next steps to take, through language adjusted to the victim's characteristics;
- Explaining the various types of support provided, conveying the message that the victim is not alone throughout this process;
- Refraining from promoting unrealistic expectations as to how the situation will be resolved;
- Explaining to the victim that, by the very nature of identity theft, other crimes can be committed against them, strengthening the professional's availability to support the victim;
- Preventing new crimes by raising awareness of the importance of adopting the prevention strategies described above in this Module.



7 - Specialised support to victims of online identity theft

c. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

Victims of identity theft may be **reluctant to report their crime to the police authorities**, especially if they have found out that the perpetrator is someone close to and trusted by them, such as a relative or friend.

In these cases, in addition to the above strategies, it is **important that the supporting professional (VSO):**

- Reinforces the victim's determination in seeking support and revealing their personal experience of cyber-victimisation;
- Assists the victim in their decision to report the crime (without taking decisions on behalf of the victim and/or influencing the process) by showing them the advantages and disadvantages of each option, for an informed decision;
- Passes on essential information to victims about their rights after they have lodged a complaint, reaffirming that support is independent of that.



7 - Specialised support to victims of online identity theft

c. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

Victims of online identity theft sometimes feel **wronged**, need to prove their innocence or feel **disappointed/frustrated** with the outcome of the criminal process.

The support professional (VSO) should be **aware** of and **act** on these thoughts by:

- Reinforcing that they believe in the victim's account;
- Validating the experience and recognising the effects caused by the victimisation situation at various levels (psychologically and emotionally, socially and in other areas impacted);
- Valuing previous attempts at protection/resolution;
- Preventing blame;
- Suggesting the sharing of feelings and fears with people trusted by the victim, recommending that these people keep their willingness to listen, without pressing for sharing;
- Explaining that recovery from victimisation is independent of the outcome of the criminal proceedings;
- Providing psychological support.



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT

SESSION PLAN 7

1. Training

Training Title Training Course Specialised Support to Victims of Cybercrime

Modules/Topics Specialised support to victims of online identity theft

Date of Session **Time** **Total Duration** 40 minutes

Trainers

2. Specific Objectives By the end of the session, the participants should be able to correctly:

- Distinguish the nature and modi operandi of online identity theft;
- List proposed intervention strategies for specialised support to victims of online identity theft;
- Recognise proposed strategies to prevent re-victimisation for intervention with victims of online identity theft.

3. Session Plan

| | Content | Methods | Resources | Assessment Activities | Duration |
|--------------|--|-----------------------|--|-------------------------|----------|
| Introduction | Activity 4 | Active | Guidance for Activity 4 and Case of Activity 4 | Observation | 5 |
| | Modi operandi and nature of the crime | Expository and active | Computer: Datashow and projection screen | Observation | 10 |
| Development | Prevention strategies | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| | Intervention strategies: <ul style="list-style-type: none"> • Strategies for preserving digital evidence • To whom and how to report • Strategies to overcome victimisation and its impacts | Expository and active | Computer: Datashow and projection screen | Observation | 15 |
| Conclusion | Concluding summary and clarification of issues | Expository and active | Computer: Datashow and projection screen | Observation | 5 |

OBSERVATIONS

Participants:

Victim Support Officers (VSO)

Date: / /

Trainer:

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT

INSTRUCTIONS AND KEY INFORMATION FOR THE TRAINER

CONTENT MATCHING

| | | |
|--|--|------------------|
| Session Plan | <i>ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims</i> | |
| | PART | CHAPTER |
| Activity 4 | No correspondence | |
| | See Guidance for Activity 4 | |
| Modi operandi and nature of the crime | No correspondence | |
| | See Module Introduction | |
| Prevention strategies | No correspondence | |
| | See Module Introduction | |
| Intervention strategies | | |
| Strategies for preserving digital evidence | No correspondence | |
| | See Module Introduction | |
| To whom and how to report | No correspondence | |
| | See Module Introduction | |
| Strategies to overcome victimisation and its impacts | Part II - Proceeding | Chapter 2 - 2.1. |
| | See Module Introduction | |
| Concluding summary and clarification of issues | No correspondence | |

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT

GUIDANCE FOR ACTIVITY 4

| Module/Topic | Specialised support to victims of online identity theft | REF. CODE | TRAINING AREA |
|--------------|---|-----------|---------------|
| Objectives | This activity aims to raise awareness for the characteristics of online identity theft, alerting in particular to the wide range of crimes within its scope. | | |
| Delivery | <p>The trainer should read the Activity 4 Case for Discussion (or ask any of the participants to read it aloud).</p> <p>A handout with this case can be distributed to the participants or projected on the screen.</p> <p>After reading it, the trainer should ask the group about the crimes in this case.</p> <p>During the group's participation, the trainer should refer to <i>National legal framework of cybercrime</i> (see Module 2) and point that there are several identifiable crimes in this case:</p> <ul style="list-style-type: none">• Creating a false email corresponds to the crime of forgery of documents (art. 256, nr. 1, al. A) of the Portuguese Penal Code);• Accessing Julio's wife email account corresponds to the crime of illegitimate access (art. 6, no. 1 of the Portuguese Cybercrime Law);• The attempts to obtain credit on behalf of Julio correspond to the crime of attempted computer fraud (art. 221, no. 1 of the Portuguese Constitution). | | |
| Notes | See Module Introduction | | |

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT

ACTIVITY 4: CASE FOR DISCUSSION

Messages looking like they were coming from the webmail service used were sent to various email addresses and asked for a password update.

Julio's wife entered her data, which allowed the perpetrator to access her email account, and consequently to much of her personal data, as well as that of her family. Julio was subsequently contacted by two credit companies who wanted to confirm that the applications to obtain credit on his behalf were legitimate. Julio, who had never applied for credit, explained that he had not contacted any of the companies. He was amazed at how much of his personal data the perpetrator knew. The applications were declined. A month later, Julio went to his bank to take out a loan to buy a new home. The loan was refused because of the many applications for credit made on his behalf in recent months.

MOD. 8

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

INTRODUCTION

This Module covers different forms of online sexual abuse of children and young people.

Online sexual abuse, as a comprehensive concept, can be defined as encompassing **any form of child sexual abuse in an online context**, which includes different manifestations of abuse and exploitation, from non-contact sexual abuse facilitated by ICT and the internet, social networks or other platforms, such as harassment and online grooming, to sharing content on the darkweb (image and/or audio) of child sexual abuse and exploitation, using previously taken photographs or video.

Particular emphasis will be placed on understanding **online grooming** and the **online dissemination of child sexual abuse content**.

The amount of child sexual abuse material (CSAM) being disseminated online keeps increasing, a trend confirmed by law enforcement authorities and non-governmental organisations dedicated to analysing and reporting sexual abuse content online. The dissemination of such content has a serious impact on victims, who suffer re-victimisation processes, every time their photos or videos are viewed and/or shared.

How this material is disseminated continues to be through peer-to-peer (P2P) networks and anonymous access, such as Darknet browsers (e.g. Tor).

In parallel, there has been a continuous increase in the distribution of CSAM via social networks. The difficulty of securing evidence in some of these networks makes investigation by the authorities particularly difficult. There are cases where such content/materials are shared by children themselves, then shared with peers who, in turn, share them with other peers until eventually these content/materials end up on CSAM distribution platforms. In many cases, perpetrators who distribute CSAM online are also involved in child sexual abuse situations. The high demand for this type of material perpetuates child abuse and continuous victimisation.

Legally, in Portugal, CSAM situations are included in the crime of child pornography.

It has been argued internationally that the concept of 'child pornography' should be abandoned as what underpins child sexual abuse is not pornography (i.e. adults engaged in consensual erotic behaviour in pictures, video and/or writing, intended to cause sexual arousal). For this reason, it is argued that rather than referring to such material as 'child pornography', the expression 'Child Sexual Abuse Material' (CSAM) should be used.

In addition to these phenomena, online grooming also deserves special attention. We will explore how online grooming operates in social networks and online games, considering that children and young people spend considerable amount of time in these platforms.

In addition to reading the content of this Module, we suggest that the trainer consults Chapter 1 - Part I of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*.

Types, modi operandi and nature of the crimes

Dissemination of child sexual abuse material [CSAM]

Child sexual abuse material generated online

Currently, two modes of disseminating child sexual abuse material online have become more frequent:

- Self-generated content by minors;
- Demand for live-streaming sessions of minors' sexual abuse.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

Self-generated content

Increased access by children and young people, at younger ages, to smartphones and other devices, combined with their perception that sharing intimate content is low-risk, has been associated with the emergence of self-generated intimate content.

A distinction should be made between **intimate content that is voluntarily (self) generated** by the child or young person and **intimate content (self) generated under coercion or extortion** by another person:

- Regarding the first category, there is an increasing number of children and young people sharing photos or videos via social networks or chat platforms with other peers and friends, and consequently becoming more vulnerable to situations of online sexual abuse and exploitation, such as online grooming by adults posing as peers.

An example is sexting, as a form of self-generated content - text, images and/or videos - of a sexual nature, which are shared usually in a consensual manner and among peers.

Although this production and sharing is voluntary, it can precipitate subsequent extortion, grooming and other forms of online sexual abuse

- Also, self-generated content can be shared firstly among peers, but also in online sexual abuse networks afterwards. Such cases may subsequently expose children and young people to coercion or extortion by others who, using threat and/or blackmail, seek to coerce children into (self) producing additional sexual content.

Live streaming of child sexual abuse

With improved internet infrastructure and connection speed, there has been an increased demand for **live-streaming child sexual abuse sessions**: watching live child sexual abuse content.

These situations are common in countries already regarded as destinations for child abuse sex tourism. These streaming channels are paid for and are often advertised on adult pornographic websites. Once this streaming service/channel is found, users are directed to encrypted platforms that allow video conferencing. Perpetrators using these streaming services/channels are often given the opportunity to provide instructions on how they want the child sexual abuse to take place, in real time. Users looking for such content can also travel to countries where live streaming sexual abuse sessions take place and watch them in person.

Online Grooming

Online grooming can be defined as a **process of manipulation** and a **form of sexual solicitation** of children and young people. It usually starts with a non-sexual approach through the internet and ICT, including online games and social networks, in order to establish a relationship of trust with the child and persuade them to meet face-to-face so that the perpetrator can consummate the sexual abuse. Establishing a relationship of trust with the child, mediated by the internet and ICT, can also aim at **persuading the child to produce and share sexual content**.

Online grooming allows perpetrators to select the type of victim they want to manipulate and entice, for example by age and/or physical appearance. In addition, online grooming allows the enticement of a large number of victims simultaneously, among other advantages for the perpetrator, such as the possibility of 'disappearing', changing their identity if the victim refuses or ignores the advances, and reappearing with another identity, in order to approach the same victim, this time knowing a little more about their limits and preferences.

Grooming via social networks and online video games

Our training regarding online grooming starts by presenting information on the increasing use of online gaming platforms (see *PowerPoint*).

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

Perpetrators take advantage of the anonymity provided by online video game platforms and the children and young people's (consumers of these platforms) low awareness of online risks of grooming and manipulation processes.

Thus, they use online gaming platforms to gain the trust of these children and young people and then convince their targets to use other online communication platforms - *Facebook® Messenger, Instagram®, WhatsApp®, Viber®, Telegram®, Snapchat®,* etc. - to keep communicating and maintaining their relationship with these children and young people and groom them for sexual purposes.

Emerging online grooming cases in this context has motivated online gaming platforms to create online grooming prevention measures, including safety policies and specific guides for children and families.

Prevention strategies

To **prevent situations of online sexual abuse**, at this point of the Module, the trainer should present the following strategies which course participants, as victim support officers/professionals (VSO) can use in the intervention with the child/youth victim and their families:

- Raising awareness of the importance of educating children and young people on how to use the internet and ICTs safely and how to identify risk situations online;
- Raising awareness of clear rules for internet and ICT use: e.g. placing videogames/computers in a common area of the home and/or allowing the use of mobile/electronic devices only in common areas of the home;
- Reinforcing the importance of adult monitoring or supervision of the online behaviour of dependant children or young people: namely if they receive calls from unknown numbers, spend a lot of time online and until very late, start suddenly to isolate themselves from family and friends, as well as the type of friend requests received and their source;
- Adults and dependant children and young people should jointly configure the privacy settings of social networks and pages/profiles by deleting personal or other information disclosing the home address, school, mobile phone number, etc;

The **family** plays a very important role in protecting children and young people from the risks of Internet and ICT use. Information on the importance of the family in preventing cybercrime against children and young people can be found in Chapter 4 - Part II of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*. Similarly, the family's involvement in supporting and intervening with children and young people victims of cybercrime is important, including educating the child or young person who is a victim for a conscious and safe use of the internet and ICTs. See Chapter 2 - Part II of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*.

Intervention strategies

Strategies for preserving digital evidence

In addition to addressing the dynamics and *modi operandi* of different forms of online sexual abuse of children and young people and presenting measures to prevent re-victimisation, the trainer should also present strategies for preserving digital evidence that can be explained to the child and young person (and their families) being supported. Let's look at some of them:

- Ceasing all communication with the perpetrator;
- Not blocking or disabling the social network or communication platform used by the perpetrator to communicate with the victim; this is even more important for communication platforms that use end-to-end encryption³⁹ - such as WhatsApp® or Viber®, among others - since it is not possible to access copies of the conversations once they have been deleted by the users;
- Saving all records of communication with the abuser (e.g. taking screenshots), including images and/or videos

³⁹ This is a security mechanism that protects data during an exchange of messages so that the content can only be accessed at both ends of the communication, i.e. by the sender and the recipient.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

sent and received;

- Saving all the information that allows identifying the perpetrator, such as: username, URL of the social network profile (See intervention strategies proposed in Module 10), Skype® ID, bank transfer details (if there were requests for money);
- Not giving in to the perpetrator's demands or blackmail;
- Filing criminal complaints with the competent authorities;
- Requesting support from victim support entities to deal with the emotional suffering caused by the victimisation situation and ensure follow-up throughout the criminal process.

To whom and how to report

Anyone coming across **online child sexual abuse material** should report it to the national authorities or competent bodies in their country, in particular bodies/platforms for reporting illegal online content, such as entities/hotlines members of INHOPE⁴⁹. These bodies not only refer the reported cases to the competent national authorities for further investigation, but also have some tools at their disposal to quickly remove these contents and preserve the evidence.

Suspected **online solicitation or sexual coercion of minors** should be reported to authorities or specialised victim support entities. It is also of the utmost importance to report these cases as soon as one is aware of them, since as a general rule there may be other children and young people in danger of sexual abuse and exploitation by the same perpetrator.

In Portugal, as all these conducts constitute sexual crimes committed against minors under the age of 18, these crimes fall under the competence of the Polícia Judiciária and must be reported to that entity or to the Ministério Público (Public Prosecution Service).

Strategies to overcome victimisation and its impacts

Some of the specificities of the intervention with children and young people victims of cybercrime detailed in Chapter 2 - Part II of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*, include:

- Taking the child or young person characteristics and **stages of development** into account;
- Considering, whenever possible, the **involvement of the family**;
- Focusing on teaching how to use ICTs and the Internet safely as a **protective behaviour against re-victimisation**.

The trainer should distribute handouts with the tables in annex on the *Key Stages in the child/young person's development process and on the Approach and communication with children and young people of different age groups* (see Session Plan).

This Module will address the particular aspects that should guide the support professional's (VSO) intervention, by exploring the **expected gains (developmental acquisitions) for each age group** and, consequently, how the communication and intervention with the child/young person victim should be conducted. It also addresses the effects of the cybervictimisation of the child/young person on their family.

Furthermore, it considers the **impacts and consequences of the sexual cybervictimisation experience** on children or young people, in line with Chapter 4 - Part I of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims* and Module 3 of this Training Course. A summary of the consequences of the sexual cybervictimisation experience is presented in the table below:

⁴⁹ INHOPE is an international network that brings together several entities/hotlines that operate online illegal content reporting services in different countries. See <https://www.inhope.org/EN>

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

| Emotional and psychological health consequences | Physical health consequences | Behaviour changes |
|--|---|--|
| <ul style="list-style-type: none"> Shock, especially when sexual violence is committed by someone known or trusted by the child or young person; Anger towards the perpetrator(s) of the crime and towards themselves for failing to prevent the victimisation situation; Guilt and shame; Anxiety, including frequent thoughts and memories about what happened; Various fears, including fear that the situation of violence will be repeated, of being alone, of nobody believing in them, of the consequences for the perpetrator [especially if the victim knows them]; Decrease in their self-esteem [no longer liking themselves]; Deep sadness. | <ul style="list-style-type: none"> Injuries caused by the violence or physical force used; Injuries directly related to sexual violence, such as injuries to the sexual organs, pain, bleeding, discharge; Sexual and reproductive health problems such as sexually transmitted infections; Unwanted pregnancies; Decreased appetite; Insomnia and nightmares [associated with constant thoughts about what happened] or excessive sleep. | <ul style="list-style-type: none"> Increased aggressiveness towards other people and themselves [including self-mutilation]; Regressive behaviour [e.g. sleeping with the light on, bedwetting]; Social isolation from colleagues/peers, friends and family; A lack of interest in school and a drop in school performance; Disinterest in previously enjoyed activities; Changes in sexual behaviour. |

Therefore, in addition to the intervention central guidelines presented in Module 4 of this Training Course, the following support **strategies** are considered particularly relevant when providing support for children and young people victims of online sexual abuse and their families (or legal guardians or other carers who are accompanying the child/young person):

- Informing in a simple, succinct and clear way, transmitting essential information to the legal guardian, carer or other adult person, or to the young person themselves, in case they come on their own, about:
- The duty to report:** It is essential that, if the situation is disclosed or there is a suspicion, the situation is reported to the police or judicial authorities to enable starting a formal investigation and protecting the child/young person from further victimisation.

Reporting is mandatory for any person who has knowledge of situations which endanger the life, physical or mental integrity or freedom of a child or young person under the age of 18.

It follows that, if the situation has not yet been reported to the competent authorities, it is the duty of the support professional (VSO) to report it as soon as they become aware of the situation.

Prompt contact with the police or judicial authorities enables the investigation to be conducted more quickly, the victim to be heard sooner and physical and/or witness evidence to be preserved.

- The importance of the child or young person being examined medically, especially when online sexual abuse results in a face-to-face (offline) sexual victimisation of the child or young person (see table above on the physical health consequences).
- Informing the children or young person that the support professional (VSO) or legal guardian will have to contact other entities such as police or judicial entities, to ensure they can be better supported.
- Explaining to the child or young person victim and to their family/legal guardians the steps following the complaint and how the criminal procedure functions.
- Providing support throughout the process, including psychological support, both to the child/young person victim and to the family/legal guardians/ carers.
- Reinforcing the prevention strategies addressed above.

In addition to these central aspects and strategies, when contacting/communicating with children or young people who are victims of online sexual abuse, the support professional (VSO) should cover the aspects and strategies already addressed in the previous Modules of the Course. See also Chapter 2 - Part II of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*. In the case of children and young

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

people, among all these strategies, we stress the importance of conveying as clearly as possible that:

- Nothing that is happening is the victim's fault;
- Nothing that the victim may have said or done justifies forcing, deceiving or persuading them to become sexually involved with another person;
- No one has the right to force the victim to have a sexual interaction against their will (neither those close to them have this right);
- The perpetrator is solely responsible for what happened to them.

Similarly, in contacting/communicating with relatives/legal guardians/carers, the support professional (VSO) should:

- Emphasise that the disclosure of cybervictimisation by the child/young person should be positively reinforced, believed and validated by meaningful persons/trusted adults;
- Reinforce to relatives/legal guardians/carers that it is fundamental that they remain available to support the child/young person who is a victim and to listen to them, without overprotection or pressure to share thoughts/emotions and/or memories about the cybervictimisation event;
- Raise awareness of the need not to share unrealistic promises or magical results with the child/young victim in the face of what may happen, both in the psychological and emotional recovery process and in the criminal process.

In the case of professionals who have accompanied the children/young victims, the support professional (VSO) should:

- Inform them about the need to comply with defined internal procedures, safeguarding the privacy of the child/young person and restricting intra- and inter-institutional sharing of information on the situation of victimisation to what is essential.

PART 2 – SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 – SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

Specialised Support to Victims of Cybercrime

PART II – SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

Module 8 – Specialised support to children and young people victims of online sexual abuse



8 – Specialised support to children and young people victims of online sexual abuse

Online sexual abuse, as a comprehensive concept, can be defined as encompassing any form of child sexual abuse in an online context.

CSEM/CSAM



Consequently, it includes different manifestations of abuse and exploitation, from non-contact sexual abuse facilitated by ICT and the internet, social networks or other platforms, such as harassment and online grooming, to sharing content on the darkweb (image and/or audio) of child sexual abuse and exploitation, using previously taken photographs or video



8 – Specialised support to children and young people victims of online sexual abuse

This material is usually disseminated through **peer-to-peer (P2P)** networks and anonymous access, such as **Darknet** browsers (e.g. Tor). But there has been a continuous increase in the distribution of CSAM/CSEM via **social networks**.

Regarding grooming – social networks and online games

In Portugal, **CSEM** and **CSAM** situations are covered by the crime of Child Pornography, article 176 of the Criminal Code

➤ Problems with terminology: the concept of pornography (i.e. adults engaged in consensual erotic behaviour in pictures, video and/or writing, intended to cause sexual arousal) does not reflect what underpins child sexual abuse.



8 – Specialised support to children and young people victims of online sexual abuse

a. Types and Modi operandi

1. Dissemination of child sexual abuse material (CSAM)

- i. Child sexual abuse material generated online
- ii. Self-generated content
- iii. Live-streaming of child sexual abuse

2. Online grooming



8 – Specialised support to children and young people victims of online sexual abuse

a. Types and Modi operandi

1. Dissemination of child sexual abuse material (CSAM)

i. Child sexual abuse material generated online

Self-generated content by minors;

Demand for live-streaming sessions of minor's sexual abuse.



8 – Specialised support to children and young people victims of online sexual abuse

a. Types and Modi operandi

1. Dissemination of child sexual abuse material (CSAM)

ii. Self-generated content

Intimate content voluntarily (self) generated by the child or young person – sharing photos or videos via **social networks** or **chat platforms** with other peers. E.g. sexting; form of self-generated content of a sexual nature - text, images and/or videos.

The child generating this content becomes more vulnerable to situations of online sexual abuse and exploitation, such as online grooming by adults posing as peers.

≠

Intimate content (self) generated under coercion or extortion by another person. Content shared usually in a consensual manner and among peers but that it can lead to subsequent extortion, grooming and other forms of online sexual abuse, particularly when disseminated in online sexual abuse networks.



PART 2 – SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 – SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

8 – Specialised support to children and young people victims of online sexual abuse

a. Types and Modi operandi

1. Dissemination of child sexual abuse material (CSAM)

iii. Live-streaming of child sexual abuse

Increased demand for **live-streaming child sexual abuse sessions**: watching live child sexual abuse content.

How? Streaming channels are paid for and are often advertised on adult pornographic websites. Once this streaming service/channel is accessed, users are directed to encrypted platforms that allow video conferencing.

Child abuse sex tourism - Users looking for such content can also travel to countries where live streaming sexual abuse sessions take place and watch them in person.



8 – Specialised support to children and young people victims of online sexual abuse

a. Types and Modi operandi

2. Grooming

Process of manipulation and a form of sexual solicitation of children and young people.

It usually starts with a non-sexual approach through the internet and ICT, including online games and social networks, in order to establish a relationship of trust with the child and persuade them to meet **face-to-face** so that the perpetrator can consummate the sexual abuse.

Establishing a relationship of trust with the child, mediated by the internet and ICT, can also aim at **persuading the child to produce and share sexual content**.

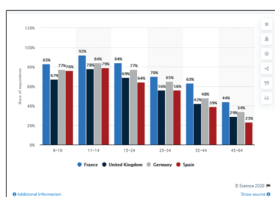


8 – Specialised support to children and young people victims of online sexual abuse

a. Types and Modi operandi

2. Grooming

Percentage of online gamers by age band in 4 European countries, January-March 2018.



8 – Specialised support to children and young people victims of online sexual abuse

b. Prevention strategies

Support professionals (VSO) can use the following strategies in the intervention with the child/youth victim and their family:

Raising awareness of the importance of educating children and young people on how to use the internet and ICTs safely and how to identify risk situations online;

Raising awareness about clear rules for internet and ICT use: e.g. placing videogames/computers in a common area of the home and/or allowing the use of mobile/electronic devices only in common areas of the home;



8 – Specialised support to children and young people victims of online sexual abuse

b. Prevention strategies

Reinforcing the importance of adults monitoring or supervision of the online behaviour of the dependant child or young people: namely if they receive calls from unknown numbers, spend a lot of time online and until very late, start suddenly to isolate from family and friends, as well as the type of friend requests received and their source;

Adults and dependant children and young people should jointly configure the privacy settings of social networks and pages/profiles by deleting personal or other information disclosing the home address, school, mobile phone number, etc.



8 – Specialised support to children and young people victims of online sexual abuse

b. Prevention strategies

The **family** plays a very important role in protecting children and young people from the risks of Internet and ICT use.

Information on the **importance of the family in preventing** cybercrime against children and young people can be found in Chapter 4 - Part II of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*.

For information on the **importance of the family's involvement in supporting and intervening** with children and young victims of cybercrime, including **educating the child or young person** who is a victim for a conscious and safe use of the internet and ICTs, see Chapter 2 - Part II of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*.



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

8 – Specialised support to children and young people victims of online sexual abuse

c. Intervention strategies

i. Preserving digital evidence

Ceasing all communication with the perpetrator;

Not blocking or disabling the social network or communication platform used by the perpetrator to communicate with the victim; this is even more important for communication platforms that use end-to-end encryption - such as WhatsApp® or Viber®, among others since that it is not possible to access copies of the conversations once they have been deleted by the users;

This is a security mechanism that protects data during an exchange of messages so that the content can only be accessed at both ends of the communication, i.e. by the sender and the recipient.



8 – Specialised support to children and young people victims of online sexual abuse

b. Intervention strategies

Saving all records of communication with the abuser (e.g. taking screenshots), including images and/or videos sent and received; Saving all the information that allows identifying the perpetrator, such as: user name, URL of the social network profile (See intervention strategies proposed in Module 10), Skype® ID, bank transfer details (if there were requests for money);

Not giving in to the perpetrator demands or blackmail;

Filing criminal complaints with the competent authorities;

Requesting support from victim support entities to deal with the emotional suffering caused by the victimisation situation and ensure follow-up throughout the criminal process.



8 – Specialised support to children and young people victims of online sexual abuse

b. Intervention strategies

ii. To whom and how to report

Online child sexual abuse content and material – national authorities or bodies/platforms supporting the reporting of illegal online content, such as bodies/hotlines members of INHOPE

Online solicitation or sexual coercion of minors – authorities or specialised victim support entities

In Portugal, the competent national authorities are: Judiciary Police or Public Prosecution Service.



8 – Specialised support to children and young people victims of online sexual abuse

b. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

In addition to the intervention central guidelines presented in Module 4 of this Training Course

Informing, in a simple, succinct and clear way, transmitting essential information to the legal guardian, carer or other adult person, or to the young person themselves, in case they come on their own, about:

o **The duty to report:** It is essential that, if the situation is disclosed or there is a suspicion, the situation is reported to the police or judicial authorities to enable starting a formal investigation and protecting the child/young person from further victimisation.

o **Reporting is mandatory** for any person who has knowledge of situations which endanger the life, physical or mental integrity or freedom of a child or young person under the age of 18.



8 – Specialised support to children and young people victims of online sexual abuse

b. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

In addition to the intervention central guidelines presented in Module 4 of this Training Course

o The importance of the child or young person being examined medically, especially when online sexual abuse results in a face-to-face (offline) sexual victimisation of the child or young person (see table on the physical health consequences).

o Informing the child or young person that the support professional (VSO) or legal guardian will have to contact other entities such as police or judicial entities, to ensure they can be better supported.

o Explaining to the child or young person victim and to their family/legal guardians the steps following the complaint and how the criminal procedure functions.

o Providing support throughout the process, including psychological support, both to the child/young person victim and to the family/legal guardians/ carers.

o Reinforcing the prevention strategies addressed above.



8 – Specialised support to children and young people victims of online sexual abuse

b. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

In addition to these central aspects and strategies, when contacting/communicating with children or young people who are victims of online sexual abuse, the support professional (VSO) should:

Reinforce the victim's courage in seeking support and revealing their personal experience of cybervictimisation.

Demonstrate that they believe what the victim is telling them about what happened without being judgmental.

Respect and promote the expression of emotions and vulnerabilities that arise when sharing the cybervictimisation experience.

Normalise the reactions presented.



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

8 – Specialised support to children and young people victims of online sexual abuse

b. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

Conveying as clearly as possible that:

Nothing that is happening is the victim's fault.

Nothing that the victim may have said or done justifies forcing, deceiving or persuading them to become sexually involved with another person.

No one has the right to force the victim to have a sexual interaction against their will (neither those close to them have this right).

The perpetrator is solely responsible for what happened to them.

Suggesting to the child or young person sharing feelings and fears with people they trust.

If the victim is young, and if they are willing and authorise, then involve relatives and/or friends in the recovery process.



8 – Specialised support to children and young people victims of online sexual abuse

b. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

Similarly, in contacting/communicating with relatives/legal guardians/carers, the support professional (VSO) should:

Emphasise that the disclosure of cybervictimisation by the child/young person should be positively reinforced, believed and validated by meaningful persons/trusted adults;

Reinforce to relatives/legal guardians/carers that it is fundamental that they remain available to support the child/young person who is a victim and to listen to them, without overprotection or pressure to share thoughts/emotions and/or memories about the cyber-victimisation event;

Raise awareness of the need not to share unrealistic promises or magical results with the child/young victim in the face of what may happen, both in the psychological and emotional recovery process and in the criminal process.



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

SESSION PLAN 8

1. Training

Training Title Training Course Specialised Support to Victims of Cybercrime

Modules/Topics Specialised support to children and young people victims of online sexual abuse

Date of Session **Time** **Total Duration** 40 minutes

Trainers

2. Specific Objectives

By the end of the session, the participants should be able to correctly:

- Distinguish the nature and modi operandi of the different forms of online child sexual abuse, namely the dissemination of online child sexual abuse content and grooming;
- List the proposed intervention strategies for specialised support to children and young people victims of online sexual abuse;
- Recognise the proposed re-victimisation prevention strategies in the intervention with children and young people who are victims of online sexual abuse.

3. Session Plan

| | Contents | Methods | Resources | Assessment [Activities] | Duration [minutes] |
|--------------|---|-----------------------|--|-------------------------|--------------------|
| Introduction | Types of online child sexual abuse: <ul style="list-style-type: none"> • Dissemination of child sexual abuse material: child sexual abuse content generated online; self-produced content; live streaming of child sexual abuse • Grooming: online grooming on social networks and online video games | Expository and active | Computer: Datashow and projection screen | Observation | 10 |
| | Modi operandi and nature of the crimes | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| Development | Prevention strategies | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| | Intervention strategies: <ul style="list-style-type: none"> • Strategies for preserving digital evidence • To whom and how to report • Strategies to overcome victimisation and its impacts | Expository and active | Computer: Datashow and projection screen; Frames - Annex ⁴¹ | Observation | 15 |
| Conclusion | Concluding summary and clarification of issues | Expository and active | Computer: Datashow and projection screen | Observation | 5 |

OBSERVATIONS

Participants:

Victim Support Officers (VSO)

Date: / /

Trainer:

⁴¹ The Tables - Annex Key Stages in the Child/Young Person's Development Process and Approach and Communication with Children and Young People of Different Age Groups, from the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*, are available on the following pages.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

INSTRUCTIONS AND KEY INFORMATION FOR THE TRAINER

CONTENT MATCHING

Session Plan

ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims

| | PART | CHAPTER |
|--|-------------------------|---------------------------|
| Types of online child sexual abuse | Part I - Understanding | Chapter 1 - 1.3. |
| | See Module Introduction | |
| Modi operandi and nature of the crimes | No correspondence | |
| | See Module Introduction | |
| Prevention strategies | No correspondence | |
| | See Module Introduction | |
| Intervention strategies | | |
| Strategies for preserving digital evidence | No correspondence | |
| | See Module Introduction | |
| To whom and how to report | No correspondence | |
| | See Module Introduction | |
| Strategies to overcome victimisation and its impacts | Part II - Proceeding | Chapter 2 - 2.1. and 2.4. |
| | See Module Introduction | |
| Concluding summary and clarification of issues | No correspondence | |

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE

Table - Annex: Key stages in the child/young person's development process

| | physical development | emotional and cognitive development (including language) | social and moral development |
|--------------------|--|--|--|
| 3-6 years | <ul style="list-style-type: none"> Can draw and demonstrates other manual activities Can write their own name The body develops, taking the forms of the adult body Increase in dexterity and coordination capacity | <ul style="list-style-type: none"> Can remember family experiences Uses some vocabulary Can adjust speech according to the interlocutor's characteristics (such as age, gender and social status) | <ul style="list-style-type: none"> Can interpret, predict and influence other people's reactions Establishes the first friendships Self-aware emotions appear (such as shame and guilt) Has some emotional control |
| 6-12 years | <ul style="list-style-type: none"> Progressive increase in weight and height Handwriting becomes smaller and more readable Drawings are more structured Games and playing involving running, excitement and competition are more frequent Develops rapid motor dexterity response capability Evidence of puberty indicators, particularly in girls | <ul style="list-style-type: none"> Thoughts and attention span are more focused Inductive reasoning Can relate experiences to specific occurrences Increase in vocabulary | <ul style="list-style-type: none"> Becomes more independent and more responsible Distinguishes between being successful and unsuccessful Is aware of own efforts vs. chance/luck in obtaining a given result Capacity to place oneself in another's position (empathy) |
| 12-18 years | <ul style="list-style-type: none"> Puberty Menstruation and fat tissue increase for girls Voice changes and an increase in muscle mass for boys Greater interest in sexuality | <ul style="list-style-type: none"> Can discuss effectively More self-conscious and focussed Development of hypothetical-deductive reasoning Can make subtle adjustments in speech Can make plans and take decisions | <ul style="list-style-type: none"> Increasing conflict with parents/family Closeness to peer group and emergence of peer pressure situations Search for one's own identity Development of intimate relationships |

Table - Annex: Approach and communication with children and young people of different age groups

| | 1-6 years | 6-12 years | 12-18 years |
|-----------------------------|--|---|--|
| Introduction | <p>Fundamentally directed at the child.</p> <p>The child is still too young to understand the information provided.</p> | <p>The child shows more interest in the information provided and greater ability to understand it.</p> | <p>The child/young person understands the information provided, but may show reluctance to participate in an intervention programme or a victim support process.</p> |
| Describing the event | <p>Expressed preferably through drawings or games, rather than verbal expression.</p> | <p>Able to communicate more details than younger children.</p> <p>Older children prefer to express themselves verbally, sometimes refusing to use drawings and games.</p> | <p>Describes the event in detail.</p> <p>There are feelings of self-culpability.</p> |
| Psychoeducation | <p>Fundamentally directed at family/parents.</p> <p>The child will assimilate simple information, such as acknowledging the situation, and they can simulate a way of dealing with it.</p> | <p>Aimed at the child, integrating the family/parents in the psycho-education process.</p> | <p>Directed to/through the child.</p> |

MOD. 9

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 9 - SPECIALISED SUPPORT TO VICTIMS OF CYBERBULLYING

INTRODUCTION

This Module is aimed at understanding the phenomenon of cyberbullying and intervening with its victims, in order to support overcoming the impacts of cyberbullying and preventing re-victimisation.

In addition to reading this Module's content, and similarly for previous modules of this Course, we also suggest that the trainer consults the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*.

Modi operandi and nature of the crime

Cyberbullying is an extension of bullying. While bullying involves 'face-to-face' aggression, in cyberbullying the aggression and the offence take place online, through the Internet and ICT.

Cyberbullying can take place by sharing aggressive or humiliating texts, photos and/or videos about someone, which impact on their identity and affect their self-esteem. The fact that cyberbullying is practiced over the Internet - on social networks and/or through messaging applications such as WhatsApp® - means that the aggressor does not have to confront the victim directly, feeling less inhibited at the time of the aggression, less afraid of being punished and therefore more powerful.

Cyberbullying can be practiced:

- one to one (only between victim and aggressor);
- one to many (for example, an aggressor posts something online that many people can see);
- many to many (when many aggressors share something that many people will be able to see).

Cyberbullying enables aggressors to act anonymously, often resorting to false identities (which allow them to dissociate themselves from the morality of their actions) and to thought processes justifying their conduct, such as:

- Blurring or minimising their role by 'displacing' or diluting their responsibility;
- Distorting or downplaying the impact of their behaviour;
- Blaming and dehumanizing the victim.

Common forms of violence in cyberbullying are:

- Flaming - online discussions, using vulgar and angry language in electronic messages;
- Harassment - repeatedly sending inappropriate, hostile and insulting messages;
- Impersonation - impersonating another person and sending/publishing material or content aiming at damaging this person's reputation or friendships;
- Outing - sharing online personal or embarrassing information or images of another person without their consent;
- Trickery - persuade someone to reveal personal/confidential or embarrassing information and then share it online;
- Exclusion - intentionally and cruelly excluding someone from an online group;
- Cyberstalking - repeated and intense harassment, which includes threats or generates significant fear;
- Happy slapping - face-to-face assaults committed by one or more persons against the victim, which are recorded and later shared on social networks.

There are also practices of cyberbullying with a sexual component, aiming at attacking the victim's dignity and private life, such as:

- Sharing online rumours or lies about the victim's sexual behaviour;
- Using offensive or discriminatory sexual language against the victim online;
- Stealing the victim's identity and subsequently sharing sexual content involving the victim or sexually harassing others;
- Using threats and intimidation on grounds of gender identity or sexual orientation of the victim;
- Body shamming - sharing derisive comments on the victim's physical appearance.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 9 - SPECIALISED SUPPORT TO VICTIMS OF CYBERBULLYING

Prevention strategies

To **prevent cyberbullying**, at this point in the Module, the trainer should provide the course participants with information about the following strategies which they, as victim support officers/professionals (VSO), can use in their intervention with the victim:

- Stopping all communications with the aggressor;
- Not blocking or disabling the social network/communications platform used by the aggressor to communicate with the victim, since platforms such as WhatsApp® or Viber® use end-to-end encryption (See Module 8);
- Not providing personal information or personal data requested through emails, messages, calls, unsolicited websites;
- Configuring the privacy settings of social networks and pages/profiles by deleting personal or other information that can identify the victim's home address, school, mobile phone number, etc;
- Activating spam and harassment filters;
- Recording important phone contacts on their mobile phone so the victim can easily ask for help if they need;
- Recording also contacts from community support resources and services that can help overcoming/recovering from victimisation;
- Finding alternative routes to usual places;
- Sharing the situation and usual routines with trusted adults;
- Trying to walk in the company of trusted people and avoid walking alone;
- Preparing the victim for the eventuality of being face to face with the online aggressor: the victim should react without violence and with serenity, seeking help as quickly as possible or people who are close by;
- Preparing the victim to act in a situation of danger: the victim should look for a safe place or somewhere busy with other people. Emergency contacts can also be activated.

Intervention strategies

Strategies for preserving digital evidence

In addition to covering the dynamics and modi operandi in cyberbullying situations and presenting re-victimisation prevention measures, the trainer should also cover strategies for preserving evidence that can be explained to the victim in their supporting process. Let's look at some of the strategies the victim should adopt:

- Once communications with the aggressor have ceased, the victim should not block or disable the social network or communication platform used by the aggressor to communicate with the victim;
- Save all communications with the aggressor (e.g. taking screenshots), including images and/or videos sent and received;
- Save all the information that allows identifying the aggressor, such as: username, social network profile's URL (see intervention strategies in Module 10), Skype® ID, etc;
- File criminal complaints with the competent authorities;
- Request support from victim support entities to deal with the emotional suffering caused by the victimisation situation and ensure follow-up throughout the criminal process.

To whom and how to report

Under Portuguese Law, minors under 12 years of age cannot be charged with a crime. So, when cyber-bullying is conducted by someone aged under 12 years, it may trigger **Promotion and Protection measures**, in accordance with the Law for the Protection of Children and Young People in Danger (Lei de Proteção de Crianças e Jovens em Perigo - Lei n.º 147/99, of 1st of September). Disciplinary measures can also be applied by schools when they become aware of cyberbullying situations.

Between the ages of 12 and 16, in Portugal cyberbullying practices can be punished by the **Educational Guardianship Law (Lei Tutelar Educativa)** when the conduct constitutes a crime:

- The practice by a minor, between the ages of 12 and 16, of an action qualified by law as a crime gives rise to the

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 9 - SPECIALISED SUPPORT TO VICTIMS OF CYBERBULLYING

application of a protective educational measure, in accordance with the provisions of this law.

According to Article 19 of the Portuguese Penal Code, after 16 years of age, any type of violence that constitutes a crime is punished in accordance with the Portuguese criminal law.

In any case, cyberbullying situations should be reported to the entities with competence to punish them:

- School (headteacher, school governors and school network directorate and, if the response from these bodies fails, the situation should be reported to the Direção de Serviço de Segurança Escolar (School Safety Service Directorate), in the case of Portugal);
- Criminal Police Bodies (through the agents or officers responsible for the Programa Escola Segura (Safe School Programme), in Portugal);
- Comissão de Proteção de Crianças e Jovens (Commission for the Protection of Children and Young People);
- Ministério Público (Public Prosecutor's Office).

Strategies to overcome victimisation and its impacts

Following the key aspects of interventions with cybercrime victims explored in Module 4 and the **prevention and intervention strategies** already outlined, it is the support professional's (VSO) responsibility to provide the victim with a set of practical guidelines. The professional should take into account the cautions regarding **communication with children and young people** of different age groups addressed in Module 8.

Furthermore, when structuring the care and support to the victim of cyberbullying, the professional should also consider the **impact of the cyberbullying experience** and the consequences felt by the victim – see Module 3 of this Training Course, as well as Chapter 4 - Part I of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*.

In addition to the reactions and consequences addressed in those resources, in the specific case of bullying against children and young people, regardless of whether it is a situation of cyberbullying or conventional bullying, there are other consequences that can be experienced by the victims being supported and that we should highlight:

- The child or young person may be afraid to go to school and do everything to avoid going (e.g. pretending to be sick);
- Drop in school performance;
- Distancing or isolating themselves from friends and other people they liked to socialise with;
- Loss of interest in previously enjoyed activities;
- Physical symptoms and health problems: difficulty falling asleep; frequent nightmares; stomach aches, sickness or dizziness (e.g. when they think they have to go to school or when they enter school); headaches; sweating, rapid heartbeat (e.g. when they think they have to go to school or when they enter school).

To address these situations, the trainer can present the following **support strategies**:

- Standardise the reactions presented;
- Provide information on the crime prevalence in the victim's age group in order to challenge the idea of 'unique vulnerability' and any resulting feelings of loneliness and misunderstanding;
- Make it very clear that the victim is not to blame for what is happening to them and that the blame and responsibility lies exclusively with the aggressor;
- Encourage involvement in previously enjoyed activities, including offline activities;
- If the victim wishes and with their permission, involve family and/or friends in the recovery process;
- Provide support throughout the process, including psychological support;
- Reinforce the prevention strategies addressed above.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 9 - SPECIALISED SUPPORT TO VICTIMS OF CYBERBULLYING

Specialised Support to Victims of Cybercrime

PART II – SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

Module 9 – Specialised support to victims of cyberbullying



Module 9 – Specialised support to victims of cyberbullying

a. Modi operandi and nature of the crime

Cyberbullying is an extension of bullying, but the aggression and the offence take place online, through the Internet and ICT.

Cyberbullying can take place by sharing aggressive or humiliating texts, photos and/or videos about someone, which impact on their identity and affect their self-esteem. The fact that cyberbullying is practiced over the Internet - on social networks and/or through messaging applications such as WhatsApp® - means that the aggressor does not have to confront the victim directly, feeling less inhibited at the time of the assault, less afraid of being punished and therefore more powerful.



Module 9 – Specialised support to victims of cyberbullying

a. Modi operandi and nature of the crime

Cyberbullying can be practiced:

- one to one (only between victim and aggressor);
- one to many (for example, an aggressor posts something online that many people can see);
- many to many (when many aggressors share something that many people will be able to see).

Cyberbullying enables aggressors to act anonymously, often resorting to false identities (which allow them to dissociate themselves from the morality of their actions) and to thought processes justifying their conduct, such as:

- Blurring or minimising their role by 'displacing' or diluting their responsibility;
- Distorting or downplaying the impact of their behaviour;
- Blaming and dehumanizing the victim.



Module 9 – Specialised support to victims of cyberbullying

a. Modi operandi and nature of the crime

Common forms of violence in cyberbullying are:

- Flaming - online discussions, using vulgar and angry language in electronic messages;
- Harassment - repeatedly sending inappropriate, hostile and insulting messages;
- Impersonation - impersonating another person and sending/publishing material or content aiming at damaging this person's reputation or friendships;
- Outing - sharing online personal or embarrassing information or images of another person without their consent;
- Trickery - persuade someone to reveal personal/confidential or embarrassing information and then share it online;
- Exclusion - intentionally and cruelly excluding someone from an online group;
- Cyberstalking - repeated and intense harassment, which includes threats or generates significant fear;
- Happy slapping - face-to-face assaults committed by one or more



Module 9 – Specialised support to victims of cyberbullying

a. Modi operandi and nature of the crime

There are also practices of cyberbullying with a sexual component, aiming at attacking the victim's dignity and private life, such as:

- Sharing online rumours or lies about the victim's sexual behaviour;
- Using offensive or discriminatory sexual language against the victim online;
- Stealing the victim's identity and subsequently sharing sexual content involving the victim or sexually harassing others;
- Using threats and intimidation on grounds of gender identity or sexual orientation of the victim;
- Body shaming - sharing derisive comments on the victim's physical appearance.



Module 9 – Specialised support to victims of cyberbullying

b. Prevention strategies

To prevent cyberbullying situations, the support professional (VSO) should ask the victim to:

- Stop all communications with the aggressor;
- Do not block or disable the social network/communications platform used by the aggressor to communicate with the victim, since platforms such as WhatsApp® or Viber® use end-to-end encryption (See Module 8);
- Do not provide personal information or personal data requested through emails, messages, calls, unsolicited websites;
- Configure the privacy settings of social networks and pages/profiles by deleting personal or other information that can identify the victim's home address, school, mobile phone number, etc;
- Activate spam and harassment filters;



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 9 - SPECIALISED SUPPORT TO VICTIMS OF CYBERBULLYING

Module 9 – Specialised support to victims of cyberbullying

b. Prevention strategies

To prevent cyberbullying situations, the support professional (VSO) should ask the victim to:

- Record important phone contacts on their mobile phone so the victim can easily ask for help if they need;
- Record also contacts from community support resources and services that can help overcoming/recovering from victimisation;
- Find alternative routes to usual places;
- Share the situation and usual routines with trusted adults;
- Try to walk in the company of trusted people and avoid walking alone;
- If the victim is confronted face to face with the online aggressor, the victim should react without violence and with serenity, seeking help as quickly as possible or people who are close by;
- In a situation of danger, the victim should look for a safe place or somewhere busy with other people. Emergency contacts can also be activated.



Module 9 – Specialised support to victims of cyberbullying

c. Intervention strategies

i. Preserving digital evidence

- Once communications with the aggressor have ceased, the victim should not block or disable the social network or communication platform used by the aggressor to communicate with the victim;
- Save all communications with the abuser (e.g. taking screenshots), including images and/or videos sent and received;
- Save all the information that allows identifying the aggressor, such as: user name, social network profile's URL (see *intervention strategies in Module 10*), Skype® ID, etc;
- File criminal complaints with the competent authorities;
- Request support from victim support entities to deal with the emotional suffering caused by the victimisation situation and ensure follow-up throughout the criminal process



Module 9 – Specialised support to victims of cyberbullying

c. Intervention strategies

ii. To whom and how to report

Under Portuguese Law, minors under 12 years of age cannot be charged with a crime. So, when cyberbullying is conducted by someone aged under 12 years, it may trigger **Promotion and Protection measures**, in accordance with the **Law protecting Children and Young People in Danger** (Lei de Proteção de Crianças e Jovens em Perigo - Lei n.º 147/99, of 1st of September).

Disciplinary measures can also be applied by schools when they become aware of cyberbullying situations.

Between the ages of 12 and 16, in Portugal cyberbullying practices can be punished by the **Educational Guardianship Law (Lei Tutelar Educativa)** when the conduct constitutes a crime:

"The practice by a minor between the ages of 12 and 16 of an action qualified by law as a crime gives rise to the application of a protective educational measure, in accordance with the provisions of this law."



Module 9 – Specialised support to victims of cyberbullying

c. Intervention strategies

ii. To whom and how to report

Article 19 of the Portuguese Penal Code, after 16 years of age, any type of violence that constitutes a crime is punished in accordance with the Portuguese criminal law.

In any case, cyberbullying situations should be reported to the entities with competence to punish them:

- School (head teacher, school governors and school network directorate and, if the response from these bodies fails, the situation should be reported to the Direção de Serviço de Segurança Escolar (School Safety Service Directorate), in the case of Portugal);
- Criminal Police Bodies (through the agents or officers responsible for the Programa Escola Segura, Safe School Programme, in Portugal);
- Comissão de Proteção de Crianças e Jovens (Commission for the Protection of Children and Young People);
- Ministério Público (Public Prosecutor's Office).



Module 9 – Specialised support to victims of cyberbullying

c. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

Support strategies:

- Standardise the reactions presented;
- Provide information on the crime prevalence in the victim's age group in order to challenge the idea of 'unique vulnerability' and any resulting feelings of loneliness and misunderstanding;
- Make it very clear that the victim is not to blame for what is happening to them and that the blame and responsibility lies exclusively with the aggressor;
- Encourage involvement in previously enjoyed activities, including offline activities;
- If it the victim wishes and with their permission, involve family and/or friends in the recovery process;
- Provide support throughout the process, including psychological support;
- Reinforce the prevention strategies addressed above.



Common Cyberbullying situations

"Cyber-bullying Facts – Top 10 Forms of Cyber Bullying" (2016)

https://www.youtube.com/watch?time_continue=186&v=0x08N5qJtsk&feature=emb_logo



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 9 - SPECIALISED SUPPORT TO VICTIMS OF CYBERBULLYING

Common Cyberbullying situations

Activity



Fonte: [BBC News](#)



Fonte: [Psychology Today](#)

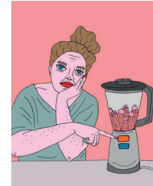


Common Cyberbullying situations

Activity



Fonte: [Vice](#)



Fonte: [Stock Market](#)



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 9 - SPECIALISED SUPPORT TO VICTIMS OF CYBERBULLYING

SESSION PLAN 9

1. Training

Training Title Training Course Specialised Support to Victims of Cybercrime

Modules/Topics Specialised support for victims of cyberbullying

Date of Session **Time** **Total Duration** 40 minutes

Trainers

2. Specific Objectives

At the end of the session, the participants should be able to:

- Distinguish correctly the nature and modi operandi of cyberbullying;
- List correctly the proposed intervention strategies for specialised support to victims of cyberbullying;
- Recognize correctly re-victimisation prevention strategies for intervention with victims of cyberbullying.

3. Session Plan

| | Content | Methods | Resources | Assessment Activities | Duration (minutes) |
|--------------|--|-----------------------|--|-------------------------|--------------------|
| Introduction | Modi operandi and nature of the crime | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| | Prevention strategies | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| Development | Intervention strategies: <ul style="list-style-type: none"> • Strategies for preserving digital evidence • To whom and how to report • Strategies to overcome victimisation and its impacts | Expository and active | Computer: Datashow and projection screen | Observation | 15 |
| | Activity 5 | Active | Guidance for Activity 5 and Case of Activity 5 | Observation | 10 |
| Conclusion | Concluding summary and clarification of issues | Expository and active | Computer: Datashow and projection screen | Observation | 5 |

OBSERVATIONS

Participants:

Victim Support Officers (VSO)

Date: / /

Trainer:

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 9 - SPECIALISED SUPPORT TO VICTIMS OF CYBERBULLYING

INSTRUCTIONS AND KEY INFORMATION FOR THE TRAINER

CONTENT MATCHING

| | | |
|--|--|------------------|
| Session Plan | <i>ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims</i> | |
| | PART | CHAPTER |
| Modi operandi and nature of the crime | No correspondence | |
| | See Module Introduction | |
| Prevention strategies | No correspondence | |
| | See Module Introduction | |
| Intervention strategies | | |
| Strategies for preserving digital evidence | No correspondence | |
| | See Module Introduction | |
| To whom and how to report | No correspondence | |
| | See Module Introduction | |
| Strategies to overcome victimisation and its impacts | Part II - Proceeding | Chapter 2 - 2.1. |
| | VSee Module Introduction | |
| Activity 5 | No correspondence | |
| | See Guidance for Activity 5 | |
| Concluding summary and clarification of issues | No correspondence | |

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 9 - SPECIALISED SUPPORT TO VICTIMS OF CYBERBULLYING

GUIDANCE FOR ACTIVITY 5

| Module/Topic | Specialised support to victims of cyberbullying | REF. CODE | EDUCATION AND TRAINING AREA |
|--------------|---|-----------|-----------------------------|
| Objectives | This activity aims to consolidate the information and programme content of this Module by addressing the nature of cyberbullying situations, as well as the intervention strategies that should be activated by VSOs when supporting victims of cyberbullying. | | |
| Delivery | <p>The trainer should hand out Activity 5 Case for Discussion to allow participants to read it individually.</p> <p>After reading, the trainer should ask the group about the forms of aggression/violence present in the case.</p> <p>During the group's participation, the trainer should highlight or reinforce, according to the participants' opinions and information shared, the aggressions in the cyberbullying situation presented: exclusion, rumour sharing and verbal aggression. In this specific case, it is important that the trainer also highlights the potential for the cyberbullying situation to co-occur with conventional bullying situations in relation to the victim [João] as the victim and the aggressor have a close relationship [i.e. they are classmates]. The possibility of online aggression situations being accompanied by offline violence [i.e. face-to-face] should be considered when defining the intervention and the strategies to prevent re-victimisation.</p> <p>Following group reflection on the bullying and cyberbullying dynamics in the case, the trainer can ask two or more participants to simulate a support session:</p> <ul style="list-style-type: none">• one of the participants should play João's role [the victim in this case], using the case description to explain, in their own words, the situation of violence experienced;• The other participant should play the role of the support professional/VSO. <p>In this simulation, it is especially important that the trainer is attentive to the participant who plays the VSO role. The supporting strategies under the heading Intervention Strategies in the Module Introduction section should be highlighted. The re-victimisation Prevention Strategies also addressed in the Module Introduction should also be explored.</p> <p>The trainer can also promote the other participants' engagement by asking for suggestions of strategies to be considered and other relevant aspects to be considered in the simulation of the support session:</p> <ul style="list-style-type: none">• providing emotional support;• collecting information;• assessing risk and defining protection measures;• identifying support needs. <p>The aim here is to articulate this Module's objectives with the programme content already covered in Module 4, namely with the central aspects of specialised support to victims of cybercrime.</p> | | |
| Notes | See Module Introduction | | |

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 9 - SPECIALISED SUPPORT TO VICTIMS OF CYBERBULLYING

ACTIVITY 5: CASE FOR DISCUSSION

João is 12 years old. His favourite activity in the last 5 months has been playing an online game. This game was played as a group and João belonged to the group created by Rui, his best childhood friend. In this group there were also other classmates, with whom João and Rui played. In the last school term, Rui had very bad grades and his parents compared him to João, saying: "You should be like João. He's a proper student!". Rui was very angry and jealous of João. Not being able to deal with his emotions, he took them out on João: he excluded him from the group and aggressively insulted him: "You suck! You don't know how to play; you just slow us all down! You're a pain in the ass! Go and study, you four-eyed nerd!"

In addition, Rui spread the rumour in the group chat that João had 'complained' to Rui's parents, saying that Rui was missing classes to play.

The colleagues took Rui's side, as they were afraid of him. Rui is two years older than the other colleagues and is taller and stronger.

MOD. 10

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

INTRODUCTION

One in three people have online relationships⁴². In this context, one in ten people mentions having already shared intimate photos of themselves.

In addition, it is believed that 55% of people who have online relationships have been victims of some form of crime⁴³.

This Module presents two phenomena of cybervictimisation associated with the risks of online presence and the use of ICT and the Internet for establishing more intimate interpersonal relationships: cyberstalking and non-consensual sharing of images.

Types, modi operandi and nature of the crime

Cyberstalking

Cyberstalking can be defined as the use of ICT to threaten or harass a victim. Similarly to stalking, cyberstalking is a type of violence characterised by its intrusive and repetitive nature in the victim's private life sphere, causing fear and insecurity. Consequently, victims experience a continuous state of anxiety that affects their quality of life, and, in extreme situations, forcing them to change their daily routines.

The fact that this persecution takes place online allows the offender(s) to have at their disposal several means to maintain their criminal activity, as well as to attack a higher number of victims. The offender may be someone the victim knows or other people close to them, such as friends or ex-partners, but also people the victim does not know.

The most common forms of cyberstalking are:

- Harassment of the victim;
- Identity theft;
- Threats;
- Unwanted sexual contact - e.g. sending, without consent, dick pics (images of male genital organs sent/received through electronic devices) by the aggressor, as a way of disturbing the victim;
- Persistent and unwanted contacts.

Non-consensual image sharing

In intimate relationships, there may be online sharing of sexual messages, videos or images, a behaviour known as **sexting** (resulting from the combination of the words 'sex' and 'texting'), which involves the exchange of erotic messages, with or without photos, via mobile phones, chats or social networks.

The consensual practice of sexting within an intimate relationship can be healthy. It may also, however, increase the vulnerability of those involved in **non-consensual image sharing**.

Non-consensual sharing of images and videos can be defined by the disclosure of an intimate image, without someone's consent who sees their image being shared, when they expected this image to be kept confidential. An intimate image is one in which a person is naked, or exposing their breasts, genital organs or anal region, or is involved in sexual activity. It can be any visual recording, including a photograph, film or video recording.

Motivations for disseminating these images and videos can be:

⁴² See <https://www.kaspersky.com/blog/online-dating-report/>.

⁴³ *Idem*.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

- **Extortion or coercing the victim:** the perpetrator of the crime, after receiving sexual videos or photographs from the victim, with their consent, threatens disseminating them if the victim does not provide new sexual self-produced content or does not agree meeting the aggressor face-to-face;
- **Revenge:** this practice is also commonly referred to as **revenge porn** and involves the non-consensual disclosure of intimate images by one of the partners, usually at the end of a relationship. It is a common phenomenon in situations of violence in intimate relationships, including domestic violence, where, at the end of the relationship, one of the partners threatens to disclose or discloses images and/or videos of their ex-partner to family and friends, social networks or even pornographic websites, as a form of retaliation for the ex-partner having ended the relationship.

Prevention strategies

In order to **prevent cyberstalking situations and non-consensual sharing of images**, at this point of the Module, the trainer should present the following strategies to the course participants, which they, as victim support officers/professionals (VSO), can use in the intervention with the victim and their family:

- Stopping all communication with the aggressor;
- Not blocking or disabling the social network/communications platform that the abuser used to communicate with the victim, since platforms such as WhatsApp® or Viber® use end-to-end encryption (See Module 8);
- Not providing personal information or personal data requested through emails, messages, calls, unsolicited websites;
- Configuring the privacy and security settings of profiles/accounts on social networks and other platforms, deleting personal or other information that could identify the home address, school/work, mobile phone number, etc;
- Activating spam and harassment filters;
- Raising awareness of the risks associated with the use of the internet and ICTs in relationships and explain how communication platforms work and how they can be used safely. With young adults and adults, it is important to address safe sexting issues, including the use of platforms that use end-to-end encryption and that have the option of not allowing images or videos to be recorded on the recipient's mobile phone;
- Editing the images/videos, namely of an intimate nature, before sharing/disseminating them, in order to protect one's identity, removing personal identification elements, such as the face, signs and/or tattoos, as well as the image georeferencing;

Intervention strategies

Strategies for preserving digital evidence

In this Module, the trainer should also present strategies for the preservation of the evidence that can be explained to the victim during the supporting process. This section of the Module explores some of the difficulties associated with preserving evidence and that arise from the characteristics of the communication platforms used (end-to-end encryption).

Let's look at some of them.

Cyberstalking and non-consensual sharing / dissemination of images occur commonly on online social networks or chat platforms, where much of the crime evidence can be found.

- The most effective method of preserving evidence in social networks is to **take screenshots** of the content to be reported. However, it is essential that the **URL** (Uniform Resource Locator) of the respective content is visible in these screenshots.
- Through the URL, even if the content is no longer available on the platform, the authorities can ask companies to provide information on who published the content.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

These preservation strategies are presented using specific examples from social networks:

- It is possible to **identify a specific URL** for a Facebook® **post or comment**:
 - Click on the time or date when the publication took place or when the comment was published;
 - By clicking on the time or date, a new window opens up in the internet browser. In this window, the URL corresponding to the publication or comment is visible. This URL must be copied/saved and shared with the authorities.

The problem of chat platforms using End-to-End encryption (E2E encryption)

In **end-to-end encryption** only the receiver and sender can see the message decrypted, which means that, if the content of the conversation is deleted, the authorities have no way of requesting the record of the conversations from the entities providing the service. These communication platforms - such as WhatsApp® - are then advantageous for potential perpetrators of this type of cybercrime.

In these cases, the need for **screen captures** as a way to preserve evidence is particularly important.

It is also important to define **automatic storage (backups)** mechanisms in the application settings in order to have access to the information, even if it is deleted by one of the interlocutors.

To whom and how to report

The types of violence described - cyberstalking and non-consensual sharing of images – can fall under different crimes in the Portuguese Penal Code, namely **privacy intrusion** (articles 192 and 197) and **illicit recording and photography** (article 199).

In the context of intimate relations within the crime of **domestic violence**, Article 152(2)(b) of the Portuguese Penal Code was introduced by Law no. 44/2018, which aimed precisely at providing protection to the victim's intimacy (namely sexuality) personal data (namely image or sound, which includes videos, films and photos) and to the victim's privacy (private sensitive data), when they are disseminated through the internet or other widespread public dissemination means (such as social networks), without the consent of the victim.

This special qualification or aggravated domestic violence crime is aimed at fighting cyberstalking in the context of domestic violence. It comprises conduct consisting of "sending offensive or threatening emails, text messages and instant messages, posting offensive comments about the victim on the internet, sharing intimate photographs or videos of the victim via the internet" and which are experienced as "more intrusive by the victims" and "cause more adverse psychological effects".

Such conduct can be reported to any criminal police or public prosecutor..

Strategies to overcome victimisation and its impacts

Following the key aspects for intervention with cybercrime victims covered in Module 4 and the prevention and intervention strategies already outlined, it is the support professional's (VSO) responsibility to provide the victim with a set of practical guidelines.

The support professional (VSO), when structuring the victim's care and support, should also take into consideration the **impact of the cybervictimisation experience** and the consequences felt by the victim – see Module 3 of this Training Course, as well as Chapter 4 - Part I of the *ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims*.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

Using the Cases in the proposed Activity (See Session Plan), the trainer will have opportunity to explore the dynamics associated with each form of cybervictimisation, as well as the consequences and key strategies that should be used in the intervention process.

In the case of **cyberstalking**, the trainer should present a set of strategies that the course participants can use in their support and intervention with the victim. Let's look at the safety strategies that the victim can use:

- Avoiding contacting and/or confronting the perpetrator of the cyberstalking behaviour;
- Not responding to any contact attempt made by the perpetrator of the cyberstalking behaviours and keep copies of these contact attempts/messages;
- Saving all letters, emails, text messages, tickets, gifts and/or other materials sent to them by the stalker;
- Informing people close to them - family and friends, work/school/gym colleagues, neighbours - of the cybervictimisation situation, so that under no circumstances will they provide information to the stalker;
- Using alternative routes to travel instead of the usual ones;
- Asking someone they trust to accompany them to the car or to the public transport they normally use;
- When travelling by car, keeping the doors locked during the journey; ensuring a safe distance from the vehicle in front in case there is a need to change lanes or route;
- Recording any suspicious incidents, creating a detailed record of the behaviour they have been subjected to;
- In a situation of danger, seeking a safe place or a busy place with people. They can also use their emergency contacts.

Let us also look at other support strategies that the professional can use:

- Explaining and reinforcing that it is not the victim's fault, it is the perpetrator of the behaviour who is to blame;
- Conveying the idea that the victim has the right to say no;
- Conveying the idea that the aggressor can make use of manipulative/blackmail strategies: to make the victim feel guilty, in order to get them to do something that they want;
- Explaining to the victim how to proceed in order to preserve the digital evidence (see information above);
- Providing safety strategies and emergency contacts;
- Informing the victim to whom and how to report;
- Providing prevention and intervention strategies to avoid new crimes (see above);
- Reinforcing the victim's resuming activities.

In the case of **non-consensual sharing of images**, the trainer should present to the course participants a set of strategies that they can use in their support and intervention with the victim:

- Validating and recognising their experience as cybervictimisation and frame the victim's reactions as an abnormal life experience;
- Reducing blame;
- Ensuring that the victim has understood that they should never give in to blackmail from the aggressor, as this will not stop the aggressor's behaviour;
- Communicating the prevention and intervention strategies outlined above in a simple, concise and clear way;
- Providing support, including psychological support;
- Considering the possibility of coordination with a psychiatry service, if there is suicidal ideation.

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

Specialised Support to Victims of Cybercrime

PART II – SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME

Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

a. Modi operandi and nature of the crime

Cyberstalking

Cyberstalking can be defined as the use of ICT to threaten or harass a victim. Similarly to stalking, cyberstalking is a type of violence characterised by its intrusive and repetitive nature in the victim's private life sphere, causing fear and insecurity. Consequently, victims experience a continuous state of anxiety that affects their quality of life, and, in extreme situations, forcing them to change their daily routines.

The fact that this persecution takes place online allows the offender(s) to have at their disposal several means to maintain their criminal activity, as well as to attack a higher number of victims.

The offender may be someone the victim knows or other people close to them, such as friends or ex-partners, but also people the victim does not know.



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

a. Modi operandi and nature of the crime

Cyberstalking

The most common forms are :

- Harassment of the victim;
- Identity theft;
- Threats;
- Unwanted sexual contact - e.g. sending, without consent, dick pics (images of male genital organs sent/received through electronic devices) by the aggressor, as a way of disturbing the victim;
- Persistent and unwanted contacts.



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

a. Modi operandi and nature of the crime

Non-consensual image sharing

Non-consensual sharing of images and videos can be defined by the disclosure of an intimate image, without someone's consent who sees their image being shared, when they expected this image to be kept confidential.

An intimate image is one in which a person is naked, or exposing his breasts, genital organs or anal region, or is involved in sexual activity. It can be any visual recording, including a photograph, film or video recording.



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

a. Modi operandi and nature of the crime

Non-consensual image sharing

Sexting, covered in Module 6 in the section on scams in intimate relationships, and focussing now particularly on the *Risks of Online Relationships*, can increase the vulnerability of those involved in non-consensual image sharing.

Motivations for disseminating these images and videos can be :

- Extortion or coercion of the victim
- Revenge



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

Non-Consensual Sharing of Images and Videos

There is a range of situations where these images can be shared or obtained without the victims' consent. Three of these situations are:

- ➔ Sextortion
- ➔ Non-consensual sharing of images (Revenge Porn)
- ➔ Grooming



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

Sextortion

One of the worst consequences of Sexting is Sextortion, a form of coercion in which the perpetrator, after consensually receiving videos or photographs of a sexual nature from the victim, threatens to disseminate them if the victim does not provide them with more photos or videos, money, or do not agree to meet face-to-face.



Amanda Todd, Toronto www.bbc.com/news/technology-2012-10

An example of one of these situations is the tragic suicide of Amanda Todd in 2012, when she was 15 years old. This was facilitated by Amanda being victimised by a person she had met in an internet chat. After she had shared a topless photo, she was coerced by this person to share more sexual content under threat of disclosure of this photo to her family and friends.



Revenge Porn



Another phenomenon associated with Online relationships is the non-consensual disclosure of intimate images by one of the partners, usually at the end of a relationship (often wrongly designated by **Revenge Porn** as it puts the blame on the victim). It is a common in situations of domestic violence, where, at the end of the relationship, one of the partners discloses images and/or videos of their ex-partner to the victim's family and friends, social networks or even pornographic websites, as a form of retaliation for the ex-partner having ended the relationship.



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

b. Prevention strategies

- Stopping all communication with the aggressor;
- Not blocking or disabling the social network/communications platform that the abuser used to communicate with the victim, since platforms such as WhatsApp® or Viber® use end-to-end encryption (See Module 8);
- Not providing personal information or personal data requested through emails, messages, calls, unsolicited websites;
- Configuring the privacy and security settings of profiles/accounts on social networks and other platforms, deleting personal or other information that could identify the home address, school/work, mobile phone number, etc;
- Activating spam and harassment filters;



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

b. Prevention strategies

- Raising awareness of the risks associated with the use of the internet and ICTs in relationships and explain how communication platforms work and how they can be used safely. With young adults and adults, it is important to address safe sexting issues, including the use of platforms that use end-to-end encryption and that have the option of not allowing images or videos to be recorded on the recipient's mobile phone;
- Editing the images/videos, namely of an intimate nature, before sharing/disseminating them, in order to protect one's identity, removing personal identification elements, such as the face, signs and/or tattoos, as well as the image georeferencing;
- Configuring privacy and security settings of profiles/accounts on social networks and other platforms.



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

c. Intervention strategies

i. Preserving digital evidence

Preserving evidence in social networks

Many Cybercrime situations occur in social networks and include Cyberbullying, identity theft, fraud. Therefore, it is important that both victims and victim support entities know how to preserve the evidence of these crimes.

The most effective method of preserving evidence in social networks is to **take screenshots** of the content to be reported. However, often this is not sufficient, and it is essential that the **URL** (Uniform Resource Locator) of the respective content is visible in these screenshots, including the screenshot's date and time.

Through the URL, even if the content is no longer available on the platform, the authorities can ask companies to provide information on who published the content.



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

c. Intervention strategies

Safeguarding evidence in social networks

The example of Facebook

A Facebook® profile may contain content that violates their community standards, but this content may refer to a particular post rather than the entire profile. Therefore, in order to safeguard the evidence and enabling the authorities to investigate, it is possible to identify the specific post's URL, following the instructions below:

1. Click on the post's time or date of publication:



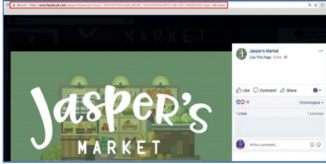
PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

c. Intervention strategies
Preserving evidence in social networks

The example of Facebook



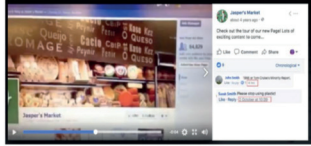
2. Clicking on the time or date of publication opens up a new window in the internet browser. You must copy the URL of this new window as it corresponds to this specific publication. It is this URL that must be shared with the authorities.

ROAR
EUROPEAN UNION
APAV
Associação Portuguesa de Apoio à Vítima

Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

c. Intervention strategies
Preserving evidence in social networks

Preserving Comments in Social Networks



As already mentioned, it is extremely important to report the specific URL of the content to be reported. To report a comment on a publication, you should follow the next steps:


ROAR
EUROPEAN UNION
APAV
Associação Portuguesa de Apoio à Vítima

Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images


c. Intervention strategies
Preserving evidence in social networks

Preserving Comments in Social Networks

1. Click on the time or date when the comment was published.



2. This opens up a new window. You should copy this URL and keep it as evidence.



ROAR
EUROPEAN UNION
APAV
Associação Portuguesa de Apoio à Vítima

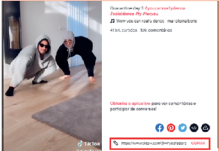
Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

c. Intervention strategies
Preserving evidence in social networks

Preserving evidence in other Social Networks

The procedure explained for Facebook can be applied to other social networks such as Instagram, for example.

In the social network TikTok, this process is quite easy as it makes available the URL for each shared video.



ROAR
EUROPEAN UNION
APAV
Associação Portuguesa de Apoio à Vítima

Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

The problem of chat platforms using End-to-End encryption (E2E encryption)

Many criminals try to persuade victims to use platforms with encryption technologies that prevent the service providers to have access to the messages.

In end-to-end encryption only the receiver and sender can see the message decrypted, which means that, if the content of the conversation is deleted, the authorities have no way of requesting the record of the conversations from the entities providing the service.

WhatsApp
Telegram
Signal
ROAR
EUROPEAN UNION
APAV
Associação Portuguesa de Apoio à Vítima

Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

The Problem of Chat Platforms Using End-to-End Encryption (E2E encryption)

In these cases, the need for screen captures as a way to preserve evidence is particularly important, as it is often the only way to prove the crime if the conversations are deleted.

It is also important to define automatic storage (backups) mechanisms in the application settings in order to have access to the information, even if it is deleted by one of the interlocutors.

WhatsApp
Telegram
Signal
ROAR
EUROPEAN UNION
APAV
Associação Portuguesa de Apoio à Vítima

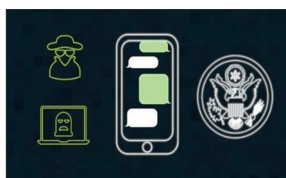
PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

Activity – Discussion

"How Encryption Works - and How It Can Be Bypassed" (2016)

<https://www.youtube.com/watch?v=1TmdsUjGv4>



Evidence Table:

Tool to help victims organising the evidence collected

| Date | What happened | Evidence about what happened | Who I suspect is the perpetrator | Evidence that they are the perpetrator | Evidence that I still need and who may have it |
|------------------|---|---|----------------------------------|---|---|
| 1-2 January 2020 | At 4pm I found intimate photos of me in the website – url:https://... | I saved these pages with intimates photos of me as a PDF in my computer | Ex-boyfriend/Ex-girlfriend | My ex-boyfriend/ex-girlfriend took these photos. He/she had threatened me with sharing these photos before. For example, (include details). I received a text message at 4pm saying "you are going to regret this". Screenshot of this message is saved in my computer. | We have a common friend (mention name) who received a message from the ex-boyfriend/ex-girlfriend that said that they were going to publish intimate photos of me. I'm waiting for this friend to send me these messages. |



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

Investigation Challenges:

- To prove that the accused is actually the person who posted the photos, and not a third party with whom the photos were shared;
- Victims are often unaware that the photos were shared outside the relationship;
- The use of smartphones makes it easier to take photos and videos without the victim's awareness;
- It is difficult to convince the victim, friends and family to save images and videos as evidence rather than deleting them.



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

b. Intervention strategies

ii. To whom and how to report

The types of violence described - cyberstalking and non-consensual sharing of images - can fall under different crimes in the Portuguese Penal Code, namely privacy intrusion (articles 192 and 197) and illicit recording and photography (article 159).

In the context of intimate relations within the crime of domestic violence, Article 152(2)(b) of the Portuguese Penal Code was introduced by Law no. 44/2018, which aimed precisely at providing protection to the victim's intimacy (namely sexuality) personal data (namely image or sound, which includes videos, films and photos) and to the victim's privacy (private sensitive data), when they are disseminated through the internet or other widespread public dissemination means (such as social networks), without the consent of the victim.

Such conduct can be reported to any criminal police or public prosecutor.



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

b. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

The non-consensual dissemination of intimate images and videos has strong impacts on victimization:

- A significant number of victims experience 'social disruption' – the victimization situation has such a strong impact that it drastically changes all aspects of the victims' lives.
- The threats are perceived as real and lead the victims to do whatever they are asked to do.
- Intense isolation from friends, family, online world and society in general.
- The victims report constant and continuous abuse by the aggressors.
- This type of situation has the potential to have a negative impact not only on the victims' lives but also on people close to them such as family and friends.



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

b. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

Strategies that the support professional (VSO) can use in situations of non-consensual sharing of images:

- Validating and recognising their experience as cybervictimisation and frame the victim's reactions as an abnormal life experience;
- Reducing blame;
- Ensuring that the victim has understood that they should never give in to blackmail from the aggressor - this will not stop the aggressor's behaviour;
- Communicating the prevention and intervention strategies outlined above in a simple, concise and clear way;
- Providing support, including psychological support;
- Considering the possibility of coordination with a psychiatry service, if there is suicidal ideation.



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

b. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

Strategies that the support professional (VSO) can use in cyberstalking situations:

- Explaining and reinforcing that it is not the victim's fault, it is the perpetrator of the behaviour who is to blame;
- Conveying the idea that the victim has the right to say no;
- Conveying the idea that the aggressor can make use of manipulative strategies: to make the victim feel guilty, in order to get them to do something that they want;
- Explaining to the victim how to proceed in order to preserve the digital evidence (see information above);
- Providing safety strategies and emergency contacts;
- Informing the victim to whom and how to report;
- Providing prevention and intervention strategies to avoid new crimes (see above);
- Reinforcing the victim's resuming activities.



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

b. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

Safety strategies that the cyberstalking victim can use:

- Avoiding contacting and/or confronting the perpetrator of the cyberstalking behaviour;
- Not responding to any contact attempt made by the perpetrator of the cyberstalking behaviours and keep copies of these contact attempts/messages;
- Saving all letters, emails, text messages, tickets, gifts and/or other materials sent to them by the stalker;
- Informing people close to them - family and friends, work/school/gym colleagues, neighbours - of the cyberstalking situation, so that under no circumstances will they provide information to the stalker;



Module 10 - Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images

b. Intervention strategies

iii. Strategies to overcome victimisation and its impacts

Safety strategies that the cyberstalking victim can use :

- Using alternative routes to travel instead of the usual ones;
- Asking someone they trust to accompany them to the car or to the public transport they normally use;
- When travelling by car, keeping the doors locked during the journey; ensuring a safe distance from the vehicle in front in case there is a need to change lanes or route;
- Recording any suspicious incidents, creating a detailed record of the behaviour they have been subjected to;
- In a situation of danger, seeking a safe place or a busy place with people. They can also use their emergency contacts.



Thank you



PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

SESSION PLAN 10

1. Training

| | | | |
|------------------------|--|-----------------------|------------|
| Training Title | Training Course Specialised Support to Victims of Cybercrime | | |
| Modules/Topics | Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual image sharing | | |
| Date of Session | Time | Total Duration | 40 minutes |
| Trainers | | | |

2. Specific Objectives

By the end of the session, the participants should be able to correctly:

- Distinguish the nature and modi operandi of online violence in interpersonal relationships, namely cyberstalking and non-consensual image sharing;
- List proposed intervention strategies for specialized support to victims of cyberstalking and victims of non-consensual image sharing;
- Recognise strategies to prevent re-victimisation proposed for intervention with victims of cyberstalking and victims of non-consensual sharing of images.

3. Session Plan

| | Content | Methods | Resources | Assessment Activities | Duration (minutes) |
|--------------|--|-----------------------|---|-------------------------|--------------------|
| Introduction | Types: <ul style="list-style-type: none"> • Cyberstalking • Non-consensual image sharing | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| | Modi operandi and nature of the crimes | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| Development | Prevention strategies | Expository and active | Computer: Datashow and projection screen | Observation | 5 |
| | Intervention strategies: <ul style="list-style-type: none"> • Strategies for preserving digital evidence • To whom and how to report • Strategies to overcome victimisation and its impacts | Expository and active | Computer: Datashow and projection screen | Observation | 10 |
| | Activity 6 | Active | Guidance for Activity 6 and Case A and Case B of Activity 6 | Observation | 10 |
| Conclusion | Concluding summary and clarification of issues | Expository and active | Computer: Datashow and projection screen | Observation | 5 |

OBSERVATIONS

Participants:

Victim Support Officers (VSO)

Date: / /

Trainer:

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

INSTRUCTIONS AND KEY INFORMATION FOR THE TRAINER

CONTENT MATCHING

| | | |
|--|--|------------------|
| Session Plan | <i>ROAR Manual - from understanding and preventing cybercrime to supporting and empowering victims</i> | |
| | PART | CHAPTER |
| Types, modi operandi and nature of the crimes | Part I - Understanding | Chapter 1 -1.3. |
| | No correspondence | |
| | See Module Introduction | |
| Prevention strategies | No correspondence | |
| | See Module Introduction | |
| Intervention strategies | | |
| Strategies for preserving digital evidence | No correspondence | |
| | See Module Introduction | |
| To whom and how to report | No correspondence | |
| | See Module Introduction | |
| Strategies to overcome victimisation and its impacts | Part II - Proceeding | Chapter 2 - 2.1. |
| | See Module Introduction | |
| Activity 6 | No correspondence | |
| | See Guidance for Activity 6 | |
| Concluding summary and clarification of issues | No correspondence | |

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

GUIDANCE FOR ACTIVITY 6

| Module/Topic | Specialised support to victims of online violence in interpersonal relationships: cyberstalking and non-consensual sharing of images | REF. CODE | EDUCATION AND TRAINING AREA |
|--------------|--|-----------|-----------------------------|
| Objectives | This activity aims to consolidate this Module's content, addressing the nature of situations of cyberstalking and non-consensual image sharing, as well as the intervention strategies to be activated by the VSO when supporting victims. | | |
| Delivery | <p>The trainer should divide the group of participants into 2 to 4 small groups. Half of the groups should be handed out Case A of Activity 6 and the remaining half should be handed out Case B of Activity 6.</p> <p>Case A portrays a cyberstalking situation and Case B a non-consensual image sharing situation (revenge porn).</p> <p>The trainer should ask each of the small groups to read carefully the respective case and define, as a group, the measures and strategies to be implemented to support each victim.</p> <p>Then, the trainer should ask the group(s) assigned to Case A to share their strategy suggestions. In the Case discussion the trainer should highlight the intervention strategies summarised in the Module Introduction.</p> <p>The trainer should repeat this procedure for discussing Case B.</p> | | |
| Notes | See Module Introduction | | |

PART 2 - SPECIALISED SUPPORT OF VICTIMS OF CYBERCRIME

MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES

ACTIVITY 6: CASE A FOR DISCUSSION

Matilde, 22 years old, university student.

One of Matilde's preferred hobbies is photography. Matilde used to spend hours taking pictures of landscapes she liked. She also used to spend a lot of time editing her photos.

One of Matilde's greatest pleasures was to check how successful her work was through the number of likes her Instagram® followers gave to her photographs published there. Therefore, her Instagram® account was 'open' and accepted all requests to be followed.

In the last 5 months ago, Matilde has been a victim of cyberstalking in social networks.

The aggressor, Carlos, approached her initially with a simple request to follow her, followed by an invitation to dinner. Matilde refused, claiming she was not interested in romantic relationships. Carlos questioned this refusal and asked Matilde why she despised him, why she rejected him. Matilde responded politely, claiming that she did not know him and therefore could not accept. Carlos' profile had no photos that could identify him.

Carlos told her that although she did not know him, he knew her well. He then began to create false profiles, using Matilde's personal data (e.g. address, date of birth, parents' address, brother's name) or threatening her (e.g. "I'll get you and you have no idea what I can do to you"; "I'll kill you, which is what you deserve"; "Nobody rejects me").

Hundreds of false profiles were created. In addition to reporting the case, Matilde was forced to delete her Instagram® profile, to move house and university. In addition to living in a state of continuous fear and insecurity, she no longer wants to take photographs.

In the first session, Matilde reports the following:

"The reason I come here is to make sure I'm doing the right things. I just want to make sure my attitude is the right one. I don't understand what I've done. Should I have said yes? Was I rude?"

ACTIVITY 6: CASE B FOR DISCUSSION

Maria, 43, shares the following in her first session:

"I was in a relationship for about 8 years. We lived together. He wasn't aggressive with me or anything like that, we got along. I just stopped liking him. I didn't feel fulfilled or happy in that relationship anymore. I ended it about 6 months ago.

Since then, he started threatening to send some photos of me, which I once stupidly sent him. They are intimate photos, in which I expose my body.

At first, it was just a request to get back together. I even understood, because I know he was desperate... I was very important to him. Moreover, he is a person who has few friends. Apart from being his wife, I was his great friend for all situations.

But after a month, the threats began to become more frequent, they increased and start to come every day. For a week now, he has been threatening to send my photos to all my friends, family and people at work.

I didn't give in. He is no longer the same person, it disgusted me! Today I woke up and he sent me a print screen first thing in the morning from an email he sent to my boss, all my work colleagues [there are 24 of us, he didn't miss anyone!], my parents, my brothers and my aunts. How can I leave the house again?

How? I can't go to work! I can't look my colleagues in the face! No one will ever take me seriously again [uncontrolled crying]. I should have given in, I should have given in... Or I should never have broken up with him, why did I break up with him? I don't want to live anymore... [uncontrolled crying]"



ROAR
empowering
victims of
cybercrime



This Manual was funded by the
European Union's Internal
Security Fund – Police



Disclaimer:

O conteúdo deste manual representa a opinião do autor apenas e é da sua exclusiva responsabilidade. A Comissão Europeia não assume qualquer responsabilidade pela utilização que possa ser feita a partir das informações contidas neste manual.

Disclaimer:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Disclaimer:

Conținutul acestei publicații reprezintă doar opiniile autorului și este responsabilitatea sa exclusivă. Comisia Europeană nu își asumă nicio responsabilitate pentru utilizarea informațiilor pe care le conține.