SEGURANÇA EM SISTEMAS DE INFORMAÇÃO: UMA ABORDAGEM SOBRE COMPRAS ONLINE

SAFETY INFORMATION SYSTEMS: AN APPROACH TO ONLINE SHOPPING

Ana Paula Moraes - anapaula-s2@hotmail.com

Douglas Francisco Ribeiro - douglas.ribeiro@ig.com.br

Faculdade de Tecnologia de Taquaritinga (FATEC) – SP – Brasil

RESUMO

O presente artigo tem como o objetivo principal abordar sobre a segurança em sistemas de informação em relação às compras online. Segundo o site Alternetiva.NET: "Com a crescente demanda das compras via internet o e-commerce tornou-se muito popular e conhecido. Com cada vez mais inovações aparecendo para esse segmento, fazer sua compra pela internet ficou cada vez mais simples, fácil, segura e divertida". Faz-se necessária, então, uma maior abordagem de todo o processo de compras, de forma a assegurar que pessoas mal-intencionadas não consigam invadir e utilizar as informações pessoais.

Palavras-chave: Segurança. Informação. Compras online.

ABSTRACT

The current article has as main goal to approach topics about security of information systems related to online shopping. According to the Alternative.NET site: "Due to the growing demand of online shopping, the e-commerce became known and very popular. With more and more innovations coming to this segment, your online purchase became simpler, easier, more secure and funnier". It is necessary to make a comprehensive approach of the entire purchasing process, to ensure that ill-intentioned people can not invade and utilize personal information.

Keywords: Security. Information. Online shopping.

COMO REFERENCIAR ESTE ARTIGO:

MORAES, Ana Paula; RIBEIRO, Douglas Francisco. Segurança em sistemas de informação: uma abordagem sobre compras online**. In: Revista Interface Tecnológica da FATEC Taquaritinga.** p. 63-72, jun. de 2016. ISSN *online* 2447-0864. Disponível em: <www.fatectq.edu.br/Interfacetecnologica>. Acesso em: dia mês e ano.

1 INTRODUÇÃO

Efetuar compras online é um habito que tem sido cada vez mais comum, principalmente para as pessoas que não tem tempo para ir até as lojas físicas. Basta alguns cliques em seu computador, no trabalho, a qualquer hora, para que o consumidor recebe seus produtos em casa.

O comercio eletrônico possui algumas vantagens em relação ao comercio convencional, tais como: mais opções de escolha, possibilitando a redução de tempo, custo de busca para clientes e fornecedores, melhor eficiência no atendimento ao cliente, com facilidade no pagamento, facilidade na comparação de preços, e sempre oferecendo mais opções de compras.

Segundo o site techtudo.com.br em sua publicação do dia 26/03/2013 diz que “No total, 61% dos participantes acreditam que as compras pela Internet são mais conscientes que em lojas físicas. “O resultado desta questão reforça que o consumidor gosta de tempo para analisar o produto, avaliar se realmente precisa dele, de modo a formar uma decisão de compra consciente. “A compra online proporciona isso”, analisa o diretor do Kuantokusta, Flávio Pagotto.

Apesar de encontrar produtos baratos e com mais comodidade na hora de efetuar uma compra online, é necessário que os consumidores prestem bem atenção em todos os sites de compras, muitos deles podem não ser confiáveis e acabam colocando o consumidor em risco podendo perder todo o dinheiro e correndo o risco de não receber o produto.

O desafio que as lojas estão enfrentando no Comércio Eletrônico é a preocupação dos consumidores em relação à segurança. Utilizar tecnologia de segurança torna-se cada vez mais importante, visando o aumento da confiabilidade.

2 SEGURANÇADA INFORMAÇÃO NAS COMPRAS ONLINE

A segurança da informação é um tema pertinente para que possa ser protegido contra todas as ameaças, minimizar qualquer tipo de risco e proteger tudo aquilo que é de valor.

Segundo Dias (2000, p.16), “Segurança é proteger as informações, sistemas, recursos e serviços contra erros, manipulação não autorizada e desastres visando à redução do impacto e diminuir a probabilidade de incidentes de segurança”.

Para os consumidores online, fica difícil saber em qual site é possível confiar para colocar seus dados pessoais e dados bancários, mas para os consumidores que já estão acostumados a efetuar compras via internet o risco de roubo de informações e fraudes também é grande.

Nada em segurança é totalmente seguro, mas assim como uma loja física precisa se preocupar com toda segurança com seus clientes, buscando sempre maneiras de assegurar as informações. No mundo virtual deve acontecer o mesmo, as lojas online sempre deverão manter um ambiente online seguro para as compras.

Quando estiver efetuando compras online é fundamental fazê-las em sites seguros e de confiança, procurando sempre o certificado de segurança do site que será representado por um "cadeado".

Cuidado ao inserir cartões de créditos na hora de finalizar a compra, observe sempre se a tela que pede as informações confidenciais, como as de pagamento, está com o cadeado ativado e se o endereço do site inicia com o HTTPS:// onde o "s" significa segurança.

Segundo o livro Guias de Segurança Online (2013, p.27), "Em qualquer atividade online, cuidado ao usar computadores ou redes de WI-FIpúblicas, pois não é difícil para outros usuários terem acesso ao que você está vendo ou comprando. Tenha a máxima cautela para não colocar suas informações salvando senhas em computadores que não são de sua propriedade.

Utilizar senhas fortes para um cadastro de compras online é essencial, para que as senhas sejam seguras o correto é:

- Criar senhas com letras, números, longas;
- Trocar a senha sempre a cada dois meses;
- Não crie senhas fáceis como datas comemorativas, número de documentos. Tenha senhas sempre diferentes.

Segundo o livro Cartilhas de Segurança para Internet (2012, p.51), "É por meio da suas contas e senhas que os sistemas conseguem saber quem você é e definir as ações que você pode realizar".

Sempre que finalizar uma compra online não deixe de efetuar o *logoff*, clicar sempre em sair, *logout* ou desconectar, e ao finalizar a compra sair para que outras pessoas não consigam ter acesso aos seus dados.

3 CERTIFICADO DIGITAL

Certificado Digital é um documento eletrônico gerado por uma autoridade certificadora confiável que contém informações sobre entidade (pessoa, empresa, site, computador entre outros), com esse tipo de documento você adquiriu segurança e conveniência em toda transação eletrônica, traz todas as facilidades de segurança para transações via internet. Com o certificado digital é possível atribuir: autenticidade, segurança, e validade jurídica.

Segundo o livro Benefícios e Aplicações da Certificação Digital (2012, p.5), "Certificação Digital é a tecnologia que adota mecanismos de segurança, através de algoritmos matemáticos, capazes de garantir autenticidade, confidencialidade, integridade e não-repúdio às informações eletrônicas".

Assinatura Digital nada mais é que a representação de um documento digital que passa a ser remetido para um terceiro com o uso da criptografia, que garante que esse documento não vai ser adulterado.

Certificado digital é mais utilizado em sites, blogs, lojas virtuais, sistemas de e-commerce, servidores web e e-mails, que tem por objetivo proteger as informações trafegadas da internet entre o servidor e o navegador web do cliente, que são através dos protocolos SSL[14] e TLS[15] que todos os dados são criptografados impedindo a falsificação de informações.

Todas as pessoas que acessam determinados sites que estejam com certificação digital se sentem com mais segurança, pois todas as informações são sigilosas e garante que o site não é falso, para sites de e-commerce é fundamental que tenha a certificação digital.

Os certificados digitais no Brasil são gerenciados pelo ICP Brasil (e-CPF,e-CNPJ, NF-e) ela é a autoridade que assegura a identidade digital das pessoas físicas e jurídicas, que garante a assinatura digital de documentos eletrônicos.

Os certificados digitaise-CPF e e-CNPJ são as identificações das pessoas físicas e jurídicas em sites, como,na receita federal que podem ser assinados digitalmente documento com validação jurídica e o certificado NF-e que foi desenvolvido para garantir arquivos de notas ficais, isso prova que uma determinada empresa que fez o envio da nota fiscal.

Os certificados digitais sãoarmazenados em um servidor, computador ou dispositivo criptográfico (Token).

[14] SSL: Sigla que significa: Secure Socket Layer.
[15] TLS: Sigla que significa: TransportLayer Security.

Token é um dispositivo físico que é distribuído por alguns bancos para garantir a segurança dos clientes quando é acessada a conta via internet, pelo caixa eletrônico ou telefone, écriada senhas de transações bancaria através da internet como a internet banking que está evoluindo a cada dia mais, com o uso do *token* diminui as chances de uma pessoa mal-intencionada querer invadir sua conta via internet.

4 PCI[16]

PCI é uma norma criada pelas operadoras de cartões de créditos como Visa e Mastercard, cujo objetivo é proteger a privacidade dos cartões de créditos e evitar fraudes.

PCI-DSS(PaymentCardIndustry – Data Security Standard)contribui para a proteção de dados dos clientes, a implementação de controles do PCI-DSS pode contribuir para que seus clientes possam usar seus cartões de créditos com confiança e segurança.

No Brasila venda via internet está evoluído muito, mas há muitas pessoas que se sentem inseguras ao efetuar uma compra online pelo cartão de crédito, por isso as empresas terão que estar sempre preparadas para proteger todas as informações pessoais do cliente como o número do cartão de credito por exemplo.

Existem requisitos de PCI-DSS para obter mais segurança como:

- Construir e manter uma rede segura.
- Proteger as informações dos portadores de cartões.
- Manter um programa de gerenciamento de vulnerabilidade.
- Implementar medidas de controle de acesso.
- Monitorar e testar as redes regularmente.
- Manter uma política de segurança da informação.
- Criptografia para proteção de dados do cartão.

5 SISTEMAS DE PAGAMENTOS

Os sistemas de pagamento online transformam telefones celulares em ferramentas seguras para compras, e é capaz de autorizar pagamento por uma rede de celular, utiliza diversas tecnologias para realizar transações como:

[16]PCI: sigla quesignifica:PaymentCardIndustry.

NFC[17] são pagamentos de aproximação de celular, é chamado de pagamentos contacless, por não precisar ter contato com a máquina de registro.

Segundo o site techtudo.com.br publicado dia 31/01/2012diz que "A NFC é uma tecnologia que permite a troca de informações entre dispositivos sem a necessidade de cabos ou fios (wireless), sendo necessária apenas uma aproximação física. A novidade teve origem no padrão RFID[18], mas se distanciou deste ao limitar o campo de atuação de frequências para uma distância de até 10 centímetros, objetivando tornar-se mais segura.

O Banco do Brasil começou a adotar os sistemas de pagamentos via smartphone, agora no Brasil essa tecnologia já chegou permitindo o pagamento de lojas físicas pela aproximação do celular em parceria com a Cielo que será usado um aplicativo Ourocard-e disponível apenas para Android.

Segundo o site tecmundo.com.br publicado dia 30/03/2015 diz que "Por meio de cartões virtuais atrelados ao cartão físico, os usuários poderão usar o aplicativo Ourocard-e – disponível apenas para Android – para fazer compras e pagar contas. O correntista pode ainda criar quantos cartões virtuais desejar, todos vinculados a um cartão de plástico, mas sem a cobrança de anuidade. "

As vantagens do NFC é a rapidez que são feitas as transações online e também não se corre o risco da clonagem, assim, quando é feita a transação é emitido uma chave de segurança no sistema eliminando a possibilidade da detecção do número do cartão de crédito.

Google Wallet também é um sistema de pagamento móvel via internet é armazenado as informações do cliente e a utilização do número de cartões de credito direto na conta da Google,em parceria com a MasterCard assim realizando pagamentos de compras online e permitindo enviar dinheiro via e-mail para qualquer conta.

O primeiro dispositivo a usar o Google Wallet foi o Nexus S de uma operadora chamada Sprint, que requer um chip NFC para poder fazer pagamentos via internet somente com a aproximação de um smartphone. O chip NFC é completamente seguro pois é desativado quando a tela do celular estiver apagada assim não correndo o risco de hackers querer invadir sua conta via internet.

O Google Wallet tem muita segurança, pois se a pessoa digitar a senha muitas vezes e der erro o aplicativo trava para a sua própria segurança e isso faz com que entre em contato com a Google.

[17] NFC: sigla que significa: Near Field Communication.
[18]RFID:sigla que significa: Radio FrequencyIDentification.

Segundo o site tecmundo.com.br publicou no dia 16/05/2013,diz que “De acordo com a página de descrição da nova ferramenta, todas as informações financeiras dos usuários vão estar, além de criptografadas, protegidas pelos “servidores de segurança” da Google. Ademais, se qualquer transação não autorizada for, de alguma forma, feita, um serviço de proteção promete cobrir em 100% o valor “perdido”.

A outros sistemas de pagamentos como a Apple Payque é um sistema de pagamento para IPhones, mas com disponibilidades por enquanto somente nos Estados Unidos desenvolvido pela Apple Inc.

O objetivo de usar a Apple Pay é a substituição da carteira por cartões de créditos sem fio para que o usuário tenha mais facilidade na hora de efetuar compras, quando realizar a compra basta aproximar o IPhones do terminal NFC e escolher a opção de pagamento, é essencial que tenha autenticação via Touch ID para poder finalizar a compra.

Touch ID é um sensor biométrico desenvolvido pela Apple Inc,queao invés da digitação desenhas, bastacolocar o dedo no botão home para ter a confirmação de sua identidade.

O código do cartão de credito para a segurança do usuário é armazenado de forma criptográfica em um chip para a proteção de todas as informações em caso de perda ou roubo para que pessoas mal-intencionadas não tenham acesso a suas informações.

Segundo o site tecnoblog.net publicado dia 09/10/2014 diz que “Em caso de perda ou roubo do iPhone, o usuário não precisará se preocupar com esta questão, portanto. De igual forma, a pessoa poderá anular transações indevidas via FindMy iPhone sem ter que cancelar o cartão”.

O objetivo de sistemas de pagamentos móveis é a utilização do celular ao invés de cartão de créditos ou débitos isso faz com que tenha mais segurança em relação as compras online via móbile.

6 CRIPTOGRAFIA

Criptografar todos os dados é muito importante, pois a criptografia transforma texto ou dados em cifras que não pode ser visualizado por ninguém, a não ser a pessoa que deveria realmente receber esses dados.

Existem dois tipos de criptografia, simétrica e assimétrica, ou também pode ser chamada de criptografia pública e privada.

Segundo Jerônimo C.Pellegrini, (2015, p.141)“A criptografia de chave privada permite proteger dados contra acesso não autorizado (um arquivo encriptado só será lido por quem conheça a chavepara desencripta-lo)”.

Segundo Paulo J. Almeida,(2012, p.18) “A Criptografia simétrica é a arte e ciência de enviar mensagens secretas. O emissor usa uma chave para cifrar a mensagem, esta é enviada até o receptor que usa outra chave para a decifrar”.

Existem dois tipos de protocolos criptográficos:

SSL[19]: é um protocolo de segurança que é criptografado entre um servidor web e um navegador para garantir que todos os dados sigilosos estejam seguros, quando optar por utilizar o protocolo SSL no seu servidor web você terá que responder algumas questões sobre seu site com, por exemplo, a URL e de sua empresa como, por exemplo, a razão social e o endereço, então o servidor criara duas chaves criptográficas que são: **chaves privadas e públicas**e então o servidor vai associar o certificado emitido pela chave privada e ira estabelecer um link criptografado entre a web site e o navegador.

TLS[20]:é um protocolo criptografado para que todas as informações estejam com segurança entre servidores e usuários, funciona em provedores de e-mails como o Gmail, por exemplo, que estará protegido desde o envio até o recebimento de mensagens. O objetivo do TLS é segurança da criptografia, eficiência relativa que tende a utilizar operações de criptografia utilizando um processo intensivo com as operações de chaves públicas, deve ser usada para estabelecer uma conexão segura.

HTTPS[21] é um protocolo de transferência de hipertexto seguro que inseri uma camada de proteção na transmissão dos dados entre o computador e o servidor, também é uma camada de segurança que utiliza os protocolos SSL e TLS, em sites que contem HTTPS são sites que contem seguranças criptografadas.

Para identificar se um determinado site está usando uma criptografia, é só identificar a barra de endereços onde vai ser possível identificar o HTTPS, muitos sites usam o protocolo HTTPS como, por exemplo: Facebook, Twitter, Google+, Google entre outros, HTTPS é baseado nas autoridades de certificação.

HTTP 2.0 é a segunda versão do protocolo de rede HTTP que é a troca ou transparecia de hipertexto, no HTTP 2.0 as requisições e respostas são paralelas e com velocidade ao carregar as páginas nos navegadores e vem com um desempenho melhor para os serviços da

[19] SSL: Sigla que significa: Secure Socket Layer**.**
[20] TLS: Sigla que significa: TransportLayer Security.
[21] HTTPS: Sigla que significa: HyperTextTransferProtocolSecure.

internet e com isso será baseado no protocolo SPDY que é um protocolo compatível ao HTTP que foi lançado pelo Google que funciona somente nos navegadores Chrome, Opera, Firefox e na plataforma AmazonSilk.

SPDY é um protocolo de rede que foi desenvolvido pela empresa de tecnologia Google e o órgão regulamentador do HTTP, implementou a versão 2.0 do HTTP que foi baseado nesse protocolo.

7 CONCLUSÃO

Hoje vivemos na era da informação onde o comercio eletrônico é o que mais cresce mundialmente, fazer compras via internet está sendo uma forma rápida, facilitando o dia-a-dia das pessoas em qualquer parte do mundo.

Os consumidores que utilizam sites para realizar suas compras além da comodidade, têm também na maioria das vezes, preços mais acessíveis, produtos mais variados e diferenciados dos que se tem em lojas físicas. O grande crescimento das compras online mudou o habito dos consumidores que estão deixando de lado as lojas físicas e optando pelas lojas virtuais, por motivo de realizar compras via internet sem sair de casa.

Quando falamos sobre compras online a vários fatores a serem abordados como a segurança da informação, com o crescimento das compras online,também aumentou as ameaças virtuais, fazendo com que os consumidores estejam atentos às vulnerabilidades, por isso,sempre será necessário a verificação de segurança como: verificar o cadeado na barra de endereços, extensões do site, pesquisando o nome do site, se a uma conexão segura como “HTTPS”, e procurando sempre a certificação do site.

Não existe segurança total para transações seja ela virtual ou não, pois pessoas mal-intencionadas se aproveitam para tentar levar vantagem, mas a muitas ferramentas desenvolvidas e aperfeiçoadas para garantir e assegurar o máximo de segurança possível como os certificados digitais, PCI, sistemas de pagamentos online através de celulares e a criptografia.

REFERÊNCIAS

ALTERNATIVE. NET, 2015. Disponível em: <http://alternative.net.br/e-commerce/>. Acesso em: 07 maio 2015.

BENEFÍCIOS E APLICAÇÕES DA CERTIFICAÇÃO DIGITAL, 2012, p.5, Disponível em: <http://www.fenacon.org.br/usuarios/arquivos%5Cpublicacoes%5CBenef%C3%ADcios_Aplica%C3%A7%C3%B5es_CD.pdf. > Acesso em: 25 março 2015

CARTILHAS DE SEGURANÇA PARA INTERNET, 2012, p.51. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 24 março 2015.

DIAS, 2000, p.16, SEGURANÇA DA INFORMAÇÃO. Preservação das Informações Estratégicas com Foco em sua Segurança". Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/silvana_crispim.pdf. > Acesso em 13 jan. 2015

DIAS, 2000, p.56, GESTÃO DE SEGURANÇA DA INFORMAÇÃO. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. > Acesso em: 13 jan. 2015

GUIAS DE SEGURANÇA ONLINE, 2013, p.27, Disponível em: <http://www.avgbrasil.com.br/docs/AVG_EBOOK.pdf > . Acesso em: 25 mar 2015.

PELLEGRINI, Jerônimo C., 2015, p.141. INTRODUÇÃO A CRIPTOGRAFIA E SEUS FUNDAMENTOS. Disponível em: <http://aleph0.info/cursos/ic/notas/cripto.pdf.>. Acesso em 13 jan. 2015

ALMEIDA, Paulo J., 2012, p.18. CRIPTOGRAFIA E SEGURANÇA. Disponível em: <http://arquivoescolar.org/bitstream/arquivo-e/195/1/CS11_12.pdf. >. Acesso em: 13 jan.2015.

TECHTUDO, 2013, Disponível em: <http://www.techtudo.com.br/artigos/noticia/2013/03/compra-online-e-mais-consciente-que-em-lojas-fisicas-revela-estudo.html. > Acesso em: 24 março 2015.

TECHTUDO, 2012, Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/01/o-que-e-nfc.html. > Acesso em 24 março 2015.

TECMUNDO, 2013, Disponível em: <http://www.tecmundo.com.br/gmail/397a82-google-wallet-novo-servico-permite-pagamento-e-envio-de-dinheiro-via-gmail.htm>. Acesso em: 24 março 2015.

TECNOBLOG, 2014, Disponível em: <https://tecnoblog.net/165116/apple-pay-nfc-iphone>/, Acesso em: 24 março 2015.