

Preocupando-se com o mundo virtual

Uma das grandes preocupações de nossas vidas modernas é nossa segurança. Nisto está incluso a segurança eletrônica, aquela em que colocamos as informações de nossas vidas, de nossas famílias e negócios do mundo real para o virtual.

A preocupação de garantir que estas informações não fiquem disponíveis ao mundo é tão importante quanto nossa subsistência ou o ar que respiramos. Quando violada pode nos afetar de diversas maneiras, em nossa estabilidade monetária, em nossa imagem ou pior, entrar no seio de nossa família e afetá-la em modos que nem sonhamos que possam acontecer. Por ser um mundo relativamente novo tendemos a nos maravilhar e não damos a devida atenção aos seus perigos, mesmo quando anunciados na mídia. O mundo virtual é tão novo (menos de 15 anos para a maioria da população) que não nos damos conta de sua complexidade e da velocidade de sua evolução.

Num estudo da Websense Security Labs, empresa global que analisa dados da web, revelou recentemente que a maioria do que vemos online ou recebemos via email é spam e pode conter códigos maliciosos.

Segundo relatório divulgado pela empresa, 95% de todo o conteúdo gerado por usuários para a web (ou seja, aquilo que vemos nas janelas do navegador) normalmente é spam, e cerca de 85% dos emails enviados contém algum tipo de *scam*, ou seja, indicam esquemas fraudulentos, o velho "conto do vigário". Além disso, mais de 70% dos sites que contém vírus são sites legítimos que foram vítimas de um ataque hacker, destaca o site TechRadar .

Com isso, a segurança na rede fica cada vez mais comprometida: de 2008 para 2009, houve um aumento de 225% no número de sites com códigos maliciosos, com 35% destes sites tendo interesse em conseguir informações confidenciais dos computadores infectados, alerta o site Daniweb .

Há também os riscos que crianças, jovens e até adultos desavisados correm quando estão navegando sem a devida supervisão. Cabe lembrar aos pais que tais cuidados com seus filhos são responsabilidade deles próprios e devem ser levadas muito a sério.

Citaremos alguns pontos em que os trabalhos de investigação e educadores de segurança aprenderam durante a realização de seus trabalhos:

- Uma em cada vinte e cinco crianças já recebeu convites sexuais de amigos virtuais durante um contato "offline", ou seja, o amigo virtual deixou de existir no mundo cibernético e passou a viver no ambiente real de seu filho.
- 4% dos adolescentes que com freqüência se conectam já receberam convites, os quais o solicitante estabelece que seja feito "offline" (telefone, correios ou pessoalmente). Os encontros "online" não supervisionados são a porta para os crimes de pedofilia e sexuais ocorridos.

Então o que podemos fazer?

Em se tratando de vírus, invasões de nossas informações e produção de senhas existem algumas dicas que apresentaremos:

Mesmo com a grande inteligência dos vírus atuais, sempre descobrindo novas formas de disseminação, explorando brechas de segurança em programas muito utilizados, até hoje a maior falha de segurança de um computador é o usuário. Isso, você mesmo!

O usuário não resiste e entra em sites duvidosos, baixa programas executáveis, cracks de sites russos, acredita em promessas de fotos e vídeos do último acidente aéreo (no qual até a caixa preta quase não escapa, imagina então, uma câmera fotográfica). Aceita, executa e re-distribui apresentações com mensagens e lindos fundos musicais (podendo conter também um vírus), etc. O usuário muitas vezes sequer lê o endereço da página para a qual está sendo direcionado ao clicar num link de e-mail. Recebi uma foto-mensagem? Opa! Deixa eu clicar aqui no fotomsg.sitequalquer.ru para entrar no site de minha operadora e ver! Isso acontece mais vezes do que você imagina!

Bons hábitos de navegação lhe trarão muito mais segurança no uso do computador que um software antivírus.

E para senhas? Flavio Amaral do Yahoo notícias traz algumas dicas transcritas aqui de forma reduzida.

“Impressionante que a cerca de dois meses atrás, alguns funcionários da nova febre da internet, o tweeter, tiveram suas contas pessoais invadidas por hackers e conseqüentemente, os servidores da empresa, devido a utilização de senhas extremamente fracas. Os cuidados básicos de escolha de senhas simplesmente não foram seguidos. Isso mostra, mais uma vez, que não adianta gastar dinheiro com programas e equipamento de segurança se as pessoas sempre serão o elo mais fraco (e fácil de quebrar) da corrente.

Vamos a primeira dica e talvez a mais relevante: não coloque todas as informações da sua vida na Internet. Para lembrar das inúmeras senhas que temos, muita gente usa coisas da vida para fazer analogia e não esquecê-las. E como as pessoas gostam de colocar tudo lá, fica fácil construir um perfil completo delas para tentar descobrir senhas. Ninguém colocaria fotos da família, viagens feitas, ou outras informações pessoais em outdoors espalhados pela cidade. Fazer isso na Internet não é nem um pouco diferente. Portanto, quanto menos munção fornecer aos bandidos, melhor.

Para senhas puramente numéricas não use datas de aniversário, casamento, nascimento de filhos, etc. No lugar disso, escolha uma data que tenha relevância somente para você como mês de entrada na faculdade ou de viagens. Mas tente não usar nada que tenha sido exposto na primeira dica.

Senhas com letras e números são mais difíceis de quebrar se usarmos a criatividade. Nunca use somente palavras encontradas em dicionários, pois existem programas especializados em quebrá-las. Em vez disso, opte por uma frase qualquer de um filme, livro ou citação que você goste. Vamos usar a frase seguinte como exemplo: Ninguém descobre esta senha. Se pegarmos as primeiras letras de cada palavra teremos ndes. Deixe alguma delas em letras maiúsculas, acrescente dois números quaisquer e se tiver boa memória para caracteres não alfanuméricos (@#\$%&*:) use-os também. A senha resultante pode ficar assim: NDes84!\$. Muito difícil de ser descoberta e não terá nada a ver com você.

Não use a mesma senha em todos os lugares, isso vale para senhas numéricas e não numéricas. Se você acessar suas contas em Lanhouses ou lugares públicos, troque sua senha assim que chegar em casa ou na empresa. E por último, troque suas senhas regularmente, pelo menos uma vez a cada dois meses, principalmente se você lida com informações de caráter restrito ou sigiloso.”

Mauro Nadruz é Administrador e Gestor de Segurança Pública e Privada, graduado pela Ulbra-RS, com certificação nacional de especialista em segurança [CES] pela ABSO, Diretor da Activeseg, com especializações em análise de risco corporativo, pessoal e patrimonial, projetos de segurança e tecnologia aplicada a segurança.