

Pina Maciel: Como se proteger de golpes de internet

24/08/2022

Já virou lugar comum conhecer alguém que já foi vítima de um golpe na internet. As modalidades são diversas, assim como as artimanhas usadas pelos criminosos para convencer suas vítimas.



Todos os dias se vê o post de algum amigo

compartilhando um print de Whatsapp, informando que alguém está se passando por ele para pedir dinheiro (sempre através do sistema Pix).

Pois bem, aqui falaremos um pouco sobre os tipos mais conhecidos de golpes, como se proteger e o que fazer após perceber que caiu num golpe.

Modalidade de golpes

Antes de falar os tipos de golpes, é bom esclarecer que todos eles são sempre fundamentados em pelo menos um dos três pilares a seguir:

Ganância, medo ou ingenuidade.

E todos exaltarão o senso de urgência para finalizar a negociação.

A falsa venda de móveis ou produtos de casa

Nesse golpe os criminosos normalmente hackeiam uma conta de rede social e fazem alguns posts com a informação de que a pessoa estaria de mudança, normalmente para fora do estado ou do país, e por essa razão precisa se desfazer de vários itens da casa.

Via de regra os valores anunciados são bem abaixo do que se espera para aqueles produtos, mesmo sendo usados. Como justificativa o golpista alega que a viagem está muito próxima e que precisa se desfazer de tudo aquilo com urgência, causando uma falsa sensação de segurança na negociação.

Aqui as vítimas e potencial são os amigos menos próximos, que não teriam a informação da mudança em primeira mão e achariam normal ficar sabendo pela internet. Além disso é muito comum que os criminosos analisem as conversas comuns na conta da pessoa hackeada, para entender a forma mais comum de diálogo dessas pessoas com seus amigos, de modo que ao entrar em contato com as vítimas, elas não percebam a diferença no jeito de conversar. Nessa modalidade os criminosos exploram a *ganância e a ingenuidade* das vítimas, oferecendo negociação extremamente vantajosa.

Para evitar cair nessa cilada, bastam poucas atitudes:

- Pergunte a alguém bem próximo da pessoa com quem você acha que está negociando, sobre a mudança ou viagem.
- Peça para fazer uma chamada de vídeo, normalmente o golpista dirá que está com problemas no celular, sem crédito ou sem conexão de qualidade, fazendo de tudo para evitar esse contato.
- Se tiver a possibilidade tente entrar em contato com o próprio titular da conta.
- Nunca transfira qualquer valor para uma conta cujo titular não seja expressamente a pessoa com quem você deveria estar falando.

Falso empréstimo

Aqui a vítima normalmente está passando por dificuldades financeiras ou tentando abrir um negócio, e decide procurar pela internet opções de empréstimos facilitados sem ter que ir a uma agência bancária negociar diretamente.

Normalmente a vítima encontrará algum site oferecendo facilidades e logo receberá o contato de algum "agente bancário" ou "gerente de contas" ou algo do tipo. Esses golpistas agem tanto na resposta como no contato ativo, utilizando de engenharia social para identificar contato de pessoas que possam estar buscando formas de empréstimos online.

Nas primeiras abordagens os estelionatários buscarão fazer um mapeamento do perfil das vítimas, como um banco normalmente faria, para deixar vítima o mais confortável e confiante possível com a negociação, no decorrer da conversa o falso atendente vai poder entender a capacidade financeira da vítima o que o permitirá ter noção de quais argumentos utilizar para lhe forçar a fazer pagamentos.

No decorrer da conversa o criminoso informará que o crédito foi aprovado e passará a colher os dados e documentos da vítima, "para fazer o contrato", após então enviará documentos com os detalhes da negociação, normalmente em algum papel timbrado de alguma instituição conhecida para conferir aparência de legitimidade.

Neste estágio da conversa normalmente a vítima já estará muito confortável e menos atenta, e é aí que começam a surgir os "custos operacionais", os golpistas pedirão que o cliente deposite o valor referente aos impostos como IOF, alguma taxa de abertura de crédito ou até mesmo honorários de um advogado ou contador. Neste ponto uma característica em comum em todos os golpes é enquanto a vítima estiver pagando, sempre existirá uma nova taxa ou tributo a pagar para prosseguir a negociação. E aqui ao perceber que não tem mais dinheiro algum para

continuar na negociação a vítima será informada que para receber os valores de volta precisa pagar a taxa de cancelamento ou "quebra de contrato", e será constantemente ameaçada com processos, ações judiciais, protestos em cartórios, ou até mesmo será estimulada a fazer um novo pagamento com a promessa de que esse será o último e que essa é a última barreira entre ele e o seu desejado empréstimo salvador.

Aqui os bandidos exploram *o medo e ingenuidade*.

O que você precisa saber para evitar cair nesse golpe:

- Prefira negociar diretamente com o banco onde você já tem algum relacionamento.
- Instituições sérias não cobram nenhuma taxa para conceder empréstimos.
- Você não paga imposto para pegar um empréstimo.
- Ao menor sinal de estranheza na negociação contate um advogado de confiança (a consulta normalmente será mais barata que as falsas taxas)
- Desconfie sempre daquilo que parece fácil demais.
- CNPJ não é atestado de idoneidade, qualquer pessoa pode abrir um CNPJ ou até mesmo usar o CNPJ de uma instituição séria para usar de pano de fundo para fraude.

Falso leilão

É lugar comum saber que é possível adquirir bens com preços bem abaixo dos padrões do mercado através de leilões, de posse dessa informação estelionatários clonam sites famosos de leilão, modificando apenas algum pequeno detalhe no endereço do site e fazendo você cair numa armadilha.

No site são expostos carros, imóveis, barcos e outros itens que normalmente atraem o interesse da população, com preços bastante convidativos, o que geralmente não causa estranheza na vítima, pois este é um comportamento normal do leilão.

As coisas começam a dar errado no momento que a vítima dá um lance e acha ter arrematado a peça, neste momento os estelionatários entrarão em contato parabenizando-a pela compra e solicitando o pagamento imediato, sob risco de perder a oportunidade de compra ou pagamento de multa.

Normalmente os criminosos enviarão um boleto estilizado e editado que terá a aparência de legítimo, exigindo que o cliente honre com o lance dado, mesmo antes de ter acesso ao lote. Movido pelo senso de urgência e pelo medo de perder a compra vantajosa a vítima realiza o pagamento e perde, aquilo que muitas vezes era uma economia de anos. Uma das características desse golpe é a de fazer a vítima gastar valores altíssimos.

Como se proteger:

- Verifique sempre todos os detalhes do URL (endereço do site) do site de leilão.



- Não dê lances antes de ver pessoalmente o item que tem interesse.
- Prefira leiloeiros já conhecidos e que tenham sido indicados por algum amigo, que já realizou compras ali.
- Não faça pagamentos antecipados, e quando for pagar qualquer boleto sempre verifique no app quem é o beneficiário que vai receber aquele valor, se for uma pessoa física ou mesmo um CNPJ que não seja do leilão, cancele o pagamento.
- Pesquise sobre a idoneidade do site realizando buscas em sites como ReclameAqui.

Golpe Pix do Whatsapp/Instagram

Esse tem sido um dos que vejo acontecer com mais frequência e sua execução é muito simples, alguém hackeia a conta de um conhecido ou familiar, ou até mesmo cria uma conta com número diferente e entra em contato com todos os amigos e familiares dizendo que mudou de número e pedindo para salvar aquele novo contato.

O modo de operação é sempre o mesmo, os bandidos se passando por alguém conhecido diz que está com problemas de internet ou que seu aplicativo não funciona e que precisa fazer um pagamento urgente, e que transferirá logo mais os valores de volta.

Apesar de já muito conhecido, esse é um dos golpes que faz mais vítimas hoje em dia, pois explora a boa vontade de ajudar.

Como evitar:

- Se alguém te pedir dinheiro, peça para fazer uma chamada de vídeo antes de enviar qualquer coisa.
- Se alguém diz que mudou de número, tente imediatamente entrar em contato com o número que você tem guardado para conferir a informação, caso não haja atendimento ligue para alguém que normalmente está sempre perto dessa pessoa.
- Não faça depósitos em contas de terceiros, se um amigo te pediu dinheiro faça a transferência exclusivamente para a conta desse amigo.
- Se o depósito é urgente e o app do banco não funciona, seu amigo pode fazer a transação direto na agência bancária, melhor que ele sofra um pequeno aborrecimento do que ele perder dinheiro. Se você realmente quer ajudar, peça que ela vá até sua casa para fazerem juntos o depósito.

Após o golpe

A variedade de golpes é imensa, seria impossível falar de todos aqui, sem tornar esse texto insuportavelmente longo, porém a maioria das dicas sobre como evitar cair servem para quase todas as modalidades de golpes.

Se as dicas daqui chegaram tarde, não se desespere ainda existe esperança.

Seja rápido



Passo 1: O primeiro passo a seguir após perceber que caiu num golpe é imediatamente entrar em contato com seu banco solicitando imediatamente o cancelamento da transferência, mesmo que seja Pix, ANOTE O PROTOCOLO DE ATENDIMENTO, NOME DO ATENDENTE, DATA E HORA DO ATENDIMENTO.

Passo 2: Entre imediatamente em contato com o banco que recebeu o valor e informe sobre o golpe em detalhes. ANOTE O PROTOCOLO, NOME DO ATENDENTE, DATA E HORA DO ATENDIMENTO.

Passo 3: Faça um boletim de ocorrência (B.O.) na delegacia mais próxima, a maioria dos estados hoje, contam com esse serviço online, sem que você precise ir até a delegacia, ANOTE O NÚMERO DO B.O E GUARDE O DOCUMENTO.

Passo 4: Faça uma reclamação no site do Banco Central do Brasil, contra o banco que recebeu os valores, segue o link: https://www.bcb.gov.br/acessoinformacao/registrar_reclamacao.

Passo 5: Tire print de absolutamente tudo! Das conversas, dos comprovantes de depósito, do Boletim de Ocorrência, enfim de tudo mesmo, e procure um advogado que seja especialista em golpes online.

Nesses casos, normalmente os golpes são praticados usando contas criadas por CPFs roubados e os bancos podem ser responsabilizados pela abertura de contas para fraudes com base na súmula 479 do STJ:

"Súmula 479 As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias."

Será considerado fortuito interno quando restar comprovado que o banco não tomou as precauções necessárias para confirmar que quem estava abrindo a conta era de fato o titular daquele CPF utilizado, conforme a Resolução nº 2.025 do Banco Central, nos termos abaixo:

"Artigo 3º As informações constantes da ficha-proposta, bem como os elementos de identificação e localização do proponente, devem ser conferidas à vista de documentação competente, observada a responsabilidade da instituição pela verificação acerca da exatidão das informações prestadas. (...) Parágrafo 2º A instituição deve adequar seus sistemas de controles internos voltados para as atividades de abertura e acompanhamento de contas de depósitos, implantados nos termos da Resolução 2.554, de 24 de setembro de 1998, com vistas a procedimentos, incluindo regras rígidas do tipo 'conheça seu cliente', que previnam a utilização das respectivas instituições, intencionalmente ou não, para fins de práticas ilícitas ou fraudulentas prever o monitoramento das atribuições conferidas na forma do parágrafo 1º, bem como adotar políticas e procedimentos, incluindo regras rígidas do tipo 'conheça seu cliente', que previnam a utilização das respectivas instituições, intencionalmente ou não, para fins de práticas ilícitas ou fraudulentas."

Uma vez que o banco seja incapaz de provar que de fato tomou as diligências obrigatórias para garantir a titularidade correta da conta aberta, ele passará a ser responsável pelos danos



sofridos pela vítima, devendo ser condenado por perdas e danos.

É importante destacar que não basta simplesmente alegar que a culpa é do banco, é dever do cidadão tomar as precauções para evitar cair nos golpes e se cair, *é fundamental seguir os passos aqui sugeridos*, pois é necessário que a vítima comunique aos bancos e lhes dê a chance de bloquear os valores antes do saque.

Fonte: <https://conjur.jumps.com.br/2022-ago-24/pina-maciel-proteger-golpes-internet/>