valor.globo.com

Fraudadores renovam golpes e pedem transferências por Pix

4-5 minutos

Banco Central organizou evento virtual para alertar sobre golpes envolvendo o Pix

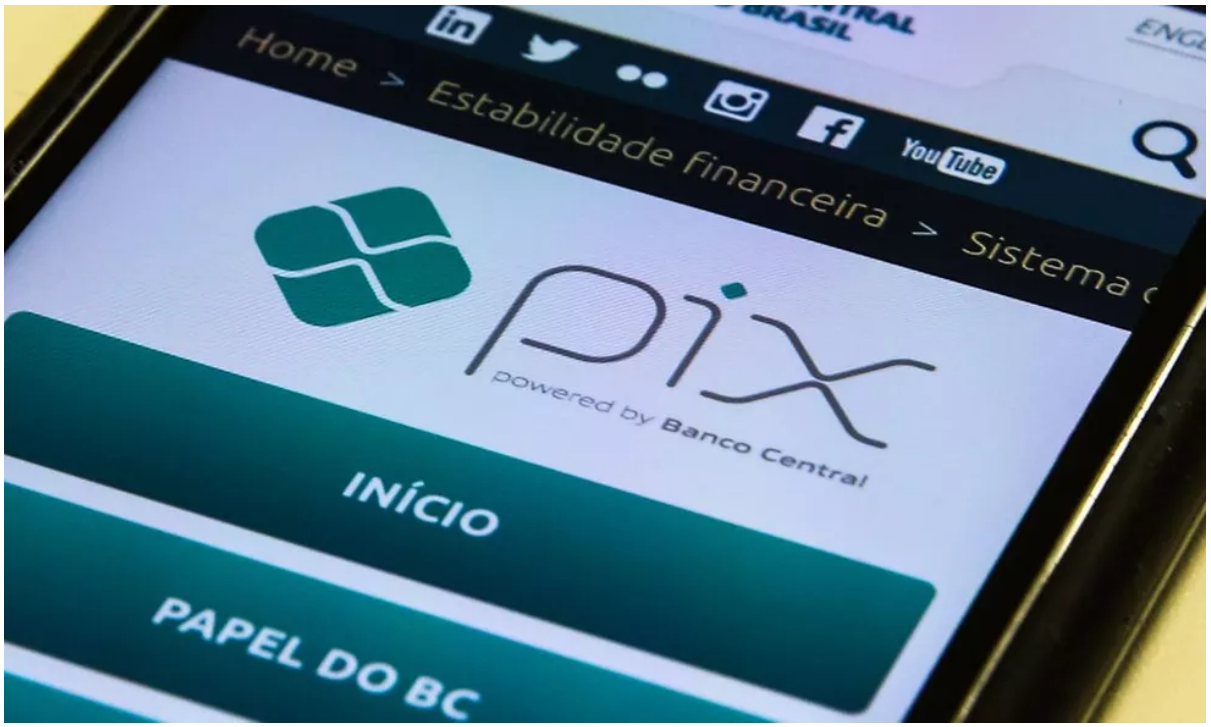
Enquete realizada pelo **Banco Central** (**BC**) em suas redes sociais mostra que 81% das pessoas que responderam à pesquisa já caíram no golpe que envolve a clonagem de **WhatsApp**. Embora não seja nova, a manobra ganhou novo impulso com a implantação do **Pix**.

De maneira geral, os golpes ligados ao sistema de pagamentos instantâneos apenas vêm ganhando nova roupagem, diz o chefe-adjunto do Departamento de Competição e Estrutura do Mercado Financeiro do BC, Carlos Eduardo Brandt, que participou nesta sexta-feira de um evento virtual com outros especialistas para alertar a respeito de golpes envolvendo o Pix. Segundo ele, justamente por não serem novas, essas manobras podem ser evitadas com alguma dose de atenção e a adoção de cuidados simples.

Principal golpe, a clonagem do aplicativo de mensagens WhatsApp pode ser realizada de duas formas: ativação da conta do usuário no aparelho telefônico do golpista ou criação de um perfil parecido com o do usuário (com o mesmo nome e a mesma foto, por exemplo) no telefone do golpista.

No primeiro caso, o golpista finge que é um prestador de serviço, muitas vezes com informações sobre o usuário, e pede que ele

compartilhe o código de registro para a ativação do aplicativo. Esse código é uma sequência numérica de seis dígitos enviada por SMS sempre que é realizada a tentativa de ativar uma conta do WhatsApp em um aparelho telefônico – nesse caso, o do golpista.



— Foto: Marcello Casal Jr/Agência Brasil

“Por exemplo, você anunciou alguma coisa em um site. A pessoa conhece o seu nome e entra em contato dizendo: olha, você tem o telefone X Y Z, estou entrando em contato porque gostaria que confirmasse para mim o código que vou enviar via SMS. Só que o código que ele está enviando não é um código de confirmação de segurança do lugar onde está o anúncio. É o código de ativação do WhatsApp”, diz o chefe-adjunto do Departamento de Tecnologia da Informação do BC, Caio Moreira Fernandes.

A partir daí, o caminho é semelhante tanto no caso da ativação do WhatsApp em um novo telefone quanto no da criação de um perfil semelhante. O golpista se passa pelo usuário e, por meio do aplicativo, aborda familiares, amigos ou colegas pedindo uma transferência, via Pix ou não.

A principal dica é simples: manter a atenção em relação a pedidos de códigos recebidos por SMS.

Mas o WhatsApp também criou ferramentas específicas para diminuir os riscos, como a verificação em duas etapas (que pode

ser acessada dentro do Whatsapp por meio de: Configurações $> Conta $> Verificação em duas etapas). Essa verificação exige que, para acessar a conta, seja digitada uma senha criada pelo próprio usuário, além do código de ativação.

O usuário também pode estabelecer que a foto do seu perfil apareça apenas para os contatos cadastrados na agenda do usuário (Configurações $> Conta $> Privacidade $> Foto de perfil $> Somente para os meus contatos).

“Isso evita que a sua foto vá parar em outro WhatsApp e alguém se passe por você”, diz Fernandes. Ele ainda alerta para a importância de sempre manter o aplicativo atualizado, já que cada versão vem com novas funcionalidades.

Outras dicas dadas por especialistas para evitar golpes no Pix são: usar sempre os canais oficiais da instituição financeira, nunca clicando em links suspeitos recebidos por e-mail, mensagem ou redes sociais; conferir os dados do destinatário antes de confirmar uma transação; desconfiar de grandes ofertas ou promessas de alto retorno financeiro, pesquisando sobre o ofertante na internet; denunciar chaves do Pix envolvidas em golpes, que dessa maneira entrarão no sistema antifraude das instituições financeiras.