Segurança em Foco

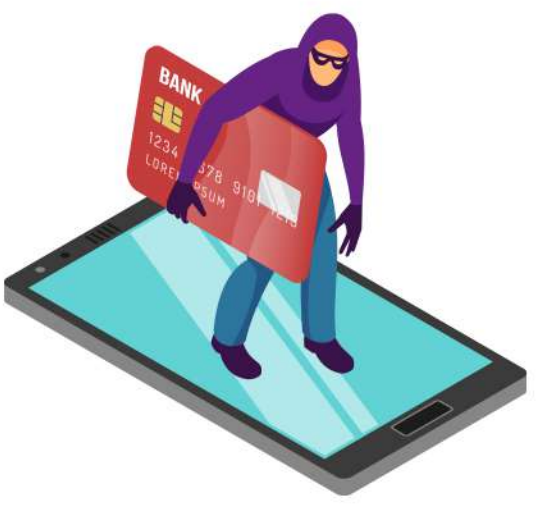
CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Segurança da Informação
ASCOM - Assessoria de Comunicação Social e Cerimonial

Cuidados ao realizar operações financeiras na Internet

Edição nº24
Junho/2022

A internet oferece uma série de facilidades para o nosso dia a dia. Podemos pagar contas, fazer compras, transferir dinheiro no conforto do sofá ou de onde estiver, tudo isso usando computadores, celulares e/ou tablets. Para realizar essas operações em um ambiente virtual seguro, os usuários devem ficar atentos e redobrar os cuidados.

São comuns roubos de senha por meio de engenharia social, pelo qual o fraudador envia e- mails ou faz chamadas se fazendo passar por um funcionário do banco. Em muitas vezes, o fraudador possui até mesmo alguns dados pessoais do cliente. Uma dica muito importante é que o banco nunca solicita a senha do cliente por e-mail ou telefone. Assim, somente informe seus dados de acesso, como número de conta e senha, no site seguro do banco. Não informe seus dados a outras pessoas ou sites que não sejam do seu banco. Lembre-se que sua senha é pessoal e intransferível.



Veja a seguir um roteiro com orientações de segurança elaboradas pela Febraban para não cair em armadilhas no internet banking ou mobile banking:

- Mantenha os antivírus originais instalados no computador atualizados para ter acesso aos serviços bancários;
- Troque periodicamente sua senha de acesso ao banco na internet e utilize sempre senhas de bloqueio de uso do seu smartphone;
- Só utilize equipamentos efetivamente confiáveis. Nunca realize operações financeiras em equipamentos públicos, desconhecidos ou que não tenham programas antivírus atualizados;
- Não utilize telefones de estranhos e de origem desconhecida para efetuar transações ou fazer ligações;
- Evite emprestar ou perder de vista seu smartphone;
- Ao ter seu telefone roubado, furtado ou perdido, informe imediatamente ao seu banco;
- Procure informar-se com o fabricante de seu smartphone quais os softwares e opções de segurança disponíveis para o aparelho;
- Fique atento ao acessar sua loja de aplicativos. Evite obter aplicativos de origem desconhecida;
- Não execute aplicações nem abra arquivos de origem desconhecida. Eles podem conter vírus, que ficam ocultos para o usuário e permitem a ação de fraudadores sobre sua conta, a partir de informações capturadas após a digitação no teclado;
- Use somente provedores confiáveis. A escolha de um provedor deve levar em conta também seus mecanismos, políticas de segurança e a confiabilidade da empresa;
- Use senhas fortes. O uso de senhas fortes e não óbvias dificulta a captura ou quebra delas por parte de programas hacker. Não utilize a mesma senha usada em redes sociais ou ambientes menos seguros;
- Não confie em e-mails de origem desconhecida. Sempre se informe com seu banco sobre os tipos de e-mails que ele costuma enviar aos clientes;
- Não clique em links de origem desconhecida. Muitos deles oferecem downloads suspeitos ou atalhos para sites falsos. Sempre que for acessar seu banco, digite o endereço no navegador, não use mecanismos de busca;
- Não use redes wireless (wi-fi) desconhecidas ou em locais públicos para efetuar transações bancárias;
- Em sua residência, mantenha sempre sua rede wi-fi protegida por senha;
- Evite navegar em sites arriscados ou de conteúdo suspeito, e só faça downloads (transferência de arquivos para o seu computador) de sites que conheça e saiba que são confiáveis;
- Utilize sempre as versões de sistemas operacionais e browsers (programas de navegação) originais e atualizados, pois geralmente incorporam melhores mecanismos de segurança;
- Evite acessar o site dos bancos redirecionado por outros sites, como os de pesquisa. Sempre acesse o site do banco diretamente pelo endereço do banco;
- Quando for efetuar pagamentos ou realizar outras operações financeiras, você deve certificar-se que está no site desejado, seja do banco ou outro qualquer, “clicando” sobre o cadeado e/ou a chave de segurança que aparece quando se entra na área de segurança do site. O certificado de habilitação do site, concedido por um certificador internacional, aparecerá na tela, confirmando sua autenticidade, juntamente com informações sobre o nível de criptografia utilizada naquela área pelo responsável pelo site (SSL);
- Tenha cuidado no uso de token. A maioria dos bancos usa o token para gerar senhas no momento de executar alguma transação. Suspeite caso o site do banco peça a senha do token mais de uma vez para a mesma sessão. Certifique-se, com o atendimento do seu banco, se o processo está correto;
- Bloquear o acesso a determinados apps específicos, exigindo uma senha para abri-lo: hoje em dia há quadrilhas especializadas em roubo de celular com o intuito de fazer transações financeiras em apps desprotegidos: a vítima está na rua falando ao celular, o ladrão rouba o aparelho e a quadrilha já começa a fazer operações usando qualquer aplicativo que tenha seu cartão salvo: aplicativos de delivery, sites de lojas, empréstimos em financeiras, etc. Assim, se seu celular permitir bloquear o acesso a esses apps, é uma boa ideia ativá-lo;
- Acompanhe periodicamente os lançamentos em suas contas. Caso constate qualquer movimentação irregular, entre imediatamente em contato com seu banco;
- Em caso de dúvida sobre algum procedimento de segurança que executou, ou sobre quais medidas de proteção estão sendo tomadas quanto à segurança das transações on-line, procure seu banco.

Sem dúvida, o meio *on line* é um facilitador para obter crédito, fazer operações e até cuidar das finanças, mas mantenha sempre vigilante para a facilidade não se tornar um problema. Fazer negócios com sites pouco conhecidos, com ofertas "boas demais para ser verdade", podem trazer grandes dores de cabeça.

Por isso, siga nossas dicas e tenha atenção às suas operações financeiras *on line*. Assim, você terá a certeza de aproveitá-las ao máximo, mas sem problemas.

Fique ligado: no próximo mês, falaremos sobre ***Os Pilares da Segurança da Informação nas Empresas***

Tribunal Regional Eleitoral - RN