

# FOLHA INFORMATIVA PHISHING

## O QUE É?

O *phishing* traduz-se no **envio em massa de mensagens de correio eletrónico (*spamming*)**, que **contêm uma ligação (*link*) para uma página da Internet e que apelam, invocando motivos urgentes, ao acesso à mesma**. Tal página é, normalmente, uma reprodução aproximada da página original de um banco, de uma entidade emissora de crédito ou de outra que permita a realização de pagamentos *online* e contém elementos identificadores da entidade autêntica e imagens a ela referentes.

No entanto, será uma página falsa. Se a vítima usar o *link* para aceder à página falsa, ser-lhe-á pedido que se identifique, introduzindo os seus códigos confidenciais referentes à sua conta bancária ou ao seu cartão. A captura, por esta via, destes dados permitirá ao criador da página aceder às contas bancárias da vítima e transferir o dinheiro que aí houver para outra conta ou utilizar o cartão de crédito em seu proveito.

## Ao fenómeno do *phishing* podem corresponder vários crimes, nomeadamente:

- O crime de falsificação de documentos (elaboração de documentos falsos);
- O crime de falsidade informática (produção de dados ou documentos não genuínos, interferindo no tratamento informático de dados);
- O crime de acesso ilegítimo (acesso não autorizado a sistema informático);
- O crime de burla informática (intervenção não autorizada no processamento de dados informáticos, para com isso obter ganhos, causando prejuízo a outrem).

No caso dos dois últimos crimes, o início

do procedimento criminal depende da apresentação de queixa por parte da vítima.

## QUEM É A VÍTIMA?

Qualquer pessoa pode ser vítima destes crimes, visto que os *e-mails* enviados no âmbito de um esquema de *spamming* são dirigidos a milhões de pessoas de forma aleatória.

Porém, existem cuidados que podem ser tidos, para se evitar tentativas de *phishing*:

- Manter sempre o computador atualizado com antivírus;
- Ter em atenção que *e-mails* escritos em mau português provavelmente farão parte de esquemas de *phishing*, mesmo que aparentemente tenham origem num remetente conhecido; o mesmo se aplica em relação a *e-mails* que anunciem que venceu algum prémio, que existe um problema com a conta de *e-mail* ou que é necessário validar os dados bancários ou de outro sistema;
- Procurar reconhecer o endereço ao receber um *e-mail* de uma instituição bancária ou de qualquer outra com quem trabalha: se não reconhecer, contactar a instituição;
- Colocar o rato sobre qualquer *link* antes de carregar no mesmo, verificando, no canto inferior esquerdo do *browser*, para que endereço será encaminhado/a e, caso o domínio do *link* seja externo ao domínio da entidade que supostamente envia o *e-mail*, abster-se de clicar;
- Verificar sempre se a ligação a um *website* se está a fazer através de "https"(modo seguro) e não "http"(modo não seguro) e, adicionalmente, verificar se surge um ícone representando

um cadeado ou uma chave;

- Ter em atenção que os bancos apenas solicitam uma pequena parte dos números do cartão matriz, para que possa realizar operações *online*.

## QUAL O IMPACTO?

O impacto económico do *phishing* consiste não apenas no montante de dinheiro que o/a perpetrador/a obtém através da prática da atividade criminosa e que a vítima perde, mas também em todos os gastos suportados pela vítima para procurar repor a sua situação. As vítimas de *phishing* vêem muitas vezes as suas poupanças dizimadas. Os bancos podem ver-se obrigados judicialmente a indemnizar a vítima pela sua perda.

Embora os efeitos ao nível psicológico variem de pessoa para pessoa de acordo com diversos fatores, entre os quais as características da vítima, alguns sintomas mais comuns são: medo, ansiedade, raiva ou mesmo desconfiança constante e prolongada no tempo em relação a tudo e todos, que muitas vítimas descrevem como "paranoia". O impacto emocional é descrito como sendo semelhante às reações das vítimas de crimes violentos. Muitas sentem a sua privacidade violada, sentem-se desamparadas, impotentes e receosas de que o crime se repita. As vítimas podem sentir-se envergonhadas e culpadas por terem sido ludibriadas.

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

O *phishing* implica ainda, para a vítima, um sério aborrecimento e muito tempo perdido para procurar reparar as suas consequências.

## QUE APOIO ESTÁ DISPONÍVEL?

Ser vítima deste fenómeno pode desencadear uma série de reações físicas e comportamentais, como as acima descritas. Pode vivenciar-se uma combinação de emoções e pensamentos com os quais é, por vezes, difícil lidar. Mesmo que estas emoções sejam reações completamente normais, pode sentir-se que se está quase a perder o controlo. É importante lembrar que, na maioria das situações, com o tempo, irá gradualmente voltar a adquirir-se 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 partilhar com um/a profissional** a experiência de vitimação, pensamentos e sentimentos. 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.

As vítimas de *phishing* encontram-se numa posição de particular fragilidade e desproteção, tendo em conta que o fenómeno criminoso, pelo seu carácter recente, ainda é pouco valorizado e compreendido pela população em geral e que existem poucas entidades preparadas para lidar com os seus efeitos.

Os casos de *phishing* podem ser muito complexos, 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 importante que a vítima de *phishing* entre em contacto com a instituição bancária, de crédito ou outra através da qual lhe foi retirado o montante monetário. Estas instituições fornecem apoio relativo à resolução prática do problema.

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.

A APAV apoia as vítimas de *phishing*:

- 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)).

## TESTEMUNHO



*Ligaram-me do Banco a dizer que tinha sido feita uma transferência suspeita da minha conta e a pedir que confirmasse que tinha sido eu a fazê-la. Entrei logo em pânico porque não tinha feito nenhuma transferência. Fui consultar a minha conta e vi que o dinheiro que lá tinha guardado tinha desaparecido. Não conseguia acreditar que aquilo me estivesse a acontecer!*



## RECURSOS APAV

<https://apav.pt/cibercrime/>  
<https://www.internetsegura.pt/>  
[www.apav.pt/folhainformativa](http://www.apav.pt/folhainformativa)