CENTRO PAULA SOUZA

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Segurança da Informação

ESTUDO DO COMÉRCIO ELETRÔNICO: INSTRUÇÕES PARA LEIGOS

TIAGO VILLELA DE CARVALHO

Americana, SP
2015

CENTRO PAULA SOUZA

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Segurança da Informação

ESTUDO DO COMÉRCIO ELETRÔNICO: INSTRUÇÕES PARA LEIGOS

TIAGO VILLELA DE CARVALHO

tiago.villela@gmail.com

Trabalho Monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec-Americana, sob a orientação da Profª Dra. Acácia de Fátima Ventura.

Área: Segurança da Informação e Fator Humano

Americana, SP
2015

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

C329m	Carvalho, Tiago Villela de Estudo do comércio eletrônico: informação para leigos / Tiago Villela de Carvalho. – Americana: 2015. 50f. Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza. Orientador: Prof. Dr. Acácia de Fátima Ventura 1. Comércio eletrônico I. Ventura, Acácia de Fátima II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana. CDU: 658.845

Tiago Villela de Carvalho

Estudo do comércio eletrônico:
Instruções para leigos

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Tecnologia e Educação.

Americana, 08 de Dezembro de 2015.

Banca Examinadora:

Acácia Ventura (Presidente)
Doutora
Fatec Americana

Maria Cristina Luz Aranha (Membro)
Mestre
Unisal Campinas

José Matias Lemes Filho (Membro)
Mestre
Fam

AGRADECIMENTOS

Agradeço, em primeiro lugar, à minha família, que me ajudou, incentivou e apoiou em todos os momentos, oferecendo as bases necessárias para me tornar quem sou.

Agradeço especialmente à professora e orientadora Acácia de Fátima Ventura, por compartilhar o seu conhecimento e a sua experiência, por dispor do seu tempo e por me mostrar que realmente seria possível.

Deixo meus agradecimentos aos amigos e professores do curso de Segurança da Informação da FATEC-AMERICANA, pelo importante apoio na realização deste trabalho.

Agradeço então a Deus, por permitir que eu chegasse até aqui.

RESUMO

O comércio eletrônico é uma realidade no Brasil e no mundo e encontra na tecnologia da informação, mais precisamente na segurança da informação, as bases para seu desenvolvimento. Uma das barreiras a serem superadas pelo comércio eletrônico é a sensação de insegurança que esse tipo de modalidade causa aos usuários, impedindo maior crescimento do setor. A pesquisa parte da indagação de como minimizar justamente essa sensação de insegurança, acreditando que a imagem negativa que o usuário detém das transações *on-line* pode ser minimizada com informação e conhecimento, ou seja, estudando a segurança da informação e a engenharia social o consumidor poderá conhecer estratégia de proteção a si e ao seu capital. O comércio eletrônico e suas vulnerabilidades podem assustar alguns indivíduos, principalmente por desconhecerem essa modalidade, porém não podem afastá-los da compra. Para tanto o estudo elaborou, no término da pesquisa, um informativo com boas práticas. Todo esse compilado de informações é capaz de oferecer ao usuário leigo conteúdo científico, de forma simples e explicativa, para que este usufrua positivamente das possibilidades que o comércio eletrônico dispõe.

Palavras Chave: Comércio Eletrônico; Segurança da Informação; Engenharia Social.

ABSTRACT

The e-commerce is a reality in Brazil and in the rest of the world, and it finds in information technology, more specifically in information security, the basis for its development. One of the barriers to be overcome by e-commerce is the feeling of insecurity that such modality causes to its users, preventing further growth of that sector. The research originates from the questioning of how to precisely minimize that feeling of insecurity, assuming that the negative image that the user holds against the online transactions can be minimized with information and knowledge, that is, by studying information security and social engineering the consumers may learn protection strategies for themselves and their capital. Electronic commerce and its vulnerabilities may scare some people off, mainly because they do not know it well enough, but they cannot drive them away from the purchase. To this end, the study developed an informative, at the end of the research, containing best practices. This whole compilation of information is able to brief the lay user with scientific content in a simple and explanatory fashion; so that the user can positively enjoy the opportunities that e-commerce may offer.

Keywords: Electronic Commerce; Information Security; Social Engineering.

SUMÁRIO

INTRODUÇÃO

O conceito de segurança da informação é definido na ISO/IEC 177799, atualizada em julho de 2007 para ISO/IEC 27002, e está ligado à proteção da informação contra vários tipos de ameaças, valendo-se da implementação de um conjunto de controles adequados, visando garantir a continuidade do negócio e minimização de riscos (FONTES, 2008). A segurança da informação depende da infraestrutura/ambiente do negócio, de políticas internas e de fatores comportamentais, sendo assim, é correto afirmar que segurança da informação está intimamente ligada à engenharia social.

A engenharia social, enquanto parte da segurança da informação, refere-se ao uso indevido de pessoas inocentes, utilizando artefatos psicológicos, para a realização de ações ou divulgações de informações privadas (FONTES, 2006), por exemplo, a prática da persuasão para que pessoas revelem dados sensíveis sobre um sistema de computador ou de informação.

O comércio eletrônico, objeto de estudo dessa pesquisa, é um tipo de transação comercial realizada utilizando meio eletrônico de dados, a Internet (ALBERTIN, 1999). Sua implementação e uso fazem parte da realidade atual e seu resultado alcança um faturamento de R$ 43 bilhões (CARNETI, 2015). Com números tão expressivos, um tema tornou-se recorrente, cada vez mais discutido e divulgado entre usuários e organizações: segurança da informação. O que impede uma parcela da população de realizar transações *on-line* é, justamente, o sentimento de insegurança que o ambiente virtual fornece. Este trabalho tem como objetivo apresentar um informativo com dicas e boas práticas almejando, desta forma, minimizar essa sensação de desconfiança por parte do usuário.

Justificativa da pesquisa: o tema comércio eletrônico é pertinente, visto os números expressivos que o mesmo tem alcançado. Atrelado ao tema, e um impeditivo para seu crescimento, é a sensação de insegurança que o ambiente virtual oferece.

"Acredita-se que, além da busca de tecnologia que garanta total segurança na Internet, as redes devem passar a ser mais confiáveis." (ALBERTIN, 1999, p. 53).

> Os bancos em todo o mundo estão a ver (sic) a fraude online como uma ameaça urgente. Segundo o Financial Fraud Action UK, só no Reino Unido as perdas da fraude online aumentaram 48% em 2014 quando comparadas com o ano anterior. Além disso, o Kasparesky Lab anunciou que o Brasil teve o maior número de utilizadores (sic) atacados por malware bancário (um dos modus operandi chave da fraude online), seguido da Rússia (HUTTON, 2015).

Embasado por Albertin e motivado pelos dados apresentados por Hutton, a pesquisa busca minimizar essa sensação de insegurança do usuário.

O problema foi: usuários e possíveis clientes do comércio eletrônico, não usufruem dessa modalidade por falta de confiança.

> Um aspecto amplamente citado dos sistemas on-line atuais é a segurança, apesar de muitos especialistas considerarem-no mais uma questão de percepção do que de realidade. Cabe lembrar que as percepções dos clientes são o que realmente importam em termos de adoção de novas tecnologias (ALBERTIN, 1999, p. 154).

A pergunta problema foi: como minimizar a insegurança que alguns usuários têm com relação ao comércio eletrônico?

As hipóteses foram: a) A falta de confiança do usuário com relação ao comércio *on-line*, oriunda da falta de conhecimento da segurança empregada neste tipo de transação; b) O usuário tem uma percepção empírica e irreal das transações *on-line* e nem mesmo informações de cunho científico são capazes de contrariar esse credo, e c) O usuário detém uma imagem negativa da segurança empregada nas transações *on-line*, o conhecimento gerado através deste tipo de pesquisa assim como o informativo gerado ao final deste, contribui positivamente para a desmistificação deste tipo de comércio.

O objetivo geral consistiu em reduzir as inseguranças de pessoas que não realizam compras virtuais através de sites, buscando elaborar um informativo de boas práticas para seu uso com maior segurança.

Os objetivos específicos foram: a) Estudar a segurança da informação e a engenharia social, objetivando identificar possíveis vulnerabilidades no comércio eletrônico, b) Estudar o comércio eletrônico no Brasil, visando conhecer seus dados;

c) Estudar o comércio eletrônico e questões relacionadas a segurança da informação; d) Elaborar um informativo com boas práticas, visando orientar positivamente usuários em compras *on-line.*

O método para o desenvolvimento deste trabalho foi o dialético, que de acordo com Lakatos e Marconi (1992, p. 106) ele: “[...] penetra o mundo dos fenômenos através de sua ação recíproca, da contradição inerente ao fenômeno e da mudança dialética que ocorre na natureza e na sociedade”.

A pesquisa foi classificada do ponto de vista de sua natureza como básica, descrita por Marconi e Lakatos (2009, p. 6): “É aquela que procura o progresso científico, a ampliação de conhecimentos teóricos, sem a preocupação de utilizá-los na prática. É a pesquisa formal, tendo em vista generalizações, princípios, leis. Tem por meta o conhecimento pelo conhecimento”.

Para a abordagem do problema utilizou-se a pesquisa qualitativa, que tem como premissa: “analisar e interpretar aspectos mais profundos, descrevendo a complexidade do comportamento humano. Fornece análise mais detalhada sobre as investigações, hábitos, atitudes, tendências de comportamento etc.” (LAKATOS e MARCONI, 2004 *apud* PEREIRA, 2012, p.12-13).

Para atingir aos objetivos foi utilizada a pesquisa descritiva que: “Delineia o que é – aborda também quatro aspectos: descrição, registro, análise e interpretação de fenômenos atuais, objetivando o seu funcionamento no presente.” (MARCONI e LAKATOS, 2009, p.6).

Para os procedimentos técnicos utilizou-se a pesquisa bibliográfica descrita como: “[...] em termos genéricos, é um conjunto de conhecimentos reunidos em obras de toda natureza.” (FACHIN, 2006, p.120).

O trabalho foi estruturado em quatro capítulos, sendo que no primeiro apresenta-se o conceito de comércio eletrônico, tipos de comércio eletrônico, dados do comércio eletrônico no Brasil, relação do comércio eletrônico e a Internet, conceito informação, conceito de segurança da informação e suas ameaças. O segundo capítulo foi dedicado à engenharia social, apresentando conceito de

engenharia social, diferenciando *hackers* e *crackers*, discutindo o perfil do engenheiro social, assim, como as técnicas e mecanismos empregados na engenharia social, ao terceiro capítulo destinou-se o estudo do comércio eletrônico e segurança da informação, apresentando conceito de ambiente virtual, sistema eletrônico de pagamento, discussão de vulnerabilidades e por fim elaboração de um informativo.

Com base nas informações conseguidas a partir dos estudos realizados nos capítulos anteriores, o capítulo quarto se reserva às considerações finais.

1 O COMERCIO ELETRÔNICO NO BRASIL E SEGURANÇA DA INFORMAÇÃO

O comércio eletrônico é uma realidade no mundo todo, trata-se de uma modalidade econômica expressiva. Seu entendimento e sua desmistificação são fundamentais para que todo o tipo de usuário tenha condições de decidir pelo uso deste tipo de transação.

1.1 CONCEITUANDO O COMÉRCIO ELETRÔNICO

O comércio eletrônico é um tipo de transação comercial (compra e venda de produtos ou serviços), efetuada em um ambiente virtual, utilizando meio eletrônico de dados, a Internet.

Segundo Albertin (2001, p. 10), comércio eletrônico pode ser definido:

> Comércio eletrônico é a realização de toda a cadeia de valor dos processos de negócio num ambiente eletrônico, através da aplicação intensa das tecnologias de comunicação e de informação, atendendo os objetivos de negócio. Os processos podem ser realizados de forma completa ou parcial, incluindo as transações negocio-a-negocio, negócio-a-cliente e intraorganizacional, numa estrutura predominantemente pública de fácil e livre acesso e baixo custo.

Limeira (2003, p. 38) afirma que: “comércio eletrônico consiste na realização de negócios por meio da Internet, incluindo a venda de produtos e serviços físicos, entregues off-line, e de produtos que podem ser digitalizados e entregues on-line, nos segmentos de mercado consumidor, empresa e governamental”.

Andrade (2001, p. 13) define da seguinte maneira: “O Comércio Eletrônico é a aplicação de tecnologias de comunicação e informação compartilhadas entre as empresas, procurando atingir seus objetivos. No mundo dos negócios, quatro tipos diferentes de comércio eletrônico se combinam e interagem”.

Neste cenário identifica-se, de um lado a empresa, que oferece um *site (*similar a uma vitrine virtual) para exposição de seus produtos. Além de descrição do produto, a loja deve disponibilizar imagens, descrição técnica, custo e formas de

pagamento visando sanar possíveis dúvidas de seus clientes, o outro extremo deste cenário.

1.1.1 Tipos de Comércio Eletrônico

Turban, Rainer e Potter (2003) conceituam as principais áreas do comércio eletrônico, Paoliello e Furtado (2004) e Nakamura (2011) aprofundam o tema, conforme abaixo:

Business-to-Business (B2B) (Negócio-Negócio) – Sigla utilizada no comércio eletrônico que define transações comerciais entre empresas, ou seja, uma empresa (indústria, distribuidor, importador ou revenda) comercializa seus produtos e serviços com outras empresas. “Na perspectiva B2B, o Comércio Eletrônico facilita as aplicações de negócios, beneficiando o gerenciamento de fornecedores, estoque, distribuição, canal e pagamento.” (PAOLIELLO e FURTADO, 2004, p. 2).

Business-to-Consumer (B2C) (Negócio-Consumidor) – Similar ao B2B, porém a transação comercial é realizada entre a empresa (produtora, vendedora e/ou prestadora de serviço) e o consumidor final. A Natureza dessa operação tende a ser apenas de consumo. “Nos Estados Unidos, as vendas via Internet passarão de 0,4% (em 1999) para cerca de 3% em 2004, do total de vendas ao consumidor final”. (PAOLIELLO e FURTADO, 2004, p. 5).

Nakamura (2011) destaca dois tipos importantes de B2C e aponta vantagens e desvantagens de cada um deles:

LEILÕES – Esta modalidade de comércio eletrônico oferece uma licitação eletrônica. A vantagem deste modelo é a conveniência, a possibilidade de acesso de qualquer lugar do mundo, flexibilidade e economia que pode proporcionar. As vantagens estão na falta de inspeção do que está sendo negociado e chances de fraude durante o pagamento do produto.

LOJAS VIRTUAIS – “é o comércio de produtos utilizando a web” (NAKAMURA, 2011, p.17). Essa modalidade apresenta duas finalidades, vitrine

virtual (usada para promover a venda de produtos ou serviços) ou de comércio *on-line* realizando a venda usando o ambiente virtual. As vantagens estão diretamente ligadas aos preços mais baixos, possíveis graças ao custo operacional menor, maior variedade de escolha e conveniência de comprar a partir de qualquer local físico (com acesso a Internet) também compõe as vantagens desta modalidade. A desvantagem é apontada na estruturação do sistema de logística, visto que as condições e prazos de entrega são determinantes venda e pós-vendas.

Consumer-to-Business (C2B) (Consumidor Negócio) – Quando existe a demanda particular por um produto ou serviço, e as organizações concorrem para suprir essa necessidade.

Consumer-to-Consumer (C2C) – (Consumidor-Consumidor) – Transação comercial entre indivíduos consumidores. Pode ser realizada diretamente entre as partes ou por intermédio de uma empresa. Exemplo: *sites* de leilões (mercado livre.com). “Esse tipo de aplicação foi um dos primeiros a resultar em sites de sucesso, provendo condições para que os consumidores comercializassem entre si uma grande variedade de bens e serviços”. (PAOLIELLO e FURTADO, 2004, p. 7).

Government-to-Citizen (G2C) (Governo-para-Cidadãos) – “Representa o comércio do governo ou outro órgão público com consumidor via *web*” (NAKAMURA, 2011, p. 17). Representado no pagamento de tributos, multas e tarifas utilizando a internet.

Government-to-Business (G2B) (Governo-para-Negócio) – Trata de negócios entre governo e empresas, utilizando a Internet para comunicação. Essa atividade pode ser representada por pregões e licitações, compras de fornecedores e etc..

Government-to-Government (G2G) (Governo-para-Governo) – Refere-se ao comércio eletrônico entre órgãos do governo. As transações governo-governo podem ser entre entidades de mesmo nível e diferentes Poderes (horizontalmente), exemplo, negócios entre Poder Legislativo e Poder Executivo ou entre entidades de

níveis diferentes (verticalmente), exemplo, negócios entre entidades da União e Estados ou Municípios.

1.2 COMÉRCIO ELETRONICO NO BRASIL

Visão Geral: Com faturamento de R$ 28 bilhões em 2013 (B2W COMPANHIA DIGITAL) e R$ 43 bilhões no ano seguinte (CARNET, 2015), o *e-commerce* brasileiro segue em ascensão e um dos fatores para este cenário positivo é o crescimento do acesso à Internet, reflexo da ampliação das vendas e uso de *tablets* e *smartphones*. A adesão aos dispositivos móveis por parte dos brasileiros é nítida e impulsionada pela redução dos preços desses aparelhos e crescimento da classe C, classe que representa 56% dos novos consumidores (CARNET, 2015).

Crescimento do Comércio Eletrônico: As previsões para os próximos anos, segundo a Associação Brasileira de Comércio Eletrônico, indicam que setor manterá altas taxas de crescimento, com ênfase na expectativa do aumento no consumo de bens digitais, tais como músicas, livros digitais (*e-books*) e até mesmo filmes *on demand*.

1.3 COMÉRCIO ELETRONICO E A INTERNET

O comércio eletrônico está presente nos variados setores econômicos, sendo a Internet o pilar que o sustenta. A Internet é um dos principais elementos do conjunto de linhas digitais por onde os dados são transmitidos na rede eletrônica (ALBERTIN, 2000, p. 40). “Nos dias de hoje, a Internet é considerada como um sistema de distribuição de informações espalhadas por diversos países” (NAKAMURA, 2011, p. 22).

Todavia algumas restrições impedem sua adoção e/ou aceitação por uma parcela da população no Brasil, dentre essas restrições, a mais significativa é o sentimento de insegurança gerado em transações *on-line* oriundo, muitas vezes, da falta de conhecimento do usuário com relação à segurança na internet (CERNEV, 2002).

O assunto segurança na Internet é amplamente discutido, complexo e igualmente questionado, até mesmo sua definição peca em clareza e objetividade, tangenciando erroneamente no conceito de privacidade, ameaça e confiança (CERNEV, 2002).

A segurança na Internet está ligada a um conjunto de regras e de medidas que devem ser seguidas, com o intuito de se obter a melhor experiência possível de negócios *on-line.*

Bhatnagar (2000 *apud* CERNEV 2002) aponta a percepção do risco relacionado à segurança na internet, como uma das principais restrições para o crescimento do comércio eletrônico.

1.4 SEGURANÇA DA INFORMAÇÃO

Segurança é um tema importante e recorrente, sua discussão e entendimento tornam-se necessários visto que sua eficiência é desafiada diariamente.

Para Albertin (2001) a questão da segurança é uma grande fonte de risco tanto para clientes quanto para empresas, tornando-se um obstáculo que deve ser superado. Para usuários, a segurança está ligada aos riscos de insucesso, falhas e fraudes no comércio eletrônico. Para a empresa, além destes riscos, está a possibilidade de não adoção do comércio eletrônico por parte de seus clientes.

> Uma fonte potencial de problemas é a preocupação dos clientes com privacidade e segurança, que poderia levar a uma forte reação contra os fornecedores que utilizam tais sistemas ou simplesmente a não utilização destes sistemas por parte dos clientes (ALBERTIN, 2001, p. 29).

Segundo Fontes (2006), o tema segurança da informação está cada vez mais presente devido três principais fatores:

- Processamento e armazenamento de informações por parte das organizações;

- Dependência do ambiente computacional para realização de negócios;

- Necessidade de acesso à informação por todos os colaboradores da organização no ambiente computacional.

1.4.1 Conceituando a Informação

Evidentemente segurança da informação e informação estão completamente atreladas entre si.

O conceito de Informação não é apenas um conjunto de dados, mas sim o ato de transformar algo primário ou com pouco significado, em um recurso de valor pessoal ou profissional (FONTES, 2006).

A relevância da informação e de sua segurança é apresentada por Fontes:

> A informação sempre foi um dos bens mais importantes da organização. A diferença é que há alguns anos a informação mais crítica para a empresa poderia ser guardada e trancada dentro de uma gaveta. Atualmente, independente do estágio de tecnologia da organização, a proteção da informação deve ser uma preocupação dos executivos e proprietários das empresas (FONTES, 2008, p.6).

Peixoto (2006, p.37) define: “A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional da empresa”.

Nakamura (2011) comenta sobre a classificação da informação, citando sua definição e alguns exemplos:

> É a tarefa de descrever as regras para seleção, manipulação, transmissão, armazenamento e exclusão de informações, analisando conforme a importância de cada informação. O tráfego das informações deve ser transmitido conforme o tipo do negócio e suas características. Como exemplos de classificação têm: confidencial, restrito, interno e de divulgação. Assim a comunicação no ambiente de trabalho será feita de forma objetiva e correta (NAKAMURA, 2011, p.34).

As definições de informação evidenciam sua importância para organizações. Cuidar e proteger esse material são deveres da segurança da informação.

1.4.2 Conceito de Segurança da Informação

A segurança da informação esta fundamentada em três pilares: confidencialidade, integridade, disponibilidade. São esses princípios básicos que norteiam sua implementação (SÊMOLA, 2003).

- Confidencialidade: o conteúdo de uma informação deve ser protegido, restringindo seu acesso e uso às pessoas que lhe são destinadas.

- Integridade: garantia de que o conteúdo disponibilizado pelo seu criador permanece sem alterações indevidas, intencionais ou acidentais.

- Disponibilidade: toda informação gerada ou adquirida deve estar disponível ao seu usuário ou instituição no momento em que os mesmos necessitem para qualquer finalidade.

Alguns autores somam aos pilares apresentados, mais três fundamentos da segurança da informação: legalidade, auditabilidade, não repúdio de autoria (FONTES, 2006).

- Legalidade: o uso da informação não deve transgredir leis, regulamentos, licenças e contratos, assim como não deve ferir princípios éticos da organização e sociedade.

- Auditabilidade: todo acesso e uso da informação devem ser registrados, havendo assim, possibilidade de identificação de quem a acessou ou a modificou.

- Não repúdio da autoria: impossibilidade de um usuário negar a autoria ou modificação de uma informação, devido mecanismos que as garantem.

De maneira clara e objetiva Sêmola (2003, p. 43) define segurança da informação, utilizando os conceitos descritos anteriormente: “Podemos definir segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

De forma ampla, somando o conceito de Sêmola aos três fundamentos apresentados por Fontes, segurança da informação pode ser definida como a proteção à informação garantindo que seu acesso só será possível à quem realmente interessar o seu conteúdo, preservando sua confidencialidade e integridade.

1.4.3 Ameaças à Segurança da Informação

Os sistemas de segurança, que compõem a segurança da informação no mundo digital, têm recebido grandes investimentos nos últimos anos e devem manter-se no planejamento financeiro e estratégico de 90,2% das empresas brasileiras (EY BRASIL, 2014). Os investimentos são destinados à manutenção e atualização dos sistemas, com objetivo de garantir o pleno funcionamento dos sistemas *on-line.*

Em contra ponto a este cenário de investimentos e proteção, está o elo mais vulnerável de toda corrente, o cliente em si. Todos os esforços para proteger os sistemas *on-line* são perdidos se o ambiente do cliente estiver vulnerável a invasões e fraudes (WONGTSCHOWSKI, 2005). As ameaças de segurança envolvendo o cliente são tão significativas que necessitam de uma atenção especial, para que seja possível entender a amplitude do problema na segurança do Comércio eletrônico (ANDRADE, 2001).

Podem-se dividir as ameaças virtuais em dois grandes grupos, ameaças que afetam o ambiente virtual e as ameaças focadas no consumidor.

Wongtschowski (2005) e Nakamura (2011) destacam e explicam as principais ameaças focadas no consumidor:

Roubo de dados – Seu objetivo é conseguir dados críticos de autenticação do consumidor, para posteriormente, de forma *off-line*, usar estes dados para se passar pela vítima. “Também chamado de ataque de personificação” (WONGTSCHOWSKI, 2005). Esse tipo de ataque pode acorrer da captura do teclado, telas e *e-mails* falsos;

Roubo de sessão – Alguns sistemas exigem senhas diferentes em cada autenticação, impedindo o sucesso de um ataque por roubo de dados. Neste caso, “o atacante espera o cliente realizar a autenticação e após isso utiliza o número de sessão do usuário para realizar transações *on-line*” (WONGTSCHOWSKI, 2005, p.20).

Modificação de transações – Assemelha-se ao roubo de sessão, o ataque ocorre *on-line* na máquina do cliente. Um aplicativo malicioso instalado na máquina do consumidor fica aguardando pela realização de uma transação, para então, modificar dados nela e enviar um pacote com essas alterações, adulterando, dessa forma, as informações da transação que o cliente esta realizando.

Man-in-the-middle **(homem-no-meio)** – Ataques que buscam interceptar dados entre cliente-servidor. O atacante consegue ler, inserir, excluir e modificar as mensagens trocas. Esse tipo de ataque pode ser utilizado para ler ou modificar os dados críticos trocados entre cliente e servidor de uma instituição.

A preocupação das organizações com proteção e segurança das informações é constante, gerando grandes investimentos em mecanismos modernos para seu controle, porém, isoladamente essas ações não são eficazes. É necessário que haja alinhamento das políticas de segurança da informação com as pessoas que

manipulam as informações, agregando assim, um novo foco para a segurança, o fator humano, que se liga diretamente à engenharia social.

2 ENGENHARIA SOCIAL E SEGURANÇA DA INFORMAÇÃO

“Segurança tem início e termina nas pessoas.” Ellen Frisch

A engenharia social é um tema que demanda muita atenção e cuidado, pois nele encontra-se o elo mais vulnerável e sempre presente, da segurança da informação: as pessoas. Entender como agem os engenheiros sociais e quais gatilhos psicológicos são utilizados para manipular usuários é fundamental para proteção de sistemas, empresas e clientes.

2.1 ENGENHARIA SOCIAL

A engenharia social vai tratar do elo mais frágil na corrente de proteção da informação, a pessoa (FONTES, 2006). O termo ganhou destaque na mídia e difundiu-se em meados dos anos 90, devido o caso do famoso *hacker* chamado Kevin Mitnick.

Nascido em 1963 na Califórnia, Mitnick iniciou sua vida de trapaças burlando o sistema de cartão de ônibus, obtendo assim, passagens municipais gratuitas, posteriormente invadiu vários computadores de operadoras de telefonia e na década de 90 acessou indevidamente provedores de Internet e empresas de tecnologia. Seu sucesso nos crimes virtuais está diretamente ligado ao comportamento das pessoas que tinham acesso às informações privilegiadas, ligando assim segurança da informação com engenharia social (CHAPPELLE, 2000).

A confidencialidade das informações, um dos pilares da segurança da informação, é de responsabilidade das pessoas que têm acesso a ela. Usuários, colaboradores, consumidores precisam conhecer os meios pelos quais agem os engenheiros sociais e devem estar atentos aos gatilhos psicológicos que servem para manipulação e obtenção dessas informações. “Cada usuário tem a responsabilidade profissional de cuidar da informação que utiliza” (FONTES, 2006, p.119.).

2.1.1 Conceito Engenharia Social

Devido aos grandes investimentos em segurança, melhorias no sistema de controle da informação, utilização avançada de criptografia, a maneira mais fácil de invadir ou acessar dados de uma organização é utilizando a engenharia social.

Fontes (2006, p. 120) define engenharia social como:

> O conjunto de procedimentos e ações que são utilizados para adquirir informações de uma organização ou de uma pessoa por meio de contatos falsos sem o uso da força, do arrombamento físico ou de qualquer brutalidade.

Peixoto (2006, p. 4) soma ao conceito de engenharia social o comportamento humano:

> É a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos.

O próprio Mitnick (2004, *apud* PEIXOTO, 2006, p. 4) define em poucas palavras engenharia social: “É um termo diferente para definir o uso da persuasão para influenciar as pessoas a concordar com um pedido”.

De acordo com Peixoto (2006, p. 36), “A engenharia social, propriamente dita, está inserida como um dos desafios (se não o maior deles) mais complexos no âmbito das vulnerabilidades encontradas na gestão da segurança da informação”.

2.2 CONCEITO *HACKER* X *CRACKER*

Determinados peritos ou especialistas em redes computacionais podem se tornar um problema para a segurança da Internet. Se por um lado seu conhecimento pode contribuir positivamente para o aperfeiçoamento tecnológico, por outro existe a possibilidade de usufruir de vulnerabilidades sistêmicas em benefício próprio. “Seja

qual for a intenção, a percepção de segurança ou risco dos usuários certamente será influenciada, na maioria das vezes negativamente" (CERNEV, 2002 , p.73).

Tais especialistas são denominados *hackers* ou *crackers*. Esses termos são empregados de forma errônea por ausência de conhecimento de seus significados, comumente os crimes virtuais são associados ao *hacker*. De fato *Hackers* e *crackers* possuem semelhanças, ambos são pessoas inteligentes e utilizam brechas na segurança da informação para terem acesso a áreas e dados restritos. A categoria que o transgressor vai se encaixar dependerá de sua postura após esse tipo de invasão.

Rufino (2002, p.16) discorre sobre o assunto:

> Desde que apareceu nos meios de comunicação, o termo hacker perdeu a conotação romântica de outros tempos, pois se antes significava aficionado por computadores (a origem é ainda anterior) agora indica piratas eletrônicos ligados a crimes utilizando computadores. Bem que se tentou (e alguns ainda tentam) associar a esses últimos o termo cracker. "aqueles que quebram sistemas", mas acredito que seja uma causa perdida.
>
> Visto que o termo ganhou uma carga pejorativa, os vendedores de serviço de segurança criaram a figura do "hacker ético", para tentar minimizar o impacto que o termo hacker causa ao cliente, e é justamente a palavra "ética" que acaba fazendo toda a diferença.

2.2.1 HACKER

Nogueira (2008, p. 61) caracteriza *hacker:*

> Este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam desafiar entre si, para ver quem consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual.

O termo *White Hat* é diretamente associado ao termo *hacker*, compondo: *Hacker White Hat.*

Assunção (2008, p. 13) define *Hacker White Hat* como:

> *'Hacker* do bem', chamado de '*hacker* chapéu branco'. É aquela pessoa que se destaca nas empresas e instituições por ter um

> conhecimento mais elevado que seus colegas, devido ao autodidatismo e à paixão pelo que faz. Não chega a invadir sistemas e causar estragos, exceto ao realizar testes de intrusão. Resumindo: tem um vasto conhecimento, mas não o usa de forma banal ou irresponsável.

"O termo Hacker está mais relacionado ao indivíduo que possui um elevadíssimo grau de conhecimento em assuntos relacionados à computação" (ALVES, 2010, p.42).

Baseando-se nestes conceitos, conclui-se que os *hackers* ou *White Hats* não têm como finalidade causar danos aos sistemas invadidos, ao contrário, muitas vezes empregam seus conhecimentos na melhoria de softwares de forma legal.

2.2.2 CRACKER

Os ataques movidos pela engenharia social, normalmente, são praticados por *crackers,* que são *hackers* mal intencionados (ALVES, 2010, p.42.).

Os *crackers* são pessoas aficionadas por tecnologia e informática. Utilizam seus conhecimentos para quebrar código de segurança e de sistema, obter senhas de acesso a redes e a dados privados, quase sempre com fins criminosos.

Para Cernev (2002, p.34) *crackers: "São* arrombadores de sistemas, operando tanto em software quanto em hardware. São persistentes, antissociais, rápidos, objetivos e não costumam deixar rastros de sua atuação".

O sinônimo para o termo *cracker* é *Black Hat* definido por Assunção (2008, p. 13):

> Hacker Black-Hat: "Hacker do Mal" ou "chapéu negro". Esse, sim, usa seus conhecimentos para roubar senhas, documentos, causar danos, ou mesmo realizar espionagem industrial. Geralmente tem seus alvos bem definidos e podem passar semanas antes de conseguir acesso onde deseja, se o sistema for bem protegido.

Os *crackers* podem ser subdivididos conforme a área de atuação ou nível de conhecimento. Duas classificações destacam-se: *phreaker* e *defacer*.

Rosa (2006, p. 62) conceitua *phreaker* como:

> Especializado em telefonia, atua na obtenção de ligações telefônicas gratuitas e instalação de escutas, facilitando o ataque a sistemas a partir de acesso exterior, tornando-se invisíveis ao rastreamento ou colocando responsabilidade em terceiros.

Os crimes mais comuns dos *phreakers* são clonagem de celulares, escutas telefônicas não autorizadas e alteração nos sistemas de cobrança da telefonia.

Defacer é quem faz uma “pichação virtual”, que no conceito de Rosa (2006, p.65) é “colocar, de forma indevida, textos ou figuras em sites de terceiros sem a devida autorização”.

2.3 PERFIL DO ENGENHEIRO SOCIAL

O psicólogo social Dr. Brad Sagarin (*apud* MITNICK e SIMON, 2006, p.189) caracteriza o engenheiro social como o profissional que:

> Emprega as mesmas técnicas persuasivas que usamos no dia-a-dia (sic). Assumimos papéis. Tentamos obter credibilidade. Cobramos obrigações recíprocas. Mas, ao contrário de nós, o engenheiro social aplica essas técnicas de maneira manipuladora, enganosa, altamente antiética e em geral com efeito devastador.

Alves (2010), diz que o engenheiro social é dotado de grande criatividade. Essa criatividade é tamanha que, na maioria das vezes, a vítima não imagina que foi usada e que facilitou de alguma forma o caminho para um invasor. Ele utiliza-se de técnicas de persuasão e explora a ingenuidade dos usuários, criando um ambiente psicológico favorável para seu ataque, valendo-se de identificações falsas, carisma e o apelo sentimental buscando a confiança de sua vítima.

Destaca que comumente o engenheiro social procura tranquilizar sua vítima, passando-se por alguém de nível hierárquico igual ou superior dentro do ambiente de trabalho ou até mesmo por clientes e fornecedores, objetivando conseguir informações, executar programas maliciosos e em casos extremos conseguir senhas de acesso.

Salienta que para conseguirem o que precisam esses mestres da arte de enganar utilizam pretextos como situações de emergência ou de segurança da empresa e normalmente, agem de forma pacienciosa, pedindo informações aos poucos e para pessoas distintas, evitando assim, que desconfianças recaiam sobre

ele. Para que um engenheiro social consiga um ataque bem sucedido, é preciso que haja bastante paciência e persistência e essa é uma de suas maiores características.

2.4 TÉCNICAS E MECANISMOS EMPREGADOS NA ENGENHARIA SOCIAL

Mann (2011 *apud* MUNIZ, 2012, p. 24-25) afirma que criar um vínculo rápido com o alvo é um fator decisivo para o sucesso do engenheiro social. Para isso, algumas técnicas são empregadas visando criar, subconscientemente, a afinidade necessária com sua vítima, tais como:

> **Espelhamento da respiração:** onde o aspecto mental de uma pessoa é refletido em seu ritmo respiratório. O engenheiro social tenta igualar-se a ela, espelhando este atributo. Não é uma técnica fácil, pois sem os movimentos certos, pode vir a parecer falso.
>
> **Ouvir de verdade:** de modo que a ideia é entender realmente o que o alvo está falando e então dar uma resposta que demonstre compreensão por parte do engenheiro social, o qual normalmente responde a própria afirmação do alvo, porém com outras palavras, levando ao alvo concordar, e assim aumentar a conexão com o engenheiro social.
>
> **Pausas na fala**: ou seja, simplesmente ouvir, é uma poderosa arma dos engenheiros sociais que leva muitas pessoas a se sentirem como se estivessem encontradas um amigo verdadeiro, mesmo estando a pouco tempo conversando com o engenheiro social.
>
> **Roteiro mental:** que consiste basicamente em fazer com que o alvo sinta que o engenheiro social realmente pensa como ele. Para tal os engenheiros sociais condicionam a mente a crer que eles realmente gostam do alvo, criando assim, subconscientemente, linguagens corporais genuínas, ou seja, os engenheiros sociais manipulam o seu próprio subconsciente a fim de tornar uma reação de conexão real.
>
> **Concordar/Identificar:** quando simplesmente concordam com as respostas do alvo e assim conduzem o ataque de modo a se identificar com ele. Situações como ter nascido na mesma região ou ter os mesmos hobbies são exemplos no qual o alvo identifica-se facilmente com o atacante, permitindo assim que o atacante ganhe mais confiança do alvo.
>
> **Vestimenta:** que consiste em permitir que o atacante se misture naturalmente em um ambiente, utilizando-se de vestimenta apropriada ao local.

Para atingir seu objetivo, o engenheiro social assume determinados papéis, adquirindo características comportamentais do papel que está interpretando e assume certos acessórios deste papel para fazer com que sua vítima deduza outras características e aja de acordo com o esperado (MITNICK E SIMON, 2006).

Mitnick e Simon (2006) citam exemplos e relatos de papéis utilizados por engenheiros sociais, tais como:

- Fingir ser um empregado de algum fornecedor, empresa parceira ou uma autoridade legal.
- Fingir ser o próprio fornecedor/ fabricante de sistemas que liga para oferecer uma atualização do sistema.
- Passar-se por suporte, oferecendo ajuda para um eventual problema e, em seguida, causar o problema descrito para manipular a vítima e fazer com que ela ligue pedindo ajuda.

Além de técnicas que se beneficiam da confiança e vulnerabilidade por parte de seus alvos, os engenheiros sociais também utilizam técnicas específicas de ataque.

Lennert e Oliveira (2011 *apud* MUNIZ, 2012, p.27-28) resumem em:

> **Pretexto:** que consiste no ato de criar e usar um cenário inventado para atacar a vítima de uma maneira que ocorra uma chance maior da vítima divulgar a informação ou realizar ações que normalmente não faria em circunstâncias comuns. É mais do que uma simples mentira, pois na maioria das vezes envolve uma pesquisa anterior e, até mesmo, interpretação de personagens (personificação) para estabelecer legitimidade na mente do objetivo.
>
> ***Phishing*:** onde o "pescador", tipicamente, envia um *e-mail* que aparentemente vem de um negócio legítimo (banco, companhia de cartão de crédito) solicitando confirmação de informações e avisos de interrupção de serviço se a informação não for fornecida. O *e-mail* normalmente, contém um link para uma *web page* fraudulenta que solicita o preenchimento de dados pessoais e bancários.
>
> ***Phone Phishing:*** onde a vítima é orientada (através de um *e-mail phishing*) para ligar para um banco e confirmar algumas informações. Um sistema típico (semelhante ao do banco) irá rejeitar as tentativas de entrada com as senhas, assegurando assim, que a vítima entre

com os *PINs* ou as senhas várias vezes, facilitando o reconhecimento das várias senhas. Sistemas mais avançados transferem a vítima ao criminoso, que nesse momento, se passa por um atendente.

Isca (*baiting*): que se utiliza de mídias físicas removíveis, como *CD ROM*, *USB flash drives*, etc., para despertar a curiosidade ou a ganância da vítima.

Quid pro Quo: onde o engenheiro social ligará aleatoriamente para vários números dizendo ser do suporte técnico de determinada empresa. Eventualmente, alguém terá um problema legítimo e necessitará de ajuda. Nesse instante, o atacante irá ajudar a resolver o problema e no meio do processo, pedirá ao usuário para tomar algumas ações que o permitirá ganhar acesso ao sistema ou lançar um *malware*.

Lixo (*dumpster diving*): uma vez que o lixo das empresas pode ser uma fonte muito rica de informações para um *hacker*. Vasculhar o lixo é um método muito usado pelos invasores, porque é comum se encontrar itens como cadernetas com telefones, organograma da empresa, manuais de sistemas utilizados, memorandos, relatórios com informações estratégicas e até anotações com *login* e senha de usuários.

Engenharia Social Inversa: que ocorre quando um *hacker* cria uma personalidade que aparece numa posição de autoridade, de modo que todos os usuários lhe pedirão informação. Se pesquisado, planejado e bem executado, o ataque de engenharia social inversa permite ao *hacker* extrair dos funcionários informações muito valiosas, entretanto, isto requer muita preparação e pesquisa.

Os mecanismos usados para proteger a informação evoluem constantemente, porém a questão do comportamento humano será crucial para que a proteção fornecida por qualquer sistema seja rompida. As brechas de segurança do comportamento humano podem frustrar a experiência positiva do comércio eletrônico.

3 COMERCIO ELETRÔNICO E SEGURANÇA DA INFORMAÇÃO

O comércio eletrônico está claramente atrelado ao tema segurança da informação, ela pode ser considerada uma barreira para o crescimento deste tipo de comércio, como explicam Vieira e Nique (1999, p. 11):

> As questões de segurança ainda permanecem como uma barreira para a maior adesão dos usuários as atividades de comércio na rede, uma vez que se identifica que a atribuição de alta importância ao fator segurança está associada com aqueles indivíduos que nunca compra pela internet.

Cernev (2002) discute e acrescenta outras visões ao termo segurança, sendo este, comumente confundido com privacidade, assim como sua falta é associada com risco. Segurança é composta de aspectos técnicos e jurídicos, mas também pode ser percebida como um aspecto subjetivo de percepção, que pode ser analisada do ponto de vista empresarial ou sob o ponto de vista do usuário. Ainda, pode estar relacionada com a concepção da Internet e sua infraestrutura, ou ser limitada aos meios de pagamento e negociações eletrônicas.

Do ponto de vista empresarial, segurança é a combinação de diversos recursos tecnológicos, políticas empresariais, prevenção, treinamento, qualificada então como dever ou missão específica de determinado departamento.

Do ponto de vista dos usuários, segurança é percebida como adjetivo e está relacionada à percepção de risco ou confiança em relação aos ambientes, tecnologias e agentes do comércio eletrônico. Ainda segundo Cernev (2002, p. 46):

> Existe uma observação na pesquisa "GVU's 10th WWW User Survey" (1998), realizada pelo Georgia Institute of Technology, ampliando a compreensão do termo segurança para os intemautas, neste caso, incluindo também os significados de privacidade, confidencialidade e prova de identidade.

A questão da privacidade liga-se diretamente com temas relacionados à segurança da informação e, por este motivo, muitos usuários confundem sua definição e implicações. “Justamente por existir esta inter-relação, os aspectos da privacidade também são reconhecidos como alguns dos maiores obstáculos para o

crescimento do CE e, consequentemente, de toda a economia.” (CERNEV, 2002, p.47).

3.1 AMBIENTE VIRTUAL

Pode ser definido como o conjunto mundial de rede de computadores e serviços de informação, implementados no ambiente digital. Oferecendo aos usuários a possibilidade de interagir, comunicar, realizar pedidos de compras ou serviços e transações de negócios com fornecedores, independente da localização física de cada indivíduo (ALBERTIN, 2000). Neste ambiente ocorrem todas as transações do comércio eletrônico.

3.1.1 Infovia

Refere-se às linhas digitais que transmitem os dados na rede eletrônica, foi criada com o intuito de descentralizar a rede, mudando assim, o conceito tradicional. Com formato baseado na Internet, ela está se tornando um sistema de redes de computadores com o uso da Internet rápida (banda larga), trafegando dados como textos, vídeos, som e imagens, de usuários residenciais, empresas, escolas e etc (ALBERTIN, 2000).

Para se estabelecer, a infovia, necessita de três elementos, em termos de infraestrutura, descrito por Nakamura (2011, p. 21):

> Equipamentos de acesso à rede: nesse segmento podem-se destacar os vendedores de hardware e software, que disponibilizam de meios físicos como roteadores e switches e também de meios de acessos como computadores e televisão a cabo, além disso oferecem plataformas de software como software de navegação na Internet e sistemas operacionais.
>
> Estrutura de acesso local: identifica-se como provedores de acesso a plataforma principal de comunicação ligando usuários e provedores de TI.
>
> Redes globais de distribuição de informação: são representadas pela infraestrutura entre países e continentes. Onde a maior parte dessa estrutura está localizada na extensa rede de fibra óptica, cabos coaxiais, ondas de rádio e satélites.

3.1.2 Internet

A Internet é uma trama (rede) de computadores de abrangência mundial que utiliza um protocolo de comunicação denominado TCP/IP – *Transmission Control Protocol/Internet Protocol*, que entrega uma linguagem comum possibilitando a interconexão entre redes de computadores, cuja finalidade é facilitar o transporte de informações (CAVALCANTI, 1997). Ravindran, Barua, Lee e Whinston (1996 *apud* ALBERTIN, 1998, p. 55), apontam que a Internet "representa um ciberespaço constituído por uma teia mundial de redes de computadores e serviços de informações".

Segundo Albertin (2000) a Internet representa um dos principais componentes da infraestrutura de rede da infovia. Atualmente, a Internet pode ser considerada um sistema de distribuição de informações, difundido em diversos países. O ambiente da web é a soma do serviço postal, do sistema de telecomunicação, pesquisas bibliográficas e Comércio Eletrônico.

3.1.3 Intranet e Extranet

A tecnologia empregada dentro das organizações, com objetivo de melhorar a conectividade e comunicação entre usuários é denominada intranet. Sua aplicação pode está presente no sistema de *e-mails* da rede local e no acesso a base de dados, isso significa, que utilizando um site intranet, informações são disponibilizadas em tempo real, agilizando assim, as tarefas dos usuários (ANDRADE, 2001).

A intranet possui características positivas, que impulsionam sua implementação, tais como: redução de custos, facilitação do trabalho em grupo para projetos, melhora no fluxo de informação, manutenção simples.

Andrade (2001) define extranet como a infraestrutura que possibilita o acesso seletivo de usuários (consumidores) e fornecedores ao website da empresa. Nela o acesso é controlado por senhas de acesso, autenticações, utilizando dessa forma, medidas de segurança da informação para limitar acessos não permitidos.

3.1.4 World Wide Web (WWW)

Refere-se a um conjunto de documentos disponíveis em computadores chamados de servidores. Esses documentos são considerados páginas da web (rede) e são armazenados em formato HTML, *Hyper Text Markup Language*, e respondem às solicitações. Para ser acessado, o *World Wide Web* necessita de uma conexão com a internet e um software chamado navegador. Com este software os usuários poderão localizar e visualizar os documentos contidos nos servidores e os dados de multimídia (ALBERTIN, 2000).

3.2 SISTEMA ELETRÔNICO DE PAGAMENTO

Os sistemas eletrônicos de pagamento para consumidores estão disponíveis desde a década de 40, representados pelo cartão de crédito. Três décadas depois, a tecnologia de pagamento eletrônico foi denominada de transferência eletrônica de fundos (*Eletronic Funds Transfer* – EFT) (ALBERTIN, 1998).

Nakamura (2011, p. 25) define pagamento eletrônico como: “qualquer pagamento que não utiliza dinheiro vivo ou cheque em formato de papel” e acrescenta: “Nada mais conveniente do que realizar um pagamento eletronicamente, onde tudo o que precisa é inserir alguns dados e confirmar via web”.

O sistema eletrônico de pagamento é de suma importância para o comércio eletrônico, por relacionar-se profundamente com aspectos da segurança e por se mostrar o pilar para a plataforma tecnológica que tornará possível a expansão do comércio eletrônico (CERNEV, 2002).

Para Albertin (1999, p. 29) transações eletrônicas e os meios de pagamento precisam de segurança, ser de fácil utilização e de baixo custo, além de apresentar de forma transparente para os usuários, seus aspectos técnicos.

> As transações de negócio eletrônicas somente podem ter sucesso se as trocas financeiras entre compradores e vendedores puderem acontecer em um ambiente simples, universalmente aceito, seguro e barato. Os tipos de sistemas eletrônicos de pagamento são: dinheiro

> eletrônico (*e-cash*), cheque eletrônico (*e-check*), cartões inteligentes (*smart cards*), cartões de crédito e cartões de débito.

O uso do sistema eletrônico de pagamento está se expandindo em vários setores atendendo o varejo, rede bancária, mercado *on-line* e até mesmo o governo. Albertin (2000) explica que o fator que impulsiona empresas a procurarem esse mecanismo é a necessidade de oferecer produtos ou serviços com custo competitivo e com boa qualidade, pois a satisfação do cliente é determinante para alcançar o sucesso do negócio.

3.2.1 Dinheiro Eletrônico

O Dinheiro eletrônico ou *e-cash* é descrito por Albertin (1998, p.61) como "um novo conceito nos sistemas de pagamento on-line porque ele combina conveniência computadorizada com segurança e privacidade." Segundo o mesmo autor, o *e-cash* precisa conter as seguintes características: "valor monetário, interoperabilidade, recuperabilidade, segurança, anonimato e liquidez" e pode apresentar-se em algumas formas, incluindo cartões pré-pagos e sistemas genuinamente eletrônicos.

> Cartões pré-pagos: os compradores podem comprar cartões pré-pagos que são aceitos por vendedores especiais. Atualmente, um dos exemplos de cartão pré-pago é o cartão telefônico, que apresenta a deficiência de não ter liquidez, ou seja, não se pode comprar mercadorias com eles. Os cartões inteligentes (*smart cards*) de múltiplas funcionalidades, anunciados por algumas empresas e que estão, no momento, em teste-piloto, devem incorporar as funções do dinheiro digital.
>
> Sistemas genuinamente eletrônicos: o dinheiro digital genuinamente eletrônico seria isento da forma física explícita, tomando-se útil para transações em redes e Internet, nas quais o comprador e o vendedor estão em localidades fisicamente remotas. O pagamento seria realizada através de deduções eletrônicas de dinheiro digital do comprador e seguida de transmissão para o vendedor. A atual transferência de dinheiro digital é usualmente criptografada por sistemas de criptografia de chave pública ou chave privada, de forma que somente o destinatário intencional (o vendedor) possa realmente utilizar o dinheiro. Entretanto, restrições institucionais, como as restrições americanas de exportação de sistemas avançados de criptografia, podem impedir a aceitação e a praticidade do dinheiro digital. Além disso, métodos que assegurem o anonimato precisam estar disponíveis, pois, de outra forma, os sistemas genuinamente eletrônicos não se tomarão alternativas de sistemas de cheque eletrônico (ALBERTIN, 1998, p.61).

Albertin (1998, p.61) conceitua e classifica sinais eletrônicos: “são projetados como analogias eletrônicas das várias formas de pagamento que têm por trás de um banco ou instituição financeira”.

> **Dinheiro ou tempo real**. as transações são estabelecidas com a troca de moeda eletrônica, por exemplo, o dinheiro eletrônico (*e-cash*).
>
> **Débito ou pré-pagamento**. os usuários pagam adiantado pelo privilégio de obter informação, por exemplo, os cartões inteligentes que armazenam dinheiro eletrônico.
>
> **Crédito ou pós-pagamento**. o servidor autentica os clientes e verifica com o banco se os fundos são adequados antes da compra, por exemplo, os cartões de crédito/débito e cheques eletrônicos (*e-check*) (ALBERTIN, 1998, p.61).

3.2.2 Cartão de Crédito

Para Abrão (1966, p.147) o cartão de crédito é “um documento comprobatório de que seu titular goza de um crédito determinado perante certa instituição financeira, o qual o credencia a efetuar compras de bens e serviços a prazo e saques de dinheiro a título de mútuo”.

Em termos atuais, é uma forma de pagamento eletrônico utilizada amplamente na Internet para aquisição de produtos ou serviços. Posteriormente essa dívida será cobrada através de uma fatura discriminando todos os gastos no período.

Para que uma transação efetuada utilizando cartão de crédito seja considerada segura, é necessário que alguns requisitos sejam atendidos:

> Cliente informa os dados do seu cartão de crédito de forma segura ao vendedor.
>
> Validação do consumidor como proprietário do cartão.
>
> Comerciante enviar as informações do débito e a assinatura do cliente ao banco.
>
> Enviar as informações ao banco do cliente para que seja autorizado e aprovação do credito do consumidor.

> Retornando os dados do cartão com autenticação do débito e autorização (NAKAMURA, 2011, p.30).

3.2.3 Cartão de Débito

Também chamado de cartão pré-pago, nesta modalidade de pagamento, o desconto ou a cobrança são efetuados em conta corrente ou poupança, imediatamente após a compra.

Nakamura (2011, p.30) explica que “o funcionamento da compra feita com cartão de débito possui grandes semelhanças ao cartão de crédito, mas a característica principal dessa forma de pagamento seria o pagamento descontar no momento da compra, sendo que o cartão de crédito disponibiliza fundos para compensar a transação”.

Por dedução, este meio de pagamento pode ser considerado mais vantajoso do ponto de vista de controle dos gastos, visto que as compras somente são aprovadas havendo fundos para isso no ato da compra.

3.3 VULNERABILIDADES

A todo o momento muitos negócios, e seus ativos físicos, tecnológicos e humanos são alvos de ameaças de toda ordem, que tentam encontrar um ponto fraco, uma vulnerabilidade capaz de potencializar sua ação.

Sêmola (2003, p. 47) define ameaças como:

> [...] agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização.

Peixoto (2006 *apud* MUNIZ, 2012) aponta algumas vulnerabilidades e ferramentas por onde usuários mal intencionados conseguem obter vantagens ou informações restritas, são elas:

Internet: pode ser uma um ótimo canal para coleta de informações do usuário, a utilização de redes sociais, buscadores (como o Google) são fontes de informações pessoais;

Intranet: utilizando o acesso remoto, o um engenheiro social é capaz de assumir o controle de um microcomputador e assim obter todo tipo de informação contida na máquina;

Pessoalmente: ponto amplamente apresentado neste trabalho é a demonstração prática de todo poder de persuasão do engenheiro social. É a exploração da vulnerabilidade humana;

Chat: também chamados de bate-papo, meio pelo qual o atacante consegue se aproximar de sua vítima e criar um laço de confiança utilizando fotos e dados falsos e assim obter a informação que deseja;

Fax: mesmo em desuso, ainda é a maneira mais simples de se obter o número de pessoas e empresas para então iniciar um ataque;

Spyware: trata-se de um programa espião. Ele instala-se de forma oculta e monitora as atividades do computador, podendo enviar informações como o seu idealizador programar;

Surfar sobre os ombros: refere-se ao ato de observar uma pessoa digitando com o intuito de descobrir ou roubar senhas e outras informações privadas;

P2P (*peer-to-peer*): tecnologia utilizada para interligar inúmeros computadores, similar a uma rede, onde cada máquina possui capacidades e responsabilidades similares. Exemplo desse tipo de aplicação: *e-mule* e *kaZaa*.

3.4 INFORMATIVO

O processo de segurança tem início com o usuário, sua postura perante as armadilhas virtuais fará toda diferença e influenciará diretamente sua experiência *on-*

line. Uma postura preventiva e a preocupação com a segurança devem ser hábitos presentes na rotina do usuário.

3.4.1 Cuidados no Correio Eletrônico

- *Phishing*: o golpista tenta obter dados pessoais ou financeiros do usuário utilizando mensagens eletrônicas, páginas falsas, formulários fraudulentos e links com códigos maliciosos.

- Seja cuidadoso ao acessar *links*, prefira digitá-los diretamente no navegador.

- Observe se o *link* descrito na mensagem é o mesmo para onde ele o direciona, faça isso posicionando o *mouse* sobre o *link* e lendo o endereço apresentado.

- Fique em alerta com mensagens que apelem por sua atenção e, de alguma forma, contenham ameaças caso os procedimentos contidos nela, não sejam seguidos.

- Não considere uma mensagem segura, com base na confiança que deposita em seu remetente, a conta do mesmo pode estar comprometida graças a uma invasão ou o nome de destinatário pode ser forjado.

3.4.2 Cuidados no Comércio Eletrônico

Neste golpe, o atacante procura obter vantagens financeiras, explorando a relação de confiança entre o cliente e o site de vendas.

- Antes de qualquer compra, faça uma busca na Internet sobre o *site* que deseja efetuar a compra, obtendo referências com outros usuários que compraram neste mesmo *site*. Existem sites específicos (como o

reclameaqui) para cadastro de reclamações, golpes e outros problemas encontrados na aquisição de produtos ou serviços.

- Faça sempre uma pesquisa de preços do produto desejado, valores muito abaixo dos praticados pelo mercado pode ser uma armadilha.

- Jamais forneça seus dados para pagamento (dados de cartão, C.P.F.) caso o *site* não apresente conexão segura. A conexão segura é identificada por apresentar no inicio do endereço a letra “S”, logo após http: *https://* , além disso o desenho de um “cadeado trancado” ficará visível na barra de endereços.

- Não realize compras *on-line* utilizando redes públicas ou em computadores de acesso compartilhado.

3.4.3 Cuidados nos Sites de Leilão

Neste golpe o vendedor ou comprador pode agir de má-fé e não cumprir com as obrigações acordadas, ou ainda, utilizar os dados pessoais e financeiros obtidos na negociação para outros fins.

- Desconfie de valores praticados muito abaixo do valor de mercado. Mesmo tratando-se de produto usado, existe um valor médio para cada produto.

- Quando a entrega da mercadoria for realizada pessoalmente, marque o encontro em local público e movimentado.

- Alguns sites fornecem um sistema de gerenciamento de pagamento, onde o valor monetário é entregue ao vendedor após resposta positiva do comprador, utilize-o sempre que possível.

- Verifique atentamente a reputação do vendedor, observe os comentários de outros compradores.

- Após o término da sua negociação avalie o vendedor, jamais qualifique-o antes de receber seu produto (o código de rastreio de uma mercadoria não é garantia de nada). Essa atitude servirá para destacar os bons negociantes e excluir os que agem de má-fé.

3.4.4 Outros Cuidados

Mantenha os programas do computador sempre atualizados, não somente antivírus, mas também o sistema operacional, navegadores, softwares de escritórios para texto ou planilha, clientes de *e-mail* e drivers em geral.

- Sempre mantenha antivírus, *antimalware* e *firewall* ativos.

- Exija sempre a instalação de programas originais.

- Utilize senhas diferentes pra cada rede social, sites de compras e *log-in* no sistema operacional. Desenvolva sempre senhas com números e letras e prefira utilizar teclados virtuais quando disponíveis.

- Todo usuário do sistema operacional deve ter uma senha pessoal e não compartilhada.

- Redes sociais são fontes de grande informação para terceiros, faça uma rigorosa configuração de privacidade e publique o que realmente achar relevante.

- Seja criterioso ao levar seu equipamento (computador, *tablet* ou *smartphone*) para manutenção, busque sempre referências das empresas que fazem esse trabalho.

- Seja cauteloso ao compartilhar qualquer tipo de informação com desconhecidos. Os engenheiros sociais têm técnicas e sabem utiliza-las para obter as mais variadas informações, sejam elas pessoais, de outrem ou mesmo de uma empresa.

“O processo de segurança é um ciclo continuo, onde deve ser sempre atualizado”. (SÊMOLA, 2003).

OBS.: como apêndice consta um informativo.

4 CONSIDERAÇÕES FINAIS

O avanço da tecnologia, sobretudo computação e telecomunicação, tornou possível a implementação de um novo modelo de comércio, o comércio eletrônico. Por meio da Internet novas possibilidades foram alcançadas e as transações comerciais ao redor do mundo tornaram-se viáveis, superando a barreira geográfica entre compradores e vendedores, sejam elas entidades físicas ou jurídicas.

A ascensão do comércio eletrônico é inquestionável, um mercado em franca expansão e desenvolvimento, porém, a aceitação do processo de compras *on-line* depende da capacidade de transpor certos obstáculos dentre eles, e motivo desta pesquisa, o fator cultural/humano e a segurança nestas transações.

O ser humano apresenta uma resistência inata ao desconhecido, a falta de entendimento dos processos *on-line*, assim como a exigência de um preparo ínfimo, resulta na falta de confiança dos consumidores em compras *on-line*, sobretudo, na segurança empregada nessas transações. Essa condição é limitadora para o crescimento deste tipo de negócio.

Todo sistema está sujeito a problemas ou falhas e a segurança no ambiente virtual não pode ser totalmente garantida pelas empresas, entretanto ferramentas e tecnologia são desenvolvidas e utilizadas de forma massiva com objetivo de conter ou minimizar ataques durante uma transação eletrônica, porém um sistema que prime pela segurança da informação não depende apenas de máquinas, mas também do próprio usuário.

O elo que mais demanda atenção quando se trata de segurança da informação é o usuário. Todo o investimento empregado para proteger as transações virtuais e as informações do consumidor será em vão se a postura de quem utiliza este sistema não for adequada. A falta de conhecimento por parte do usuário gera grandes brechas de segurança, que são prontamente utilizadas por engenheiros sociais.

Trazer ao usuário o conhecimento de como agem os engenheiros sociais, o que buscam e onde atacam, assim como as vulnerabilidades de sistema, é oferecer a chance de escapar, se proteger e usufruir do comércio eletrônico, tentado dessa

forma, transpor a barreira da insegurança que separa clientes e vendedores no mundo virtual. Com essa premissa, a pesquisa entrega diversas informações relativas ao comércio eletrônico, segurança da informação, engenharia social e oferece um informativo conciso, objetivo e direcionado ao usuário leigo, promovendo uma maior inteiração entre as partes, aproximando de forma segura, o usuário/consumidor das variadas possibilidades que as transações *on-line* disponibilizam.

A partir desta pesquisa outras podem se desdobrar, sobretudo de cunho quantitativo, mensurando e qualificando usuários que se beneficiaram das informações e do informativo trazidos neste trabalho, passando assim a realizarem transações no comércio eletrônico.

5 REFERÊNCIAS

ABRÃO, Nelson. Direito bancário. Revista dos Tribunais. São Paulo: Globo. 1966, p.147.

ALBERTIN, A. L. **Comercio eletrônico:** situação atual e tendências. São Paulo: FGVEAESP, 2001. Relatório de Pesquisa - NPP, n" 38.

_____. **Comércio eletrônico.** 2.ed. São Paulo: Atlas, 2000.

_____. **Comércio eletrônico:** Modelo, Aspectos e Contribuições de sua Aplicação. São Paulo: Atlas, 1999.

_____. **Comércio eletrônico:** Benefícios e aspectos de sua aplicação. RAE – Revista de Administração de Empresas, São Paulo, v.38, n.1, p.52-63, jan/mar. 1998. Disponível em: http://www.scielo.br/pdf/rae/v38n1/a06v38n1.pdf. Acesso em: 07 Out. 2015. 15h30.

ALVES, Cássio Bastos. **Segurança da informação vs. Engenharia social**: Como se proteger para não ser mais uma vítima. 2010. Artigo de graduação – Centro Universitário do distrito Federal.

ANDRADE, Rogério de. **Guia Prático de E-Commerce**. São Paulo: Angra, 2001.

ASSUNÇÃO, Marco Flávio Araújo. **Segredos do Hacker Ético**. 2ª ed. Florianópolis/SC: Visual Books. 2008, p.13.

B2W, COMPANHIA DIGITAL. **Institucional/Comércio Eletrônico no Brasil.** Disponível em: http://www.b2wdigital.com/institucional/comercio-eletronico-no-brasil . Acesso em 13 set. 2015. 10h23.

CARNETI, Karen. **Comércio eletrônico fatura R$ 43 bi e registra crescimento de 26% nas vendas em 2014** (30/01/2015). Disponível em: http://info.abril.com.br/ noticias/internet/2015/01/comercio-eletronico-fatura-r-43-bi-e-registra-crescimento-de -26-nas-vendas-em-2014.shtml. Acesso em: 04 set. 2015. 18h09.

CAVALCANTI, J. C. A Internet, o modelo nacional e uma proposta de enfoque para uma política de tarifas em sua operação no país. **Revista de Economia Política**. São Paulo, v. 17, n. 2, p. 130-143, abr./jun. 1997.

CERNEV, Adrian Kemmer. **Segurança na internet:** A percepção do usuário como fator de restrição ao crescimento do comércio eletrônico no Brasil. 2002. Dissertação de pós-graduação. Faculdade Getúlio Vargas.

CHAPPELLE, Joe. **Takedown** (2010) (filme). Disponível em: https://www.youtube.com/watch?v=0eubQrFUBwk . Acesso em 26 set. 2015. 15h45.

EY BRASIL. **Empresas brasileiras ampliam investimento em Segurança da Informação.** (03/02/2014). Disponível em: http://www.ey.com/BR/pt/Services/Release_Pesquisa_EY_Ataques_Ciberneticos . Acesso em: 16 set. 2015. 14h28.

FACHIN, ODÍLIA. **Fundamentos de metodologia.** 5ª ed. São Paulo: Saraiva. 2006.

FONTES, Edison Luiz Gonçalves. **Praticando a segurança da informação.** Rio de Janeiro: Brasport. 2008.

_____. **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva. 2006.

HUTTON, Laura. **Fraude online:** o aumento das ameaças num mundo em tempo real (12/08/2015). Disponível em: http://businessanalytics.pt/fraude-online-o-aumento-das-ameacas-no-mundo-e-em-tempo-real/. Acesso em: 13 out. 2015. 14h45.

ISO/IEC 27002. **Código de Prática para a Gestão de Segurança da Informação**. 2013. p. 4. Disponível em: http://pt.slideshare.net/Exin/o-que-mudou-com-a-reviso-da-norma-iso-270022005-para-a-verso-2013. Acesso em: 23 out. 2015.

LAKATOS, Eva Maria e MARCONI, Marina de Andrade. **Metodologia do trabalho científico.** 4ª ed. São Paulo: Atlas. 1992, p. 106.

LIMEIRA, T.M.V. **E-Marketing** - O marketing na internet com casos brasileiros. São Paulo: Saraiva. 2003.

MARCONI, Marina de Andrade e LAKATOS, Eva Maria. **Técnicas de pesquisa.** 7ª ed. São Paulo: Atlas, 2009. p. 6.

MITNICK, Kevin D. e SIMON, William L. **A arte de Invadir**: as verdadeiras histórias por trás das ações hackers, intrusos e criminosos eletrônicos. São Paulo: Pearson. 2006.

MUNIZ, Júlio Fidélis Silveira. **Estudo de práticas de segurança da informação com vistas à engenharia social em ambientes corporativos.** (2012). Monografia. Universidade São Francisco. Disponível em: http://lyceumonline.usf.edu.br/ salavirtual/documentos/2358.pdf. Acesso em 29 set. 2015. 10h16.

NAKAMURA, ANDRÉ MASSAMI. **Comércio eletrônico riscos nas compras pela internet.** (2011). Monografia. Faculdade de Tecnologia de São Paulo. Disponível em: http://www.fatecsp.br/dti/tcc/tcc0027.pdf. Acesso em: 13 out. 2015. 20h40.

NOGUEIRA, Sandro D'amato. **Crimes de informática**. São Paulo: BH, 2008. p.61.

PAOLIELLO, Claudio de Mello e FURTADO, Antonio Luz. **Sistemas de Informação para Comércio Eletrônico.** (2004) Pontifícia Universidade Católica do Rio de Janeiro. Disponível em: ftp://ftp.inf.puc-rio.br/pub/docs/techreports/04_27_ paoliello. pdf. Acesso em 13 out. 2015. 20h23

PEIXOTO, Mário César Pintaudi. **Engenharia social e segurança da informação na gestão corporativa.** Rio de Janeiro: Brasport, 2006. p. 4.

PEREIRA, Camila C.P. **Manual de Orientação de Monografia.** (2012) Instituto Federal de Educação, ciência e tecnologia. Disponível em: http://www.ifmg. edu.br/site_campi/s/images/matriz-cursos/tecnico/FORMATACAO_DO_TRABALHO_ tecnologos.pdf. Acesso em 17 out. 2015. 16h20.

ROSA, Fabrízio. **Crimes de Informática**. 2ª ed. Campinas/SP: BookSeller. 2006. p.62 e p. 65.

RUFINO, Nelson Murilo de O. **Segurança Nacional:** Técnicas e Ferramentas de Ataque e Defesa de redes de Computadores. São Paulo: Novatec. 2002. p.16.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Elsevier. 2003.

TURBAN, Efraim e RAINER, R. Kelly; POTTER, Richard E. **Administração de Tecnologia da Informação**. Rio de Janeiro: Campus. 2003.

VIEIRA, B.L.A.; NIQUE, W. M. Comércio eletrônico via internet: entendendo a internet como canal de compra. Artigo. In: **Encontro anual da Associação Nacional de Programas de Pós Graduação em Administração**, 23º. (1999). Foz do Iguaçu. Disponível em: http://www.anpad.org.br/diversos/trabalhos/ EnANPAD/ enanpad_ 1999/MKT/1999_MKT26.pdf. Acesso em 05 out. 2015. 13h10.

WONGTSCHOWSKI, ARTHUR. **Segurança em aplicações transacionais na internet:** o elo mais fraco. (2005). Dissertação de mestrado. Escola Politécnica da Universidade de São Paulo. Disponível em: http://www.teses.usp.br/teses/disponiveis/3/3141/tde-05092006-175654/publico/ArthurWongtschowski.pdf. Acesso em: 13 out. 2015. 20h30.

6 APÊNDICE