ESTADO DE MINAS

Publicado em 17/06/2024 - 05:55

Caminhos para escapar de fraudes e golpes bancários

COMO EVITAR GOLPES

Paulinho Miranda

CARTÃO
Nunca entregue seu cartão a ninguém. Os bancos não pedem os cartões de volta, mesmo se houver a possibilidade de fraude ou defeito.

COMPRAS
Ao terminar de realizar uma compra na maquininha, verifique o nome no cartão e o valor.

SEGURANÇA
Ative duplo fator de autenticação.Sempre ative a função de segurança "duplo fator de autenticação" em suas contas na internet.

LIGAÇÕES
Se receber contato em nome do banco solicitando para ligar para sua Central de Atendimento, ligue a partir de outro aparelho e nunca forneça sua senha para o atendente.

LINKS
Nunca clique em links desconhecidos. Sempre confira a origem das mensagens ao receber promoções e e-mails que se dizem do banco.

ONLINE
Cuidado em compras online. Dê preferência a sites conhecidos e confira sempre se o endereço do site é o verdadeiro.

PIX
Sempre confira o nome do recebedor ao pagar um boleto, realizar transferências ou Pix.

CAIXA ELETRÔNICO
Nunca envie fotos, vídeos ou capturas de tela pelo celular. Se precisar de auxílio no caixa eletrônico, peça ajuda a um funcionário do banco.

O REPERTÓRIO VARIADO DOS ESTELIONATÁRIOS

ALESSANDRA MELLO E THIAGO BONNA

As tentativas de golpe bancário envolvendo cartão e pix viraram uma rotina na vida do cidadão brasileiro em um mundo cada vez mais virtual. Diariamente, criminosos ligam para potenciais vítimas, a partir de números diversos de telefone, simulando gravações de centrais de atendimento ao cliente de instituições bancárias. Outra artimanha já conhecida é o envio de informações via mensagem para induzir a transferência de valores para contas dos golpistas.

Só em Minas Gerais, foi registrado um aumento de 39,7% nos crimes de estelionato virtual, de acordo com dados do Anuário de Segurança Pública, publicado no ano passado pelo Fórum Brasileiro de Segurança Pública com dados de 2022. Conforme o documento, cerca de 35 mil pessoas foram vítimas no estado de golpes na internet, inclusive via redes sociais, no intervalo de tempo mencionado, contra aproximadamente 25 mil casos registrados no relatório anterior, divulgado com informações de 2021.

Em todo o Brasil, foram registradas 200 mil ocorrências da modalidade em 2022, ante um consolidado de 120 mil no ano anterior, uma diferença percentual de 66%. Os números, no entanto, apresentam limitações, pois não há informações públicas fornecidas por seis estados: Bahia, Ceará, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul e São Paulo.

Dados do Banco Central também revelam um volume elevado de fraudes envolvendo o pix, o meio de pagamento mais usado hoje no país. Foram 2,5 milhões de casos no ano passado.

Para tentar prevenir as fraudes, a Federação Brasileira de Bancos (Febraban) e o Banco Central lançaram campanhas educativas. As entidades também criaram um guia alertando para as fraudes mais comuns usadas pelas quadrilhas.

> AO MESMO TEMPO QUE TRAZEM PRATICIDADE, NOVAS TECNOLOGIAS SIGNIFICAM TERRENO FÉRTIL PARA CRIMINOSOS. NÚMERO DE GOLPES VIRTUAIS CRESCEU 40% EM MINAS GERAIS E 66% NO BRASIL

Se os esforços do crime organizado aumentam a cada ano, é preciso prevenção. A orientação principal passa por nunca fornecer quaisquer dados por telefone ou mensagem e sempre desconfiar de qualquer contato, pois os bancos nunca ligam para o cliente pedindo informações pessoais, senhas, atualizações de sistemas, chaves de segurança ou qualquer tipo de pagamento para supostamente regularizar dívidas.

"Ao receber uma ligação suspeita solicitando senhas ou dados pessoais, desligue imediatamente e, de outro telefone, entre em contato com os canais oficiais do seu banco", alerta José Gomes, diretor do Comitê de Prevenção a Fraudes da Febraban.

Segundo ele, a Federação Brasileira de Bancos tem investido recursos em tecnologia para evitar as fraudes, além de manter uma parceria com a Agência Nacional de Telecomunicações (Anatel) para bloquear os números de telefone usados nos golpes da falsa central telefônica.

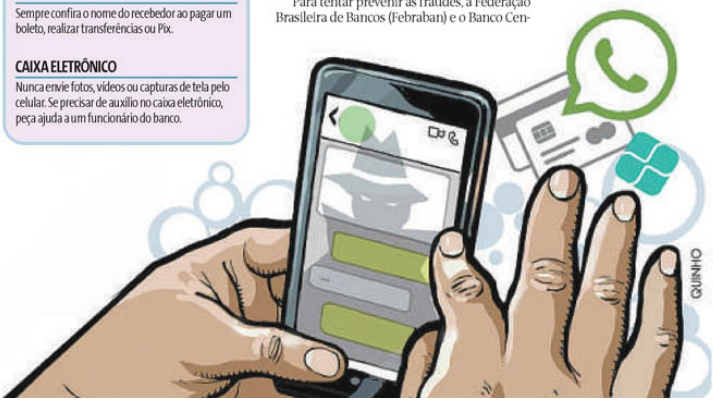
O advogado, criminólogo e policial reformado Jorge Tassi, especialista em casos de estelionato, afirma que o mais importante para evitar fraudes é sempre desconfiar, prestar atenção nos detalhes, não agir de impulso e nunca repassar dados pessoais.

"Entre no site ou aplicativo do seu banco; entre no site que você vai fazer uma compra ou doação; analise; pesquise os links; não acredite em preços muito aquém do mercado; e nunca forneça dados de sua conta para desconhecidos", afirma.

Em suma, é preciso sempre duvidar de quem pede dados ou algo antes para oferecer a solução depois, destaca o especialista. Em relação aos golpes em que estelionatários se passam por pessoas da família, a dica é sempre pedir um tempo e ligar na sequência para o familiar para conferir se é ele mesmo quem está pedindo doações, pagamentos ou transferências.

No caso de golpe, ele recomenda que a vítima nunca apague mensagens no WhatsApp, e-mails ou conversas, pois elas podem servir de prova para tentar reaver valores juntos às instituições bancárias. "Se você tomou todas as medidas de precaução a chance de conseguir reaver os valores na Justiça é maior", assegura.

Outra dica, segundo ele, é agir de imediato e nunca deixar para outro dia. "Enquanto você espera, o estelionatário está na boca do caixa esperando para sacar o dinheiro", diz. Entre seus clientes, afirma Tassi, as maiores vítimas são quase sempre pessoas idosas que não dominam as ferramentas da tecnologia. Para ele, quanto mais informação a população tiver sobre golpes, menos sucesso os estelionatários terão.



QUINHO

►►►

GOLPE DO PIX

Esses cuidados ajudam a prevenir golpes como o sofrido por um advogado que pediu anonimato à reportagem do EM. Ele foi informado de uma suposta transação suspeita em sua conta e, para bloqueá-la, teria que ler um QR Code enviado por mensagem no celular. Ao realizar essa operação, a vítima foi enganada e fez um depósito na conta do golpista. O dinheiro, cerca de R$ 5 mil, nunca foi recuperado.

Caso também de uma aposentada, que também preferiu não se identificar. Ela afirmou ter recebido uma mensagem em seu telefone celular de uma pessoa se passando por seu filho. Minutos após o primeiro contato, o golpista disse que estava com a conta travada e pediu para que ela pagasse uma conta, enviando um código do pix. Ela fez o pagamento e só depois descobriu que se tratava de um golpe.

DEVOLUÇÃO DO DINHEIRO

Em alguns casos é possível reaver o dinheiro, mas, para isso, é muito importante fazer a comunicação do golpe o mais rápido possível. No caso do pix, o Banco Central criou, em 2021, uma ferramenta batizada de Mecanismo Especial de Devolução (MED) para facilitar estornos em caso de fraudes, o que aumenta as possibilidades de recuperar recursos em transações feitas pela ferramenta de pagamento instantâneo. O prazo máximo para comunicação é de 80 dias.

Ao fazer o comunicado do golpe, via aplicativo, telefone ou pessoalmente na agência bancária, no prazo mais rápido possível, os recursos são bloqueados na conta do recebedor para análise detalhada do caso.

Se o banco concluir que houve fraude, as quantias são devolvidas à vítima. Entretanto, essa devolução está condicionada à existência de valores na conta do fraudador, ou seja, a instituição financeira não paga a vítima com recursos próprios.

Na última quinta-feira (13), o Banco Central e a Febraban anunciaram que estão estudando conjuntamente melhorias no Mecanismo Especial de Devolução, que envolvam o bloqueio de valores triangulados, ou seja, passados pelo golpista de uma conta para a outra para dificultar o rastreio do dinheiro.

A proposta da Febraban é que seja feito o bloqueio de valores nessa triangulação de contas. O objetivo é reduzir a prática das diferentes modalidades de fraudes e golpes utilizando o pix como meio.

"Já observamos que os criminosos espalham o dinheiro proveniente de golpes e outros crimes em várias contas, de forma muito rápida. Por isso, é importante aprimorar o sistema para que ele atinja mais camadas", afirma Walter Faria, diretor-adjunto de Serviços da Febraban. Batizado de MED 2.0, o projeto foi proposto pela federação e será deseknvolvido até 2025. Assim, a implementação seria feita em 2026, conforme o cronograma da entidade. ■

GOLPES SEM FIM

CONFIRA COMO AGEM OS BANDIDOS

GOLPE DA FALSA CENTRAL DE ATENDIMENTO
O golpista liga para a vítima fingindo ser funcionário de um banco ou empresa e informa que a conta da pessoa foi invadida, clonada ou que apresenta outro problema. Para solucionar, ele pede dados pessoais e financeiros. Em alguns casos, ele pede que ligue na central do banco, no número que aparece atrás do cartão, mas não desliga a primeira ligação e simula ser da central pedindo dados da conta, dos cartões e a senha.

GOLPE DO LINK FALSO
A vítima clica em um link de origem desconhecida ou de baixa credibilidade que foi enviado por e-mail, redes sociais, por aplicativo de mensagem, como o WhatsApp ou Telegram; ou sites falsos. Ao acessar esses links maliciosos, são usados subterfúgios para que a pessoa coloque seus dados bancários.

GOLPE DO FALSO BOLETO
Um boleto falso chega para a vítima, seja por correspondência, e-mail - sendo possível até direcionar para páginas falsas que farão o download - ou aplicativo de mensagens, podendo ser de banco ou mesmo de uma loja. A vítima paga, mas o valor vai para o golpista e não para o verdadeiro credor.

GOLPE NO WHATSAPP
Os golpistas cadastram um número de WhatsApp no aparelho deles. Para prosseguir na operação, o aplicativo pede um código de segurança que é enviado para o número real. Precisando disso, eles entram em contato com a vítima se passando como SAC e solicitam o código. Se entregue, eles clonam o perfil da vítima e pedem dinheiro ou dados para os contatos dela.

GOLPE DO FALSO MOTOBOY
O golpista liga se passando por um funcionário do banco alertando que o seu cartão foi clonado. Ele solicita a senha, pede que o cartão seja cortado, mas que não destrua o chip. Em seguida, ele diz que um funcionário passará na casa do cliente para recolher o cartão cortado. Como o chip não foi danificado, pode ser usado normalmente.

Paulinho Miranda

ROUBO DE CELULARES
O criminoso rouba o celular da vítima e, além da perda do aparelho, os dados guardados no telefone podem ser usados para retirar dinheiro da conta ou contrair empréstimos.

GOLPE DA MAQUININHA QUEBRADA
O vendedor ou entregador de delivery golpista, na hora de cobrar pelo cartão, apresenta um equipamento com o visor danificado ou que dificulte a visualização do valor cobrado. A vítima, distraída ou com pressa, coloca a senha e só depois percebe que a cobrança foi de um valor muito superior ao que deveria ter sido cobrado. Em alguns casos, o golpista convence a vítima que houve um erro na cobrança ou que existe um frete pela entrega e cobra um valor a mais.

GOLPE DO FALSO LEILÃO
Golpistas criam sites de leilões falsos e anunciam itens com valores bem abaixo do mercado. Eles pedem que os "compradores" paguem rapidamente, usando transferências, depósitos ou mesmo PIX, com a justificativa que é para não perder os descontos. Os produtos nunca são entregues.

GOLPE DO FALSO PRESENTE
Comum em datas especiais, um entregador golpista chega em sua casa e fala que enviou um presente para você, mas cobra uma "taxa" para entregar o item. Na máquina, usa a mesma prática do 'golpe da maquininha quebrada'.

SENHAS EM AGÊNCIAS BANCÁRICAS
Golpistas se passam por funcionários de banco e ficam atentos quando a pessoa digita a senha no caixa eletrônico. Também podem roubar seu celular para buscar informações bancárias guardadas no aparelho

GOLPE DO FALSO EMPRÉSTIMO
Golpistas fazem anúncios nas redes sociais de empréstimos em condições muito atrativas simulando instituições bancárias e financeiras. Quando a pessoa preenche o cadastro, os criminosos enviam um contrato falso e pedem o pagamento de uma taxa para liberação do valor.

ACESSO REMOTO AO CELULAR
O golpista se passa por um funcionário de banco e afirma que teve movimentações suspeitas na conta da vítima. Para solucionar ele pede para que seja instalado um aplicativo. Quando o aplicativo é instalado, todos os dados que estão no celular ficam disponíveis.

GOLPE DA TROCA DE CARTÃO
O vendedor golpista fica de olho enquanto o cliente digita sua senha na máquina e troca o cartão ao devolvê-lo para a vítima. A prática também pode acontecer em quem oferece ajuda em caixa eletrônico

Veículo: Impresso -> Jornal -> Jornal Estado de Minas - Belo Horizonte/MG

Seção: Economia **Pagina:** 10 e 11

Copyright © Clipclap 2025.