

FEBRABAN**Febraban**
news

21/09/2020



Conheça as tentativas de golpes financeiros mais comuns na pandemia e saiba como evitá-los

[MAIS NOTÍCIAS](#)

No período de isolamento social, bancos registraram aumento de 80% nas tentativas de ataques de phishing, alta de 70% na fraude do falso funcionário e crescimento de 65% no golpe do motoboy; tipificação de crime digital é necessária para coibir delitos

Com a pandemia do novo coronavírus, criminosos estão aproveitando o maior tempo online das pessoas e o aumento das transações digitais devido ao isolamento social para aplicar golpes financeiros. Mensagens de ofertas tentadoras e atrativas que, na verdade, direcionam para sites falsos, ou ainda o uso de avisos para que a pessoa recadastre urgentemente seus dados junto a uma instituição, escondem crimes que levam muita dor de cabeça e causam grande prejuízo financeiro para o consumidor.

Levantamentos feitos pela FEBRABAN (Federação Brasileira de Bancos) mostram o crescimento de tentativas de várias modalidades de fraudes financeiras contra os brasileiros durante a crise da Covid-19. No período de quarentena, as instituições registraram aumento de 80% nas tentativas de ataques de *phishing* - que se inicia por meio de recebimento de e-mails que carregam vírus ou links e que direcionam o usuário a sites falsos, que, normalmente, possuem remetentes desconhecidos ou falsos.

O golpe do falso motoboy teve aumento de 65% durante o período de isolamento social. Já os golpes do falso funcionário e falsas centrais telefônica cresceram 70%. Recentemente, a FEBRABAN também revelou que no período da quarentena houve alta de 60% em tentativas de golpes financeiros contra idosos, o que resultou em uma campanha de alerta com o

apoio da Secretaria Nacional de Promoção e Defesa dos Direitos da Pessoa



Ministério da Mulher, da Família e dos Direitos Humanos,



FEBRABAN e seus bancos investem constantemente em campanhas e ações de conscientização em seus canais de comunicação com os clientes para orientar a população a se prevenir de fraudes. “Queremos contribuir para o desenvolvimento de uma cultura de prevenção a fraudes e do uso seguro dos canais digitais no país”, afirma Isaac Sidney, presidente da FEBRABAN.

Ele ressalta que os bancos investem cerca de R\$ 2 bilhões por ano em sistemas de tecnologia da informação (TI) voltados para segurança – valor que corresponde a cerca de 10% dos gastos totais do setor com TI para garantir a tranquilidade de seus clientes em suas transações financeiras cotidianas.

Atualmente, 70% das fraudes estão vinculadas à engenharia social, que consiste na manipulação psicológica do usuário para que ele lhe forneça informações confidenciais, como senhas e números de cartões para os criminosos. “Seja pelo telefone, por e-mail, pelas mídias sociais, SMS, o fraudador solicita dados pessoais do cliente, como números de cartões e senhas, em troca de algo, ou ainda induz o usuário a ter medo de alguma situação”, alerta Adriano Volpini, diretor da Comissão Executiva de Prevenção a Fraudes da FEBRABAN. “Os dados pessoais do cliente jamais são solicitados ativamente pelas instituições financeiras. Na dúvida, sempre procure seu banco para obter esclarecimentos.”

Entretanto, adverte que a população tem um comportamento de segurança no mundo digital diferente do mundo físico, em que as pessoas já se acostumaram a tomar cuidados com carteiras, pertences e celulares, quando estão em locais públicos e de grande movimentação. Conscientemente, as pessoas sabem o que podem ou não podem fazer, discernimento não tão comum no mundo digital.

Outro ponto que merece atenção no combate aos golpes financeiros é a ausência de uma lei federal que tipifique os crimes cometidos pelos meios digitais, o que gera grande prejuízo para toda a população brasileira, empresas privadas e o setor público. Atualmente, três projetos tramitam no Congresso, entre eles, o 2.638, que dispõe sobre a tipificação criminal de furto mediante fraude eletrônica, do deputado Marcelo Ramos (PR/AM).

“A certeza da impunidade gera um incentivo e um impulso ainda maior para que o crime aconteça. Caso o PL seja aprovado, existirá muito mais subsídios e condições de gerar uma punição mais efetiva contra os criminosos”, afirma Volpini.

Conheça os principais golpes aplicados e como eles devem ser evitados

FEBRABAN



Golpe do Falso Funcionário do banco

news

O que é: O fraudador entra em contato com a vítima se passando por um falso funcionário do banco ou empresa com a qual o cliente tem um relacionamento ativo. O criminoso informa que há irregularidades na conta ou que os dados cadastrados estão incorretos. A partir daí, solicita os dados pessoais e financeiros da vítima. Com os dados em mãos, o fraudador realiza transações fraudulentas em nome do cliente.

Como evitar: O cliente deve sempre verificar a origem das ligações e mensagens recebidas contendo solicitações de dados. É importante ressaltar que o banco nunca liga para o cliente pedindo senha nem o número do cartão e também nunca liga para pedir para realizar uma transferência ou qualquer tipo de pagamento. Ao receber uma ligação suspeita, o cliente deve desligar, pegar o número de telefone que está no cartão e ligar de outro telefone para tirar a limpo essa história.

Phishing (pescaria digital)

O que é: O phishing, ou pescaria digital, é uma fraude eletrônica cometida pelos engenheiros sociais que visa obter dados pessoais do usuário. A forma mais comum de um ataque de phishing são as mensagens e e-mails falsos que induzem o usuário a clicar em links suspeitos. Também existem páginas falsas na internet que induzem a pessoa a revelar dados pessoais. Os casos mais comuns de phishing são e-mails recebidos de supostos bancos com mensagens que afirmam que a conta do cliente está irregular, ou o cartão ultrapassou o limite, ou que necessita revalidar seus pontos nos programas de fidelidade, atualizar token ou, ainda, que existe um novo software de segurança do banco que precisa ser instalado imediatamente pelo usuário.

Como evitar: Sempre verifique se o endereço da página de internet é o correto. Para garantir, não clique em links: digite o endereço no navegador. Além disso, nunca acesse links ou anexos de e-mails suspeitos. Mantenha seu sistema operacional e antivírus sempre atualizados. Sempre prefira comprar em sites conhecidos, e nunca use computadores públicos para comprar algo no comércio virtual. Não repasse a outra pessoa nenhum código fornecido por SMS ou imagem de um QR Code enviado para autenticar alguma operação. Na dúvida, fale com seu banco.

Golpe do falso motoboy



O que é: O golpe começa com uma ligação ao cliente, de uma pessoa que se apresenta como funcionário do banco, e diz que o cartão foi clonado, informando que o cartão deve ser cancelado. Para isso, diz o golpista, bastaria cortá-lo ao meio e enviar o pedaço restante pelo atendimento eletrônico. O falso funcionário pede que a senha seja digitada no telefone, e fala que, por segurança, um motoboy irá buscar o cartão para uma perícia. O que o cliente não sabe é que, com o cartão cortado ao meio, o chip permanece intacto, e é possível realizar diversas transações.

Como evitar: Fique atento! Nenhum banco pede o cartão de volta ou envia qualquer pessoa ou portador para retirar o cartão na casa dos clientes. Então, desligue o telefone e ligue, de outro aparelho, para o banco, para verificar se realmente houve alguma irregularidade.

Golpe do falso leilão

O que é: O fraudador envia um link à vítima que simula um falso leilão. Para que possa ser dado um lance, a vítima tem que preencher formulários com seus dados pessoais e financeiros ou depositar um valor na conta do fraudador. Com dados como senha, número do cartão e CPF, o fraudador consegue fazer transações fraudulentas em nome do cliente.

Como evitar: O cliente nunca deve enviar dados, senhas e acessos a ninguém. É necessário sempre verificar a origem dos links recebidos antes de clicá-los. Além disso, deve-se verificar a veracidade do site de leilão e avaliações de outros usuários.

Golpe do WhatsApp

O que é: Os golpistas descobrem o número do celular e o nome da vítima de quem pretendem clonar a conta de WhatsApp. Com essas informações em mãos, os criminosos tentam cadastrar o WhatsApp da vítima nos aparelhos deles. Para concluir a operação, é preciso inserir o código de segurança que o aplicativo envia por SMS sempre que é instalado em um novo dispositivo. Os fraudadores enviam uma mensagem pelo WhatsApp fingindo ser do Serviço de Atendimento ao Cliente do site de vendas ou da empresa em que a vítima tem cadastro. Eles solicitam o código de segurança, que já foi enviado por SMS pelo aplicativo, afirmando se tratar de uma atualização, manutenção ou confirmação de cadastro. Com o código, os bandidos conseguem replicar a conta de WhatsApp em outro celular. A partir daí, os criminosos enviam mensagens para os contatos da pessoa, fazendo-se passar por ela, pedindo dinheiro emprestado.

Como evitar: Uma medida simples para evitar que o WhatsApp seja clonado é

FEBRABAN ativo, a opção “Verificação em duas etapas”
(Configurações > Conta > Verificação em duas etapas). Desta forma, é
Febraban necessário criar uma senha que será solicitada periodicamente pelo app.
news Essa senha não deve ser enviada para outras pessoas ou digitadas em links
recebidos.

Golpe do extravio do cartão

Como é: No trâmite de entrega do cartão até a vítima, fraudadores furtam a correspondência contendo este cartão. Depois, ligam para a vítima se passando por um funcionário do respectivo banco informando que houve problemas na entrega do cartão. Para a resolução deste suposto problema, solicitam à vítima a senha deste cartão. Com os dados descobertos, fazem transações em nome da vítima.

Como evitar: O cliente nunca deve enviar dados, senhas e acessos a ninguém. Também nunca deve preencher formulários na internet com dados pessoais e financeiros sem verificar a origem. Caso o prazo de entrega do cartão se esgote, é preciso informar o gerente sobre o atraso.

Golpe do delivery

Como é: O cliente faz seu pedido via aplicativo. O entregador apresenta uma maquininha com o visor danificado ou de uma forma que impossibilite a visualização do preço cobrado na tela, sendo um valor acima do real cobrado. Só depois de algum tempo, a vítima percebe que efetuou um pagamento elevado.

Como evitar: O cliente deve sempre checar o preço cobrado no visor da maquininha e nunca deve aceitar maquininhas onde os valores que são cobrados não estejam visíveis. De preferência em fazer o pagamento via aplicativo e não no momento da entrega.

FEBRABAN – Federação Brasileira de Bancos

Diretoria de Comunicação
imprensa@febraban.org.br

FEBRABAN

Febraban
news



Av. Brig. Faria Lima, 1.485 - 14º andar • CEP.: 01452-002 - São Paulo • PABX .: 55 11 3244 9800 / 3186 9800

© FEBRABAN - Todos os direitos reservados