Ataques tiram sono das empresas
Ataide de Almeida Jr.

Vazamentos de informações pessoais na internet aumentam e provocam problemas para usuários e companhias — como Facebook e Sony. Saiba como se proteger, tendo um bom pacote de segurança instalado no PC

"Podemos combinar as informações enviadas da sua conta com informações de outros serviços ou de terceiros para uma experiência melhor e aprimorar a qualidade dos nossos serviços." Esse trecho está diluído na maior parte das políticas de privacidade dos sites.

Mas, infelizmente, só é lembrado quando os dados de quem se cadastra em um serviço de e-mail ou em uma rede social vazam e, muitas vezes, caem nas mãos de cibercriminosos.

Isso ocorre com uma frequência cada vez maior. Segundo estudos da organização DataLoss DB, só em 2010 foram 498 casos de vazamento de informações no mundo. Este ano, já chega a 197. A maior parte, quase 30%, causada por ataques de cibercriminosos.

Há uma mudança de perfil nos ataques. Eles estão ficando mais complexos e isso faz com que sites tenham que se antecipar a essas ações.

"Hoje, a grande parte das corporações faz investimento para proteger os dados de fora para dentro, mas não o contrário", diz Vicente Lima, diretor comercial da Symantec Brasil. "A maioria das informações que se perdem atualmente deve-se à falta de investimento em ferramentas para proteger os dados dos usuários." Pela segunda vez em menos de um ano, o Facebook deixou vazar dados de usuários para terceiros. A empresa de segurança Symantec informa que, apenas em abril, cerca de 100 mil aplicativos utilizados na rede social tinham acesso a arquivos, fotos e — pasmem — conversas dos cadastrados. A brecha de segurança existe desde 2007, quando a empresa de Mark Zuckerberg liberou o uso de programas dentro do site. Por esse motivo, a companhia de segurança não divulgou uma estimativa de quantos cadastros vazaram. "É preciso ter em mente qual site será acessado.

O usuário tem que confiar as suas informações apenas em algo que tem uma reputação construída — e mesmo assim desconfiar", ressalta Lima.

Dois ataques de hackers também balançaram a gigante japonesa Sony. Quase 100 milhões de usuários com contas na PlayStation Network (PSN), a rede que dá acesso a jogos multiplayers e possibilita baixar conteúdo extra, tiveram nomes, endereços, e-mails, data de nascimento, logins e senhas roubadas.

O segundo foi no provedor So-Net, também da Sony — no qual um intruso roubou pontos virtuais (uma espécie de recompensa dos usuários) no valor de US$ 1,2 mil. A empresa estima um prejuízo de US$ 3,2 bilhões este ano, o maior da história da companhia. "O processo de manutenção do sistema de segurança desses serviços não termina nunca. É impossível saber se alguém está 100% seguro contra esses ataques", disse Howard Stringer, presidente - executivo da Sony em entrevista ao Wall Street Journal.

GEOLOCALIZAÇÃO

A maior parte dos smartphones possui um sistema de geolocalização integrado ao aparelho. Quando ativado, o sistema permite fazer a localização de uma loja nas redondezas, utilizar os serviços de mapa e o GPS, além de utilizar aplicativos como o foursquare. No entanto, dois pesquisadores do Reino Unido revelaram que o iPhone guarda todas as informações de localização do usuário desde que foi lançado o iOS 4 (sistema operacional dos celulares da Apple). O pior é que toda informação de onde o usuário esteve não tinha nenhum tipo de proteção.

"Essa é uma tecnologia muito interessante e traz uma série de benefícios, como localizar lugares próximos. Mas, a partir do momento que se assume uma nova tecnologia, sempre

acaba tendo um componente de risco junto. O mínimo cuidado que o usuário tem que ter é se informar do tipo de segurança que o serviço provê, como os seus dados serão usados. Leia o contrato de adesão e a política de privacidade. Ninguém lê essas cláusulas e lá pode estar escrito que vai compartilhar sua informação", aponta Lima.

A empresa de Steve Jobs tentou minimizar o problema."A Apple não está rastreando a localização do iPhone. A Apple nunca fez isso e não tem planos de fazê-lo. As informações de localização que os analistas viram no iPhone não é a localização presente ou passada do aparelho, mas a localização de redes Wi-Fi e torres de celular ao redor do iPhone. Iremos parar de armazenar este cache na próxima atualização de software", afirmaram diretores da empresa, em nota. Logo depois, o iOS 4.3.3, que corrige o problema, foi liberado para os dispositivos.

O vazamento de informações não é a única ameaça para o futuro da internet. Segundo a empresa de software de antivírus Kaspersky, em 2020 os cibercrimes devem ser divididos em dois grupos. Um será especializado em ataques às empresas, às vezes sob encomenda.

As espionagens comerciais, roubos de bancos de dados e ataques à reputação organizacional terão uma alta.

Os hackers e os especialistas da área de TI entrarão em confronto no campo de batalha virtual. As agências federais de combate ao crime cibernético deverão se envolver no processo.

Já o segundo grupo se especializará nos ataques com impactos na vida diária das pessoas comuns, como transporte público e outros serviços.

O sustento dessa nova geração de hackers terá como foco a exploração desses sistemas para livre utilização, além de remover e alterar dados pessoais de outros usuários para proveito próprio.

PROTEJA-SE

- Instale e atualize as soluções de segurança do seu computador, como antivírus e firewalls
- Evite a todo custo anexos de remetentes desconhecidos; se realmente precisa fazer isso, passe o antivírus primeiro nas mensagens
- Nunca use computadores públicos para fazer transações bancárias ou compras pela internet. Esses computadores podem estar contaminados com vírus e cavalos de tróia
- Evite comprar usando rede wi-fi pública, como as disponíveis em alguns aeroportos, cafés e shoppings. A troca de informações, geralmente, é feita por um canal sem proteção e pode ser facilmente interceptada
- Antes de entrar em qualquer serviço de e-mail gratuito ou rede social, leia a política de privacidade para saber o que será feito com seus dados
- Aceite participar de aplicativos de terceiros em rede sociais somente se tiver certeza da reputação da empresa
- Desconfie de programas que prometem enriquecer sua fazenda FarmVille ou que vai te dar várias moedas para o Colheita Feliz
- No Facebook, antes de aceitar aplicativos de terceiro, verifique quais dados do perfil ele terá acesso

Fonte: BitDefender

Cuidados necessários na hora de acessar

Ninguém está a salvo dos vírus, spywares, malwares, spams, phishing e outras ameaças da internet. Segundo o relatório de abril deste ano da Symantec, 85 ataques por dia foram identificados — o maior índice desde março de 2009. Um em cada 168 e-mails continha vírus e um em cada 1,37 mensagens do correio eletrônico eram spams. Nem mesmo os websites estão seguros.

O mesmo estudo mostra que, em abril, quase 2,4 mil páginas na rede hospedavam malwares ou programas indesejados — como aquelas barras de ferramentas —, sendo que 33% desses são recém-lançados.

Para tentar acessar sites, emails e redes sociais de forma segura é preciso tomar vários cuidados. Há 10 anos, bastava ter um antivírus instalado no computador para coibir o ataque de vírus. No entanto, com a sofisticação dos cibercriminosos, as empresas de segurança investem em pacotes de proteção completos, que vão do acesso à internet até a verificação de acesso a sites proibidos para crianças.

O tamanho e a velocidade desses pacotes de segurança também ficaram melhores. O produto da McAfee, por exemplo, realiza a varredura 327% mais rápido e as atualizações só são iniciadas quando o computador estiver ocioso. Já o Total Security da BitDefender ajuda a identificar as aplicações que estão tornando o sistema lento e o recurso implementa as correções para melhorar a segurança e o tempo de resposta de todos os computadores da rede.

O Panda Internet Security 2011, por exemplo, identifica as páginas que não são seguras para usuário, além de bloquear os e-mails de phishing — as mensagens que imitam páginas de banco e que podem roubar as contas e senhas dos utilizadores.

O da Kaspersky oferece proteção em tempo real, monitora atividades suspeitas e bloqueia ações perigosas antes que possam causar danos ao computador — e o melhor é que o software trabalha em segundo plano e não consome todos os recursos do computador.

PAGO OU GRATUITO?

Escolher um antivírus gratuito pode acabar sendo uma economia que não vale a pena, mas em muitos casos pode quebrar um galho. O AVG oferece uma boa solução, na versão gratuita, contra vírus e spywares. No entanto, outras áreas importantes do computador, como proteção na hora de fazer compras e transações bancárias, podem ficar expostas.

Outra diferença que faz com que as soluções de segurança gratuitas percam pontos para as pagas é a ausência de atualizações prioritárias. Na maior parte dos antivírus gratuitos, a atualização do banco de dados de ameaças é feita primeiro para quem possui o programa pago.

Há ainda a vantagem do suporte on-line para quem compra o software.

VITRINE

NORTON 360 VERSÃO 5.0
A nova versão do Norton combina o melhor do antivírus com proteção ao e-mail, navegação na internet e, inclusive faz backup de arquivos importantes. O software ainda encontra e corrige problemas de desempenho no computador.
Preço: R$ 169 (licença para três computadores por um ano)

F-SECURE INTERNET SECURITY 2011
Proteção contra vírus e spywares, além de um firewall extra para coibir a ação de hackers está presente na solução da F-Secure. A empresa finlandesa ainda tem um controle para os pais bloquearem sites impróprios para crianças.
Preço: R$ 119,90 (licença para três computadores por um ano)

PANDA GLOBAL PROTECTION
A nova versão do Global Protection aprimorou a proteção contra os malwares e também o Panda USB Vaccine, que protége o PC e a unidade USB, como pendrives, contra infecção. Além disso, possibilita acesso remoto ao PC de onde o usuário estiver.
Preço: R$ 159 (licença para três computadores por um ano)

MCAFEE TOTAL PROTECTION 2011
Uma das melhores ferramentas do McAfee é o McAfee SiteAdvisor, que ajuda o usuário a conhecer os riscos de um site antes de clicar. A proteção avançada contra phishing alerta também sobre páginas que podem tentar roubar dados ou obter acesso às suas informações financeiras.
Preço: R$ 108 (licença para três computadores por um ano)

KASPERSKY INTERNET SECURITY 2011
A solução da Kaspersky combina a segurança essencial de software antivírus com níveis adicionais de proteção, como o firewall e o controle dos pais. Tecnologias inovadoras oferecem proteção em tempo real, monitoram atividades suspeitas e bloqueiam ações perigosas.
Preço: R$ 149,95 (licença para três computadores por um ano)

GRATUITOS

AVG
Oferece proteção básica para vírus e spyware para Windows. O pacote gratuito conta ainda com proteção nas redes sociais e na computação nas nuvens. Com a tecnologia Smart Scannig, o sistema funciona mesmo com o usuário longe do PC.

AVAST!
Em uma comparação feita pela organização AV-Comparatives, o Avast superou os concorrentes pagos no quesito velocidade. No entanto, o programa oferece apenas proteção contra vírus e spywares.

AVIRA PERSONAL
Com 25 anos de tradição, o Avira é um dos softwares de proteção para o computador mais utilizado pelos usuários. De acordo com a empresa, além de vírus, o programa protege de cavalos de tróia e propagandas indesejadas.

Fonte: Jornal do Commercio, Rio de Janeiro, 1 jun. 2011, Seudinheiro, p. B-8.