Na Mídia

13/02/2021 | Folha de S.Paulo

O que fazer em caso de golpe virtual? Confira dicas de especialistas

Reforçar senhas e não clicar em links suspeitos estão na lista de atitudes simples para não ser vítima

Amanda Lemos

Os últimos vazamentos de dados registrados neste ano mostram como é preciso estar antento à segurança digital e a brechas quem podem fazer o internauta cair em novos golpes virtuais.

Em janeiro, o dfndr lab, laboratório de cibersegurança da Psafe, registrou um megavazamento que expôs dados de mais de 220 milhões de brasileiros, com nome completo, CPFs, CNPJs, data de nascimento e outras informações.

Depois, mais um megavazamento foi registrado. Desta vez dados mais de 100 milhões de contas de telefonia celular foram expostos na deep web, espaço no qual o rastreamento dos computadores usados pelos cibercriminosos é praticamente impossível.

E foi descoberto que o perfil do Facebook de 8 milhões de brasileiros estão sendo negociados em um fórum cibercriminoso, segundo o jornal O Globo, em um pacote que inclui ainda número de telefone, sexo, local de residência e de trabalho das vítimas.

Com informações de virtualmente toda a população sendo negociadas e milhões de outros dados também à disposição de hackers, é preciso reforçar a segurança digital.

Advogados e especialistas recomendam, entre outras dicas, ficar mais atento com qualquer atividade fora do normal, como compras não autorizadas. Ou seja, é preciso conferir com mais frequência extratos de contas bancárias e de cartões de crédito.

Confira o que fazer em caso de golpes e como evitar a situação.

FUI VÍTIMA DE UM GOLPE, O QUE DEVO FAZER?

Se observar alguma transação ou compra que não tenha feito, entre em contato imediatamente com o banco e tente bloquear o valor. Este é o primeiro passo recomendado pela Polícia Civil de São Paulo, que lançou neste mês um guia sobre o que fazer em caso de crimes eletrônicos.

Em seguida, tire cópia do comprovante de pagamento feito e dos demais documentos correlatos. Com essas informações em mãos, procure a delegacia mais próxima ou registre um boletim de ocorrência eletrônico, que deve ser feito em até 48 horas.

Durante a pandemia, as autoridades passaram a reforçar a necessidade de se fazer o BO online. O registro em delegacias especializadas em crimes digitais deve ser reservado para situações mais robustas de invasões de empresas, explica a advogada Fabyola En Rodrigues, sócia de penal empresarial do Demarest.

Também é possível checar suas movimentações financeiras, desde informações de empréstimo até chaves cadastradas no Pix, por meio do Banco Central. Basta entrar no site do Registrato e se registrar para ver sua atividade bancária.

Administrado pelo BC, o Registrato permite que o cidadão tenha acesso a relatórios com informações sobre seus relacionamentos com as instituições nanceiras, suas operações de crédito e operações de câmbio. O Banco Central afirma que o sistema é rápido e seguro.

COMO DEVO ME PROTEGER PARA NÃO CAIR EM GOLPES VIRTUAIS?

A troca de senhas deve ser feita com maior frequência, diz a advogada Tatiana Campello, sócia de privacidade de dados, tecnologia e cibersegurança da Demarest. Campello também recomenda usar sequências fortes, com números, caracteres especiais e alternação entre letras maiúsculas e minúsculas.

“Ative as notificações de gastos no cartão de crédito e outras ferramentas que podem para verificar com periodicidade suas questões financeiras”, lembra a especialista.

Também é comum hackers entrarem em contato com uma possível vítima pedindo senhas, confirmações de cadastro e até mesmo dinheiro –como nos casos em que criminosos se passam por uma pessoa conhecida para pedir valores por meio de aplicativos de conversas.

Uma boa forma de “desmascarar” um golpista é questioná-lo, explica George Bonfim, advogado especializado em direito digital.. “Ele sempre vai deixar uma brecha. O questionamento direto tende a levar a pessoa a titubear, e ele acaba ficando intimidado”.

Alguns sites oferecem serviços para que o internauta descubra se seus dados foram vazados. Especialistas, porém, não recomendam seu uso, porque podem servir como isca para a vítima confirmar que existe de fato. E como o primeiro megavazamento expôs dados de mais de 220 milhões de brasileiros –mais que a população do país, portanto estima-se que foram vazadas informações de pessoas que já morreram–, parta do pressuposto que você também foi vítima.

“Colando seus dados pessoais [em sites que oferecem serviços de checagem], você pode cair em 'phishing'”, diz Bonfim. “Desconfie de links que recebe pelo celular, confira a mensagem antes de clicar e fique atento a ligações que pedem informações pessoais”, recomenda o advogado.

QUAIS SÃO OS GOLPES MAIS COMUNS?

Phishing

O criminoso envia links, emails e SMS com mensagens que, na maioria das vezes, exploram emoções

(curiosidade, oportunidade única, medo etc.), induzindo a vítima a clicar em links e anexos que pegam dados pessoais ou levam a cadastros que roubam informações.

Falso funcionário ou falsa central de atendimento

O estelionatário finge ser funcionário de uma instituição financeira e diz estar com problemas de cadastro ou irregularidades na conta. A vítima fornece informações sobre sua conta e, com isso, o bandido realiza transações fraudulentas.

Falso motoboy

Integrantes de quadrilha ligam para a vítima e dizem pertencerem à central de relacionamento do banco. Afirmam que houve problemas com o cartão da vítima e pedem que ela digite sua senha numérica no teclado do telefone. Na sequência, dizem que enviaram um motoboy na casa da vítima para pegar o cartão. Em posse do cartão e a senha, realizam operações fraudulentas.

Pedidos de dinheiro

Primeiro, os hackers clonam uma conta de app de mensagens, como o Whatsapp. Na sequência, pedem dinheiro a contatos da vítima se passando por ela.