APCS/DGPAd

Guia de prevenção:
Cuidados para realização de transações bancárias
(computadores ou dispositivos móveis)

POLÍCIA CIVIL SÃO PAULO SP

Departamento Estadual de Investigações Criminais
DEIC

DIVISÃO DE CRIMES CIBERNÉTICOS

Cuidados para realização de transações bancárias

Atualmente transferir dinheiro é fácil e rápido, principalmente com o uso de ferramentas como o PIX. Mas essa agilidade também é aproveitada por criminosos e golpistas. Com alguns cuidados com sua segurança pessoal e precauções a serem tomadas com seus dispositivos, transferir valores virtualmente não se tornará uma dor de cabeça.

Antes de mais nada, tome algumas precauções para sua segurança pessoal:

Evite utilizar seu smartphone em locais públicos e de forma desatenta, seja em ligações, mensagens ou manuseio de aplicativos. Criminosos podem se aproveitar de um segundo de sua distração e subtrair seu telefone ainda desbloqueado!

Evite realizar transações bancárias em seu smartphone ou manuseá-lo no interior de seu veículo estacionado (muito menos no veículo em movimento). Procure um local seguro para usar seus dispositivos. A luz da tela do seu celular pode chamar a atenção de pessoas e criminosos, mesmo que seu veículo possua película nos vidros.

Caso seja possível ter mais de um aparelho celular, circule em via pública apenas com o telefone que não tenha o aplicativo do banco instalado. Se ele for subtraído, ninguém conseguirá acessar sua conta bancária, mesmo que instale o aplicativo do banco, já que o aplicativo precisa de uma autenticação feita por você e pelo banco (exemplo: autorizar o smartphone em um caixa eletrônico usando sua senha ou impressão digital).

Seja o mais discreto possível com suas redes sociais. Não ostente valores ou bens e evite compartilhar localizações ou sua rotina. Essas informações podem ser acessadas e utilizadas por criminosos.

Cuidados para realização de transações bancárias

Após cuidar da sua segurança, é hora de cuidar da segurança do seus dispositivos e de sua conta bancária:

Jamais acesse “links” desconhecidos enviados para seu celular ou computador. Estes “links” podem conter um vírus espião, também chamado de “spyware”, que infecta seu dispositivo e coleta informações pessoais, informações de navegação na internet e vários outros dados particulares.

Adote, em todos os sistemas operacionais, aplicativos e dispositivos que puder, a verificação em duas etapas para criar uma camada extra de proteção e dificultar a invasão por cibercriminosos.

Não armazene qualquer tipo de senha no seu dispositivo (muito menos senhas bancárias ou senhas de desbloqueio). Um descuido muito comum é, por exemplo, armazenar senhas em um arquivo do bloco de notas no celular ou computador. Esse arquivo com suas senhas pode ser facilmente encontrado se um cibercriminoso invadir seu dispositivo.

Permita, sempre que possível, o compartilhamento de sua geolocalização com a sua instituição bancária no momento em que realizar transações bancárias. No caso de alguma transação fraudulenta, é possível saber onde ela ocorreu.

Solicite que sua agência bancária fixe limites de transferência TED, DOC e PIX (diários, mensais etc) para valores adequados à sua movimentação financeira normal.

Com esses simples cuidados você realizará suas transferências por smartphone ou computador de modo muito mais seguro.

Cuidados para realização de transações bancárias

Se você for vítima de um golpe envolvendo transações bancárias:

Procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através da Delegacia Eletrônica:

https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home