ContasConnosco
Cofidis

SEGURANÇA DIGITAL: COMO IDENTIFICAR E EVITAR BURLAS ONLINE

Usar a internet tem inúmeras vantagens, mas também alguns perigos como as burlas online. Através de métodos sofisticados e tirando partido da distração dos destinatários, os fraudulentos conseguem aceder a dados sensíveis e até a contas bancárias.

CONHEÇA OS MÉTODOS MAIS USADOS E SIGA AS NOSSAS DICAS PARA GARANTIR A SUA SEGURANÇA DIGITAL.

PHISHING, SMISHING OU VISHING

- Estes métodos envolvem e-mails, *SMS* ou telefonemas, onde o burlão se faz passar por um funcionário de uma entidade fidedigna.
- O objetivo é obter informações sensíveis através de cliques em anexos ou links maliciosos.
- Utilizam uma linguagem que exige uma ação importante e de carácter urgente.

COMO EVITAR:

- Verifique a veracidade do remetente;
- Esteja atento a erros ortográficos;
- Suspeite se lhe pedirem dados pessoais;
- Não se deixe convencer por promessas, solicitações autoritárias ou pedidos urgentes;
- Não clique em links ou anexos suspeitos.

PROTEJA-SE DE EVENTUAIS FRAUDES:

Preocupamo-nos com a sua segurança e, por isso, alertamos regularmente para *tentativas de ataque em nosso nome* de que pode ser alvo.

PHARMING

- É uma técnica que o encaminha para páginas falsas quando tenta aceder a um site através do endereço legítimo e, através do download de ficheiros maliciosos, é instalado um vírus no seu computador.
- Recorre a páginas falsas de comércio online, do setor financeiro e de plataformas de pagamento online.
- O objetivo é roubar informações sensíveis e confidenciais como dados pessoais, dados bancários e credenciais de login.

COMO EVITAR:

- Altere as configurações de fábrica do router Wi-Fi;
- Use um antivírus e mantenha-o atualizado;
- Desconfie de ofertas que parecem boas demais para ser verdade;
- Aceda apenas a links que começam por https:// em vez de http://;
- Verifique a aparência do site e a existência de erros ortográficos no conteúdo ou nos links;
- Não clique em links ou anexos duvidosos.

MALWARE

- Recorre a softwares maliciosos como spyware, ransomware e adware, com o objetivo de roubar informações
- O spyware é instalado no computador sem que se aperceba.
- O ransomware destrói ou bloqueia o acesso a dados e, posteriormente, é feito um pedido de resgate para que possa recuperar os mesmos.
- O adware exibe pop-ups publicitários que incentivam o clique.

COMO EVITAR:

- Mantenha o sistema operativo atualizado e use programas antivírus e anti-spyware;
- Tenha sempre a firewall ativa;
- Use ligações seguras e não confie em pop-ups que peçam para transferir softwares;
- Evite clicar em links, abrir anexos ou fazer transferências suspeitas;
- Limite a partilha de ficheiros.

IDENTIDADE ROUBADA

- Os dados pessoais são utilizados para criar documentos falsos e praticar crimes que causam danos ou difamam a vítima.
- Geralmente, estes dados são usados para criar perfis falsos nas redes sociais, abrir contas bancárias e pedir cartões de crédito, débito ou empréstimos.

COMO EVITAR:

- Não partilhe informações confidenciais por e-mail, SMS ou redes sociais;
- Crie passwords fortes e mantenha-as seguras;
- Use, sempre que possível, a *autenticação multifator*;
- Monitorize regularmente a atividade das suas contas bancárias e redes sociais.

COMO CRIAR UMA PASSWORD SEGURA:

- Não usar dados ou sequências óbvias;
- Ter no mínimo 8 caracteres;
- Misturar letras maiúsculas, minúsculas, números e caracteres especiais;
- Trocar letras por números;
- Usar ferramentas de geração de passwords;
- Não repetir passwords em diferentes contas.

COMPRAS ONLINE

- Venda de bens ou serviços que não existem ou que não correspondem ao que é anunciado.
- O objetivo é aceder a dados confidenciais do comprador e ganhar dinheiro.

COMO EVITAR:

- *Compre em sites ou lojas online* conhecidas;
- Desconfie de preços muito baixos e da pressão de vendedores;
- Não aceite propostas de pagamento fora das plataformas reconhecidas com o pretexto de não pagar comissões;
- Use métodos de pagamento seguros como cartões virtuais e não partilhe dados de contas bancárias.

MB WAY

- Estas burlas ocorrem em contexto de vendas online onde há um aproveitamento do *desconhecimento sobre o MB WAY*.
- O burlão pede o número de telemóvel associado ao MB WAY para pagamento, mas envia um pedido de dinheiro em vez de uma transferência.
- Com isto, associa o contacto telefónico do desconhecido à sua conta MB WAY, dando-lhe acesso ao seu dinheiro.

COMO EVITAR:

- Não siga instruções de desconhecidos para fazer pagamentos por MB WAY;
- Não partilhe o código MB WAY nem associe a sua conta a números de terceiros;
- Monitorize regularmente a atividade da aplicação;
- Mantenha os seus dados pessoais atualizados na conta bancária.

MENSAGENS WHATSAPP

- O fraudulento faz-se passar por alguém da sua família ou círculo de amigos, através de um número desconhecido, e constrói uma história para lhe pedir dinheiro.
- Pode também enviar mensagens em nome de entidades fidedignas com ofertas ou pedidos para o incentivar a clicar em links, partilhar informações pessoais ou realizar pagamentos de dívidas.

COMO EVITAR:

- Limite a partilha de informações sensíveis nas redes sociais;
- Analise o conteúdo das mensagens e, se for suspeito, contacte a pessoa conhecida para confirmar se lhe foi algum pedido através de outro contacto;
- Não clique em links ou ficheiros suspeitos;
- Bloqueie de imediato o contacto utilizado.

CRÉDITO ONLINE

- Através do nome e da imagem de entidades autorizadas a conceder crédito, o burlão recorre a mensagens por e-mail, WhatsApp, redes sociais ou anúncios em plataformas com a promessa de dinheiro fácil e imediato.
- É feito um pedido de pagamento antecipado de comissões, seguros ou cheques pré-datados.

COMO EVITAR:

- Consulte a *lista de entidades autorizadas* a conceder crédito no site do Banco de Portugal;
- Desconfie se as condições forem boas demais para ser verdade ou de expressões como "crédito rápido, crédito entre particulares, sem precisar de bancos ou garantia de sigilo";
- Não partilhe os seus dados bancários nem realize qualquer pagamento solicitado.

14 PRÁTICAS PARA GARANTIR A SUA SEGURANÇA DIGITAL

01. Evite equipamentos e redes de internet públicas.
02. Mantenha o antivírus, o anti-spyware e o firewall atualizados.
03. Altere a palavra-passe do Wi-Fi regularmente.
04. Use passwords fortes e não as reutilize em contas diferentes.
05. Não escreva as suas passwords em locais de fácil acesso.
06. Utilize a autenticação multifator.
07. Bloqueie os seus dispositivos quando não os estiver a usar.
08. Aceda a aplicações bancárias apenas nos seus dispositivos.
09. Não abra nem clique em links de mensagens ou e-mails suspeitos.
10. Escreva o endereço eletrónico para aceder a sites.
11. Verifique se o endereço começa com https:// e com o símbolo do cadeado.
12. Não faça downloads de fontes desconhecidas.
13. Não partilhe dados confidenciais em sites não certificados.
14. Use métodos de pagamento seguros como cartões virtuais.

CAIU NUMA ARMADILHA?

Uma burla online, mesmo que não consumada, é punível com pena de prisão e multa. No entanto, é necessário agir para que exista um procedimento criminal:

1. Se envolver contas bancárias, contacte o seu banco de imediato;
2. Recolha todas as provas possíveis (print screens de conversas, mensagens, etc.)
3. Dirija-se à PSP, GNR, PJ ou Ministério Público e apresente queixa. Se preferir, pode recorrer à *queixa eletrónica*.