

Foram mostradas as principais características das estratégias usadas nas fraudes e dicas de como se proteger. Não conseguiu acompanhar o programa ao vivo? Clique no link que está na matéria e assista na íntegra à LiveBC sobre o assunto.

O Banco Central (BC) lançou, neste mês, em parceria com diversos criadores de conteúdo digital, a campanha “Antes de confiar, melhor verificar” para reforçar a usuários do Sistema Financeiro Nacional (SFN) que é preciso ficar atento contra golpes. Na LiveBC de junho, Carolina de Assis Barros, Diretora de Relacionamento, Cidadania e Supervisão de Conduta do Banco Central, falou sobre como se proteger e evitar ser vítima de fraudes. A live está disponível no [canal do BC do YouTube](#).

Carolina explicou que o BC tem três eixos de atuação na prevenção contra golpes: atuação junto a bancos e instituições financeiras com normas e fiscalização; cooperação estreita com órgãos de segurança pública; e educação financeira do cidadão.

“Os dados pessoais no sentido amplo, incluindo as senhas, se transformaram em parte crucial do nosso patrimônio. Por isso, é preciso zelar e cuidar. Uma das melhores formas de se resguardar é com informação, mais especificamente, com educação financeira”, destacou a Diretora do BC.

Segundo Carolina, as principais características da conduta dos criminosos envolvem momentos de distração e de fragilidade da vítima, por exemplo, quando a pessoa está negativada e precisa de um empréstimo. Ela detalhou que a estratégia usada, muitas vezes, é criar uma sensação de urgência – como quando dizem que o cartão foi clonado ou que a oferta daquela barganha tem hora para terminar –, e oferecem uma saída simples para um problema ou condições vantajosas em uma negociação.

Por isso, a diretora frisou que, em tempos de digitalização da comunicação e do SFN, proteger dados pessoais e senhas é crucial.

Ao lembrar que o melhor escudo do cidadão ainda é a informação, neste caso, a educação financeira, informou que o BC tem uma série chamada “[BC te Explica](#)” que trata, entre outros temas, do combate a golpes e fraudes.

Ela detalhou alguns dos roteiros mais usados nas fraudes e como se precaver. Por exemplo, quando a vítima cai no conto do banco ou financeira falsos. Segundo Carolina, no golpe do empréstimo falso, que, muitas vezes, pressupõe um depósito antecipado, que também é forjado, são oferecidas condições vantajosas, como taxas mais baixas que as praticadas pelo mercado. O criminoso vai pedir adiantamento para fazer/pagar um “cadastro, pagar uma garantia, o IOF ou taxa para o BC liberar”. Depois disso, ele normalmente some com esse pagamento antecipado, e a vítima fica sem esse dinheiro do adiantamento e sem o empréstimo.

Para se proteger em casos como esse, a diretora ressaltou que é preciso verificar se a instituição financeira que o consumidor vai utilizar é regulada pelo BC, por meio do site da autarquia, desconfiar de ofertas muito abaixo do mercado e que não façam as exigências comuns de um banco (tais como cadastro e garantias), desconfiar de links com ofertas de empréstimo, bem como nunca fazer pagamento antecipado para receber empréstimo, principalmente para conta de pessoa física, pois isso não é prática de instituição regulada pela autoridade monetária.

Para checar se uma instituição financeira é autorizada, regulada ou supervisionada pelo BC, acesse <https://www.bcb.gov.br/meubc/encontreinstituicao>.

Outra situação mostrada na live é quando a vítima recebe uma ligação de alguém que diz que há uma compra não reconhecida ou qualquer outro problema com o cartão. Em função disso, ele precisa de dados do cartão para sustar a tal compra, mas esses dados, na verdade, são utilizados futuramente pelos fraudadores em outras compras. Ou quando a vítima é informada que “o banco”

está mandando um motoboy para recolher o cartão e averiguar o problema. Esse cartão certamente também será utilizado por ele em compras futuras. Como se proteger?

A regra, segundo a diretora do BC, é lembrar sempre de que as centrais de atendimento não costumam fazer ligações para os clientes. Essas ligações são exceção e não regra, disse. A seguir, Carolina elencou o que fazer em uma situação como essa: desconfie do número que aparece no visor, mesmo quando o identificador de chamadas mostra o nome do banco ou números conhecidos como sendo os do banco; desligue imediatamente ou não atenda à ligação – em caso de dúvidas, depois ligue para o seu gerente ou para o banco (se possível, use um telefone diferente) –; não forneça dados ou senhas em ligações recebidas; saiba que a instituição financeira jamais vai enviar um motoboy até você; e, se precisar cancelar um cartão, você mesmo deve destruí-lo na sequência.

Senhas e Pix

Carolina aproveitou a live para elencar alguns cuidados a serem tomados com dados pessoais, como não compartilhar senhas com outras pessoas ou em redes sociais; usar senhas mais elaboradas e únicas para cada conta; mudar regularmente as chaves em sites de finanças pessoais e de compras; utilizar antivírus nos dispositivos em que acessa os bancos e faz compras; adotar autenticação em dois fatores sempre que estiver disponível; bem como não aceitar ajuda de estranhos para pagar contas, sacar dinheiro ou fazer outras operações em caixa eletrônico. Se precisar de ajuda, procure um funcionário do banco uniformizado e identificado. Na hora de usar a senha, ela reforçou ser preciso total foco e atenção: confira sempre onde vai digitar o código e o que digitou.

E quando o assunto é o Pix, onde está o perigo? A Diretora de Relacionamento do BC destacou que o Pix é seguro, rápido e gratuito. O problema, segundo ela, não está no Pix, que é só um meio de pagamento. A questão, nesse caso, reforçou Carolina, é a manipulação e exploração de falhas humanas para cometer crimes financeiros.

Carolina deu dicas para evitar cair em golpes envolvendo o sistema de pagamento instantâneo. Confira algumas a seguir: não cadastre chaves Pix em links e sites desconhecidos; não aceite acesso remoto em seu dispositivo para testar segurança; antes de efetivar um Pix, confira os dados do destinatário e o valor; e, por último, se fizer um Pix e descobrir que era golpe, informe imediatamente o seu banco, que vai acionar o Mecanismo Especial de Devolução (MED), e marcar a chave Pix do recebedor como suspeita.

Para tirar outras dúvidas sobre golpes financeiros e saber como se proteger, o BC disponibiliza a página [FAQs \(bcb.gov.br\)](https://www.bcb.gov.br/faq), que reúne várias dicas e exemplos para não ser vítima de criminosos.

Clique [aqui](#) para ver (ou rever) a Live BC #34.

Fonte: [BCB](#), em 18.06.2024.