Escrito por SINDINOTARS
Qui, 31 de Outubro de 2019 08:06 -

No início deste ano, um estudo realizado pela consultoria EY e pela IIF, englobando 74 organizações de 29 países, concluiu que 81% das instituições colocam a segurança cibernética como prioridade. Em 2017, o Relatório de Ameaças à Segurança na Internet (ISTR, na sigla em inglês) constatou que o Brasil foi um dos países que mais gerou ciberataques no mundo. Ou seja, é possível afirmarmos que os riscos do meio virtual são inúmeros e parcialmente desconhecidos. Ainda que presentes em nossa realidade, os assaltos a bancos e ataques a caixas eletrônicos têm se tornado menos frequentes com o passar dos anos. Em compensação, os golpes online gerados através de transações financeiras realizadas pela internet, crescem a cada dia. Os crimes digitais, hoje, tornaram-se mais sofisticados e difíceis de serem descobertos.

A “dedicação” de muitos golpistas atualmente está em explorar falhas de usuários comuns ao invés de focar em invasões virtuais a sistemas de grandes corporações ou redes empresariais. Um simples e-mail falso que direciona para sites fraudulentos pode resultar no roubo de dados sigilosos ou na instalação de softwares espiões com essa mesma intenção.

Uma das práticas mais comuns para se roubar dados de cartão de crédito e informações pessoais é o Phishing. Basicamente, consiste na criação de um site idêntico ao da instituição financeira onde, por meio dele, é possível ter acesso a dados que o usuário cadastrou.

Os já famosos vírus, também são capazes de criar uma mesma identidade visual de uma página de internet banking ou então alterar a interface, de modo que ela possa solicitar as informações essenciais para se proceder com um processo fraudulento.

Há ainda casos recorrentes de alteração de boletos em tempo real, para que, no momento da transação, a quantia caia em uma conta administrada por criminosos. Alguns hackers conseguem também interceptar a mensagem que contém um boleto, alterar e reenviar para o devedor, se passando pelo emitente. É possível ainda, instalar um programa ilícito no computador do usuário, que altera um boleto autêntico em sua própria máquina, sem que o cliente perceba a intercorrência.

As táticas são muitas e se renovam a cada dia. Neste caso, a solução é se precaver. Para o usuário, é essencial que as transações financeiras sejam realizadas por uma rede corporativa e que se atente às atualizações e recomendações sugeridas pelo banco. É importante também cultivar o hábito de mudar periodicamente as senhas de acesso, definindo-as com alternância de números e letras e evitando caracteres que remetam a datas de aniversário ou placas de carro.

Ao abrir a página web da instituição financeira, certifique-se de que ela é confiável. Procure pelo Selo de Certificado Digital de Segurança, representado por um cadeado ao lado do endereço do site e não o acesse por meio de links enviados por e-mail ou SMS.

Quando receber um boleto, faça uma comparação com os dados das faturas anteriores pagas, como CNPJ, razão social e número do banco recebedor, que corresponde aos três primeiros dígitos da linha digitável. Fique atento aos erros de ortografia e linguagem informal, boletos falsos geralmente são mal escritos. Por fim, antes de acessar algum link enviado

externamente, mantenha o mouse sobre o endereço para verificar sua procedência. Na maioria das vezes, o URL real será mostrado no rodapé da tela.

Fonte:
Escriba