O golpe da mão fantasma, também conhecido como golpe do acesso remoto, tem se tornado cada vez mais comum. Neste tipo de crime, o bandido se passa por um funcionário do seu banco e entra em contato com você por SMS, e-mail ou até WhatsApp. A mensagem geralmente informa que é necessário atualizar o aplicativo do banco e pede que você clique em um link para fazer essa atualização.

No entanto, ao clicar no link, você acaba baixando um vírus no seu celular. Esse vírus permite que os hackers tenham acesso remoto ao seu aparelho, podendo visualizar suas configurações, acessar seus aplicativos e, o mais grave, fazer login na sua conta bancária, principalmente se a sua senha estiver salva em algum local no dispositivo, como um bloco de notas, ou no próprio navegador.

Com acesso total ao seu celular, os criminosos começam a movimentar o seu dinheiro, realizando transferências para contas de terceiros, pagando boletos e até solicitando empréstimos em seu nome.

Como se proteger

Sempre que receber mensagens ou ligações que pareçam vir do seu banco, desconfie! Nenhuma instituição financeira envia mensagens solicitando que você baixe aplicativos ou faça atualizações por meio de links.

Além disso, use senhas fortes, ative a autenticação em duas etapas e evite armazenar informações de acesso no seu dispositivo.

Fique atento e converse com seus amigos e familiares sobre esse golpe. Muitas pessoas não estão por dentro das táticas usadas pelos golpistas e uma simples conversa pode ajudar a evitar que se tornem vítimas.

Fonte: Viva Previdência, em 18.11.2024.