31/10/2019 07:11 - Polícia Civil alerta sobre o aumento de golpes por mensagens e links enviados por celular

O aparelho celular é uma ferramenta essencial para muita gente, por ser um dos principais meios de comunicação. Mas de uns tempos pra cá tem sido muito usado por criminosos, que aplicam golpes utilizando mensagens via SMS ou aplicativos de mensagens instantâneas, como o WhatsApp. O que tem chamado a atenção de especialistas é a quantidade de pessoas que estão caindo nos golpes.

A estudante Letícia Rodrigues explica que sempre teve cautela antes de acreditar nas mensagens que recebe. Mensagens, segundo ela, de promoções, bancos, atualização de dados, vendas, entre outras, mas afirma conhecer pessoas que já foram vítimas.

"Já recebi mensagens pedindo para clicar em links, e atualizar meus dados bancários. Mas logo percebi que poderia ser um golpe, pelo fato de não ter conta naquele banco. Já o meu primo acabou caindo e passando informações pessoais. Por sorte deu tudo certo, mas foi um grande susto", afirmou a jovem.

COMO O GOLPE FUNCIONA

Não é difícil encontrar vítimas hoje em dia devido à semelhança com mensagens reais de instituições e a falta de atenção da maioria das pessoas, explicou o delegado responsável pelo Núcleo de Combate as Defraudações, Swami Otto. Segundo ele, os criminosos se aproveitam da ingenuidade e falta de atenção das vítimas.

"Existe três tipos de golpes de estelionato que são os mais comuns: golpes por mensagens SMS, pelo WhatsApp e o conhecido como resgate do chip. Os nomes mudam, mas em todos eles a vítima tem a privacidade invadida e acaba saindo no prejuízo", alertou Swami Otto

Ele explica que nos golpes por mensagens de SMS, o criminoso costuma se passar por determinado banco, informando sobre possíveis bloqueios, atualização cadastral entre outras invenções. O objetivo é induzir a vítima a clicar em links, ou informar os dados bancários.

Já os golpes em aplicativos de mensagens costumam ser feitos por meio do compartilhamento de mensagens falsas. Dois tipos estão em alta: anúncios de vendas de produtos a preço de custo, onde o golpista copia informações de um venda real e se passa pelo vendedor, ou cria uma possível venda por preços muito baixos. E no outro tipo de golpe, o criminoso clona o aplicativo de mensagens, e acaba se passando pela vítima e enviando mensagens a amigos e familiares.

"Nesse tipo de golpe onde o aplicativo é clonado, é comum o criminoso pedir uma ajuda ou transferência urgente, com valores que chegam até cinco mil reais, por exemplo, afirmando que depois devolve a quantia. Sem confirmar quem realmente está do outro lado da tela, os familiares acabam transferindo o valor para outras contas, e só depois descobrem que caíram em um golpe", explicou o delegado.

Já o golpe conhecido como Resgate do Chip ou Golpe do Chip, em alguns casos o criminoso paga propina a pessoas que trabalham com serviços de chips e operadoras para que forneçam dados.

"Em mãos de um novo chip, o criminoso ativa a linha da vítima e faz uso das contas e informações salvas na nuvem por exemplo. Enquanto usa o novo chip, a vítima fica inabilitada sem usar serviço da operadora, e pensando ser algum problema de rede, acaba esperando o chip voltar a funcionar, sem saber que está sendo vítima de um golpe", salientou o delegado.

COMO SE PROTEGER

Ativar a Confirmação em duas etapas no aplicativo de mensagens evita clonagem e invasão de criminosos

Embora os golpes estejam cada vez mais reais, é possível encontrar falhas e adotar medidas de segurança que protejam o usuário, sem deixar de usar o celular, esclareceu Swami. Uma das dicas, segundo o delegado, é certificar a veracidade do conteúdo dessas mensagens.

''Nós orientamos população a nunca clicar em links, e antes observar se a mensagem foi enviada por um número de telefone, o que já entrega o golpe. Nos casos de mensagens de banco, a instituição não costuma pedir dados, e o melhor a se fazer é procurar a instituição pessoalmente" esclareceu.

Já em mensagens compartilhadas nos aplicativos, ele explica que o correto é não sair compartilhando sem verificar os anúncios, propagandas, e leilões de veículos por exemplo. “Instituições financeiras e órgãos públicos não costumam usar esse tipo de serviço e sim, sites oficiais. Uma dica importante é ativar a segurança do próprio whatsapp, indo em (Configurações ou Ajustes), clicando na aba (Conta) e depois (Confirmação em Duas Etapas), ativar e criar um código único que só a pessoa saiba. Dessa forma o golpista não conseguirá clonar o aplicativo”, concluiu.

Caso seja uma vítima a recomendação é procurar a delegacia mais próxima e registrar um Boletim de Ocorrência, com todas as informações de forma que seja possível encontrar os responsáveis.

Fonte: Secom - Governo de Rondônia

Notícias RO