99 – Maio 2008

Kit de Sobrevivência Online

Procurando ser prático, claro e objetivo proponho dez atitudes que podem aumentar sua segurança nas transações Internet.

1-Saiba onde esta pisando.

O primeiro e mais importante passo é conhecer seu apetite para risco. Isso porque realizar pagamentos pela Internet não é 100% seguro e é prudente conhecer o limite de seu cartão de crédito, por exemplo, para então avaliar sua disposição e sensibilidade caso haja uma fraude. Na prática, avalie o prejuízo potencial comparado ao benefício trazido pela comodidade de realizar o pagamento e a própria compra do conforte de sua casa ou escritório.

2-Saiba de quem está comprando.

Em teoria, comprar pela Internet é negociar com um servidor web e uma aplicação que, por vezes, sequer se sabe onde fisicamente está localizada. Entretanto, na prática, conhecer a empresa que está por trás da operação e a sua reputação no mercado pode reduzir sensivelmente suas chances de perda. Procure referências publicadas na própria Internet, especialmente nos sites de reclamação e certifique-se das políticas de privacidade adotadas pela empresa e comumente divulgada em seu próprio site de e-commerce.

3-Saiba como suas informações são transmitidas.

O momento em que se fornecem os dados de pagamento é considerado o mais crítico para a segurança, por isso, certifique-se de identificar as características de segurança desse ambiente. A maneira mais simples de identificar o nível mínimo de proteção é procurar na base do seu browser Internet a existência de um cadeado amarelo indicando estar fechado.
Significa dizer que a comunicação entre seu computador e o servidor de e-commerce está sendo codificada e, portanto, todas as informações de pagamento que estão sendo fornecidas estão confidenciais.

4-Saiba as características do meio de pagamento.

No momento de realizar um pagamento online, muitos podem ser os modelos adotados pelos sites de e-commerce, mas se puder escolher, prefira aqueles que operam em parceria com as próprias operadoras de cartão de crédito ou com os sites especializados, reconhecidos publicamente, que intermediam o processo de pagamento do início ao fim, como o Paypal. Isso porque não há ninguém mais interessado em proteger seus dados de pagamento senão as próprias operadoras de cartão, o que gera certo grau de tranqüilidade e evita que se tenha que confiar em cada site de e-commerce e em suas práticas de proteção e confidencialidade. Esses processos costumam sem bem automatizados e depois de

concluído, a própria operadora ou intermediário se encarrega de comunicar o sucesso do pagamento ao site para que o processo de compra seja concluído.

5-Saiba se seu computador está comprometido.

Muitas vezes a fraude ocorre não por falha de segurança na transmissão dos dados ou por descuido do site de e-commerce, mas por uma falha do usuário ao proteger seu próprio computador. Esta vulnerabilidade permite que estranhos possam, mesmo que remotamente, monitorar o uso do seu computador e com isso "grampear" a comunicação justamente no momento em que você fornece os dados de cartão para o site de e-commerce. De posse desses dados, terceiros poderão forjar operações legítimas e assim gerar prejuízos. Por isso, verifique se seu antivírus está atualizado, o computador desinfectado e especialmente, se seu computador não apresenta qualquer sinal de comportamento suspeito. Neste caso, não realize pagamentos através dele.

6-Saiba como escolher a senha.

É sempre muito difícil escolher uma senha, e pior, ter de escolher uma senha diferente para cada serviço ou até mesmo, cada site de e-commerce. De qualquer forma, este comportamento é crítico e adotar senhas fracas pode comprometer a segurança de seus dados e gerar prejuízos. Por isso, respeitando as limitações de cada sistema ou site de e-commerce, procure formar senhas difíceis de serem descobertas. Misture números aleatórios com letras e se possível, caracteres especiais. Mas não seja criativo demais a ponto de esquecê-la ou até mesmo ter de anotá-la para se lembrar depois. Para os usuários intensos que têm de manter dezenas de senhas, recomendo o uso de programas especialistas que com uma chave de criptografia única, consegue armazenar todas as suas senhas de forma segura.

7-Saiba escolher a melhor forma de pagamento.

Nem sempre a forma mais prática é a melhor para o uso da Internet. Se a escolha for o pagamento com cartão de crédito, escolha àquele que possui o menor limite e passe a adotá-lo apenas para compras online, assim você terá mais controle e ainda correrá menos riscos em função do baixo potencial de prejuízo definido pelo limite. Alternativamente, se o site de e-commerce permitir, procure utilizar o serviço de empresas intermediárias mundialmente conhecidas, como o Paypal, evitando que você tenha que revelar seus dados de pagamento para todo site Internet onde realiza transações. Feito isso uma única vez com o intermediário, ele se encarregará de confirmar o pagamento sem expor e trafegar seus dados sigilosos integralmente.

8-Saiba recuar mesmo que o impulso diga o contrário.

A Internet ainda é uma terra sem lei, ou melhor, sem os mesmos controles que se tem no mundo real. Por isso, é possível encontrar de tudo na grande rede. De lojas tradicionais que expandiram sua operação, àquelas das quais nunca se ouviu falar, estabelecidas fisicamente e legalmente não se sabe onde, e por vezes, vendendo produtos a preços irresistíveis. Neste caso o melhor a fazer é resistir. Não que não se possa realizar bons negócios com empresas

novas de forma segura, mas em geral, toda essa obscuridade pode representar um golpe, uma armadilha e, portanto, prejuízo para o comprador. Existem golpes grosseiros de fácil identificação em que se realiza um pagamento e nunca se recebe o produto, mas outros são bem profissionais fazendo com que o comprador se sinta feliz com o pagamento e o recebimento do produto por um preço honesto, quando na verdade, o golpista se beneficia não pela realização do negócio em si, mas por ter capturado seus dados de pagamento para uso subseqüente sem autorização.

9-Saiba transformar a compra online em uma experiência positiva.

Riscos na compra online existem, assim como muitos outros presentes no dia-a-dia do mundo real, só que esses, de certa forma, nós já sabemos administrar. Assim, não faça com que a decisão de realizar uma compra online se transforme em um martírio. O primeiro passo é compreender os riscos envolvidos e ponderá-los com os benefícios deste novo modelo. Depois de tomada a decisão com base na análise, siga os passos mencionados acima e descanse com a certeza de ter feito o melhor que poderia ter sido feito. Comprar online e perder horas de sono não faz sentido, não compensa. Não se sinta pressionado pela sociedade se não se sentir confortável em ser realizar transações pela Internet, ou então, simplesmente comece pequeno. Primeiro com um cartão de crédito especial de pequeno limite, usado apenas em sites conhecidos e para compras pequenas. Só o tempo e sua própria experiência poderá ajudá-lo a superar os medos e os riscos inerentes a este tipo de operação.

10-Saiba reagir em caso de risco de fraude.

Se mesmo depois de todo cuidado houver algum sinal de fraude ou vazamento de informação, não se desespere. O primeiro passo é comunicar ao seu banco ou operadora do cartão de crédito a possível operação ilegítima ou ainda, sua percepção de fraude. Isso os ajudará a identificar a fraude em andamento e, por vezes, interrompê-la antes mesmo de se consumar. Ou ainda, impedirá que novas fraudes ocorram com o mesmo meio de pagamento, permitindo também que o fato de você mesmo ter comunicado um comportamento suspeito, o isente de futuras responsabilidades. Nestes casos o tempo corre contra você e quanto mais demorada for sua reação, mais tempo o golpista terá para ampliar a extensão dos seus prejuízos. Se por fim você for lesado, não acredite que a Internet é ruim. Ela só é diferente e você não terá sido nem o primeiro e nem o último a ser lesado por um golpe que agora é também praticado online.

Marcos Sêmola *é Global IT GRC Manager da Shell International Limited Gas & Power na Holanda, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Membro fundador do Institute of Information Security Professionals of London. MBA em Tecnologia Aplicada, Professor da FGV com especialização em Negociação e Estratégia pela London School, Bacharel em Ciências da Computação, autor de livros sobre gestão da segurança da informação, governança e inteligência competitiva. Visite www.semola.com.br ou contate marcos@semola.com.br*