Segurança online

Como estar atento e evitar os perigos da internet

Recebeu um *e-mail* do seu banco?

Veja com atenção... Pode ser *phishing*.

- O *phishing* recorre a mensagens de e-mail que aparentam ter origem fidedigna, por exemplo do seu banco mas que provêm de impostores.
- O seu objectivo é fazê-lo partilhar dados pessoais, financeiros ou códigos de segurança.
- São bastante semelhantes aos que são enviados por Bancos e outras entidades.
- Pedem para descarregar um anexo ao e-mail ou clicar num *link*.
- Utilizam linguagem que transmite urgência na execução do que é pedido.

Como evitar:

- Manter o *software* e antivírus atualizados.
- Comparar o *e-mail* com os que já recebeu daquela entidade.
- Verificar se vem do endereço habitual.
- Estar atento a erros de escrita.
- Suspeitar se lhe pedirem dados pessoais.
- Reencaminhar o *e-mail* para o endereço habitual do seu Banco e não *responder*.
- Não clicar nos *links* nem descarregar ou abrir os anexos.

Como aceder ao *homebanking* do seu Banco?

- Redija o endereço do seu banco no *browser*
- Este endereço deve sempre começar por https://
- Apenas aí pode aceder ao seu *homebanking*
- Nunca aceda através de *links* em mensagens de email, endereços gravados nos *Favoritos* ou no *Histórico*, nem através de anúncios ou de pesquisas na internet

Vai usar o *homebanking*?

Atenção aos sites bancários falsos.

- São sites parecidos com os originais, mas falsos.
- Podem ser direcionado para estes sites através de *phishing*.
- Muitas vezes, têm janelas "pop-up" que podem os seus dados de acesso.
- Têm mensagens com palavras como "Urgente".

Como evitar:

- Cuidado com sites com falhas no design ou erros de escrita.
- Verificar se o endereço do site tem um cadeado ou começa por https.
- Não clicar em janelas pop-up.
- Escrever sempre o endereço de email do seu banco manualmente e não clicar em *links* enviados por e-mail.

Já ouviu falar de *Pharming*?

- O *pharming* é um crime virtual no qual o tráfego de um *site* é manipulado através de *links* fraudulentos para roubar informações confidenciais dos utilizadores.
- Ao clicar num *link* que pode receber por *e-mail* ou estar acessível noutro sítio despretensão da internet, é direcionado para uma página desconhecida, que não parece suspeita.
- Ao entrar nessa página, e sem perceber, instala *malware* (códigos maliciosos) no seu computador.
- É então direcionado para um site fraudulento, idêntico ao real que recolhe dados bancários e pessoais.

O que a Caixa pode fazer por si?

A Caixa nunca recorre a **sms** ou **emails** com pedidos de acesso a *links*. Tenha isso em atenção e proteja-se.

Saiba mais aqui

A Banca tem alertado para exemplos de ataque de que os seus clientes podem ser alvo. Por exemplo, a Caixa disponibiliza informação concreta sobre este tema no seu site.

Saiba mais aqui.

Como evitar:

- Não responder a *e-mails* que peçam *PIN*, *passwords* ou outros dados pessoais.
- Desconfiar de *e-mails* que têm como tema algo preocupante ou excitante.
- Visitar o site que conhece e verificar se a informação consta no site.
- Não clicar em *links* em mensagens de *e-mail* ou em chats se suspeitar da mensagem ou não conhecer o emissor.
- Manter o antivírus atualizado.

SMS do seu Banco?

Leia duas vezes
Pode ser *Smishing*

- Através de um **SMS** tentam obter dados pessoais, financeiros ou de segurança.
- Pedem para clicar num *link* ou ligar para um número.
- O objetivo da mensagem é *verificar*, *atualizar* ou *reativar* a sua conta.
- O *link* direciona para uma página falsa.
- O número de telefone direciona para uma empresa falsa.

Como evitar:

- Não carregar em *links*, anexos ou imagens. Tenha este procedimento como regra.
- Em caso de dúvida, esclareça-se com a entidade emissora.
- Não responder a **SMS** que lhe peçam o PIN, *passwords* de acesso ou outros códigos de segurança e acesso a entidades bancárias ou outras por exemplo a Autoridade Tributária.

Não consegue aceder ao seu computador?

Pode ser *ransomware*

- É um tipo de *software* malicioso.
- É distribuído através de *e-mails* de *phishing* ou anúncios *pop-up*.
- O objetivo é restringir o acesso ou inserir dados comprometedores num computador.
- Permite manobras de chantagem sobre a vítima ou pedido de um resgate.
- A vítima não consegue aceder a ficheiros que foram encriptados sem o seu consentimento.
- Podem ser encriptados ficheiros em unidades partilhadas, drives **USB**, discos externo.
- Na prática, impedem-lhe o acesso aos dados do computador.

Como evitar:

- Manter o sistema operativo e o antivírus atualizados.
- Ativar um bloqueador de janelas de pop-up.
- Se for vítima deste crime, não pague o resgate e participe o sucedido às forças de segurança ou ao Ministério Público.
- Fazer regularmente cópias de segurança dos ficheiros.

Compras *online*

Se é bom demais pode ser fraude

Como evitar:

- Aceda sempre a sites seguros e certificados, identificados com https://
- Optar por sites nacionais, porque é mais fácil reclamar.
- Ver as avaliações e comentários antes de comprar.
- Confirmar se a loja tem um espaço físico e várias formas de contacto.
- Usar apenas serviços de pagamento seguros e que recorram à autenticação forte. Saiba mais sobre este assunto neste artigo do Saldo Positivo.
- Se optar pelo cartão de crédito, recorra a um pré-pago ou opte de pagamento com limites no valor a transferir.
- Evite redes públicas para compras, pagamentos ou para aceder ao *homebanking*.
- Desconfiar de ofertas de descontos ou produtos miraculosos.
- Tenha atenção ao uso dos seus cartões de pagamento e códigos de acesso às contas. Confira aqui como proceder.

Saiba mais sobre compras online neste **Guia das Compras Online** do Saldo Positivo

Identidade Roubada

Há alguém a fazer-se passar por si?

Boa parte das fraudes online implicam a apropriação de identidade alheia ou de informações pessoais. As informações são usadas para:

- Fazer-se passar por si em sites ou redes sociais.
- Abrir contas bancárias em seu nome.
- Fazer transferências bancárias ou beneficiar de serviços em seu nome.
- Pedir cartões de crédito e débito ou empréstimos bancários.

Como evitar:

- Escolher *passwords* com oito ou mais dígitos com letras, números e símbolos.
- Nunca partilhar as *passwords*.
- Alterar regularmente as *passwords*.
- Nunca responder a chamadas ou e-mails com pedidos de *passwords* ou outros dados pessoais.
- Monitorizar a atividade do seu perfil.
- Nunca publicar informações pessoais nas plataformas sociais, por exemplo. Leia mais sobre este assunto neste artigo Saldo Positivo.
- Se suspeitar que o seu perfil em redes sociais está comprometido, mude as *passwords* de acesso e as configurações de privacidade da conta.
- Suspeitar se receber um e-mail com um *link* com pedido de acesso.
- Verificar regularmente os extratos bancários.
- Comunicar ao Banco despesas ou movimentos suspeitos na sua conta.

Mensagem de amor ou romance fraudulento?

Abriu o *Messenger* ou *Whatsapp* e tem uma mensagem apaixonada de alguém que conheceu recentemente online? Será que está em segurança? Talvez não.

Sinais a ter em atenção:

- Pedem-lhe imagens ou vídeos íntimos?
- Alegam estar em dificuldades e pedem dinheiro?
- Contam-lhe uma história rebuscada?
- Pedem-lhe para guardar ou pedir dinheiro a terceiros?
- Dizem que vão oferecer uma elevada quantia de dinheiro em troca de algum favor?
- As mensagens que enviam são vagas ou mal escritas?

Saiba mais sobre este assunto neste artigo do Saldo Positivo

Como evitar:

- Ter cuidado com os dados pessoais em redes sociais ou sites de encontros.
- Ao conhecer alguém online deve avançar com cautela e fazer perguntas.
- Pesquisar online a foto e o perfil da pessoa.
- Verificar se as fotos e perfil já foram usados noutros sites.
- Ter atenção a erros de escrita, dados estranhos nas histórias ou desculpas, como dizer que a câmera não funciona.
- Nunca partilhar material comprometedor que possa ser usado contra si.
- Se combinar um encontro, diga à sua família e amigos onde vai.
- Nunca enviar dinheiro ou dados de cartões de crédito, contas ou cópias de documentos pessoais.
- Nunca transferir dinheiro a pedido de outra pessoa.

Cuidado com as chamadas

O perigo não está só na internet. O *vishing* (combinação das palavras *voice* e *phishing*) é um esquema no que se procura *obter dados pessoais, financeiros ou de segurança ou transferências de dinheiro através de chamadas telefónicas.*

Como evitar:

- Anote o número de quem liga e diga que vai ligar de volta.
- Ligue para a entidade para confirmar se a chamada foi feita; não ligue devolvendo a chamada, porque o número pode ser falso.
- Nunca partilhe o *PIN* do cartão de crédito ou débito nem a *password* do seu *homebanking*.
- Tenha especiais cautelas com pedidos de transferência de dinheiro.
- Tenha uma atitude atenta e denuncie situações sobre as quais tem a mais leve suspeita junto do seu banco.

24 formas de estar seguro 24 horas por dia

1. Evitar usar equipamentos públicos conectados à *internet*.
2. Proteger o seu equipamento com antivírus, *antispyware* e *firewall* atualizados.
3. Aceder ao *homebanking* apenas a partir do seu computador e em redes seguras.
4. Nunca utilizar palavras-passe óbvias (por exemplo, 123456 ou data de nascimento)
5. Nunca divulgar as suas palavras-passe a terceiros.
6. Evitar escrever *passwords* e códigos ou guardar essa informação em locais facilmente acessíveis.
7. Evitar imprimir dados confidenciais.
8. Bloquear o computador se tiver de se afastar dele.
9. Ativar o bloqueio automático dos dispositivos e usar *PIN* ou *password* para aceder
10. Garantir que o *Wi-Fi* em casa tem uma *password* forte e secreta e alterá-la regularmente.
11. Nunca abrir e eliminar imediatamente *e-mails* suspeitos.
12. Nunca clicar em *links* nem fazer downloads de fontes desconhecidas.
13. Nunca abrir *e-mails* ou mensagens se estiver com pressa ou a prestar pouca atenção.
14. Nunca inserir dados confidenciais e outras informações em sites que desconheça.
15. Nunca aceder a páginas através de *links* em mensagens de *e-mail* ou de resultados de pesquisas.
16. Aceder aos sites de modo manual com registo de endereço eletrónico.
17. Verificar se o endereço começa com https:// e com o símbolo do cadeado.
18. Nunca divulgar a totalidade das coordenadas do cartão matriz de acesso ao *homebanking*.
19. Procurar informações sobre o vendedor antes de fazer compras.
20. Utilizar cartões virtuais criados no multibanco ou *homebanking* para as compras *online*.
21. Usar métodos de pagamento seguros, como cartões com limite de crédito ou prazo de validade reduzidos ou procedimentos de autenticação adicionais.
22. Guardar registos das operações efetuadas.
23. Consultar regularmente os movimentos da conta bancária.
24. Contactar o Banco e as autoridades caso sejam detetados movimentos não autorizados.

Tome nota:

Quer saber mais sobre segurança online?
Faça o curso **Cidadão Cibersaguro** através do Centro Nacional de Cibersegurança.
O curso decorre online, é gratuito e tem a duração de três horas.

Autenticação forte = Mais segurança nos acessos online

É um procedimento que traz mais segurança aos serviços online, nomeadamente os de pagamento levados a cabo pelas entidades financeiras e bancárias. A identidade do cliente é validada em situações que possam envolver risco de fraude financeira ou outros abusos. Os prestadores de serviços devem pedir aos utilizadores pelo menos dois elementos que comprovem a sua identidade. Estes elementos têm obrigatoriamente de pertencer a duas das três categorias de autenticação forte:

Conhecimento: algo que apenas o utilizador conhece (palavra passe, código ou um número de identificação pessoal).

Posse: Algo que apenas o utilizador possui, por exemplo, um telemóvel.

Inerência: Algo que se constitua como característica biométrica do cliente. Por exemplo, impressão digital ou reconhecimento facial.

Consulte mais artigos sobre este assunto:

- *Nova diretiva europeia vem revolucionar os seus pagamentos*
- *O seu cartão deve estar apenas associado ao seu telemóvel*
- *Chave Móvel Digital: identidade digital segura nos Serviços públicos e privados*

Saldo Positivo