

Crimes cibernéticos: a vítima é você

Crimes financeiros, roubo de dados, golpes virtuais, *bullying* cibernético, roubo de identidade, pornografia e pedofilia infantil, privacidade, estão atualmente entre os temas que mais atraem a atenção quando se fala em tecnologia e segurança da informação. São diversos os casos que vimos na mídia e ouvimos falar, isso quando não conhecemos alguém ou fomos nós mesmos vítimas de um golpe, de uma fraude, ou de um ataque onde os criminosos se valeram da utilização de recursos de tecnologia da informação.

Para melhor lidar com alguns dos problemas oriundos da atual sociedade da informação, cabe a cada um de nós buscar informações que possam esclarecer como os criminosos operam no meio virtual, e quais práticas podem minimizar os riscos de ser mais uma vítima.

Nesse sentido, devemos estar conscientes de que apesar de utilizações empolgantes que surgem com o uso da Internet, é necessário estarmos alertas aos riscos que vêm junto com essa utilização.

Correios eletrônicos e programas de mensagens instantâneas são formas muito comuns de tentativa de comprometimento de um computador. É muito fácil realizar uma impostura do remetente, alterar o link de um e-mail para direcionar para outro endereço, adicionar anexos que exploram vulnerabilidades em um grande número de computadores, entre outras práticas.

Com a utilização dos *phishing scams* (vide figura 1), que estão cada vez mais sofisticados e muitas vezes focados em alvos específicos (*spear phishing*), o usuário deve desconfiar se um e-mail não é esperado ou se possui algo que é muito bom (ou muito ruim). Em dúvida, entre em contato com o remetente ou cheque com a equipe de segurança de sua empresa.

Além disso, devemos considerar que os navegadores são os principais meios de interação com a Internet e têm sido um alvo considerável por parte dos criminosos. Por oportuno, é altamente recomendável manter o seu navegador sempre atualizado com a última versão, observando que o mesmo procedimento deve ser buscado com o sistema operacional e demais aplicativos em seu computador. Programas como *Secunia Personal Software Inspector* auxiliam bastante nessa tarefa de checar se o seu computador está com todos os programas atualizados. E procure também não instalar *plugins* ao seu navegador, pois eles adicionam mais vulnerabilidades, e, se o fizer, mantenha-os atualizados. O *Qualys Browser Check* pode ajudar na checagem do navegador e seus *plugins*.

Informações pessoais têm sido largamente utilizadas por quadrilhas, que buscam utilizá-las para diversas atividades criminosas, desde montar um perfil com vistas à realização de um sequestro até a de furtos em residências desocupadas. Divulgue sua preocupação com privacidade para os seus familiares e amigos, pois, eles podem estar colocando informações pessoais e fotos suas sem o seu conhecimento, com especial atenção às redes sociais.

Especialmente, converse com seus filhos sobre os riscos do uso da Internet, estabelecendo regras de uso, definindo um usuário com permissões limitadas ao computador, e, se for o caso, configure ou instale um programa para monitorar e controlar o acesso. Lembre-os que uma informação na Internet pode ser lida por milhares de pessoas e permanecer armazenada por muitos anos. Mesmo que seja apagada a informação pode estar armazenada em algum sítio fora do seu controle. Os estragos podem impactá-lo não apenas no presente, como por exemplo o caso de um aluno expulso de uma escola primária devido a postagens no *twitter*, e também no futuro, em situações que empregadores vasculham a vida de potenciais empregados.



Figura 1: Phishing Scam

Trate as suas senhas pensando nos problemas que pode ter caso alguém as utilize e se faça passar por você. Pense que se a senha é fácil de adivinhar, um criminoso poderá facilmente acessar sua conta. As perguntas para recuperação de senha também devem ser bem pensadas, pois muitas vezes a resposta pode ser encontrada na Internet. De modo geral, uma senha deve possuir dez ou mais caracteres, sendo pelo menos um número, uma letra maiúscula e um caractere especial.

A utilização de dispositivos móveis também tem sido abordada por diversas maneiras pelos criminosos. O valor de um *laptop*, *smartphone* ou *pendrive* pode ser interessante para um meliante, mas, em muitos casos, a informação armazenada nestes dispositivos possui um valor muito maior do que o próprio bem. Para tanto, proteja estes dispositivos com senhas, utilize criptografia para tornar a informação ilegível para alguém que não tenha a senha e desabilite o *bluetooth* quando não o estiver utilizando. Se for doar algum dispositivo, faça uma deleção segura (*wipe*) antes de doá-lo.

Preste também muita atenção a redes *wi-fi* públicas, onde todo o tráfego pode ser interceptado e suas informações monitoradas, sendo que já foram reportados diversos casos de redes falsas criadas por criminosos especialmente para este fim. Utilize rede privada virtual (VPN) para transmitir dados importantes ou logar em sua rede e nunca entre com informações pessoais ou financeiras em computadores que você não controla, especialmente os de cyber cafés e de lobbies de hotéis.

Enfim, mesmo com a adoção de todas as devidas salvaguardas possíveis (criptografia, senhas de difícil adivinhação, atualização de programas, utilização de antivírus e *firewall*, VPN, etc), sempre haverá o risco de ser vítima de um crime cibernético. Fique alerta para mensagens do seu antivírus, senhas que não funcionam mais, repentina degradação de performance do seu computador e comportamento incomum do seu navegador. Em caso de suspeitas, cabe contatar um especialista em crimes cibernéticos ou as autoridades competentes o quanto antes e não realizar nenhuma operação que possa comprometer ou contaminar provas.

Marcelo Caiado, M.Sc., CISSP, GCFA, EnCE, trabalha como Perito em Informática na Procuradoria Geral da República. Possui mais de 10 anos de experiência nacional e internacional em segurança da informação e investigação de crimes cibernéticos. É professor em cursos de extensão e de pós-graduação, além de palestrante em diversos seminários e conferências.