NOTA TÉCNICA DE ESCLARECIMENTO – 03/2023

A Superintendência de Inteligência Legislativa (SUINT) vem alertar para uma nova forma de golpe: "**O Golpe do SMS**", que passou a ser usados como *modus operandi*, pelos agentes criminosos, no intuitivo de atrair vítimas, enviando mensagens por SMS, levando-as a *clicarem* em links ou realizarem ligações a falsas centrais telefônicas.

As "falsas mensagens", via SMS, são enviadas às vítimas com conteúdo diverso, para chamar atenção, tais como: *falsos alertas de bancos sobre compras realizadas ou transações bancárias*; *supostos acessos à conta bancária da vítima*; *avisos sobre a expiração de pontos obtidos em programas de milhagens, falsas propostas de negociação de dívidas, onde simulam ser contato da Serasa ou da Recovery*, além de outros.

Após os agentes criminosos "fisgarem a presa", fazendo-as **ligar** para uma falsa central telefônica ou **clicar** em links, acontece o seguinte: **1) no caso de Links**, a vítima é direcionada para uma página na qual precisa inserir *login* e senha. Com isso, os agentes criminosos têm acesso aos dados da vítima, para usufruí-los ilegalmente; **2) no caso de ligação** para central telefônica, os agentes criminosos, também, enviam mensagem informando, falsamente, que um empréstimo foi aprovado, ou uma *transferência/Pix*, foi efetivada, fornecendo um contato para dúvidas.

O **uso do *ardil***, também, acontece quando os agentes criminosos enviam mensagens informando sobre que uma **suposta compra**, geralmente em **lojas de departamento** ou **sites de compras**, foi concluída e inclui um número telefônico para mais dúvidas e informações. Na sequência, a vítima acredita que houve uma compra não reconhecida em seu cartão ou que um empréstimo foi realizado em sua conta, faz a ligação para o número informado, quando é direcionada às centrais falsas.

Algumas vítimas, relatam ter recebido instruções para instalar um suposto **aplicativo** no celular, para reverter a falsa transação feita. No entanto, trata-se de **programa** para possibilitar que os agentes criminosos tenham acesso remoto ao celular da vítima e ao aplicativo do banco. Com isso, realizam transferências diretamente da conta da vítima. Outras vítimas disseram, que após ligarem para a falsa central, acabaram sendo induzidas a fazer transferências.

É preciso **orientar** que: se a mensagem enviada estiver com o **nome do banco escrito errado**, **faltando uma letra ou com ponto entre as letras**, se trata de Golpe. Nenhum banco enviará mensagem com grafia errada para o cliente.

Para entrar em contato com seu banco, procure os telefones corretos no site oficial ou dentro do aplicativo da instituição financeira. Outra opção é buscar atendimento pelo chat dentro do aplicativo.

Lembre-se que, em nenhuma hipótese, o banco entrará em contato pedindo que o cliente faça uma transação pelo telefone. Além disso, nunca forneça seus dados em ligações, formulários na internet, nem código recebido pelo celular. Por fim, esteja sempre atento e desconfie, caso haja algo fora do padrão de atendimento do seu banco.