Veículo: O Liberal		
Data: 12/02/2017	**Caderno:** Poder	**Página:** 16
Assunto: Aplicativo		
Tipo: Notícia	**Ação:** Espontânea	**Classificação:** Positiva

Aplicativos facilitam operação bancária

TECNOLOGIA

Internet facilita a vida dos usuários, mas exige cuidado com ladrões virtuais

VITO GEMAQUE
Da Redação

Os aplicativos de bancos para smartphones e tablets tem facilitado o dia a dia de muitas pessoas em tarefas que antes só eram possíveis indo a uma agência bancária ou caixa eletrônico. A mobilidade dos aplicativos tem o seu preço. Se por um lado, os clientes não precisam mais andar com dinheiro para realizar depósitos ou pagamentos, por outro, o roubo de informações dos celulares por criminosos virtuais (crackers) é um risco presente. Alguns cuidados básicos podem impedir esse roubo.

O publicitário Erik Lopes, 27 anos, quase não vai mais a agências bancárias. Ele resolve todas as suas necessidades por meio do celular e do computador. Como medida de segurança, Erik evita andar com dinheiro, tenta fazer todas as transações por meio da internet ou de cartões de débito e crédito. "Facilitou muito, eu odiava ir para banco pegar a fila. Pelo menos algumas coisas o aplicativo resolve bem, como pagar as contas, as fatura de código de barras e transferências. Teve uma época, por exemplo, que tive que fazer muitos pagamentos por causa de um projeto e foi tudo por transferência. O aplicativo ajudou muito. Quando preciso pagar alguém uso o aplicativo, não saco mais dinheiro", contou.

Os criminosos também se aperfeiçoaram. Com o mundo se tornando cada vez mais digital, os ladrões buscam a mercadoria mais preciosa: informações pessoais. Diferentes tipos de golpes virtuais podem enganar até as pessoas mais atentas. Há seis meses, Erik foi vítima de um golpe conhecido por "phishing" - palavra em inglês que remete a "pescaria". Os criminosos tentam "pescar" informações pessoais dos usuários, como números de cartões de crédito e senhas bancárias, seja por de e-mails, links ou sites falsos de instituições financeiras ou órgãos públicos. Erik havia pensava ter acessado o site oficial de seu banco, mas estava em um site "clone" criado para roubar informações.

"Tive problema e foi pelo computador. Ele pegou um vírus e tentaram fazer uma transferência da minha conta. O banco notou a ação, bloqueou e me ligou na hora. Eles não me falaram da quantia que tinha sido, mas aquilo não correspondia ao meu hábito bancário. Eles detectaram que poderia ser fraude", relembra.

O site falso havia sido totalmente copiado do original, apenas uma coisa estava diferente. "O site era idêntico só que tinham algumas coisas diferentes. Tinha uma coisa besta que era diferente do original. No normal, quando fazia o login, tinha que clicar no meu nome e depois colocar a senha. Já no outro pedia para digitar o login e a senha eletrônica. Pensei 'acho que o site mudou', mas depois que entrei estranhei porque deu como se o sistema estivesse fora do ar. No mesmo dia me ligaram do banco", conta.

Algumas ações de segurança digital simples podem dificultar a ação dos criminosos. Segundo o professor do curso de Ciência da Computação da Universidade Federal do Pará (UFPA) Roberto Samaroni, que tem doutorado em segurança digital, não há sistema totalmente seguro. Entretanto, as pessoas podem dificultar muito a vida dos criminosos. "As pessoas precisam entender que o celular é como se fosse um computador de bolso. O celular é passível dos mesmos risco que o computador que você tem em casa, com um potencial maior, porque você está usando ele na rua e pode ser roubado", alerta.

De acordo com Samaroni, o elo mais frágil da segurança na internet é o usuário final. Como bancos e empresas de tecnologia sempre estão atualizando programas e procurando se defender de invasões, o usuário final pode ser a porta de entrada para os aproveitadores. O professor ressalta que o comportamento das pessoas é fundamental para que os dados fiquem seguros. "Depende muito delas. As pessoas precisam de conhecimento também, não só com relação a celular, mas em computação em geral. O usuário final não é corretamente treinado para se defender de ataques. Tem que pensar será que aquele site é confiável, se você não me conhece, porque você abriria um link que eu te passei?", falou.

TARSO SARRAF / O LIBERAL

Erik Lopes usa o celular para tudo, mas já sofreu tentativa de golpe na internet

É vírus!

CONHEÇA AS INFECÇÕES MAIS COMUNS NA INTERNET

Phishing
→ É a tentativas de obter senhas, número de cartões de crédito e outros dados pessoais. Emails, sites falsos e até links de mensagens de Whatsapp podem ser "phishing"

Malwares
→ Termo do inglês para "malicious software" (software nocivo ou software malicioso), que são os programas destinados a infiltrar-se em um sistema de computador de forma ilícita, com o intuito de causar danos, alterações ou roubo de informações

Cavalo de Troia
→ Também conhecidos como "trojans", são malwares que entram no computador e criam uma porta para uma possível invasão. Permanecem ocultos enquanto instalam ameaças mais robustas em computadores e laptops

Veja como se manter seguro

1 - Ter um programa antivírus no smartphone, tablete ou computador
2 - Ter o programa de antivírus e o sistema constantemente atualizados
3 - Somente baixar aplicativos e programas das lojas oficiais para Android e iPhone
4 - Ver nas informações dos aplicativos de bancos se o nome da empresa que oferece o aplicativo e o email do desenvolvedor correspondem ao banco
5 - Não ter senhas fáceis como data de nascimento ou iniciais de nome e nem gravar as senhas no celular
6 - Utilizar o bloqueio de tela com senha para usar o dispositivo