Desconfiar é a melhor maneira de se movimentar no mundo digital

SEGURANÇA Partilhar um simples vídeo pode abrir caminho a uma série de fraudes e burlas na internet. Desconfiar primeiro e clicar depois é a melhor opção. É também preciso ter cuidado com as compras *online*, a principal razão de queixa dos portugueses. O melhor é utilizar cartões de pagamento temporários evitando assim partilhar dados dos seus cartões de crédito. Já agora, não acredite em tudo o que vê ou ouve.

TEXTO **ISABEL LARANJO**

Bruno Castro é especialista em cibersegurança e análise forense.

ANDRÉ ROLO / GLOBAL IMAGENS

Hoje assinala-se o *Dia Europeu da Internet Segura*. Só que, ao utilizarmos a internet, sabemos que estamos expostos aos mais variados riscos. Bruno Castro, CEO da Visionware, empresa especializada em cibersegurança, deixa o alerta: "Primeiro vou dar um conselho que dou sempre, em todas as conferências que faço: devemos aplicar exatamente as mesmas regras que utilizamos no nosso dia a dia. Não devemos andar à noite sozinhos, não devemos andar em zonas perigosas, não falar com estranhos. Ou seja, o que fazemos na nossa vida normal devemos replicar na nossa vivência digital. Há uma analogia direta e é essa que faço, até com os meus filhos".

As redes sociais, usadas em massa em todo o mundo, são outro dos perigos à espreita por detrás de um *smartphone*, *tablet* ou computador. "O LinkedIn, o Facebook, o Tinder... Eu falar com um estranho por via digital é exatamente a mesma coisa que estar a falar com um estranho na rua. Se as pessoas aplicarem esta regra, de desconfiarem de estranhos, creio que a maior parte dos esquemas fraudulentos vão passar-lhes ao lado", afiança o especialista em cibersegurança e análise forense. "Ativar o sentimento de insegurança e perigosidade, que ativa quando vai a passar na rua, à noite, sozinha, ou num bairro complicado, aplica-se às redes". O especialista acrescenta, ainda, que a internet dá uma falsa sensação de segurança que deve ser combatida. "A pessoa pensa que por estar em casa, sentada no seu sofá, tem uma segurança digital. Não têm".

A utilização do *wi-fi* também deve ser controlada, sobretudo em locais públicos. "Quando estamos a utilizar uma rede pública, num hotel, numa estação de serviço, num aeroporto, recomendo logo que não utilize essas redes públicas, oferecidas, para aceder a serviços sensíveis. Não deve, por exemplo, aceder ao *homebanking*, ao *site* das Finanças, ao *e-mail*... E porquê? Porque é uma rede que não controlamos, pública, oferecida. Até pode servir para ouvir música, para ver o Youtube também serve, mas para ir ao *site* do banco não é seguro".

As compras *online* são outra dor de cabeça para muitos portugueses. Só no ano passado o Portal da Queixa recebeu quase 25 mil reclamações, relacionadas com fraudes associadas a compras. A maior parte dos consumidores pagou por produtos que nunca chegou a receber. Perante isto, ao pedir o reembolso do dinheiro este também nunca apareceu. Bruno Castro explica: "Se lhe aparecer uma oferta fantástica, do outro mundo, desconfie! Há ofertas que aparecem de repente só para aquela pessoa, quase como um Euromilhões por anúncio, isso é algo de falso, com certeza. Lá está, faça como faria na rua. Se um desconhecido lhe viesse vender um bilhete de lotaria, alegadamente premiado, certamente não o aceitaria". Ainda assim, para o especialista em cibersegurança, é possível fazer compras na internet sem ser enganado. "Deve verificar-se se o *site* é credível, fazer uma pesquisa, ir ao *site* da oferta, procurar na net se é um *site* seguro ou não".

> *'Olá Mãe! Olá Pai!': "Hoje em dia já aparece a foto do filho que foi roubada nas redes sociais. (...) Até já é possível fazer vídeos falsos da pessoa. Por isso, nunca acreditem em tudo o que ouvem e vêem."*
>
> **Bruno Castro**
> *CEO da Visionware*

As formas de pagamento também devem ser cuidadas. "Não quer dizer que não faça compras na internet, mas é preciso cautela", adenda Bruno Castro. "Recomendo sempre que as pessoas não disponibilizem os seus cartões de crédito, mas sim cartões virtuais. Estes têm a vantagem de conseguir, por exemplo, controlar o valor que utiliza". E dá um exemplo: "Eu crio um cartão MBNet, e, nesse caso, carrego-o com 100 euros para uma compra que custa 99. Se alguém me roubar aquele cartão, ou até se a plataforma onde fiz a compra o perder, eu só perco um euro". De resto, quanto a compras, Bruno Castro acrescenta: "Nunca é demais ver se o *site* é fidedigno. É preciso fazer uma pesquisa *online* por aquele *site*. E, inclusive, já há serviços na *net* que verificam a credibilidade dos *sites online* de compras. Estabelecem níveis de credibilidade. Por exemplo, quero comprar uma televisão, umas peças para o carro ou uma roupa e aparece-me determinado *site* no Facebook. Eu posso ir à *net* procurar e validar a credibilidade daquele *site*, *online*. Não é mais do que ir validar, previamente à compra, se o *site* é, realmente, credível".

A usurpação de identidade é outra preocupação dos especialistas em cibersegurança. "Hoje em dia já acontece em redes profissionais como o LindekIn, por exemplo. Surgem propostas de parcerias, o envio de documentos, contratos, o que seja, e na realidade o que lhe estão a enviar é um documento, ou um *link*, que ao ser aberto tem um vírus que lhe está a roubar a sua *password*".

E, muitas vezes, não são só *links*. "Pode ser, até, um documento *word* que, ao ser aberto, tem esse vírus por detrás", alerta Bruno Castro.

Para aceder às suas próprias contas na internet, seja de redes sociais ou outros serviços, Bruno Castro avisa: "Devemos aplicar mais do que um fator de autenticação: ou seja, não utilizar apenas a *password*. Devemos usar dois fatores de autenticação. Por exemplo, uso a *password*, mas também utilizo um *token* que vai aparecer no meu telemóvel. Aliás, este sistema já é obrigatório na banca". Os próprios utilizadores podem fazê-lo facilmente, pesquisando por MFA (*Multi Factor Authentication*) e seguir os passos."

Já agora, não caia na burla 'Olá mãe!' 'Olá Pai!'. "Hoje em dia já aparece a foto do filho, que foi roubada das redes sociais. Mais uma vez, desconfie sempre". Com a Inteligência Artificial (IA) até já é possível fazer vídeos falsos da pessoa. Bruno Castro finaliza: "Por 100 dólares, na internet, faz-se um vídeo de alguém. Por isso, nunca acreditem em tudo o que ouvem e veem."

isabel.laranjo@dn.pt

24 696

Reclamações apresentadas ao Portal da Queixa, durante o ano de 2023, relacionadas com burlas *online*. Isto representa um grande aumento face ao período homólogo de 2022, altura em que foram feitas 14 638 queixas. Ou seja, em 2023 houve mais 37% de queixas por causa deste tipo de crime. A maior parte das queixas tem a ver com compras *online*. Em muitos casos, os utilizadores não chegaram a receber qualquer produto.

5 milhões

Total de prejuízos causados aos utilizadores da Internet que foram alvo de burlas *online*. A análise é feita pelo Portal da Queixa e, feita uma média, o valor fica em 364 euros por cada pessoa que é burlada na internet. Muitos dos enganados pediram o reembolso do que pagaram ao não receberem os produtos comprados. A não-execução dos reembolsos representa 57,8% do total das reclamações.