

ESTELIONATO

Golpes virtuais, PREJUÍZOS REAIS

Engenharia social e vazamento de dados alimentam fraudes no país. Por trás de aparelhos eletrônicos, criminosos usam informações pessoais para enganar as vítimas. Especialistas detalham as fraudes mais comuns e dão dicas de como se proteger

» DARCIANNE DIOGO

Por mais de dois meses, uma farmácia de manipulação no Noroeste foi alvo de uma golpista que, com comprovantes falsos de Pix, conseguiu levar produtos no valor de R\$ 9 mil. Tainá Monteiro Neves, 35 anos, fingiu ser cliente e, pelo WhatsApp, solicitava os pedidos em nome de terceiros. O crime foi descoberto após uma investigação interna na empresa. A fraude é mais uma no leque de golpes que começa no ambiente virtual, onde a agilidade das transações e a dificuldade de rastreamento favorecem a ação de estelionatários.

O alvo de Tainá eram garrafas térmicas de uma marca renomada — a unidade custa de R\$ 200 a R\$ 400. Para driblar a conferência de pagamentos, ela usava nomes e telefones diferentes nos pedidos pelo WhatsApp, inclusive, o dela mesma. A estratégia de pagamentos era calculada. “Quando a compra é via Pix, usamos uma plataforma para enviar um link, por meio do qual o cliente paga e podemos verificar. Mas ela, como tinha a chave do nosso Pix, enviava o comprovante falso antes mesmo de as funcionárias enviarem o link de pagamento. Então, tínhamos a crença de ser cliente antiga”, relatou, ao **Correio**, a dona da farmácia, Flávia Ribeiro.

O setor financeiro da empresa descobriu um padrão e constatou a fraude. O caso foi registrado na polícia em 23 de julho. Na semana passada, Tainá tentou aplicar o golpe novamente, para obter três garrafas. Ao ir buscá-las, foi presa em flagrante. “Acionamos a polícia e achávamos que ela tinha descoberto, pois não respondia às mensagens e estava demorando a aparecer. Mas deu certo”, contou Flávia. A ficha criminal da golpista incluiu 13 ocorrências semelhantes. Entre elas, um golpe aplicado em uma clínica de estética do Lago Sul, onde fez procedimentos de R\$ 35 mil sem pagar. Apesar disso, a Justiça concedeu a liberdade a Tainá e impôs medidas cautelares.

Golpe em expansão

Casos como esse se multiplicam no país e atingem vítimas de todas as idades, sobretudo idosos. O delegado-chefe da Delegacia de Combate aos Crimes Cibernéticos (DRCC), João Guilherme, explica que a engenharia social adotada pelos criminosos — narrativas elaboradas para enganar — é carregada de emoção, recheada de detalhes e convincente. “No golpe do WhatsApp, por exemplo, o estelionatário cria um perfil falso e se passa por um familiar para pedir dinheiro. A vítima, acreditando estar ajudando um parente em apuros, transfere quantias elevadas que dificilmente serão recuperadas.”

De acordo com o investigador, criminosos têm usado o chamado sistema VoIP (Voz sobre IP), tecnologia capaz de fazer chamadas telefônicas usando a internet em vez das linhas telefônicas tradicionais. “Eles colocam o número da própria vítima, ou de um banco, no caso do golpe da central de atendimento, por exemplo, e conseguem ludibriar”, destaca.

As investigações também se concentram no combate à matéria-prima dos golpes: o vazamento de dados pessoais. Há plataformas

Material cedido ao Correio



Tainá Monteiro, 35 anos, fingia ser cliente e, pelo WhatsApp, fazia os pedidos em nome de terceiros. Ela foi presa após comprar R\$ 9 mil em uma farmácia com comprovantes falsos de Pix

Três perguntas para

Marco Tulio Castro, advogado especialista em direito digital e sócio do WCV Advogados Associados

Quais são os principais crimes previstos no Código Penal e no Marco Civil da Internet que se aplicam aos golpes virtuais mais comuns?

Existem vários crimes que podem ser caracterizados nos golpes virtuais mais praticados no Brasil atualmente (perfis falsos no WhatsApp; phishing por e-mail e SMS; promoções falsas em redes sociais; falso suporte técnico etc.), dependendo da situação concreta. Podemos mencionar estelionato; invasão de dispositivo informático, se houver invasão de conta/dispositivo para obter dados; falsa identidade, se existir uso de nome ou identidade alheia para obter vantagem; falsificação de documento particular e furto mediante fraude com uso de dispositivo eletrônico ou informático. O Marco Civil da Internet, como o próprio nome estabelece, não prevê crimes específicos, mas estabelece responsabilidades e obrigações aos agentes econômicos que utilizam a internet.

Quando um golpe acontece,

quais provas digitais têm mais peso jurídico para responsabilizar o autor?

É fundamental que as provas digitais sejam coletadas de forma a garantir a sua integridade. Alguns exemplos de provas que possuem elevado valor jurídico em discussões sobre golpes virtuais são registro de acesso a aplicações (logs) e registros de conexão à internet, que podem ser solicitados com fundamento no Marco Civil da Internet. A realização de uma ata notarial (documento lavrado por um tabelião, que descreve um determinado conteúdo digital) pode ser extremamente útil em casos dessa natureza.

Quais medidas a vítima pode adotar para aumentar as chances de recuperar valores — e quando isso é possível?

A vítima deve ter cuidado para preservar as provas, realizar o mais rapidamente possível uma comunicação ao banco, serviço ou operador envolvidos, bem como realizar um registro de ocorrência.

clandestinas que vendem informações confidenciais, como CPF, RG, nomes e telefones de familiares. “As pessoas físicas tendem a ser o alvo dos estelionatários, porque conseguir os dados é mais fácil, embora pessoas jurídicas também sofram com esse tipo de crime”, acrescenta.

Alisson Possa, professor de direito digital do Ibmec Brasília, explica a evolução dos golpes virtuais, que combinam o uso de dados pessoais com a conquista da confiança, fazendo as vítimas

acreditarem que estão em contato com uma empresa real. “Os golpes mais famosos envolvem contatos via WhatsApp ou ligação telefônica, nas quais os criminosos se passam por empresas famosas e, com base em informações reais, induzem as vítimas a realizarem transferências e pagamentos. Outro golpe famoso são as ‘ofertas imperdíveis’ por redes sociais ou e-mail, nas quais o consumidor é direcionado a um site que replica exatamente a empresa/marca original, sendo induzido a fazer compras falsas.”

Artigo

Celular: amigo íntimo, perigo oculto

Sabe aquele aparelhinho que usamos todos os dias? O nosso melhor amigo, que não largamos por nada? Sim, acertou! O nosso celular virou o fiel escudeiro, nosso “bom-dia” pioneiro. Ao despertar, a primeira consulta a aplicativos de mensagens é para ele, antes mesmo de cumprimentar quem dormiu ao nosso lado. Mas, ironicamente, não cuidamos muito bem do nosso amiguinho digital. É como ter um carro de luxo e nunca fazer a revisão. Não atualizamos seu “cérebro” (o sistema operacional), somos desleixados com a segurança, deixando-o desprotegido (com senhas frágeis, por exemplo) e não aplicamos as “vacinas” periodicamente (aplicativos de antivírus).

E tem mais: tudo que falamos no dia a dia pode ficar registrado ali. Sim, ele nos “escuta” e nos direciona a acessar informações baseado no que ele ouviu. Você comenta sobre uma preferência por hambúrgueres e, dias depois, ele já te bombardeia com anúncios de lanchonetes próximas, como se tivesse lido sua mente. Ele “ouviu” sua conversa e determinou sua preferência.

Sabendo de toda essa vulnerabilidade e da



nossa falta de atenção, o crime organizado tem se aproveitado. Roubos de dados que comprometem nossas informações pessoais e financeiras são uma realidade brutal. É um fato: nos últimos anos, bilhões de reais foram roubados de contas correntes de pessoas físicas por meio de fraudes digitais, muitas delas realizadas via WhatsApp. A vítima, acreditando estar ajudando um ente querido em apuros, na verdade está sendo enganada por um fraudador. A manipulação emocional é a ferramenta.

O cidadão deve estar atento aos golpes digitais. Para isso, é crucial seguir algumas práticas que podem blindar você de boa parte desses riscos. Preste atenção a estas dicas essenciais: senhas fortes, duplo fator de autenticação, desconfie de ligações e mensagens, tenha cuidado com links e promoções milagrosas e siga as recomendações de atualização do sistema operacional do seu celular e dos aplicativos. O “inocente” celular, que nos acompanha em cada passo, pode se tornar, sem a devida atenção, a porta de entrada para esses perigos. Sua segurança digital começa e termina com você. Desconfie, eduque-se e proteja seu melhor amigo.

Eduardo Nery, CEO da Every Cybersecurity e especialista em proteção de dados

Saída

Após o golpe, a empresária Flávia Ribeiro padronizou o serviço via Pix. “Agora, só efetuamos a venda dessa forma quando a nossa funcionária envia o link de pagamento ao cliente”, afirma. O protocolo é o mesmo adotado por Victor Melo Bijos, 29, dono da Pure Pizza, no Guará 2, para evitar possíveis golpes.

O empresário trabalhava somente com delivery e não tinha um sistema que garantisse a

segurança para pagamentos via Pix. A partir de 2022, com a abertura da loja física, optou pelo investimento de R\$ 399 mensal. “O sistema que uso só autoriza o pedido após a transação pelo link. Conseguimos ver a entrada do dinheiro na hora. Não vejo como um gasto, mas como investimento. Coloquei para não correr o risco de não receber”, afirma.

O professor Alisson dá algumas dicas. Uma delas é estar atento a qualquer tentativa de cobranças via WhatsApp ou ligação.

“O ideal é sempre buscar a empresa diretamente por meio dos sites ou aplicativos oficiais para verificar a veracidade das cobranças. Para os golpes de sites falsos, é importante verificar se o endereço do site é realmente o oficial.” Ao perceber que caiu em uma armadilha, o primeiro passo, segundo ele, é entrar em contato com o banco para relatar o caso e solicitar a devolução dos valores transferidos para o suposto golpista, além de registrar o boletim de ocorrência.