Medidas simples podem aumentar segurança contra crimes eletrônicos

Apesar do avanço dos recursos eletrônicos e das medidas administrativas e jurídicas no combate aos crimes cibernéticos, o descuido das pessoas continua criando a ocasião que “faz o ladrão”. A Lei 12.735, que tipificou infrações cibernéticas no Brasil, por exemplo, foi publicada no dia 3 de dezembro e entra em vigor em março. Mas de nada adiantam ferramentas sofisticadas se as pessoas deixam de tomar as precauções mais simples, conta a jornalista Kashmir Hill, da revista *Forbes*.

Há sistemas de segurança elaborados especialmente para a comunidade jurídica, especialmente sensível a roubos de dados. Afinal, o acesso de intrusos a informações confidenciais de clientes, de casos em andamento, do escritório do advogado, da sala do promotor ou do gabinete do juiz pode gerar consequências irreversíveis.

"Absolutamente nada é seguro. Quanto mais potencialmente valiosa a informação, haverá maior investimento em inteligência e espionagem para obtê-la", diz o advogado **Jair Jaloreto**, especializado em crimes financeiros. "As informações só devem estar disponíveis a quem interessa: ao advogado, seu cliente e o juiz da causa."

Antes de armar um sistema sofisticado de segurança para transformar seu ambiente em uma fortaleza contra ataques cibernéticos, o profissional deve se preocupar com coisas mais simples, tais como "fechar a porta da casa". Isso significa adotar medidas mínimas de proteção de dados em smartphones, tablets e computadores. E o mais importante: tornar isso um hábito.

"De fato, vem ocorrendo um aprimoramento tecnológico e jurídico para aumentar a esfera de proteção dos usuários da rede mundial de computadores. Mas enquanto os próprios usuários não se conscientizarem de que suas ações ou omissões podem se consistir em verdadeiros gatilhos para a prática de atos lesivos por terceiros, nada será suficientemente eficaz", diz o advogado **David Rechulski** , especializado em crimes cibernéticos.

A Forbes relaciona dez medidas "arroz-com-feijão" às quais qualquer profissional, incluindo os da comunidade jurídica, deve se habituar para se proteger contra bisbilhoteiros, intrusos e criminosos. Algumas recomendações, apesar de parecerem óbvias, são desprezadas por pessoas que não podem ser consideradas ingênuas:

1. Faça o que todos sabem que é óbvio: use senhas para proteger seus dispositivos
Parece inacreditável, mas muitos usuários de smartphones, tablets e computadores não se dão ao trabalho de registrar senhas ou não têm paciência para digitá-las, quando querem usar seus dispositivos. Isso equivale a deixar algo valioso no banco do carro e com a porta destrancada. Nenhum ladrão resiste à ocasião. Não é uma necessidade apenas para quem tira fotos comprometedoras com o celular — fotos que acabam na Internet. É uma necessidade de proteger mensagens e documentos confidenciais.

"Muitos internautas também têm o péssimo hábito de salvar, para preenchimento automático, suas senhas ou chaves de acesso para login", diz Rechulski. "Fraudes corporativas, envolvendo perdas milionárias porque funcionários compartilharam seus logins e senhas, em violação à política de

segurança da informação, já se tornaram uma rotina."

2. Crie alertas do Google
Você pode criar alertas com o seu nome, o nome do escritório e palavras-chave ligados a suas informações confidenciais. Se qualquer deles for mencionado na Internet, você recebe um alerta por e-mail. Os alertas também são úteis para se acompanhar algum tema de interesse do usuário.

3. Use as redes sociais com moderação
Muitos assuntos privados caem em mãos erradas ou se tornam objeto de investigação porque as pessoas não tomam essa simples providência: ir à configuração de privacidade do Facebook para trocar o acesso público para personalizado, limitando o acesso de pessoas à página. Certifique-se de configurar a privacidade em todas as redes sociais.

Além disso, é preciso declinar o convite das redes sociais para atualizar seu perfil. Via de regra, redes sociais são um perigo constante. São altamente susceptíveis a falhas de segurança e uma fonte de provas contra o usuário, quando qualquer tipo de suspeita recai sobre ele.

"Não escreva nada na internet e nas redes sociais que não possa ser escrito em um outdoor", recomenda Jaloreto. "Mesmo que uma prova obtida de forma ilícita for assim considerada por decisão judicial, certamente influenciará o julgador que a ela teve acesso, e pode ser um problema ainda maior se vir a público", ele diz.

4. Desconecte-se do serviço ao terminar de usá-lo
Depois de se comunicar pelo Linkedin, Twitter, Facebook, MSN, Gmail ou qualquer serviço de e-mail baseado na Internet, não se esqueça de "sair" ou fazer o "logout". Isso impede que qualquer pessoa que tenha acesso a seu dispositivo — emprestado, perdido ou roubado — tenha acesso a seu conteúdo. No caso de usar um computador emprestado ou em qualquer lugar público, isso se torna especialmente importante. Mesmo que esteja atrasado ou com pressa, perca mais alguns segundos e evite um problema maior.

5. Não divulgue seus dados pessoais
Não informe a sites de lojas, organizações ou pessoas seu endereço de e-mail, número de telefone ou CEP, a não ser a quem você confia. Muitas lojas vendem seu "perfil" e seus "interesses de compra". Em alguns casos, você pode optar por não fornecer essas informações.

6. Criptografe seu computador
A palavra "criptografia" pode soar como uma traição à simplicidade prometida para esses procedimentos de segurança, mas é uma coisa fácil de fazer. Criptografar seu computador significa que qualquer outra pessoa precisa ter sua senha — ou chave criptográfica — para ter acesso ao conteúdo em seu disco rígido. Em um Macintosh, basta ir a “Preferências”, “Segurança”, “Filevault” e “Ativar”. Em PCs, pode-se usar, por exemplo, o Bitlocker. No caso de advogados, promotores e juízes, essa medida é indispensável.

7. Ative o segundo passo de autenticação do Gmail
Essa simples medida pode tornar praticamente impossível violar suas mensagens de e-mail por alguém

que tenha acesso a seu smartphone ou tablet. Para que outra pessoa tenha acesso a suas mensagens, ela precisa ter, além de seu nome de usuário e sua senha, um código que é enviado para seu telefone. A Google diz que milhões de pessoas utilizam essa ferramenta. Para qualquer outro serviço de e-mail baseado na Web, procure conhecer suas medidas extras de segurança.

8. Pague em dinheiro por itens "embaraçosos"
Em muitos países, como nos EUA, todas as transações feitas por meios eletrônicos são facilmente rastreadas e o comprador é identificado. "Assim, se você é um defensor da vida saudável, mas por qualquer motivo come um hambúrguer e batatas fritas, pague em dinheiro", diz a jornalista Kashmir Hill. Pessoas importantes já tiveram problemas por causa do tipo de vídeos que alugaram nas locadoras, que pagaram por algum meio eletrônico.

"Também é comum, em alguns sites de comércio eletrônico, o armazenamento do número do cartão de crédito dos usuários para compras regulares. Essas práticas, dentre outras igualmente temerárias, mais cedo ou mais tarde, se reverterão em prejuízo certo, em transtornos gravíssimos. E, às vítimas, só restará o arrependimento por terem contribuído inadvertidamente com seu próprio malfeitor", diz Rechulski.

9. Limpe o histórico e os cookies de seu navegador
Se você não toma essa providência frequentemente, configure seu navegador para que faça isso automaticamente a cada sessão. Você também pode configurar o navegador para não registrar o histórico dos sites que visita. Existem add-ons, como o TACO, que o ajudam a reduzir o rastreamento de sua navegação.

10. Use máscara de IP
Toda vez que você visita um website, deixa uma pista de sua "presença", na forma de informação de IP. Quando o proprietário do site checa sua analítica, consegue detectar essa informação. Se você não quer deixar pistas, deve usar um software que mascara seu endereço de IP.

"Logo, a segurança da informação só será efetiva quando sustentada, preponderantemente, pelo tripé consciência em boas práticas de uso, tecnologia de proteção sistêmica e efetiva aplicação da lei contra os cibercriminosos", conclui Rechulski.

Date Created
07/01/2013