Veja como garantir a segurança das comunicações pela internet

O mundo virtual está cada vez mais perigoso. Tal como o mundo real. A internet, extremamente útil, mas traiçoeira, obriga os usuários a se preocuparem com *spywares*, *malwares*, *sneakwares*, *phishing* e outros "*softwares* maliciosos" — além do vírus de cada dia. As notícias de que o governo americano e o britânico têm capacidade de interceptar informações que correm pela web, de qualquer cidadão do mundo, trouxeram mais preocupações. E lembram aos operadores da Justiça uma fragilidade particular: a quebra da confidencialidade se tornou fácil no mundo virtual.

O assunto da segurança na internet voltou a esquentar. Jornais e *sites* especializados, como o *ExtremeTech*, *Surveillance Self-Defense* e o *The Guardian*, começaram a publicar dicas de proteção às comunicações pela internet e por telefone. Algumas coisas podem ser feitas, como mascarar o endereço de IP do dispositivo conectado à internet, usar criptografia em todas as comunicações — embora isso possa ser uma tarefa complexa — ou dar preferência à rede privada virtual (VPN), entre outras.

Porém, a bisbilhotice de órgãos de segurança não é a única preocupação. É preciso dar maior importância à segurança de tudo o que se faz na internet, especialmente a comunicações confidenciais, movimentação de contas bancárias e uso de cartões de crédito. Assim, antes de mais nada, cada usuário que queira fechar a porta a ladrões de informações, mensagens, documentos, dados de cartão de crédito e de conta bancária tem de criar sua própria política de segurança. E isso começa pela coisa mais simples: a criação de senhas seguras.

Há recomendações que não são novas, mas que também não são muito observadas. Por exemplo, senhas para redes sociais e de qualquer *site* que exige um *login* para ser usado não podem ser as mesmas para acessar aplicativos de correspondência e envio de arquivos confidenciais por *e-mail*, *dropbox* ou qualquer protocolo de transferência de arquivos (FTP). E as senhas usadas para gerir contas bancárias e cartões de crédito têm de ser diferentes de todas elas e entre si.

É uma recomendação difícil de se colocar em prática. Afinal, seriam tantas senhas que poucos conseguiriam memorizá-las. Porém, existem formas de amenizar a situação. Uma é criar sistemas próprios. Outra é usar programas de gerenciamento de senhas. Um exemplo é o LastPass, que "lembra" todas as credenciais de *login* do usuário e preenche automaticamente os campos, se o usuário quiser. As senhas são armazenadas e um "keylogger", um programa que registra tudo o que é digitado — o mesmo *keylogger* que, muitas vezes, é usado para a criação de *spywares*, *softwares* de *phishing*, etc.

Assim, só é preciso lembrar a senha desse programa — uma senha que tem de ser inesquecível, obviamente, para que todas as senhas não fiquem eternamente perdidas no *keylogger*. O LastPass trabalha com todos os navegadores mais populares da internet e tem uma versão gratuita — uma versão "gratuita", com um preço: o usuário é obrigado a conviver com mensagens publicitárias. Para se livrar delas e desbloquear algumas funcionalidades para comunicações móveis, é preciso fazer uma assinatura anual que, nos EUA, custa US$ 12 por ano.

A alternativa seria fazer anotações em uma caderneta e colocá-la na gaveta. Não das senhas, em si, porque isso seria um disparate. Mas de palavras ou frases que fazem você se lembrar da senha e que só

2023 - www.conjur.com.br - Todos os direitos reservados.

você pode decifrar. Por exemplo, qual é a senha da anotação "Viagem mais sonhada", para sua conta no banco? A resposta é "Aporue+2015". Sua viagem dos sonhos é ir à Europa em 2015. Europa de trás para a frente é "Aporue". O "mais" na anotação é o sinal "+".

Outro exemplo: qual é a senha da anotação "Chico e telefone" para o cartão de crédito? Resposta: "menCacoe&1243". Chico, filho de amigos, falava essa palavra "mencacoe", quando tinha três anos. Inesquecível. O telefone da família terminava em 1243. O "e" da anotação é o sinal "&". Você, certamente, conseguirá criar coisas melhores.

Se você conhece palavras de algum dialeto ou de um idioma pouco popular, pode encontrar palavras para a senha e colocar a anotação em português na caderneta. Palavras que constam de dicionários são mais facilmente descobertas e, portanto, não devem ser usadas. É preciso ser criativo: fabricar palavras, usar palavras de idiomas pouco conhecidos, utilizar palavras excêntricas inesquecíveis, escrever palavras de trás para a frente. A senha deve ser formada por essa palavra, com o uso de letras maiúsculas e minúsculas (nem sempre na primeira letra; às vezes pode estar na sílaba acentuada) ou, ainda, números e sinais (como *, +, &, $ e outros).

O nível de segurança das senhas tem de ser muito alto. Mas o que se faz é o contrário. A senha mais popular do mundo, por exemplo, é "monalisa" — muito fácil de decifrar para os peritos. A maioria das senhas ainda é formada por uma palavra ou duas palavras emendadas, em letras minúsculas, como era uma exigência no passado.

Existe toda uma ciência, hoje, sobre a atividade de "quebrar" senhas, que é longamente analisada em um estudo do professor da Universidade de Cambridge Joseph Bonneau.

Não cair nas garras de *hackers*, sejam os malandros cibernéticos ou oficiais dos altos escalões governamentais de uma nação poderosa, é mais uma questão de bom senso do que de alta ciência. Não ter um sistema pessoal seguro de senha, clicar em um *link* enviado por qualquer meio, em vez de digitá-lo no campo para a URL no navegador, abrir anexos enviados por *e-mail* por desconhecidos são riscos que desafiam o bom senso.

Inimigo oculto
No entanto, todos os esforços para se criar uma senha segura podem ser inúteis se um *spyware* que registra toques no teclado se instalar em seu computador. Assim, um bom programa de proteção contra vírus, *spywares* e outros *softwares* maliciosos é indispensável, apesar de usuários avançados reclamarem que eles reduzem o desempenho do computador. Mas isso é brincar com fogo. Um *software* malicioso e sorrateiro pode se instalar no computador, sem deixar o menor sinal.

Muitos *sites* obrigam o usuário a se registrar para que tenha acesso a seu conteúdo. No mínimo, você terá de informar ao *site*, aos órgãos de segurança dos EUA e ao mundo seu endereço de *e-mail*, nome de usuário e senha. Mas há uma maneira de dar a volta por cima nessa exigência, em vez de utilizar a "monalisa" mais uma vez. O *software* BugMeNot, por exemplo, permite ao usuário utilizar contas de *login* compartilhadas. É uma maneira de ver conteúdo gratuito sem realmente se registrar.

Fazer atualizações constantes do sistema operacional também é uma medida necessária. No entanto,

2023 - www.conjur.com.br - Todos os direitos reservados.

sistemas operacionais como o Windows só fazem a atualização de seus próprios *softwares* ou aplicativos. Não detectam necessidades de atualização de outros *softwares*, como Adobe Flash, Firefox etc. O Personal Software Inspector (PSI), gratuito, faz uma auditoria do sistema e aponta todos os programas que precisam ser atualizados.

Para as firmas de advocacia, a forma mais segura de proteger seus *e-mails* com informações confidenciais ainda é a criptografia e, frequentemente, a autenticação das mensagens. Isso impede que o conteúdo do *e-mail* seja lido por bisbilhoteiros. Existem diversas ferramentas para criptografar mensagens de *e-mail*, que usam chaves públicas e privadas. Geralmente, a ferramenta de criptografia automática é paga. A gratuita tem de ser trabalhada manualmente.

Java Script, Java, Flash, Silverlight e outros *plugins* são ferramentas interessantes, às vezes necessárias, mas também são perigosas. Assim, é bom instalar um *software* que bloqueia o JavaScript e outros, a não ser para os *sites* que o usuário confia. Por exemplo, quem usa o Firefox pode instalar a extensão NoScript , que se baseia em uma lista de exceções (*whitelist*) de *sites* seguros para permitir a execução de JavaScript, Java, Flash e demais *plugins*. Em outras palavras, é um programa que considera todos os *sites* "culpados", até que se provem inocentes.

Entretanto, a senha dos sonhos a ser "quebrada", para os criminosos cibernéticos, é a do cartão de crédito. E a perícia deles é certamente maior do que os dotes computacionais dos usuários comuns da Internet. Por isso, uma nova prática vem se popularizando nos EUA, aos poucos: solicitar a alguma administradora de cartão de crédito um limite baixo, como, por exemplo, de US$ 200. O saldo desse cartão é mantido sempre o mais baixo possível. Quando se quer fazer uma compra pela internet, esse é o cartão a ser usado.

Date Created
16/06/2013

2023 - www.conjur.com.br - Todos os direitos reservados.