

# FOLHA INFORMATIVA

# BURLAS ONLINE

## O QUE É?

No contexto das burlas *online* mais praticadas em Portugal, podem distinguir-se 3 tipos:

- **Burlas no comércio eletrónico:** muitas vezes, associadas a *websites* de compras *online* que disponibilizam serviços em que os/as utilizadores/as podem vender/adquirir bens;
- **Burlas bancárias:** associam-se, com frequência, a esquemas de *phishing*, decorrendo através de *e-mail* fraudulento que imita a comunicação realizada pela entidade bancária dos/as destinatários/as; neste âmbito, esses destinatários/as podem ser persuadidos da necessidade de introdução dos seus dados bancários que, deste modo, ficam disponíveis para serem utilizados pelo/a autor/a da burla;
- **Burlas nos relacionamentos amorosos (romance scams):** pressupõem o estabelecimento de uma relação amorosa/emocional com o alvo, através da *Internet* e das Tecnologias de Informação e Comunicação (TIC), como forma de obter benefício, particularmente financeiro, por exemplo, através da transferência de dinheiro por parte da vítima para o/a autor/a da burla.

No que diz respeito ao crime, o/a agente que pratica uma burla *online*, poderá cometer uma das duas modalidades previstas no Código Penal português: burla, prevista e punida no artigo 217º do código penal, e burla informática, prevista e punida no artigo 221º do código penal. Na **burla**, o elemento essencial do crime materializa-se na indução em erro de alguém, implicando, para tal, a colaboração da vítima a atuar de acordo com uma vontade viciada. Já na **burla informática**, verifica-se um atentado direto ao património, que é levado a cabo

por meios informáticos. O computador surge como mecanismo de ação do/a agente, logo, não pode ser alvo de engano. Ao contrário do crime de burla, na burla informática não é necessário que se verifique um enriquecimento do/a autor/a, bastando o *animus* de enriquecimento. Nesse sentido, a burla informática também não pressupõe a necessidade de se verificar a intenção de induzir alguém em erro, sendo somente necessário, para a prática do crime, a verificação de configuração incorreta de programa informático que se concretize na sua total ou parcial reestruturação, no aditamento, alteração ou supressão de fases do programa e/ou na introdução de novas instruções.

Assim sendo, em Portugal, será punido pelo crime de burla o/a agente que, através do uso da *Internet* e das TIC, como é o caso das redes sociais, finge um relacionamento amoroso com a vítima, com o intuito de que a mesma lhe entregue dinheiro.

Já na prática de burla informática, o/a agente cria, através de meios informáticos, um *e-mail* falso, fazendo-se passar pela entidade bancária da vítima, solicitando o acesso a *link* para introdução de dados bancários. O referido *link* poderá remeter para *website* construído para ser muito semelhante ao da entidade bancária, levando a que a vítima acredite na sua legitimidade.

## QUEM É A VÍTIMA?

Qualquer pessoa pode ser vítima de burlas *online*. Veja-se o caso das burlas bancárias associadas ao envio diário de *e-mails* de *spam* e que têm o potencial de afetar milhões de utilizadores/as a uma escala global.

Existem, porém, estratégias e comportamentos que aumentam a proteção contra este tipo de situações, tais como:

- Não fornecer informação pessoal ou dados pessoais através de *e-mail*, mensagens, chamadas e/ou *websites* não solicitados, mesmo que o pedido pareça proveniente de entidades legítimas. Em caso de dúvida, antes do fornecimento de qualquer dado, deverá contactar-se a referida entidade;
- Verificar o *URL (Uniform Resource Locator)* - endereço *web* - dos *websites* e *links* partilhados/recebidos por mensagem ou *e-mail*, antes de clicar, para confirmar a sua legitimidade;
- Identificar *websites* e *links* seguros - os endereços seguros apresentam um certificado '*https://*' e a imagem/ícone de um cadeado, com a informação de que a ligação é segura;
- Verificar o nome do remetente do *e-mail*, já que gralhas ou outro tipo de erros poderão ser indicativos de que o remetente do *e-mail* não é/representa quem diz/aparenta ser;
- Verificar a fotografia de perfil (e.g., através do motor de busca de imagens *Tin Eye* ou do *Google Chrome*, carregando, para o efeito, no botão do lado direito do rato e escolhendo a opção "pesquisar imagem no *Google*");
- Efetuar pesquisa no *Google*®, copiando parágrafos de mensagens recebidas via *chat* ou *e-mail*, de forma a perceber se é uma abordagem/comunicação já conhecida e denunciada por outras pessoas;
- Verificar erros ortográficos que indiquem que a língua em que a pessoa está a comunicar não é a sua língua nativa;

• Verificar se o/a agente ou pessoa que está a comunicar realiza vários pedidos para que a comunicação seja efetuada através de plataformas de *chat* como, por exemplo, *Facebook*®, *WhatsApp*®, *Kik*®, *SMS*, *Messenger*® ou *Skype*®.

## QUAL O IMPACTO?

O **impacto económico** das burlas *online* não diz apenas respeito ao montante de dinheiro que a vítima perde e que o/a autor/a obtém através da prática da atividade criminosa, incluindo também os gastos suportados pela vítima para procurar repor a sua situação. As vítimas de burlas *online* deparam-se, muitas vezes, com as suas poupanças dizimadas.

Embora os **efeitos ao nível psicológico** variem de pessoa para pessoa, de acordo com diversos fatores e com o tipo de burla, alguns sintomas mais comuns são: medo, ansiedade, raiva ou desconfiança constante e prolongada, por vezes descrita como “paranoia”. Muitas vítimas de burlas *online* percebem ainda como violada ou desrespeitada a sua privacidade, sentindo-se desamparadas, impotentes e receosas de que o crime se repita.

A insegurança gerada pela perda de estabilidade financeira assume também particular relevância, no que respeita ao impacto emocional. Adicionalmente, estas vítimas têm ainda de lidar com a desilusão de, na generalidade dos casos, não ser possível identificar o/a autor/a do crime.

## QUE APOIO ESTÁ DISPONÍVEL?

Ser vítima deste tipo de crimes pode desencadear uma série de reações físicas e comportamentais, como as acima descritas. Pode despoletar uma combinação de emoções e pensamentos com os quais é, por vezes, difícil lidar. Mesmo que estas emoções sejam reações completamente normais, a vítima pode sentir que está a perder o controlo. É importante lembrar a vítima que, na maioria das situações, com o tempo, irá gradualmente voltar a adquirir um sentimento de controlo sobre a sua vida.

O acesso a serviços de apoio à vítima pode revelar-se essencial para ultrapassar ou, pelo menos, minimizar o impacto do crime. Muitas vezes, é difícil e perturbador falar sobre o crime, mas pode ser positivo para a vítima partilhar com um/a profissional a experiência de vitimação, incluindo os pensamentos e sentimentos precipitados pela situação vivida e seus efeitos. Para além disso, os/as profissionais (Técnicos/as de Apoio à Vítima) podem auxiliar a vítima a lidar com as diferentes necessidades – jurídicas, psicológicas, sociais, práticas, etc. - resultantes do crime sofrido.

Algumas burlas *online* podem ser muito complexas, pelo que **as vítimas necessitam de apoio individualizado e qualificado** para as auxiliar a recuperar dos efeitos do crime. Será, designadamente, necessária ajuda para operar meios informáticos, que as

vítimas poderão não dominar. É também importante o contacto com a instituição bancária, de crédito ou outra entidade através da qual tenha sido retirado à vítima o montante monetário.

Para além disso, a vítima tem direito a beneficiar de serviços de apoio, antes, durante e após o processo-crime, podendo também recorrer a estes serviços ainda que não tenha denunciado o crime. A APAV disponibiliza, de forma gratuita, confidencial, qualificada e humanizada, apoio emocional, acompanhamento psicológico, informação jurídica, encaminhamento social e auxílio em questões práticas a todas as pessoas que foram ou são vítimas de crime.

Poderá contactar a APAV:

- Pela Linha Internet Segura - 800 21 90 90 | chamada gratuita | dias úteis das 09h às 21h | [linhainternetsegura@apav.pt](mailto:linhainternetsegura@apav.pt);
- Pela Linha de Apoio à Vítima - 116 006 | chamada gratuita | dias úteis das 09h às 21h;
- Através de qualquer Gabinete de Apoio à Vítima da APAV (contactos em [https://apav.pt/apav\\_v3/index.php/pt/contactos](https://apav.pt/apav_v3/index.php/pt/contactos)).



### RECURSOS APAV

<https://apav.pt/cibercrime/>  
<https://www.internetsegura.pt/>  
<http://infovitas.pt>  
<https://www.apav.pt/folhainformativa>