Segurança online

Como estar atento e evitar os perigos da internet

Recebeu um *e-mail* (que parece ser) do seu banco?

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

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

Como evitar:

- Manter o ***software*** e o antivírus atualizados;
- Comparar o ***email*** com os que já recebeu da mesma entidade;
- Verificar se chegou através do endereço habitual;
- Estar atento a erros de escrita;

Como aceder ao *homebanking* do seu Banco?

- Escreva o ***endereço do seu banco*** no ***browser***;
- Este endereço deve sempre começar por ***https://***;
- Nunca aceda através de ***links*** em mensagens de email, endereços gravados nos Favoritos ou no Histórico do dispositivo, nem através de anúncios ou de pesquisas na ***internet***.

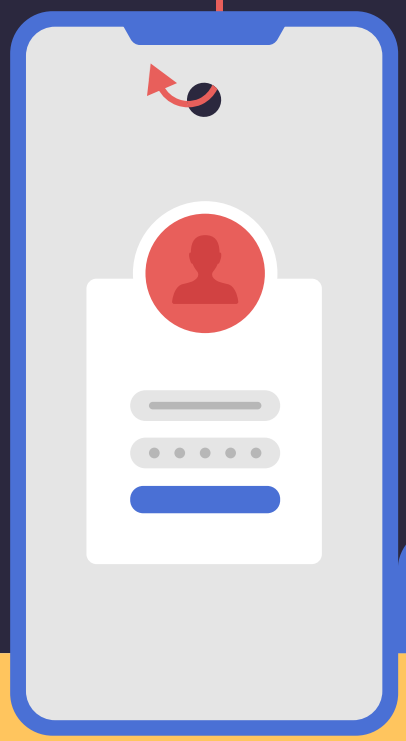
Vai usar o *homebanking*?

Atenção aos sites bancários falsos.

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

Como evitar:

- Suspeitar se lhe pedirem ***dados pessoais***;
- Reencaminhar o ***email*** para o endereço habitual do seu banco e não responder;
- Não clicar nos ***links***, nem descarregar ou abrir os anexos.



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

Já ouviu falar de *Pharming*?

- O ***pharming*** é um crime virtual que utiliza ***links*** fraudulentos para roubar informações confidenciais dos utilizadores;
- Ao clicar num ***link*** que pode receber por ***email*** ou estar acessível noutro sítio desprotegido da ***internet***, é direcionado para uma página desconhecida, que não parece suspeita;
- Ao entrar nessa página, 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.

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

Saiba mais aqui

Como evitar:

- Não responda a emails que peçam PIN, ***passwords*** ou outros dados pessoais;
- Desconfie de ***emails*** que têm como tema algo preocupante ou excitante;
- Visite o site que conhece e verificar se a informação está lá;
- Não clique em ***links*** em mensagens de email ou em chats se suspeitar da mensagem ou não conhecer o emissor;
- Mantenha o antivírus atualizado.

Recebeu uma SMS?

Leia duas vezes
Pode ser *Smishing*

- Através de um SMS os infratores 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 clique em ***links***, anexos ou imagens. Tenha este procedimento como regra;
- Em caso de dúvida, esclareça-se com a entidade que teria enviado a mensagem;
- Não responda a SMS que lhe peçam o PIN, ***passwords*** de acesso, outros códigos de segurança, acesso a entidades bancárias ou outras, como por exemplo a Autoridade Tributária.

Não consegue aceder ao seu computador?

Pode ser *ransomware*

- É um tipo de ***software*** malicioso;
- É distribuído através de emails 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;
- Deixa de conseguir aceder a ficheiros que foram encriptados sem o seu consentimento;
- Podem ser encriptados ficheiros em unidades partilhadas, ***drives*** USB, discos externos ou na ***cloud***;
- Na prática, impedem-lhe o acesso aos dados do computador.

Como evitar:

- Mantenha o sistema operativo e o antivírus atualizados;
- Ative um bloqueador de janelas de ***pop-up***;
- Se for vítima deste crime, não pague o resgate e participe o sucedido às autoridades ou ao Ministério Público;
- Faça regularmente cópias de segurança dos ficheiros.

Compras *online*

Se é bom demais pode ser fraude

Siga estas recomendações para comprar online em segurança e evitar fraudes:

Mensagem de

- Aceda sempre a sites seguros e certificados, identidicados com ***https://***;
- Analise as avaliações e comentários antes de comprar;
- Confirme se a loja tem um espaço físico ou várias formas de contacto;
- Use apenas serviços de pagamento seguros e que recorram à ***autenticação forte***;
- Se optar pelo cartão de crédito, recorra a um pré-pago, ***cartão virtual*** ou uma ***app de pagamento*** com limites no valor a transferir;
- Evite redes públicas para compras, pagamentos ou para aceder ao ***homebanking***;
- Desconfie de ofertas de descontos ou produtos milagrosos;
- Tenha atenção à utilização dos seus ***cartões de pagamento*** e códigos de acesso às contas.

Tome nota:

A CGD nunca envia SMS ou ***emails*** com ***links*** para acesso direto às suas contas, nem pede que revele os seus códigos de acesso ou ***passwords*** por estas vias. Desconfie e reporte qualquer mensagem ou chamada suspeita que peça esse tipo de informação. Em caso de dúvida, contacte diretamente o apoio oficial do banco.

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

Cuidado com as chamadas Pode ser *vishing*.

O perigo não está só na internet.
O *vishing* (combinação das palavras voice e *phishing*) é um esquema em que se procura obter dados pessoais, financeiros e 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 o faça devolvendo a chamada, porque o número pode ter custos associados;
- Nunca partilhe o PIN do cartão de crédito ou de débito, nem a ***password*** do seu ***homebanking***;
- Tenha especiais cautelas com pedidos de transferência de dinheiro;

Como evitar:

- Desconfie de ***QR codes*** colados sobre o original ou impressos de forma amadora;
- Depois de ler o código, verifique o endereço antes de tocar em "Abrir";
- Mantenha o antivírus ativo no telemóvel e desative a abertura automática de links de QR.

Vishing com voz clonada por

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 financeiras 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 contêm erros ortográficos?
- Alguns burlões gravam videochamadas íntimas para depois chantagear a vítima (***sextorsão***).

Como evitar:

- Tenha cuidado com os dados pessoais em ***redes sociais*** ou sites de encontros;
- Quando conhece alguém online deve avançar com cautela e fazer várias perguntas;
- Pesquise ***online*** a foto e o perfil da pessoa; Verifique se as fotos e o perfil já foram usados noutros locais;
- Tenha atenção a erros de escrita, dados estranhos nas histórias ou desculpas, como dizer que a câmara não funciona;
- Nunca partilhe material comprometedor que possa ser usado contra si;
- Se combinar um encontro, diga à sua família e amigos onde vai;
- Nunca envie dinheiro ou dados de cartões de crédito, contas ou cópias de documentos pessoais;
- Nunca ***transfira dinheiro*** a pedido de outra pessoa.

Clonagem de cartão SIM (SIM-Swap)

- Cada vez mais burlões conseguem convencer a operadora a emitir uma 2.ª via do cartão SIM, passando a receber todas as SMS de validação do banco;
- Sinal típico: perde subitamente serviço de voz e dados.

- Tenha uma atitude atenta e denuncie situações sobre as quais tem a mais leve suspeita junto do seu banco.

Quishing (Phishing via QR code)

- Um código QR pode ser usado como ***link*** disfarçado: basta apontar a câmara para ser redirecionado para um site falso ou para descarregar uma app maliciosa;
- Costuma surgir em parquímetros, cartazes ou PDFs recebidos por email.

Inteligência Artificial

- Alguns criminosos recorrem a ***deepfakes*** de voz para imitarem um familiar ou funcionário do banco, pedindo códigos ou transferências;
- O número no visor também pode ser falsificado (***spoofing***).

Como evitar:

- Desligue e ligue de volta para o número oficial da entidade;
- Combine uma "palavra-passe familiar" para pedidos urgentes;
- Nunca revele códigos de autenticação recebidos por SMS ou ***app***.

Como evitar:

- Peça à sua operadora um bloqueio de ***port-out*** (PIN de transferência);
- Prefira ***apps*** de autenticação (TOTP/ push) em vez de SMS, quando possível;
- Ative alertas de movimentos bancários fora do comum.

Mensagem "Olá mãe/ Olá pai" (WhatsApp)

- Os criminosos fazem-se passar por um filho ou outro familiar e enviam uma mensagem, de um novo número, semelhante a esta:
- "Perdi o telemóvel, este é o novo número, preciso de dinheiro urgente";
- Pedem transferência por ***MB Way*** ou IBAN.

Como evitar:

- Ligue ou faça videochamada para o número antigo;
- Faça perguntas cuja resposta só esse familiar saiba;
- Nunca envie dinheiro ou códigos MB Way antes de confirmar a veracidade da mensagem.

SIM *Swapping*: saiba o que é e como proteger o seu telemóvel *neste artigo do Saldo Positivo*.

Promessas de lucro fácil?

Pode ser fraude de investimento.

- Cuidado com ofertas de ***investimento milagrosas*** que surgem por telefone, email ou nas ***redes sociais***;
- Nestes esquemas, são prometidas oportunidades com lucro elevado, rápido e garantido, praticamente sem risco (por exemplo, investimentos em ***ações***, ***ouro*** ou, mais recentemente, em ***criptomoedas***);
- Podem contactá-lo repetidamente por telefone, com muita insistência, descrevendo um cenário de ganhos fáceis. É comum dizerem que a oferta é por tempo limitado e exclusivamente para si, pedindo até sigilo;
- O objetivo é convencê-lo a transferir dinheiro para uma conta.

Como evitar:

- "Retorno garantido" = sinal de fraude. Recuse;
- Verifique se a entidade está registada na CMVM;
- Peça conselhos financeiros a alguém de confiança, antes de investir.

Ligaram-lhe do "suporte técnico"?

Cuidado!

- Chamadas que alegam vírus no seu computador e pedem que instale ***software*** de acesso remoto;

  Depois orientam-no a entrar no banco ***online*** para "pagar o serviço", roubando credenciais ou dinheiro.

Como evitar:

- Desligue de imediato chamadas não solicitadas;
- Nunca instale programas ou dê acesso remoto a desconhecidos;
- Reporte à Polícia Judiciária e bloqueie o número.

24 formas de estar seguro 24 horas por dia

1. Mantenha antivírus e ***software*** atualizados em todos os dispositivos.
2. Proteja o wi-fi de casa com password robusta e WPA2/WPA3.
9. Verifique a reputação das lojas antes de comprar online.
10. Não clique em links nem faça ***downloads*** de fontes desconhecidas.
17. Desative NFC/Bluetooth quando não usa.
18. Use encriptação de disco em portáteis e ***smartphones***.

3 Use ***passwords*** fortes e únicas para cada conta.

4 Utilize um gestor de ***passwords*** fidedigno.

5 Ative a autenticação de dois fatores (2FA) sempre que possível.

6 Nunca revele todos os códigos do ***homebanking*** nem códigos SMS.

7 Aceda ao banco apenas a partir de dispositivos e redes de confiança.

8 Apague de imediato ***emails*** ou mensagens suspeitas.

11 Use cartões virtuais MB Net ou MB Way/PayPal nas compras online.

12 Faça ***backups*** regulares dos ficheiros importantes.

13 Bloqueie o ecrã quando se afasta do dispositivo.

14 ***Instale apps*** apenas de lojas oficiais.

15 Ative alertas de movimentos bancários fora do comum.

16 Defina limites de valores para cartões e MB Way.

19 Verifique se os sites começam por ***https://*** e apresentam o símbolo do cadeado.

20 Nunca aceda ao banco a partir de ***links*** em ***emails*** ou de resultados do Google.

21 Guarde registos de todas as operações financeiras.

22 Contacte o banco e as autoridades se detetar movimentos suspeitos.

23 Tenha uma "palavra-passe familiar" para emergências.

24 Atualize periodicamente as perguntas de recuperação das contas.

Tome nota:

Esteja atento às sugestões de boas práticas ***transmitidas pelo seu Banco***. A segurança da sua conta e dos seus dados depende de si. Se seguir as sugestões do seu Banco, reforça a sua e evita cair em esquemas.

Saiba Mais Aqui.

Autenticação forte = Mais segurança nos acessos online

É um procedimento que traz mais segurança aos serviços ***online***, nomeadamente os de pagamento das 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.

Tome nota:

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

Consulte mais artigos sobre este assunto:

- ***Já usou a Chave Móvel Digital?***
- ***Cookies nos sites: o que são e para que servem***
- ***Banco online: principais cuidados de segurança em cada acesso***
- ***Lei do cibercrime: o que fazer se for vítima de um crime informático?***
- ***Conta pirateada nas redes sociais: saiba o que fazer***
- ***Como posso abrir uma conta à distância em segurança?***
- ***Como evitar que o seu cartão seja clonado***
- ***Os dez truques para resistir ao noticiário fake***
- ***Conheça as principais burlas online e saiba como proteger-se***
- ***Glossário do mundo da tecnologia: 28 termos que deve conhecer***
- ***Apps de controlo parental: qual a utilidade e como funcionam***

Saldo Positivo