UNIVERSIDADE FEDERAL DE ALAGOAS (UFAL)
INSTITUTO DE COMPUTAÇÃO (IC)
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

DISCIPLINA: Comércio Eletrônico

PERÍODO: 2012.1

SEMANA 03: Segurança na Internet e Meios de Pagamentos no E-Commerce

As Questões Éticas e as Questões Legais

Na teoria, pode-se distinguir entre questões éticas e questões legais. Caso a lei seja infringida, caracteriza-se um ato ilegal. As leis constituem-se em regras estritamente legais que regem os atos dos cidadãos sob sua jurisdição. Já a ética é o ramo da filosofia que trata do que é considerado certo ou errado. O que é antiético não é necessariamente ilegal.

Neste contexto, o *e-commerce* abre um novo espaço de atividades não regulamentadas, no qual a definição de certo ou errando nem sempre é clara. Deste modo, os profissionais que atuam neste âmbito precisam de diretrizes que definam quais comportamentos são razoáveis sob um dado conjunto de circunstâncias.

A Privacidade

Em geral, privacidade significa o direito de não ser incomodado, bem como o direito de estar livre de intrusões pessoais despropositadas.

Com o aumento do uso de internet para realização de negócios e de sua interligação com grandes bancos de dados, surgiu uma dimensão inteiramente nova para o acesso e utilização de dados.

É notável que os sistemas que acessam vastas quantidades de dados podem ser utilizados para o bem da sociedade, seja na redução de fraudes, da má administração governamental, da evasão de impostos, fraudes de seguros sociais, sonegação de pensões alimentícias e etc. A questão é saber até que ponto cada indivíduo pode perder sua privacidade para que as entidades governamentais possam deter aqueles que infringem a lei.

Eis alguns modos utilizados para coletar informações sobre indivíduos:

- ✓ Leitura do que os indivíduos publicam em fóruns ou redes sociais;
- ✓ Procurando dados sobre o indivíduo em diretórios de internet;
- ✓ Gravando as ações do indivíduo enquanto ele navega pela Web;
- ✓ Lendo e-mail de um indivíduo; e
- ✓ Solicitando que um indivíduo preencha um registro.

Registro em Sites

Atualmente, a maioria dos sites que atuam no segmento de varejo, solicita que seus clientes preencham cadastros. Durante o processo, o cliente informa voluntariamente informações como: nome, endereço, número de telefone, endereço de e-mail, hobbies e etc. Normalmente, em troca das informações, os sites oferecem algum tipo de vantagem como participação em promoções, descontos e etc.

Cookies

Outra possibilidade para coletar informações sobre um indivíduo é a utilização de cookies. Um cookie é uma pequena quantidade de dados que é trocada sucessivamente entre um site e o navegador de um usuário, enquanto este acesso o site. Desta maneira, os cookies permitem que os sites monitorem as atividades dos usuários sem pedir a sua identificação.

Proteção da Privacidade

Dentre os princípios éticos utilizados pelas maiores potências do *e-commerce*, estão os seguintes:

- ✓ Notificação/conscientização – o consumidor deve ser notificado sobre a prática de informações de uma entidade antes da coleta de informações pessoais. Também

deve poder tomar decisões sobre o tipo e a extensão da divulgação das informações, com base nas intenções da parte que as está coletando.

- ✓ Escolha/consentimento – o consumidor deve ser conscientizado acerca das opções que tem quanto ao modo como suas informações pessoais podem ser utilizadas. O consentimento pode ser dado pelas cláusulas de não adesão, que exigem algumas providências para impedir a coleta de informações. Além disso, o consumidor pode dar seu consentimento por cláusulas de adesão, que requerem algumas providências para permitir a coleta de informações.

- ✓ Acesso/participação – o consumidor deve ter o direito de acessar suas informações pessoais e contestar a validade dos dados.

- ✓ Integridade/segurança – deve-se dar garantia ao consumidor de que seus dados pessoais estão seguros e são exatos. Quem coleta os dados deve tomar providências para garantir que os dados estejam protegidos contra perda, acesso não autorizado, destruição e utilização fraudulenta.

- ✓ Cumprimento/recurso – deve sempre existir um método de cumprimento e recurso. As intervenções são a intervenção governamental, a legislação para recursos privados ou a auto-regulamentação.

Direitos Sobre a Propriedade Intelectual

Segundo a Organização Mundial de Propriedade Intelectual, a Propriedade Intelectual refere-se a "criações de intelecto: invenções; obras literárias e artísticas; símbolos; nomes; imagens e desenhos usados no comércio".

No e-commerce, há três tipos principais de Propriedade Intelectual: Direitos Autorais; Marcas Registradas; e Patentes.

Direitos Autorais

Direito autoral ou *copyright* é uma concessão exclusiva do governo que confere ao seu proprietário um direito essencial exclusivo de: reproduzir uma obra, total ou

parcialmente e distribuí-la, apresentá-la ou exibi-la ao público sob qualquer forma ou maneira, inclusive a internet.

Em geral, existem direitos autorais para as seguintes obras:

- ✓ Obras literárias (ex: livros, softwares);
- ✓ Obras musicais (ex: composições musicais);
- ✓ Obras dramatúrgicas (ex: peças de teatro);
- ✓ Obras artísticas (ex: desenhos, pinturas); e
- ✓ Gravações sonoras, filmes, transmissões, programas a cabo.

Neste contexto, as marcas d'água digitais podem ser utilizadas por empresas para proteger o direito autoral. As marcas d'água digitais são identificadores exclusivos inseridos no conteúdo digital. Apesar de não impedirem as cópias ilegais, este recurso facilita o trabalho de programas que são utilizados para identificar cópias ilegais e notificar o proprietário do direito.

Marcas Registradas

A marca registrada é um símbolo utilizado por empresas para identificar seus bens e serviços. O símbolo pode ser composto de palavras, desenhos, letras, números, formas, uma combinação de cores ou outros identificadores semelhantes. Essas marcas precisam estar registradas em um país para que sejam protegidas por lei. Essas marcas devem ser distintivas, originais e não enganosas. Uma vez registrada, sua vigência é eterna, desde que se pague a taxa de registro.

O proprietário de uma marca registrada tem direitos exclusivos para:

- ✓ Usar a marca em bens e serviços para os quais ela foi registrada;
- ✓ Tomar medidas legais para impedir que a marca seja utilizada, sem consentimento, em bens e serviços (semelhantes) para os quais ela foi registrada.

Patentes

A patente é um documento que confere ao seu proprietário os direitos exclusivos sobre uma invenção durante um determinado número de anos. Este advento serve para proteger invenções tecnológicas tangíveis. Uma invenção pode estar sob forma de um dispositivo físico ou de um método ou processo para fabricar um dispositivo físico.

Cibercrime

Muitos crimes tradicionais agora são cometidos por meio de computadores e transferiram-se para a internet. No entanto, dependendo da jurisdição, esses crimes não são processados judicialmente como crimes de computador.

Desta maneira, em geral, são taxados como cibercrimes a ciberinvasão e o cibervandalismo. A ciberinvasão assemelha-se ao arrombamento e invasão, exceto pelo ponto de entrada que é a internet. Enquanto isso, o cibervandalismo ocorre quando um acesso não autorizado à internet resulta em arquivos, programas ou hardware danificados. Esses dois atos também são caracterizados como ciberataques.

Em geral, os protagonistas dos ciberataques são:

- ✓ *Hackers* – hoje, este termo refere-se a todas as pessoas que violam sistemas de computador, independentemente de sua motivação;

- ✓ *Crackers* – abreviação para "*Criminal Hackers*" refere-se aos hackers que usam sua aptidões para cometer atos ilegais ou para causar danos deliberadamente.

- ✓ *Script Kiddies* – são crackers inexperientes, movidos pelo ego, que usam informações e software (scripts) que baixam na internet para infligir danos a sites que escolhem como alvos.

Questões de Segurança

- ✓ Autenticação – O processo pelo qual uma entidade verifica se outra é realmente quem diz ser denomina-se autenticação. A autenticação requer evidências sob

forma de credenciais, que podem ser uma senha, um cartão inteligente ou uma assinatura;

- ✓ Autorização – É a etapa que assegura o acesso a certos recursos. Comparam-se as informações sobre a pessoa que requer o acesso a um recurso e com as informações de acesso associadas ao recurso que está sendo acessado;

- ✓ Auditoria – É o processo de coleta das informações sobre as tentativas de acessar determinados recursos, usar determinados privilégios. Através dela é possível reconstituir as ações que foram executadas e, muitas vezes, identificar especificamente a pessoa ou programa que executou tais ações;

- ✓ Confidencialidade – Informações confidenciais e sensíveis não devem ser reveladas a indivíduos, entidades ou processos de software não autorizados;

- ✓ Integridade – É a capacidade de proteger dados contra alteração ou destruição por ações não autorizadas ou acidentais;

- ✓ Disponibilidade – Um site de *e-commerce* é considerado disponível se uma pessoa ou programa pode obter acesso às suas páginas, dados ou serviço sempre que necessário.

- ✓ Irretratabilidade - É a capacidade de limitar a possibilidade de que as partes contestem que uma transação legítima ocorreu.

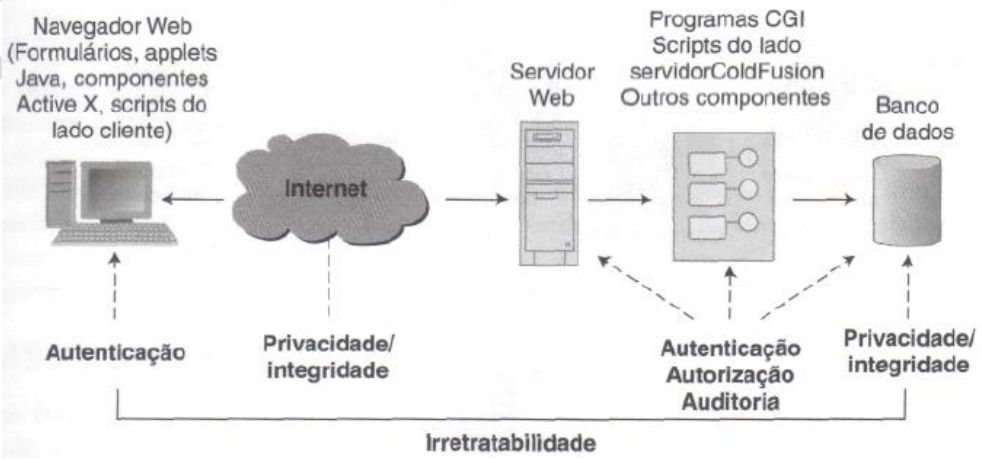

Figura 1. Questões de Segurança no e-commerce

Fonte: TURBAN (2004).

Tipos de Ciberataques

Os especialistas em segurança na internet caracterizam dois tipos de ataques: os não técnicos e os técnicos. No ataque não técnico, também conhecido como ataque de engenharia social, o agente atacante usa persuasão para enganar as pessoas e fazê-las revelar informações sensíveis ou executar ações capazes de comprometer a segurança de uma rede. Por outro lado, o conhecimento de software e de sistemas é fator essencial para o ataque técnico.

- ✓ Ataques de Recusa de Serviço – o atacante utiliza software especializado para enviar uma grande quantidade de pacotes de dados a um computador-alvo, no sentido de sobrecarregar seus recursos. No ataque distribuído de recusa de serviço, o atacante obtém acesso a um grande número de computadores na internet. Uma vez obtido o acesso, o hacker carrega um software especializado, que fica dormente até receber o comando para iniciar o ataque.

Os códigos malignos, conhecidos como *malware*, são classificados pelo modo como se propagam. Alguns podem ser benignos, porém todos tem potencial para causar danos.

- ✓ Vírus – É um código que se insere por si só em um computador, inclusive em seus sistemas operacionais, com a finalidade de propagar-se. Para ser ativado, requer a execução do programa de seu hospedeiro. Dentre os problemas que pode causar estão a exclusão indesejada de arquivos e danos ao disco rígido.

- ✓ *Worm* – É um programa que pode rodar independentemente, consumindo os recursos de seu hospedeiro por dentro para poder manter-se e propagando uma versão completa de si mesmo para outra máquina.

- ✓ Vírus de Macro e *Worms* de Macro – É executado quando o objetivo da aplicação (planilha, texto, e-mail) que contem o macro é aberto ou quando um procedimento particular é executado.

- ✓ Cavalo de Tróia – É um programa que aparentemente tem uma função útil, mas contém uma função oculta que representa um risco para a segurança, visto que dá ao seu criador o controle parcial ou total da máquina do usuário.

Tecnologias de Segurança

- ✓ *Firewall* – É um nó de rede que consiste em hardware e software capazes de isolar uma rede privada de uma rede pública. Alguns firewalls filtram dados e requisições transferindo-os da internet pública para uma rede privada, com base nos endereços de rede do computador que está enviando ou recebendo a requisição. Outros bloqueiam os dados, dependendo do tipo de aplicação que está sendo acessada.

- ✓ Sistemas de Detecção de Invasão – É uma categoria especial de software que pode monitorar a atividade em toda uma rede ou em um computador local, detectando atividades suspeitas e agindo automaticamente quando necessário.

- ✓ Gerenciamento do Risco de Segurança – É um processo sistemático para determinar a probabilidade de vários ataques à segurança e identificar as ações necessárias para evitar ou minimizar os efeitos dos ataques. É dividido em quatro etapas: avaliação, planejamento, implementação e monitoração.

Infraestrutura de Chave Pública

Considerada a base dos pagamentos eletrônicos (*e-payment*) seguros, a infraestrutura de chave pública (PKI) representa os componentes técnicos, a infraestrutura e as práticas necessárias para habilitar a utilização de criptografia de chave pública, assinaturas digitais e certificados digitais uma aplicação de rede. A PKI é o fundamento de várias aplicações de rede, incluindo o gerenciamento da cadeia de suprimentos, as redes virtuais privadas, o e-mail seguro e as aplicações de intranet.

- ✓ Criptografia – A criptografia garante a confidencialidade e a privacidade de uma mensagem durante o seu trajeto por uma rede ao criptografá-la de tal modo que

seja difícil, caro ou muito demorado para uma pessoa não autorizada decriptá-la (remontá-la).

Comprimento da chave	Número de chaves possíveis (2x)	Tempo para verificar todas as chaves à taxa de 1,6 milhão de chaves por segundo	Tempo para verificar todas as chaves à taxa de dez milhões de chaves por segundo
40	1.099.511.627.776	8 dias	109 segundos
56	72.057.594.037.927.900	1.427 anos	83 dias
64	18.446.744.073.709.600.000	365.338 anos	58,5 anos
128	3,40282E + 38	6,73931E + 24 anos	1,07829E + 21 anos

Figura 2. Aspectos de Criptografia
Fonte: TURBAN (2004).

- ✓ Assinaturas Digitais – Baseadas em chaves públicas, as assinaturas digitais são usadas para autenticar a identidade do remetente de uma mensagem ou documento. Podem ser usadas ainda para garantir que o conteúdo original de uma mensagem ou documento não foi alterado.

- ✓ Certificados Digitais – Verificam se o detentor de uma chave pública ou privada é quem diz ser. Emitido por entidades certificadoras, um certificado contém itens como o nome do proprietário, período de validade, informações sobre a chave pública e um *hash* assinado de dados.

Padrões para Pagamentos Eletrônicos

São muitas as instituições envolvidas em pagamentos eletrônicos, de maneira que se tornou necessário utilizar protocolos universalmente aceitos para garanti-los. Em geral, dois tipos de protocolos são utilizados:

- ✓ Segurança de Camada de Transporte – O SSL (*Security Socket Layer*) utiliza certificados padrão para autenticar e criptografar dados, a fim de assegurar privacidade ou confidencialidade;

- ✓ Transações Eletrônicas Seguras – Com o TLS (*Transport Layer Security*) é possível criptografar números de cartões de crédito enviados do navegador de um consumidor para o site de um comerciante. Primeiro é preciso verificar a validade do número do cartão, depois o banco do consumidor deve autorizar cartão e, em seguida, a compra precisa ser processada. O protocolo criptográfico utilizado para transações completas deste tipo são conhecidos como SET (*Secure Electronic Transaction*).

Cartões de Pagamento

Os cartões de pagamento se dividem em três categorias:

- ✓ Cartões de Crédito – concede ao seu portador crédito para fazer compras até um limite fixado pelo emitente;

- ✓ *Charge Cards* – tecnicamente, o portador do *charge card* recebe um empréstimo por 30 a 45 dias equivalente ao débito apresentado no extrato;

- ✓ Cartões de Débito – o custo de um item comprado sai diretamente da conta corrente do portador.

Carteiras Eletrônicas (*E-Wallets*)

É um componente de software que o usuário baixa em seu computador e no qual armazena números de cartões de crédito e outras informações pessoais. Ao utilizá-la em um site que aceita este tipo de software, todas as informações necessárias são preenchidas automaticamente com um clique.

Cartões Inteligentes

É parecido com os outros cartões plásticos de pagamento, mas se diferencia por conter um microchip embutido, que pode ser um microprocessador combinado com um chip de memória ou apenas um chip de memória com lógica não programável. O microprocessador pode adicionar cancelar ou manipular as informações contidas no cartão, enquanto o chip de memória pode executar somente transações pré-definidas.

Pagamentos Sem Fio

Serviço que habilita os assinantes sem fio a utilizarem seus telefones móveis para que estes realizem pagamentos de compras em lojas conveniadas. Após enviar os dados da compra, o usuário recebe uma mensagem via sms solicitando a senha para autorizar a compra. A cobrança será efetuada em sua conta de telefone.

Cheque Eletrônico (*e-check*)

É a versão eletrônica de um cheque. Os *e-checks* contêm as mesmas informações de um cheque em papel, podem ser usados onde quer que se usem os cheques e sua estrutura legal é a mesma dos cheques de papel. São mais rápidos e mais baratos.

Outras formas de pagamento: eCoin, Qpass, Visa Cash, Mondex, Pagamentos P2P, Pagamentos B2B.

Referências

ALBERTIN, A. L. **Comércio Eletrônico**: Modelo, Aspectos e Contribuições de Sua Aplicação. São Paulo: Atlas, 2010.

TURBAN, Efraim; KING, David. **Comércio Eletrônico**: Estratégia e Gestão. 1ª Ed. Prentice Hall, São Paulo, 2004.