Defesa contra os Hackers

Lívia Silva Simões

Luis Filipe Barcelos Matoso

Samuel Jackson Amaral Martucheli

Thales Filizola Costa

Vitor Fonseca de Melo

Resumo: Os crimes virtuais acontecem todos os dias e você pode ser a próxima vítima se não ficar atento. Mostraremos os tipos de ataques hackers mais comuns e apresentaremos dicas para evitar cada um desses ataques. A intenção desse trabalho é impedir que hackers tenham acesso ao seu perfil em redes sociais e à sua conta bancária.Eduardo Martins Barbosa

Desde sua criação em 1969, a Internet tem se tornado parte do cotidiano de cada vez mais pessoas, permitindo desde o entretenimento até a execução de tarefas rotineiras, como consultar extratos bancários. Muitos dos usuários disponibilizam informações pessoais na rede de computadores, em redes sociais como Orkut, Facebook e Twitter, e tem acesso a dados privados através dela. Porém, nem todos tomam as devidas precauções para proteger suas informações na rede de computadores, se tornando vítimas dos crimes virtuais.

Os crimes cometidos pelos denominados *cyber* criminosos vão desde roubos de perfis nas redes sociais para difamação do usuário, o que provoca desconfortos e situações, no mínimo, embaraçosas, até roubos de senhas de cartões de crédito, ou bancárias causando prejuízos financeiros e inconvenientes tanto para os cliente quanto para a empresa envolvida.

Para saber como se proteger, e não ser alvo desses ataques hackers*,* é preciso conhecer a maneira de agir desses criminosos para roubo de informações. Uma das maneiras mais comuns, ocorre com a instalação de programas conhecidos como Cavalos de Troia (*Trojan*) no computador da vítima. Tais programas funcionam como um espião que passa relatórios completos aos hackers sobre as atividades realizadas pelo usuário na máquina. Nesse relatório encontram-se dados como as senhas digitadas no teclado para acesso a qualquer serviço feito pelo usuário.

A única maneira de se proteger desses ataques é impedir a instalação desses programas espiões na máquina. Um *trojan* é instalado na máquina com permissão do usuário, porém de maneira que ele não se dê conta de que é esse o tipo de software que está sendo instalado. Apoiando-se na curiosidade das vítimas, anúncios em sites do tipo “Clique aqui”, ou e-mails com alegações falsas sobre fotos ou vídeos de artistas ou da própria vítima em situações embaraçosas, são os principais disfarces dos programas mal-intencionados. A vítima acaba abrindo um link onde as supostas fotos ou vídeos poderiam ser vistos, ou clicando no anúncio, e permitindo a instalação de um falso *plugin*. É preciso portanto, usar o bom senso evitando abrir e-mails não desejados e de fontes desconhecidas. Além de tomar as devidas precauções durante a navegação e manter um antivírus instalado e atualizado na máquina para detectar possíveis ameaças.

Outro tipo de ataque ocorre com a disseminação de e-mails que tentam convencer a vítima a contribuir com altas quantias de dinheiro sobre pretextos falsos, seja oferecendo grandes oportunidades ou pedidos de ajuda. Na edição desse mês (novembro/10), a revista Super Interessante traz a reportagem
“Caímos nos golpes da web”, descrevendo o golpe virtual mais comum no Brasil, “e-mails em que o seu banco pede um recadastramento ou a instalação de algum software.” Se a vítima cai nesse golpe, as informações bancárias fornecidas “vão parar nas mãos de bandidos”.

Como os criminosos se apoiam na generosidade e na ganância dos usuários, para se proteger desses golpes, o melhor é estar sempre atento e desconfiar de toda a história que lhe for contada. Averiguar

se o pedido de ajuda é sincero e se a história é real antes de fazer doações, ou verificar se as ações que prometem alta rentabilidade são reais e confiáveis antes de investir, são atitudes necessárias e precatórias. Vale sempre lembrar que agências bancárias nunca pedem informações sigilosas por e-mail. E em caso de dúvidas, o recomendado é ligar para a agência, ou ir até lá.

Roubo de senhas porém, é algo que ocorre muito antes do advento da Internet. Muitas pessoas, temendo esquecer-se das senhas que usa, deixam as mesmas anotadas e as guardam em lugares pouco seguros, próximos ao computador, por exemplo. Esses lugares são intuitivos, e seriam os primeiros lugares em que alguém, com intuito de furtar sua senha, iria procurar. O recomendado, portanto, é criar senhas fáceis de se memorizar, para que não seja necessária anotá-la em nenhum local. Ou então guardar a senha em locais seguros, dos quais só você tenha conhecimento ou acesso.

Senhas fáceis, porém não são senhas óbvias, como data de nascimento ou nome de pessoas próximas como namorado(a), esposo(a), etc. Sempre que possível use combinações entre letras e números, além de caracteres especiais, como exclamação (!), cifrão ($) e arroba (@). É possível também trocar letras, por outros caracteres que tenham um formato parecido, como por exemplo, trocar o dígito“1” pela exclamação “!”, ou a letra “S”, pelo cifrão “$”. Iniciais de trechos de músicas ou livros, ou palavras-chaves e acontecimentos que sejam marcantes também podem ser usados para criar senhas fáceis de se lembrar, mas não fáceis de se adivinhar.

Se proteger dos cyber crimes, é então uma tarefa fácil. É possível aproveitar as facilidades que a Internet trouxe na execução de tarefas cotidianas e aproveitar as novas formas de entretenimento que ela proporciona tomando apenas alguns cuidados. A dica é sempre desconfiar e utilizar o bom senso para garantir uma boa navegação.

Referências

VAN DEURSEN, Felipe. Caímos nos golpes da Web. Revista Super Interessante, São Paulo, e. 284, p. 68-73, nov. 2010.