No Golpe do Acesso Remoto, também conhecido como Golpe da Mão Fantasma, criminoso entra em contato com a vítima se passando por um falso funcionário do banco e pede a instalação de um aplicativo no celular para verificar falsas irregularidades na conta do cliente

Com a crescente digitalização da sociedade, os criminosos têm aproveitado o crescimento exponencial das operações digitais para aplicar golpes na população. Destacam-se os crimes que usam a 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, ou faça transações em favor das quadrilhas.

Entre eles está o Golpe do Acesso Remoto, também conhecido como Golpe da Mão Fantasma. O fraudador entra em contato com a vítima se passando por um falso funcionário do banco. Usa várias abordagens para enganar o cliente: informa que a conta foi invadida, clonada, que há movimentações suspeitas, entre outras artimanhas. E diz que vai enviar um link para a instalação de um aplicativo que irá solucionar o problema. Se o cliente instalar o aplicativo, o criminoso terá acesso a todos os dados que estão no celular.

A FEBRABAN esclarece que os aplicativos dos bancos contam com o máximo de segurança em todas as suas etapas, desde o seu desenvolvimento até a sua utilização. Não há registro de violação da segurança desses aplicativos, os quais contam com o que existe de mais moderno no mundo para este assunto. Além disso, para que os aplicativos bancários sejam utilizados, há a obrigatoriedade do uso da senha pessoal do cliente.

No caso do Golpe do Acesso Remoto, os criminosos realizam pesquisas no aparelho buscando por senhas eventualmente armazenadas pelos próprios usuários em aplicativos e sites.

Muitos usuários anotam suas senhas de acesso ao banco em blocos de notas, e-mails, mensagens de Whatsapp ou em outros locais do celular. Também há casos de clientes que usam a mesma senha de acesso do banco em outros aplicativos, sites de compras ou serviços na internet, e estes apps, em grande parte dos casos, não contam com sistemas de segurança robustos e a proteção adequada das informações dos usuários.

“O banco nunca liga para o cliente pedindo para que ele instale nenhum tipo de aplicativo em seu celular. Também nunca liga pedindo senha nem o número do cartão ou ainda para que o cliente faça uma transferência ou qualquer tipo de pagamento para supostamente regularizar um problema na conta”, alerta Adriano Volpini, diretor do Comitê de Prevenção a Fraudes da FEBRABAN.

“Se receber esse tipo de contato, desconfie na hora. Desligue e entre em contato com a instituição através dos canais oficiais e de um outro telefone para saber se algo aconteceu mesmo com sua conta”, acrescenta Volpini.

Campanhas de conscientização

A FEBRABAN e seus bancos investem constantemente e de maneira massiva em campanhas e ações de conscientização em seus canais de comunicação com os clientes para orientar a população a se prevenir de fraudes. Nas redes da Federação, a comunicação antifraudes e golpes prossegue de forma ininterrupta por meio do site https://antifraudes.febraban.org.br/.

Além da realização de campanhas educativas, os bancos investem cerca de R$ 3 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.

Os bancos associados também contam com o que há de mais moderno em relação à segurança

cibernética e prevenção a fraudes, como mensageria criptografada, autenticação biométrica, tokenização, e usam tecnologias como big data, analytics e inteligência artificial em processos de prevenção de riscos. Estes processos são continuamente aprimorados, considerando os avanços tecnológicos e as mudanças no ambiente de riscos.

Adicionalmente, os bancos também atuam em parceria com forças policiais para auxiliar na identificação e punição de criminosos virtuais. Desde 2015, a FEBRABAN fechou um acordo de cooperação técnica com a Polícia Federal, chamado Operação Tentáculos, para o combate às fraudes eletrônicas bancárias. Neste período, através dos trabalhos de inteligência e investigação da Polícia Federal, já foram deflagradas mais de 60 operações como Boleto Real, BR 153, Creeper, Valentina, entre outras.

Conheça outros golpes aplicados pelos criminosos e como eles devem ser evitados

Golpe do Falso Motoboy

Como é

O golpe começa quando o cliente recebe uma ligação do golpista que se passa por funcionário do banco, dizendo que o cartão foi fraudado. O falso funcionário solicita a senha e pede que o cartão seja cortado, mas que o chip não seja danificado. Em seguida, diz que o cartão será retirado na casa do cliente. O outro golpista aparece onde a vítima está e retira o cartão. Mesmo com o cartão cortado, o chip está intacto e os fraudadores podem utilizá-lo para fazer transações e roubar o dinheiro da vítima.

Como evitar

Fique atento! Os bancos nunca pedem o cartão de volta nem mandam portadores até a sua casa para buscá-lo. Se receber esse tipo de ligação ou visita, não entregue nada para ninguém e ligue imediatamente para o seu banco, de preferência de um celular, para saber se existe algum problema com a sua conta.

Golpe da Falsa Central de Atendimento

Como é

O fraudador entra em contato com a vítima se passando por um falso funcionário do banco ou empresa com a qual ela tem um relacionamento ativo. Informa que sua conta foi invadida, clonada ou outro problema e, a partir daí, solicita os dados pessoais e financeiros da vítima. E até mesmo pede para que ela ligue na central do banco, no número que aparece atrás do seu cartão, mas o fraudador continua na linha para simular o atendimento da central e pedir os dados da sua conta, dos seus cartões e, principalmente, a sua senha quando você a digitar.

Como evitar

Se receber esse tipo de contato, desconfie na hora. Desligue e entre em contato com a instituição através dos canais oficiais, de preferência usando o celular ou aplicativos móveis, para saber se algo aconteceu mesmo com sua conta. 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.

Golpe no WhatsApp

Como 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, têm acesso a todo o histórico de conversas e contatos. A partir daí, os criminosos enviam mensagens para os contatos, passando-se pela pessoa, pedindo dinheiro emprestado.

Desconfie de pessoas pedindo dinheiro ou seus dados por aplicativos de mensagem. Geralmente os golpistas apelam para alguma urgência falsa e pedem depósitos e transferências via Pix para contas de terceiros ou então para pagar alguma conta.

Como evitar

Primeiro, proteja o seu WhatsApp de invasões e clonagens. Nas configurações do aplicativo, clique em “Conta”, depois em “Confirmação em Duas Etapas” e ative essa funcionalidade de segurança com uma senha. Você diminui a chance de golpistas roubarem seu número. E nas configurações de privacidade, deixe a sua foto de perfil pública apenas para os seus contatos, assim ninguém a utiliza para golpes. Nunca compartilhe o código de segurança. E caso receba mensagens de parentes ou conhecidos pedindo dinheiro emprestado, confirme a identidade de quem está do outro lado.

Golpe da troca do cartão

Como é

Golpistas que trabalham como vendedores prestam atenção quando você digita sua senha na máquina de compra e depois trocam o cartão na hora de devolvê-lo. Com seu cartão e senha, fazem compras usando o seu dinheiro. O mesmo pode acontecer com desconhecidos oferecendo ajuda no caixa eletrônico. Eles se aproveitam de alguma dificuldade sua no terminal eletrônico para pegar rapidamente o seu cartão e depois devolver um que não é seu, ao mesmo tempo que espiam sua senha.

Como evitar

Fique sempre atento na hora das compras. Confira se é mesmo o seu nome impresso no cartão devolvido e, se possível, passe você mesmo o cartão na maquininha em vez de entregá-lo para outra pessoa. Nos caixas eletrônicos, procure funcionários do banco devidamente uniformizados, não aceite ajuda de desconhecidos.

Golpe do link falso

Como é

Um golpe em que normalmente ofertas muito atrativas chegam por e-mail ou redes sociais como iscas para que os usuários informem seus dados como número de CPF, conta, cartões e senhas. Essas mensagens também podem instalar vírus e aplicativos que roubam seus dados por meio de links maliciosos, permitindo os golpistas acessarem todas as suas contas.

Como evitar

Desconfie de mensagens que você não pediu ou aprovou, e de ofertas em que o desconto é tentador demais. Fique atento ao e-mail do remetente, empresas de grande porte não utilizam contas privadas como @gmail, @hotmail ou @terra e entidades públicas sempre usam @gov.br ou

@org.br. Em caso de links, confira se o endereço da página corresponde ao correto. Em caso de dúvida, não clique.

Golpe do falso leilão

Como é

Golpistas criam sites falsos de leilão, anunciando todo tipo de produto por preços bem abaixo do mercado. Depois pedem transferências, depósitos e até dinheiro via Pix para assegurar a compra. Geralmente apelam para a urgência em fechar o negócio, dizendo que você pode perder os descontos. Mas nunca entregam as mercadorias pagas. Além disso, os fraudadores podem se aproveitar para roubar informações importantes como CPF e número de conta das vítimas.

Como evitar

Sempre pesquise sobre a empresa de leilões em sites de reclamação e confira o CNPJ do leiloeiro. Nunca faça transações financeiras em sites que não tenham o cadeado de segurança no navegador e certificados digitais para transações, nem faça transferências para contas de pessoas físicas.

Golpe do falso empréstimo

Como é

Organizações criminosas se passam por falsas instituições financeiras e oferecem empréstimos com condições muito vantajosas para o consumidor. As quadrilhas fazem anúncios em sites na internet e oferecem crédito, com condições muito atrativas, inclusive, prometem liberação fácil de dinheiro para consumidores negativados. Quando o interessado preenche o cadastro nestes sites fraudulentos, os bandidos entram em contato e pedem que ele assine um suposto contrato, mas, sem que o usuário perceba, colocam cláusulas impondo multas, caso haja desistência. Para que o falso empréstimo seja liberado, os bandidos pedem o pagamento de taxas e impostos e dizem que a prática é normal.

Como evitar

A FEBRABAN alerta que não existe nenhum tipo de empréstimo em que a pessoa tenha que fazer qualquer tipo de pagamento antecipado, seja de impostos, de preenchimento de cadastro ou de supostos adiantamentos de parcelas, e esclarece que este tipo de abordagem é fraude. Em todas as operações de crédito regulares, o cliente recebe o dinheiro e não tem que pagar nada para obter o empréstimo. Desconfie de sites na internet que ofereçam crédito com condições vantajosas. Sempre pesquise e verifique se a instituição é autorizada pelo Banco Central a oferecer empréstimos

Fonte: FEBRABAN, em 26.08.2022