Paulo Beleza Vasconcelos

> > Cidadão Ciberseguro

Fiz uma aquisição de um produto online, e passados 3 dias começo a receber avisos por email de que a encomenda está em Portugal e que é necessário o pagamento de 1.99 Euros para finalizar a entrega com a DHL. O email é muito bem feito e convincente, mas é *phishing* naturalmente. A ocorrência dos dois factos terá sido coincidência? Talvez não. A quantia pedida era muito parecida com aquela que havia sido aceite aquando da aquisição para o transporte.

De novo, já sabemos que somos rastreados por onde andamos no espaço virtual, assim como no espaço real, com monotorização via câmaras, registo de portagens, pagamentos por cartão e posicionamento via rede móvel e GPS.

Mas nunca é demais ilustrar, porque é fácil esquecer, que vivemos num meio perigoso. O cibercrime é no espaço virtual, mas é bem real.

No final do mês passado, o Ministério Público fez mais um alerta de cibercrime sobre roubo de dados de cartões de crédito via o uso abusivo das imagens da Autoridade Tributária (AT), dos CTT e da EDP. Dias antes, foram clientes do Crédito Agrícola alvo deste tipo de campanhas de *phishing*, e, alguns dias depois, clientes do Millennium BCP. Ouvidas as notícias, parece que não seríamos nós enganados, mesmo perante a sofisticação e semelhança das imagens corporativas, e que isto só acontece aos incautos. Pois aqui é que o pensamento falha. Mais cedo ou mais tarde, num momento de mais impetuosidade ou de distração, podemos ser levados a fazer aquilo que só os "nabos" fazem. Aliás, com a pandemia, os casos têm aumentado, tendo o número de queixas triplicado (dados do Gabinete de Cibercrime do Ministério Público - https://cibercrime.ministeriopublico.pt/).

O objetivo do *phishing* é obter dados pessoais com valor para serem usados ou vendidos para extorsão, furto monetário, roubo de identidade. Esta é a técnica que caracteriza o processo pelo qual o defraudador se faz passar por uma instituição conhecida e credível, em geral via email, para instigar o defraudado a preencher um formulário falso ou a visitar uma página que solicite credenciais de autenticação, dados de cartões de crédito, dados pessoais entre outros. Há designações para variantes do *phishing* para meios de contacto diferenciados: *smishing* quando é enviada uma SMS ou uma MMS, *vishing* quando o defraudado é incitado a contactar por telefone a entidade pela qual o defraudador se quer passar.

No caso reportado da AT, o email revela que o destinatário "tem direito a um reembolso de imposto" cobrado em excesso pelo Estado e indicando, de seguida, que "para receber o seu

reembolso, preencha e envie o formulário de devolução", o qual está disponível numa página cuja ligação é indicada. Outro exemplo é o de faturas erradamente debitadas em duplicado, pelo que se instiga o cliente a reclamar o reembolso através de uma ligação. Naqueles em que há lugar a pedido de pagamento, exemplo DHL e CTT, os valores em causa são de pouca monta para tentar credibilizar o pedido (grão a grão enche a galinha o papo).

Nunca é demais alertar: nunca se deve aceitar ofertas voluntárias (ninguém dá nada a ninguém), nunca se deve pressionar em ligações no corpo do email ou abrir anexos de remetentes inesperados, nunca se deve fornecer dados pessoais nem palavras-chave. De novo, parece óbvio, mas fazemo-lo várias vezes … em particular aceitar condições quando se instala *software* ou seguir ligações em emails ou redes sociais. Tente perceber o domínio de onde são provenientes tais mensagens e detetará, muitas vezes, domínio suspeitos (por exemplo, o da DHL Express que me foi endereçado era proveniente de adminas51475876@apotheke-friesenplatz17.de).

Estão na ordem do dia as aulas *online* e os cursos a distância. O Centro Nacional de Cibersegurança (CNCS) faculta o curso Cidadão Ciberseguro, com o objetivo de dotar o cidadão com as competências para navegar de forma segura no ciberespaço. O curso é online, gratuito, e apenas exige que se inscreva em https://www.nau.edu.pt/curso/cidadao-ciberseguro/; melhore a sua cidadania e até pode obter um certificado.

Já agora, repare que as ligações que aqui foram mencionadas são seguras; são ligações https. O HTTPS, em português, Protocolo Seguro de Transferência de Hipertexto, trabalha o http em conjunção com outro protocolo - *Secure Sockets Layer* (SSL) – para o transporte de dados de forma segura, ou seja, a comunicação é feita de forma encriptada. Uma última recomendação: pretendendo entrar no seu *homebanking*, digite explicitamente o endereço com https e nunca use um motor de busca para lhe dar a ligação ao seu banco!