

# Segurança na Internet

*Dailton Felipini*

Ameaças a nossa segurança tornaram-se quase uma rotina nos dias de hoje, portanto, era de se esperar que, no ambiente da Internet, isso não fosse diferente. E realmente não é! Assim como no mundo de tijolos, onde temos de trancar as portas e janelas de nossa casa, colocar grades, alarmes e tomar inúmeros outros cuidados, no ambiente virtual também temos de nos proteger de ocorrências como a clonagem do site, o roubo de senhas, o acesso a informações sigilosas trocadas entre o site e o visitante, entre outras. Existem alguns métodos para aumentar a segurança nas transações on-line, e os principais você vai conhecer agora.

**A certificação.** Uma questão central para o usuário é ter certeza de que ele está transacionando com a loja correta, ou seja, não está trocando informações com o clone de um site conhecido. Para isso, existe o processo de certificação, no qual empresas conhecidas como “autoridades certificadoras” desempenham papel semelhante ao do nosso velho e conhecido cartório de registro. Elas vão certificar a identidade do servidor, isto é, vão garantir aos visitantes de seu site que ele é realmente o que eles pensam que é. Existe um processo complexo de troca de chaves pública e privada por trás da certificação, mas o que o usuário vê é um selo que atesta a identidade do site e garante que ele está trocando informações com a empresa correta. Ao clicar no selo, o visitante pode conferir se os dados do certificado, como nome da empresa, endereço completo, URL, conferem com os do site que ele está visitando. A certificação pode ser obtida diretamente da autoridade certificadora, ou indiretamente pelo seu fornecedor de hospedagem, que vai estender essa facilidade a todos os sites hospedados em seu servidor. Essa é a situação mais comum, tendo em vista que uma certificação não é um investimento barato para uma pequena empresa.

**A encriptação de dados.** A encriptação, ou cifração, é o uso de uma tecnologia de segurança que protege a privacidade das informações trocadas entre o site e o visitante. O sistema embaralha as informações de forma que, se um terceiro conseguir acesso aos dados, eles estarão truncados, não podendo, portanto, ser utilizados. De forma simplificada, o processo funciona da seguinte maneira: O visitante, ao preencher dados em formulários do site certificado, protegido por uma camada SSL (Secure Socket Layer), já recebeu do órgão emissor da certificação uma chave pública a qual o navegador utiliza para encriptar os dados e enviar de volta ao servidor. Este, munido de uma chave privada, decifra os dados para obter os dados digitados pelo visitante.

**Segurança nas transações com cartão de crédito.** O cartão, que é o meio mais prático de pagamento no e-commerce, também é o que desperta maior receio por parte do consumidor on-line. O risco de expor os dados do cartão a terceiros é a grande preocupação de muitos clientes que, mesmo possuindo o cartão, preferem fazer pagamentos usando o boleto bancário, o que demanda mais trabalho para quem compra e para quem vende, além de resultar em maior demora na entrega da mercadoria adquirida. As administradoras de cartão vêm aprimorando os sistemas de segurança da informação no processo de pagamento on-line, de forma a tornar o uso do cartão o mais seguro possível, o que é plenamente justificável, uma vez que a segurança na Internet é fundamental para maior confiança do consumidor nas compras on-line e, conseqüentemente, para o lucro dessas empresas nesse novo canal de comercialização. Anteriormente, era um fator crítico de segurança o fato de as lojas virtuais armazenarem em seus sistemas o número do cartão dos clientes, visto que isso aumentava exponencialmente os riscos de acesso indevido a essa informação. Já no sistema atual, o número do cartão não fica em poder do lojista. O cliente digita o número e a data de validade de seu cartão através de uma interface segura com a administradora do cartão, e esses dados não são fornecidos à loja. Uma novidade, implantada recentemente pela operadora Visanet, é o chamado sistema VBV, que, no momento da compra, cria mais um patamar de segurança ao levar o comprador à página do banco emissor para autenticação por meio de uma senha. É provável que, da mesma forma que não temos um mundo 100% seguro, nunca tenhamos uma internet 100% segura. No entanto, se cada lojista se preocupar com a segurança de sua loja virtual e tomar medidas preventivas como as abordadas aqui, minimizará bastante os riscos, levando-os para um nível plenamente aceitável.

Dailton Felipini, é Mestre em Administração pela Fundação Getúlio Vargas e professor de e-commerce na Universidade Ibirapuera. Autor de vários ebooks e editor dos sites: <http://www.e-commerce.org.br/> e <http://www.abc-commerce.com.br/>