

FEBRABAN, bancos e parceiros promovem até sexta-feira (26) a 1ª edição da Semana da Segurança Digital de 2021 com o objetivo de alertar o consumidor para o uso seguro da internet e dos canais digitais

A FEBRABAN - Federação Brasileira de Bancos e 30 bancos intensificam até sexta-feira (26) suas ações de comunicação para contribuir com o uso seguro da internet e dos canais digitais contra golpes e fraudes no ambiente digital. A ação faz parte da 1ª edição da Semana da Segurança Digital de 2021, que começou na última segunda-feira (22), e orienta a população a se prevenir de fraudes, que geram prejuízos financeiros e dão muita dor de cabeça ao consumidor.

Neste ano, os participantes, que incluem parceiros como o Banco Central, associações, empresas e as polícias Civil e Federal, estão divulgando dicas de como se prevenir dos principais golpes e fraudes digitais que dão dor de cabeça aos consumidores, entre eles, golpes que envolvem o Pix, o novo sistema de pagamento instantâneo, que permite pagamentos e transferências de dinheiro durante 24 horas por dia, 7 dias por semana, em até 10 segundos.

As tentativas de golpe registradas com o Pix e relatadas por instituições financeiras foram identificadas como ataques de phishing, que usam técnicas de engenharia social, que consistem em enganar o indivíduo para que ele forneça informações confidenciais, como senhas e números de cartões. 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.

Conheça a seguir os principais golpes envolvendo o Pix e saiba como se prevenir**Golpe da clonagem do Whatsapp**

Entre os meios usados pelos bandidos está o Whatsapp. Os criminosos enviam uma mensagem pelo aplicativo fingindo ser de empresas 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 por transferência via Pix.

Uma medida simples para evitar que o WhatsApp seja clonado é habilitar, no aplicativo, a opção "Verificação em duas etapas" Configurações/Ajustes > Conta > Verificação em duas etapas. Desta forma, é possível cadastrar uma senha que será solicitada periodicamente pelo app. Essa senha não deve ser enviada para outras pessoas ou digitadas em links recebidos.

Golpe de engenharia social com Whatsapp

Em outra fraude que usa o Whatsapp, o criminoso escolhe uma vítima, pega sua foto em redes sociais, e, de alguma forma, consegue descobrir números de celulares de contatos da pessoa. Com um novo número de celular, manda mensagem para amigos e familiares da vítima, alegando que teve de trocar de número devido a algum problema, como, por exemplo, um assalto. A partir daí, pede uma transferência via Pix, dizendo estar em alguma situação de emergência.

Nesta fraude, o bandido nem precisa clonar o whatsapp da pessoa, e usa a estratégia de pegar dados pessoais da vítima e de seus contatos. A FEBRABAN alerta que é preciso ter muito cuidado com a exposição de dados em redes sociais, como, por exemplo, em sorteios e promoções que pedem o número de telefone do usuário.

Ao receber uma mensagem de algum contato com um número novo, é preciso certificar-se que a

pessoa realmente mudou seu número de telefone. O cliente sempre deve suspeitar quando recebe uma mensagem de algum contato que solicita dinheiro de forma urgente. Não faça o Pix ou qualquer tipo de transferência até falar com a pessoa que está solicitando o dinheiro.

Golpe do falso funcionário de banco e das falsas centrais telefônicas

Outros golpes praticados são os do falso funcionário e falsas centrais telefônica de instituições financeiras. 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 oferece ajuda para que o cliente cadastre a chave Pix, ou ainda diz que o usuário precisa fazer um teste com o sistema de pagamentos instantâneos para regularizar seu cadastro, e o induz a fazer uma transferência bancária.

É importante ressaltar que os dados pessoais do cliente jamais são solicitados ativamente pelas instituições financeiras, tampouco funcionários de bancos ligam para clientes para fazer testes com o Pix. Na dúvida, sempre procure seu banco para obter esclarecimentos.

Golpe do bug do Pix

Outra ação criminosa que está sendo praticada por quadrilhas e que envolvem o Pix é o golpe do "bug" (falha que ocorre ao executar algum sistema eletrônico). Mensagens e vídeos disseminados pelas redes sociais por bandidos afirmam que, graças a um "bug" no Pix, é possível ganhar o dobro do valor que foi transferido para chaves aleatórias. Entretanto, ao fazer este processo, o cliente está enviando dinheiro para golpistas.

Os canais oficiais do Banco Central já alertaram que não há qualquer "bug" no Pix. A FEBRABAN ressalta que o cliente sempre deve desconfiar de mensagens que prometem dinheiro fácil e que chegam pelas redes sociais ou e-mail.

Segurança

De acordo com Adriano Volpini, diretor da Comissão Executiva de Prevenção a Fraudes da FEBRABAN, os bancos estão usando toda sua expertise com todos os sistemas de pagamentos agora para o Pix. Para isso contam com as melhores tecnologias e o que há de mais moderno em relação à segurança cibernética e prevenção a fraudes.

Volpini afirma que os cuidados que o cliente deverá ter na hora de fazer uma transação através do PIX deverão ser os mesmos que adota ao fazer qualquer transação financeira. "Sempre é necessário checar os dados do recebedor da transação Pix (pagamento ou transferência), seja para uma pessoa ou um estabelecimento comercial", afirma.

O cadastramento das chaves Pix também deve ser feito diretamente nos canais oficiais das instituições financeiras, como o aplicativo bancário, internet banking, agências ou através de contato feito pelo cliente à central de atendimento. "O consumidor não deve clicar em links recebidos por e-mails, pelo WhatsApp, redes sociais e por mensagens de SMS, que direcionam o usuário a um suposto cadastro da chave do Pix", diz.

Sobre a Semana de Segurança Digital

A Semana da Segurança Digital está em sua terceira edição, e o setor bancário se alinha mais uma vez a ações similares desenvolvidas tanto Estados Unidos desde 2003, como na Europa, desde 2012, e que envolvem vários setores da economia.

Até sexta-feira (26), os participantes divulgarão dicas de como se prevenir dos principais golpes e fraudes digitais. Cada participante desenvolverá livremente suas ações de conscientização para seus clientes.

Para saber mais sobre os participantes e outras dicas de prevenção a fraudes e golpes no mundo digital, clique em:

<https://portal.febraban.org.br/noticia/3599/pt-br/>

Fonte: FEBRABAN, em 24.02.2021