

Quadrilhas se aproveitam do aumento das transações digitais causado pelo isolamento social para aplicar golpes e capturar dados de clientes; um deles está relacionado ao auxílio emergencial criado pelo governo federal

A FEBRABAN e os bancos têm reforçado a importância do uso dos canais digitais para evitar as aglomerações e combater a proliferação do novo coronavírus. Por meio do internet banking e dos aplicativos das instituições financeiras, é possível realizar quase todas as operações bancárias e ter acesso a diversos produtos e serviços (fazer transferência, tirar extrato, pagar contas, pedir empréstimo, negociar dívidas, contratar seguros etc).

Entretanto, é importante redobrar os cuidados de segurança, pois quadrilhas estão se aproveitando deste momento de uso mais intenso dos meios digitais para aplicar golpes.

Os métodos dos bandidos não são novos. Eles usam a chamada engenharia social, que são armadilhas que os golpistas criam para obter dados, senhas e informações pessoais dos clientes, ou ainda levá-los a fazer pagamentos em benefício dos criminosos.

O golpe do falso motoboy é um bom exemplo do aumento da atividade das quadrilhas. Nele, criminosos entram em contato com as vítimas se fazendo passar pelo banco para comunicar a realização de transações suspeitas com o cartão de crédito do cliente.

Após usar técnicas de engenharia social para obter informações sigilosas, como senhas e dados pessoais, os golpistas informam que um motoboy será enviado para recolher o cartão supostamente clonado para que sejam feitas outras análises necessárias para o cancelamento das compras irregulares.

Para passar uma imagem de segurança, os criminosos orientam a vítima a cortar o cartão ao meio, no sentido do comprimento, para inutilizar a tarja magnética, antes de entregá-lo ao motoboy. No entanto, o chip permanece intacto, o que permite que a quadrilha faça compras com o cartão, ainda que o plástico esteja partido ao meio.

"Os bancos nunca enviam funcionários para recolher os cartões dos clientes", alerta Walter de Faria, diretor-adjunto de Operações da FEBRABAN - Federação Brasileira de Bancos. Ele completa que "quando o cliente for descartar um cartão, é importante inutilizar o chip para impedir que novas compras sejam feitas".

Outro exemplo de golpe que surgiu na esteira da pandemia causada pelo novo coronavírus são as dezenas de aplicativos falsos relacionados ao auxílio emergencial de criado pelo governo federal. Os golpistas se aproveitam da necessidade de as pessoas se cadastrarem para receber o benefício, para roubar a informações sigilosas.

"A mistura de medo da doença e a confusão trazida pelo excesso de fontes de informação criam o ambiente perfeito para a ação dos golpistas", diz Faria.

Ele reforça a importância de manter uma postura vigilante para evitar cair em um desses golpes. "Desconsiderar qualquer informação que não esteja nos canais oficiais dos governos e empresas é um bom caminho. Em caso de dúvida sobre a veracidade de uma mensagem ou conteúdo, interrompa a operação e entre em contato com o SAC (Serviço de Atendimento ao Consumidor) do prestador do serviço ou vendedor do produto para confirmar se aquilo é real."

Para reduzir os riscos de ser vítima de golpistas, a FEBRABAN destaca as seguintes orientações:

- o banco não liga nem encaminha links por SMS, WhatsApp ou e-mail pedindo atualização dos dados, sincronização de token ou desbloqueio de cartão;

- o site oficial para se cadastrar para receber o auxílio emergencial é <http://auxilio.caixa.gov.br>;
- o cadastramento para receber o auxílio emergencial também pode ser realizado pelo app específico da Caixa, que deve ser baixado apenas na loja oficial de aplicativos do sistema operacional do seu dispositivo;
- não clique em nenhum link. Digite, no navegador, o endereço eletrônico do banco ou da loja em que pretende realizar a transação ou compra;
- sempre baixar qualquer aplicativo apenas da loja oficial do sistema operacional do seu dispositivo;
- não repasse seus dados para nenhuma pessoa intermediar a concessão do auxílio emergencial. Apenas a Caixa avalia e confirma quem é elegível ao benefício e eles não procuram as pessoas ou usam serviços de terceiros;
- o banco não entra em contato para pedir cadastro de favorecido, transferências, transações para testes ou estorno de valores nem desbloqueio de cartão
- o banco não entra em contato para dizer que sua conta será bloqueada por falta de atualização cadastral
- também não envia ninguém em sua casa para retirar seu cartão, notebook, computador, tablet, celular ou o chip dele
- como também não entra em contato para pedir atualização ou sincronismo de token
- fique atento a links encurtados e desconhecidos por sms ou e-mail. Não clique nem informe seus dados

Home office

- mantenha antivírus e sistema operacional de seu computador sempre atualizados;
- evite plugar pendrives desconhecidos em seu computador, eles podem conter vírus;
- cuidado ao clicar em links enviados por e-mail;
- se estiver utilizando um computador pessoal que é compartilhado com a família, crie um usuário específico para as atividades do trabalho;
- configure senhas fortes em seu wifi residencial (evite senhas óbvias);
- altere a senha padrão do seu roteador;
- em caso de suspeita de qualquer comprometimento da segurança, altere suas senhas imediatamente;
- não utilize redes públicas

Fonte: FEBRABAN, em 20.04.2020