Etec Adolpho Berezin
Mongaguá/SP

Bárbara Rodrigues de Oliveira

Henry Mitsuo Kasai

Matheus Gois Rocha

Rafaela Fonseca Bortkevitch

Raquel Nazaré Belfort Costa

MEDIDAS DE SEGURANÇA PARA PROFISSIONAIS NOS COMÉRCIOS ELETRÔNICOS

Orientadora Prof. Graciete Henriques dos Santos

Mongaguá

06/2021

Bárbara Rodrigues de Oliveira

Henry Mitsuo Kasai

Matheus Gois Rocha

Rafaela Fonseca Bortkevitch

Raquel Nazaré Belfort Costa

MEDIDAS DE SEGURANÇA PARA PROFISSIONAIS NOS COMÉRCIOS ELETRÔNICOS

Trabalho de Conclusão de Curso apresentado à Escola Técnica Estadual Adolpho Berezin, como parte dos requisitos obrigatórios para a obtenção do título de Técnico em Informática.
Profa. Orientadora: Graciete Henriques dos Santos

Mongaguá

06/2021

Dedicamos este trabalho a professora Graciete Henriques e a todos os professores, que nos deram todo suporte ao longo do curso, sempre com muito empenho e compreensão.

AGRADECIMENTOS

Agradecemos, primeiramente, a Deus por nos proporcionar saúde nesses tempos difíceis. Aos nossos familiares, amigos e professores pelo incentivo, e a todos os microempreendedores e espectadores do nosso trabalho.

"Feliz aquele que transfere o que sabe e aprende o que ensina."

(Cora Coralina)

RESUMO

Tendo em vista o crescimento em demasia da procura e interesse por parte de microempreendedores em arquitetar seu próprio negócio de maneira *online* após a pandemia do Covid-19 e, em suma, por consequência do aumento de compras e vendas feitas pela internet, pesquisa-se sobre Medidas de Segurança para Profissionais nos Comércios Eletrônicos, a fim de conscientizar aqueles que buscam a autonomia para coordenar as próprias vendas, de maneira segura e eficiente no meio digital. Para tanto, é necessário o conhecimento no que se diz respeito à segurança da informação, analisar vulnerabilidades e, consequentemente, estar ciente de como evitá-las. Realiza-se, então, uma pesquisa de campo descritiva e quantitativa e diante disso, verifica-se que os conhecimentos neste quesito são limitados para a maioria dessas pessoas, o que impõe a importância do uso do produto final (*checklist*) na realização de vendas satisfatórias no meio *online*.

PALAVRAS-CHAVES: Segurança. E-commerce. Internet. Microempreendedor.

ABSTRACT

In view of the excessive growth in demand and interest by microentrepreneurs in designing their own online businesses after the Covid-19 pandemic and, in short, as a result of the increase in purchases and sales made over the internet, a research about Safety Measures for Professionals in Eletronic Commerce was made, in order to raise awareness of those who seek autonomy to coordinate their own sales, safely and efficiently in the digital environment. Therefore, it is necessary to have knowledge regarding information security, analyze vulnerabilities, and consequently be aware of how to avoid them. Both descriptive and quantitative field research were made, and in view of this, it was verified that the knowledge in this regard is limited for most of these people, which imposes the importance of using the final product (checklist) in making sales satisfactory online.

Keywords: Safety. E-commerce. Internet. Microentrepreneur.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE PÁGINAS DO MANUAL

SUMÁRIO

INTRODUÇÃO

Observando o universo da pandemia de Covid-19 ocorrida no ano de 2020, é notório que parte dos microempreendedores faliram por não possuírem alternativas cabíveis para continuar com as suas vendas, nas quais, até então dependiam totalmente da realização presencial. Visando superar tal situação e se adaptar ao “novo normal”, muitos deles optaram pelas vendas remotas que, por sua vez, eram consideradas como algo completamente novo e, até mesmo, suspeito para essas pessoas.

As vendas *online* são consideradas como práticas seguras na pandemia, afinal, evitam o contato direto com outros indivíduos, o que diminui a disseminação do vírus e permite que o trabalho dos empresários não se estagne. Entretanto, o comércio eletrônico pode conter diversificados problemas de segurança, algo que é totalmente inviável quando se trata de vendas, visto que dados pessoais são constantemente inseridos, expondo assim tanto os vendedores como os clientes.

Neste sentido, a pesquisa de campo é criada no intuito de trazer as principais informações sobre a segurança digital, visando evitar futuros problemas relacionados a desinformação deste assunto. No final do desenvolvimento, é disponibilizado ao leitor uma *checklist* que o auxiliará na abertura do comércio eletrônico, trazendo mais assertividade as atividades do mesmo.

No desenvolver do trabalho verificam-se os conceitos relacionados à segurança da informação, seguido dos tipos mais comuns de ataques e das suas possíveis soluções ou prevenções. Por fim, é demonstrado a importância do conhecimento obtido pelo trabalho de conclusão de curso e é disponibilizado, através da *checklist*, o auxílio aos microempreendedores que optaram por ter um negócio virtual.

O estudo se justifica quando é relacionado ao contexto atual e a situação dos microempreendedores. Além disso, levando em conta o avanço e a modernização da tecnologia, tais conhecimentos tornam-se importantes para todos aqueles que se preocupam com a privacidade e segurança nos meios virtuais. Em suma, o estudo realizado beneficia todos os tipos de leitores.

1. PROBLEMA / NICHO DE MERCADO

1.1 Introdução / público alvo

Com a pandemia do Covid-19, muitos indivíduos que antes não se arriscavam nas compras virtuais, começaram a fazê-las por conta da necessidade do momento, sendo assim, os comércios que não estavam aptos a essa nova realidade, precisaram se adaptar a tais mudanças na economia, como é exemplificado pelo CEO da ONCLICK Marcel Farto,

> Um exemplo é a marca de calçados femininos, Arezzo. Nos últimos meses, com as lojas fechadas, o e-commerce tornou-se o principal canal de vendas. Os vendedores, antes presenciais, ganharam um acesso ao estoque da loja virtual e começaram a vender via plataforma. Antes eram apenas 100 consultores digitais, hoje são 5 mil e um aumento de 10% a mais nas vendas do que na Black Friday, antigo recorde (2020).

Na corrida pela continuação de suas vendas, empreendedores de todas as áreas começaram a investir nos meios virtuais (FARTO, 2020). As questões de segurança da informação, apesar de ser primordial em vendas online, podem ser deixadas de lado por falta de conhecimento. Tais atos geram muitos problemas, afinal, em compras virtuais desprotegidas, dados importantes ficam vulneráveis. Isso causa abalos financeiros, além de deixar a empresa em questão malquista por aqueles que tiveram experiências ruins.

A explanação dessas informações elucida tal problema, se tornando algo extremamente útil, afinal, com o acesso as orientações de segurança e alternativas viáveis relacionadas, infortúnios como este podem ser cessados.

Tratando-se de uma pesquisa científica voltada para a segurança das vendas nos meios virtuais, sugere-se que o público alvo em questão seja os microempreendedores possuintes de comércios eletrônicos, visando trazer dicas e possíveis soluções pertinentes a essa área de problemas.

1.1 Problema / lacuna

Por meio deste estudo, serão abordados os problemas da incredulidade dos microempreendedores relacionados as criveis ameaças de segurança nos seus comércios eletrônicos (ataques por *phishing*, *pharming*, DDoS, *cross-site scripting*, roubo de dados e fraude amigável), vulnerabilidades, métodos de proteção, consequências da falta de segurança, privacidade e ética virtual.

1.2 Objetivo

Diante dos prováveis problemas que um microempreendedor pode enfrentar ao tentar preservar a segurança de seu comércio eletrônico, será elaborado uma pesquisa descritiva abordando processos e mecanismos de defesa que um comércio eletrônico deve apresentar, dentre os quais podem ser destacados a necessidade de implementar o processo de autenticação, criptografia e *Firewall* para tornar segura cada transação eletrônica.

Contudo, a criação de um comércio com uma criptografia de alto nível não é fácil de se atingir, adversidade que pode ser solucionada através da terceirização da segurança do comércio. Consequentemente, serão listados selos e certificados digitais baseados em padrões internacionais (ISO) de técnicas de criptografia.

Ao final do projeto descritivo, um modelo de *checklist* será confeccionado a partir das informações contidas na pesquisa, auxiliando o microempreendedor que busca se aventurar no meio eletrônico. A mesma conterá os requisitos essenciais para um comércio eletrônico mais seguro, sendo assim, os microempreendedores leigos na área de TI conseguirão ter acesso a essas informações.

2. EMPRESA

2.1 Missão

Buscamos proporcionar autonomia, confiança e segurança aos microempreendedores ingressantes no mercado digital, indicando os possíveis erros de segurança e auxiliando na tomada de decisão.

2.2 Visão

Desejamos a conscientização de todos os microempresários do mundo, fazendo com que conheçam e saibam diferenciar um site seguro de um site que possua segundas intenções.

2.3 Valores

- Honestidade e transparência com o microempreendedor;
- Enaltecimento da informação;
- Valorização da ética digital;
- Qualidade da segurança;
- Responsabilidade.

2.4. Logo

Figura 1 - Logo: Equipe BOTS

2.5 Slogan

Compreendendo os erros para elevar os sonhos!

3. FUNDAMENTAÇÃO TEÓRICA

3.1 Segurança da informação

Informação é um conjunto de dados e conhecimentos relacionados a um determinado indivíduo e/ou organização.

No contexto digital, é possível ter acesso a diversos tipos de informações, o que desfia a necessidade de uma segurança sempre assertiva e livre de vulnerabilidades. Para alcançar tal ideal, o conhecimento sobre os riscos é indispensável, afinal, saber sobre o assunto torna a defesa cada vez mais satisfatória. Portanto, a segurança da informação vem como uma aliada para todos os microempresários que visam manter o nome do seu negócio em alta, pois resolvendo problemas como estes, que são riscos para ambas as partes (cliente e comerciante), fazem com que o objetivo principal, a venda, ocorra de maneira eficiente e sem preocupações posteriores.

3.1.1 Tríade CIA

A Confidencialidade, Integridade e Disponibilidade (*Confidentiality, Integrity and Availability* – CIA), diz respeito as propriedades básicas previstas na segurança da informação de qualquer software. Levar tais parâmetros em consideração no momento da construção de um comércio eletrônico, é o mínimo esperável.

Confidencialidade

De acordo com a NBS (Nomenclatura Brasileira de Serviços), a confidencialidade se trata das informações pessoais que devem ser manuseadas, apenas, por entidades confiáveis.

Para se denominar um certo dado como confidencial, o mesmo não deverá ser acessado por indivíduos aleatórios ou comprometido por terceiros. Portanto, possuir confidencialidade é abonar as especificidades dos dados.

Integridade

De acordo com Brook (2010, *apud* ABREU, 2011), a integridade é à certificação da veracidade dos dados, sendo assim, estes não terão qualquer tipo de mudança ou quebra por pessoas não autorizadas.

> Existem basicamente dois pontos durante o processo de transmissão no qual a integridade pode ser comprometida: durante o

> carregamento de dados e/ou durante o armazenamento ou coleta do banco de dados.

Disponibilidade

Refere-se, justamente, a disponibilidade das informações quando solicitadas. Para ser alcançada, deve ser realizada em meios seguros e funcionais, possuindo alternativas cabíveis para quaisquer imprevistos de hardware ou software. Sendo assim, trata-se de um grande desafio, visto que o bom funcionamento e o tempo de espera curto para o usuário torna-se responsabilidade inteiriça da empresa em questão (BROOK, 2010 *apud* ABREU, 2011).

3.2 Segurança na Internet

Para iniciar os estudos sobre a segurança na internet, é indispensável o entendimento de como a internet funciona. Assim sendo, a afirmação de que a internet não é um canal seguro para o envio dados, pode ser descrita como a base para a busca de qualquer estudo envolvendo a segurança no meio digital.

3.2.1 Wide Area Networks (WANs)

Uma troca de dados pode ser realizada através de sinais realizados entre dois ou mais dispositivos por um meio de transmissão, o qual pode ser físico como cabos de par trançado, coaxial, fibra óptica, ou não, como qualquer espaço livre. Os meios de transmissão de dados realizados por elementos físicos são caracterizados por sistemas de comunicação local (LANs). Contudo, quando se trata da internet, as redes de comunicação para grandes áreas (WANs) que são as verdadeiras necessidades de entendimento (RHEE, 2003).

Ao contrário de redes LAN, que são limitadas a uma pequena área geográfica dependente de aparelhos físicos, as redes WAN possibilitam a transmissão de dados por uma vasta área, as quais podem cobrir desde países como o mundo inteiro (RHEE, 2003).

3.2.2 Protocolos e padrões

Uma vez que está compreendido o quê são redes LAN e WAN, é fundamental entender a diferença entre os termos protocolos e padrões, de modo que os conhecimentos sobre como ocorre a troca de dados entre dois sistemas possa ser assimilado de forma dedutiva (FOROUZAN e FEGAN, 2009).

Para que ocorra a comunicação entre dois sistemas é necessário haver um conjunto de regras que regem a forma que tal informação será comunicada. Dentre os principais elementos essenciais em protocolos são: sintaxe, semântica e sincronismo.

3.2.2.1 Sintaxe

A sintaxe pode ser caracterizada como a estrutura dos dados, tendo que o primeiro byte pode significar o endereço de remetente, em seguida o destinatário, e o restante dos bytes a mensagem (FOROUZAN e FEGAN, 2009).

3.2.2.2 Semântica

Já a semântica pode ser classificada como um padrão a ser seguido, uma vez que é necessário definir se determinado endereço é do remetente ou do destinatário (FOROUZAN e FEGAN, 2009).

3.2.2.3 Sincronismo

Temporização ou sincronismo refere-se à quando e a velocidade que os dados serão enviados, tendo vista a necessidade de se atentar que um remetente enviando dados a uma velocidade maior que seu recebimento ao receptor podendo haver a perda ou danificação da mensagem (FOROUZAN e FEGAN, 2009).

Os padrões, todavia, são essenciais para estabelecer um modelo a ser seguido em um mercado ou rede mundial. De acordo com Behrouz Forouzan e Sophia Fegan (2009), autores do livro “Protocolo TCP/IP - 3.ed.”,

> eles fornecem diretrizes para fabricantes, fornecedores, órgãos governamentais e outros provedores de serviços, para garantir o tipo de operação conjunta necessário no mercado atual e nas comunicações internacionais.

Existem duas categorias para diferenciar os padrões, são elas: “por fato” e “de direito”, ou seja, os padrões “por fato” são aqueles que não foram aprovados por um organismo constituído, mas adotados pelo uso popular. Logo, os padrões “de direito” são legalmente aprovados por uma legislação (FOROUZAN e FEGAN, 2009).

3.2.3 Protocolos TCP/IP

De acordo com os conhecimentos concebidos anteriormente, é possível apresentar o principal conjunto de protocolos da internet, o TCP/IP, os quais foram desenvolvimentos e utilizados de forma prática antes da criação do modelo OSI, o qual apesar de envolver uma série de estudos especializados, pode ser caracterizado meramente teórico, enquanto o conjunto de protocolos como funcional (FOROUZAN e FEGAN, 2009).

Constituído de cinco camadas, as quais são: física, enlace de dados, rede, transporte e aplicativo, tal conjunto de protocolos, diferente do modelo OSI, é relativamente independente, tendo que há uma hierarquia dos protocolos superiores serem suportados por protocolos inferiores, variando de acordo com as necessidades do sistema tratado. Sua conexão pode ser estabelecida por uma rede LAN e WAN (FOROUZAN e FEGAN, 2009).

3.2.3.1 Camada física e de enlace de dados

Os protocolos da camada física e enlace de dados não apresentam qualquer especificidade, sendo compostos de protocolos padrão (FOROUZAN e FEGAN, 2009).

3.2.3.2 Camada de rede

Diferente das primeiras duas camadas, a camada de rede apresenta o IP (*Internet Protocol*), o qual tem como base quatro protocolos: ARP, RARP, ICMP e IGMP (FOROUZAN e FEGAN, 2009).

3.2.3.3 Camada de transporte

Os protocolos envolvendo a camada de transporte apresentam a funcionalidade de enviar uma mensagem em execução para outro. Os protocolos são: UDP, TCP e SCTP (FOROUZAN e FEGAN, 2009).

3.2.3.4 Camada de aplicação

Possivelmente a principal camada para o usuário, a camada de aplicação é a responsável por estabelecer a comunicação entre os protocolos de transporte e os programas que serão utilizados. Os principais protocolos dessa camada são: HTTP, FTP, DNS, DHCP, SSH e entre outros (FOROUZAN e FEGAN, 2009).

3.3 Segurança de Rede de comunicação

Como consequência da evolução da tecnologia, o aumento das vulnerabilidades existentes relacionadas a quebra de segurança de determinado sistema aumentou (NAKAMURA e GEUS, 2007). Contudo, a melhoria de segurança de uma rede pode não parecer uma prioridade para muitas empresas principalmente no meio empresarial, onde ocorre uma competitividade entre outras empresas do ramo, portanto, é essencial abordar como o desenvolvimento da tecnologia abrangeu nas formas de invadir uma rede de segurança.

Assim como foi descrito anteriormente, o conjunto de protocolos TCP/IP foram introduzidos com a internet, proporcionando uma conexão global de envio de dados, por outro lado, embora sendo um grande marco de desenvolvimento para a humanidade, também existem certos problemas criados a partir de tal evolução. O envio mal-intencionado de malwares ou qualquer ação para o malefício de alguém gera uma vulnerabilidade sobretudo em redes com fins lucrativos, onde há a troca financeira que pode ser burlada (NAKAMURA e GEUS, 2007).

Diante de tamanha vulnerabilidade, será abordado no capítulo atual técnicas e tecnologias capazes de fornecer uma defesa contra tentativas de invasão em uma rede de comunicação.

3.3.1 Política de segurança

A primeira técnica de segurança para ser utilizada como base para as tecnologias posteriores é a política da empresa em relação ao assunto, ainda que sendo algo facilmente criado teoricamente, não é o mesmo que sua incorporação na prática.

Um exemplo para embasamento de uma estrutura de política de segurança é composto por um constante monitoramento das redes; o entendimento geral de cada integrante da empresa sobre a importância da segurança, tendo que a preservem; um conteúdo de política fácil de entender e acessível; uma estratégia de produção de forma que os implementos de segurança não interfiram diretamente no trabalho de cada um; uma instalação tecnológica flexível com múltiplas alternativas de proteção (NAKAMURA e GEUS, 2007).

3.3.2 Firewall

Diante de uma invasão virtual, a primeira linha de defesa é o *firewall*, isto é, um sistema capaz de reforçar o controle de acessos entre duas redes, tendo que a restrição é proporcional a segurança.

De acordo com Brent Chapman em seu livro *“Building Internet Firewalls”*, de 1995, um firewall é composto por diversos componentes. Os quatro primeiros componentes necessários para o funcionamento firewall são: filtros, proxies, bastion hosts e zonas desmilitarizadas, e os três outros restantes recomendados são: NAT (Network Address Translation), Rede privada virtual ou VPN (*Virtual Private Network*) e autenticação, sendo todas necessárias para a segurança de uma rede (NAKAMURA e GEUS, 2007).

3.3.3 Sistema de detecção de intrusão

O sistema de detecção de intrusão ou IDS (Intrusion Detections System), é caracterizado como uma tecnologia capacitada de detectar uma invasão no sistema. No entanto, a detecção pode ocorrer de diversas formas baseadas com a localização de arquivos (NAKAMURA e GEUS, 2007).

3.3.3.1 Host-Based Intrusion Detection System (HIDS)

A detecção no contexto tem como base o host, ou seja, de acordo com arquivos de logs ou de agentes de auditoria, portanto, o HIDS monitora alterações no sistema, como privilégios de usuários, processos do sistema, uso da CPU, programa executados e entre outras alterações (NAKAMURA e GEUS, 2007).

3.3.3.2 Network-Based Intrusion Detection System (NIDS)

A base da NIDS é o monitoramento do tráfego de segmento da rede, atuando através de uma comparação e análise dos pacotes com padrões e assinaturas já conhecidos (NAKAMURA e GEUS, 2007).

3.3.3.3 Knowledge-Based Intrusion Detection

A abordagem baseada no conhecimento é a mais utilizada pelas IDS, tendo o funcionamento semelhante ao de um antivírus, no qual as detecções são feitas

baseadas em uma base de dados de ataques conhecidos (NAKAMURA e GEUS, 2007).

3.3.4 Criptografia

A criptografia é um ramo da segurança baseado na ocultação da mensagem, portanto havendo possibilidades infinitas no meio, tais possibilidades serão abordadas ao decorrer do trabalho.

3.4 Segurança de Aplicação

Para se pensar em segurança, primeiro é preciso definir qual é sua significância para os clientes. Tendo em vista não apenas os computadores, a segurança de aplicações é cada vez mais investigada com o passar do tempo, conforme notamos a crescente popularização do uso de dispositivos como aparelhos celulares. Hoje, a utilização de softwares é tida como uma importante ferramenta das empresas, facilitando e otimizando os processos de trabalho antes realizados tradicionalmente. Com a gradativa importância deste aspecto, é crucial que a segurança seja equivalentemente confiável, uma vez que ameaças como o vazamento de dados podem comprometer o estado financeiro de uma empresa, além de prejudicar diretamente sua credibilidade no mercado. Fabricantes de softwares frequentemente demonstram o interesse quanto a manter seus programas seguros, uma vez que atualizações podem permanecer sendo lançadas de tempos em tempos, bem como as aplicações em código aberto podem ter o apoio de diversos desenvolvedores, sugerindo melhorias e correções vistas como imprescindíveis.

3.4.1 Pagamento

Uma vez dentro do *e-commerce*, quando é realizado uma compra online, há a indispensabilidade de analisar se o site é seguro ou não. A confiança se torna um elemento vital para a construção, manutenção e ampliação de relacionamentos duradouros (EISINGERICH e BELL, 2007).

O pagamento dos produtos adquiridos diante destas aplicações pode ser feito de diferentes maneiras, sendo elas instantâneas e teoricamente oferecedoras de uma segurança confiável que lhe retorne o suporte necessário. Os principais métodos de pagamento existentes atualmente são os boletos bancários, transferências *online*,

gateways de pagamento e intermediários de pagamento. De acordo com Larissa Lotufo (2017):

> Os boletos são títulos de cobrança amplamente utilizados como meio de pagamento dentro do *e-commerce*. Neste documento há as informações referentes aos dados do recebedor – como banco utilizado, titular da cobrança, data de vencimento do título, valor a ser quitado etc – que usualmente são passadas através de um código de barras; A transferência *online* permite ao usuário pagar de maneira imediata pelo serviço que busca em sua loja, isso porque nesse método há a confirmação direta com a conta bancária do comprador; Os *gateways* de pagamento são sistemas de integração que realizam a transmissão de informações acerca dos pagamentos eletrônicos junto a bancos ou operadoras de cartão de crédito; Os intermediários de pagamento são empresas que facilitam o processo de pagamento para o e-commerce, oferecendo um suporte amplo desde a disponibilização de meios até o oferecimento de serviços antifraude.

É importante ressaltar que, para cada método de pagamento, há vantagens e desvantagens. Contudo, para que todos sejam colocados em prática efetivamente, é primordial que não haja possíveis ameaças para a empresa e, em adição, para o cliente que as utiliza.

3.4.2 Privacidade

A privacidade é algo de suma importância para os usuários, pois muitos, sem perceber, acabam permitindo o uso de *cookies* para sites e aplicativos. Os chamados "*cookies* de navegador" são cada vez mais utilizados como opção de ferramenta de coleta de informações para monitorar e compreender o comportamento dos internautas (LINS, 2000). Logo, isso cede aos aplicativos e sites a troca de dados dos seus usuários. Quando um indivíduo se depara com outros aplicativos oferecendo propagandas que estão no seu histórico de pesquisa, provavelmente o site acessado utiliza *cookies*. Segundo Bernardo Lins (2000):

> Nos últimos dez anos, o assunto da privacidade ganhou novas facetas, em virtude da disseminação das tecnologias de tratamento da informação. São essencialmente três os fenômenos que vêm contribuindo para uma maior preocupação com o tema: primeiramente, a estruturação de bases de dados, que abriu a possibilidade de se cruzar informações com grande facilidade, construindo perfis detalhados de praticamente qualquer pessoa, a um custo baixo, até

> mesmo sem a ciência do interessado; em segundo lugar, a disseminação da informática, que culminou com a ampla utilização da Internet, estimulando praticamente a todos a manterem em forma digital as suas informações, facilitando a sua coleta; e, finalmente, a padronização de equipamentos e sistemas, o que facilitou a aquisição de informações mantidas por usuários de informática, inclusive sem o seu conhecimento.

3.5 Vulnerabilidades

A vulnerabilidade no ramo computacional está diretamente vinculada às fraquezas de um determinado software, que acabam por permitir ataques, dos mais diversos métodos, os quais reduzem a garantia da informação.

Diante de toda a tecnologia disponibilizada nos dias atuais torna-se inevitável que ocorram falhas até mesmo nas mais elaboradas seguranças computacionais existentes.

3.5.1 Métodos de avaliação para redes e sistemas computacionais

Existem diversos métodos para avaliar um sistema ou rede de sistemas de informação, um dos mais conhecidos baseia-se na utilização de profissionais que atuam no ramo da segurança computacional, o método "*penetration testing*", que em sua forma abreviada é conhecido por "*pentest*".

Pentest trata-se de um método de avaliar e descobrir vulnerabilidades em uma rede ou sistema operacional (GIAVAROTO e SANTOS, 2013 *apud* FONSECA DA SILVA e PEREIRA, 2019).

3.5.2 Termos recorrentes na segurança computacional

Dentre os termos mais discutidos pela segurança computacional estão "*Hackers*" e "*Crackers*", atualmente, devido a uma maior divulgação dessas práticas, existe uma grande confusão entre ambos os termos.

Pode-se definir *Hackers* como indivíduos dedicados, que utilizam os seus conhecimentos com o objetivo de se beneficiarem. Diferentemente do *Hacker*, os *Crackers* têm o objetivo de violar das mais diversas formas softwares e redes de variados tipos.

3.5.3 Hackers e a vulnerabilidade computacional

Segundo Wilhelsm, o grupo tratado coletivamento como *Hackers*, é normalmente subdividido em duas categorias (2009, *apud* FONSECA DA SILVA e PEREIRA, 2019):

- *Black Hat Hackers*: pessoas que usam seus conhecimentos para ter acesso não autorizado a sistemas.
- *White Hat Hackers*: pessoas que fazem seu trabalho em um aspecto profissional, com tempo de trabalho e custos pré-definidos em contratos formais, visando à melhoria de segurança ou procurando vulnerabilidades no sistema.
- *Gray Hat Hackers*: pessoas que praticam atos legais como os *Black Hat Hackers* e também praticam atos ilegais, assim como os *White Hat Hackers* (FERREIRA, 2012 *apud* FONSECA DA SILVA e PEREIRA, 2019).

3.5.4 Falhas na segurança computacional

Devido ao constante avança tecnológico, o ser humano foi capaz de criar “códigos”, capazes de explorar as mais diversas falhas na segurança computacional, temos como exemplo o *exploits* e o *shellcode*.

- *Exploits*: Sequência de comandos ou dados com objetivo de aproveitar-se de uma vulnerabilidade.
- *Shellcode*: Comandos executados com o objetivo de explorar vulnerabilidades.

Para Anwar, existem diversos padrões de *shellcode*, acessíveis para os mais diversos tipos de sistemas e arquiteturas (2009, *apud* FONSECA DA SILVA e PEREIRA, 2019).

Outra maneira de explorar as vulnerabilidades é utilizando a Engenharia Social na empresa, segundo Flora (2010, *apud* FONSECA DA SILVA e PEREIRA, 2019) a mesma tem por objetivo obter acesso a informações, sendo obtida por meio da enganação ou explorando a confiança das pessoas.

3.5.5 Phishing e Pharming

Atualmente, alguns dos ataques mais comuns que podem ser observados em comércios eletrônicos são os de *phishing* e *pharming* (LATZE, 2007).

Em um ataque de *phishing*, ocorre a utilização de métodos de engenharia social para roubar dados, um exemplo, é fazer com que o usuário insira informações pessoais em um *site* falso (LATZE, 2007).

Já os ataques de *pharming*, podem ser descritos como mais sofisticados em relação ao anterior, uma vez que se utiliza da manipulação do DNS dos arquivos *host* do usuário para redirecioná-lo a um servidor malicioso, podendo ser exemplificado como uma imitação do site original (LATZE, 2007).

De acordo com Carolin Latze (2007):

> There are several common solutions to overcome these problems. In general, they can be classified into “Bigger Warning Messages”, “Better Passwords”, “SSL Extensions” and “Trusted Devices”.

A primeira solução destacada, mensagens de aviso maiores, são as soluções que propõem a utilização dos chamados áreas confiáveis no navegador para exibir certificados (HERZBERG & GBARA apud LATZE, 2007), ou que envolvam o monitoramento dos *websites* visando detectar *spoofing* sites, ou seja, sites falsos ou falsificados que buscam enganar o usuário (CHOU, LEDESMA, TERAGUCHI, BONEH & MITCHELL apud LATZE, 2007).

Já a segunda, como pode ser entendido pelo nome, melhores senhas, são as que propõem a geração de senhas novas para cada conta (ROSS, JACKSON, MIYAKE, BONEH e MITCHELL apud LATZE, 2007).

A extensão do SSL (*Secure Sockets Layer*), antecessor do TSL (*Transport Layer Security*), visa juntar a autenticação SSL com a autenticação do usuário, uma forma de dificultar ataques de *pharming* (OPPLIGER, HAUSER, BASIN, RODENHAEUSER & KAISER apud LATZE, 2007).

O último conjunto de soluções, envolve a utilização de dispositivos confiáveis, sendo proposto o uso de "*secure wallet*", o que pode ser traduzido para carteira segura, para armazenar credenciais e decidir se um site é autêntico. Contudo, é necessário ressaltar, que tal solução é vulnerável na primeira conexão (GAJEK, SADEGHI, STÜBLE & WINANDY apud LATZE, 2007).

3.5.6 Ataque DDoS

O ataque DDoS, de acordo com o raciocínio de Noureldien (2002, apud RAMOS, VASCONCELOS & TORRES, 2016), possui a finalidade de abrandar ou anular a disponibilidade de um serviço para determinado usuário. Pode ocorrer em sistemas operacionais, serviços de redes ou em qualquer outro cenário virtual. O

objetivo deste, em suma, é fazer com que as vítimas não consigam realizar as operações.

Há demasiadas maneiras de barrar um serviço, dentre elas, a queda de energia elétrica, ataques físicos, incêndios e a utilização de mensagens maliciosas. Neste contexto, tal ação faz com que a vítima não consiga obter comunicação.

Conforme esclarecido por Ramos, Vasconcelos e Torres (2016), para se prevenir contra os ataques, usa-se ferramentas de monitoramento de redes. Podendo ser definidos por:

> “IDS (Sistemas de detecção de intrusos) são softwares capazes de analisar o sistema operacional evitando ataques de invasão em tempo real e também analisa os pacotes que trafegam na rede comparando-os com assinaturas de ataques, caso seja positivo, de acordo com configurações definidas pelo administrador da rede, ele pode impedir o ataque.”

3.5.7 Cross-site scripting

Na vulnerabilidade de segurança intitulada "*Cross-site Scripting* (XXS)", é primordialmente usufruída da confiança que há por meio do usuário e um site particular. Ademais, há duas maneiras como a ameaça pode ser explorada: de forma persistente e refletiva.

A caracterizamos como persistente quando há a inserção de um código de programação web (HTML) nocivo em sites. Logo, torna-se conspícuo ao usuário.

A refletida, por sua vez, altera valores utilizados pelo aplicativo para enviar variáveis entre duas páginas. A ameaça pode estar oculta no formato de um e-mail de caráter malicioso, fazendo com que o usuário clique no link disfarçado e, deste modo, o roubo ocorra. Utilizar um buscador para fazer com que uma mensagem de alerta seja visualizada em JavaScript é outro exemplo válido. Uma vez tendo o XSS refletido, torna-se viável o roubo de *cookies* e, posteriormente, o roubo da identidade. Uma forma pertinente de prevenir tais atos é aderindo o uso de antivírus confiáveis, além de utilizar complementos que bloqueiem estes scripts dos sites.

3.5.8 Fraude amigável

Com o aumento de cliente nos comércios eletrônicos o número de pessoas mal-intencionadas no site aumenta consequentemente, os quais podem realizar atos ilegais como acessar informações particulares, por exemplo.

O ato de fazer uma compra e solicitar *chargeback* (dinheiro de volta) mesmo após receber o produto em perfeito estado é conhecido como fraude amigável, o indivíduo que realiza tal prática pode ser incriminado por estelionato.

Geralmente a compra ocorre com o cartão de amigos ou familiares, porém, sem o consentimento dos mesmos. Nem sempre a pessoa pode estar agindo de má-fé, em muitos casos esse tipo de fraude ocorre por falta de atenção na hora da compra.

Torna-se importante que os microempreendedores tomem alguns cuidados para não acabarem caindo nesse tipo de fraude como, sempre emitir nota fiscal, por exemplo.

4. METODOLOGIA DE PESQUISA

A atual análise baseou-se na realização de uma pesquisa de campo descritiva e quantitativa, através do *Google Forms* (formulário do *Google*), que visou trazer informações relacionadas ao conhecimento em vendas por meios virtuais dos microempreendedores, eventualmente explicando o motivo de suas principais dúvidas sobre a segurança virtual e criando, com base nestes dados, uma cartilha de apoio para os seus futuros comércios eletrônicos.

Foi preferido o uso de um formulário virtual e fontes primárias inerentes, pois relaciona-se diretamente com o tema proposto e está de acordo com as normas de preservação da saúde nos períodos da pandemia de Covid-19.

A pesquisa é constituída por quatorze questões em sua totalidade, inicia-se com duas perguntas de caráter eliminatório sucedido das demais. Dez delas são fechadas, três são de múltipla escolha e uma é dissertativa, objetivando o entendimento técnico que propõe este trabalho.

O estudo, compartilhado em um grupo específico de vendas de uma rede social e enviado diretamente a alguns comerciantes, iniciou-se na data 17 de dezembro de 2020 às 12 horas, finalizando no dia 19 de fevereiro de 2021 às 16 horas, sendo o universo pesquisado em seu total de 41 pessoas.

Uma cópia do formulário utilizado para pesquisa encontra-se em APENDICE A.

5. ANÁLISE DE DADOS (pesquisa de campo)

O universo pesquisado é formado por microempreendedores e pessoas ligadas ou interessadas por vendas de todo o Estado de São Paulo, finalizando com o total de 41 participantes.

O formulário utilizado foi dividido em três seções, sendo: (I) interesse prévio e utilização de um comércio, eletrônico ou não; (II) perfil do entrevistado; (III) área, local de vendas e conhecimentos gerais sobre comércios nos meios virtuais.

5.1 Interesse prévio e utilização de um comércio, eletrônico ou não

A pesquisa é direcionada para microempreendedores que anseiam por realizar as suas vendas nos comércios eletrônicos, portanto este bloco de questões visa separar pessoas que, posteriormente, não responderiam as perguntas de maneira assertiva.

Gráfico 1 - Você possui ou pretende ter um comércio?

Como podemos verificar no Gráfico 1, 31,7% dos entrevistados, mesmo ligados à área de vendas, não possuem um comércio e não se interessam pela abertura do mesmo. 68,3% deles responderam que mantém um negócio comercial ou que abririam um futuramente.

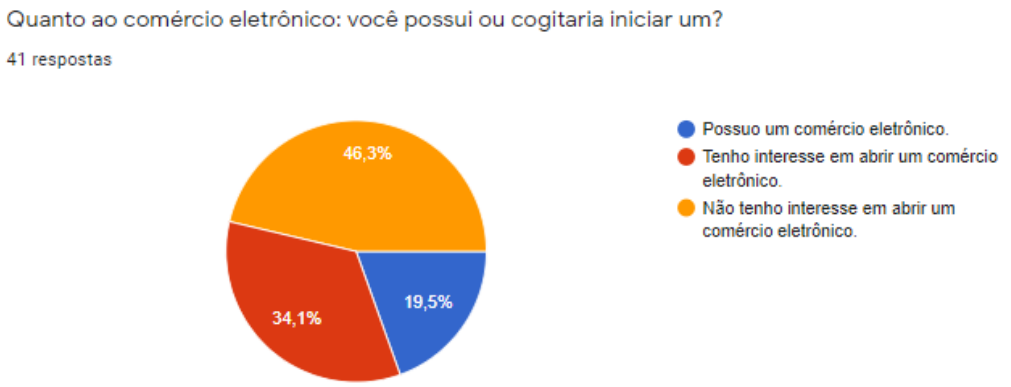


Gráfico 2 – Quanto ao comércio eletrônico: você possui ou cogitaria iniciar um?

Relacionado aos comércios eletrônicos (Gráfico 2), 46,3% não se interessam pelas vendas em meios virtuais, 34,1% se interessam por elas e 19,5% já o possuem.

Os não interessados, finalizam o questionário de imediato e, portanto, não influenciam nos demais dados da pesquisa.

5.2 Perfil do entrevistado

Alguns elementos podem ser diretamente relacionados com a desinformação dos comerciantes. Para um maior aprofundamento neste quesito foi criado este bloco de questões.

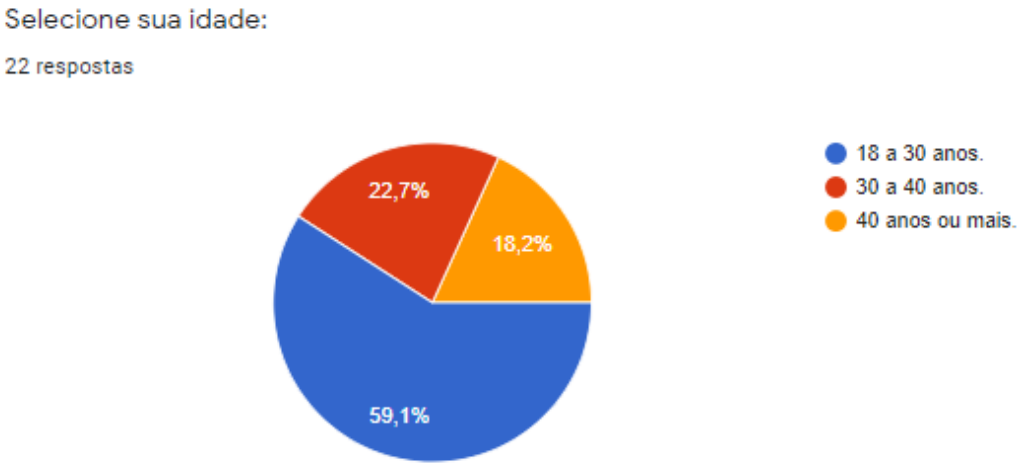


Gráfico 3 – Selecione sua idade

Conforme verificamos no Gráfico 3, 59,1% dos participantes da pesquisa têm entre 18 e 30 anos, 22,7% destes tem de 30 a 40 anos e 18,2% têm mais de 40 anos de idade.

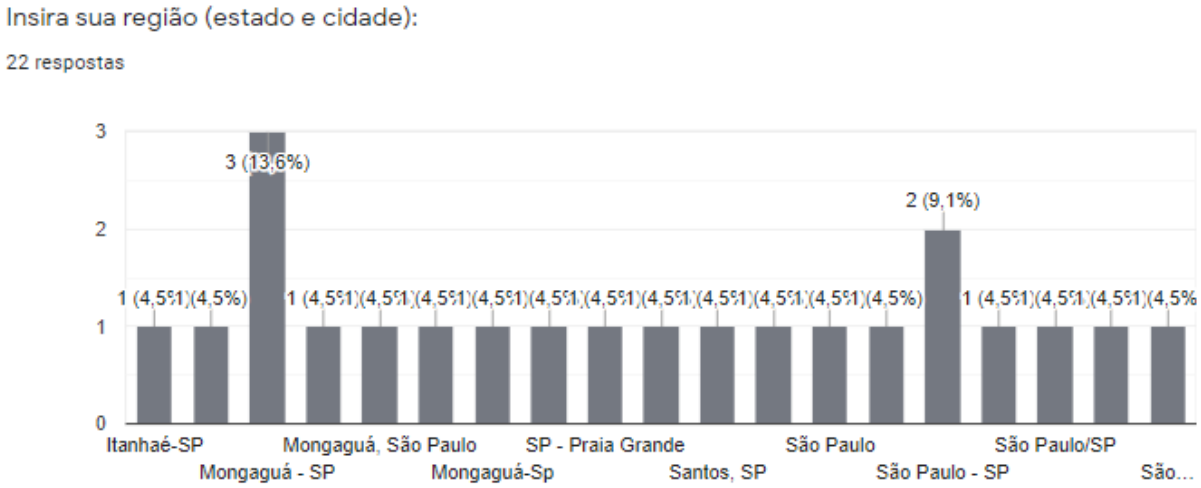


Gráfico 4 – Insira sua região

Das 22 respostas sobre região, 9 pessoas são de Mongaguá, 5 são da capital de São Paulo, 1 é de São Bernardo do Campo, 1 é de Itanhaém, 2 são de Praia Grande, 2 são de Santos, 1 de São Vicente e 19 entrevistados optaram por não responder.

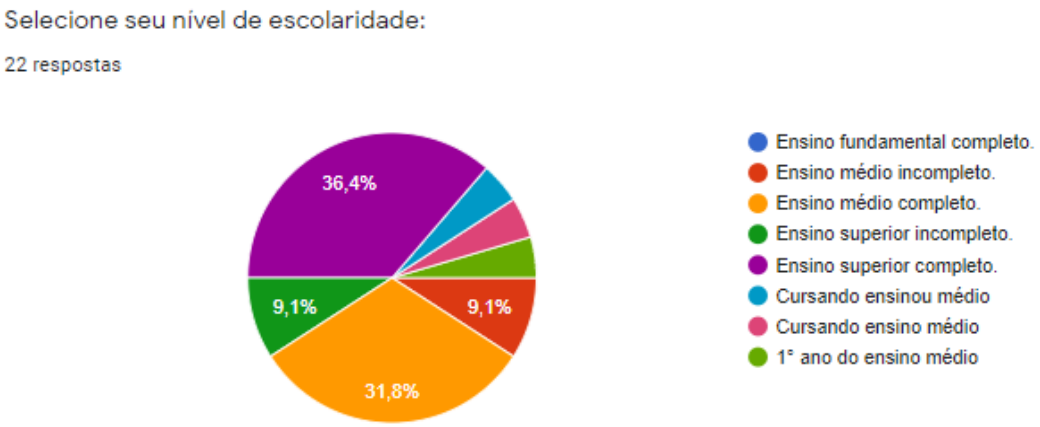


Gráfico 5 – Selecione seu nível de escolaridade

Quanto a escolaridade (Gráfico 5), 36,4% possuem ensino superior completo, 31,8% possuem ensino médio completo, 9,1% possuem ensino superior incompleto e 9,1% possuem ensino médio incompleto.

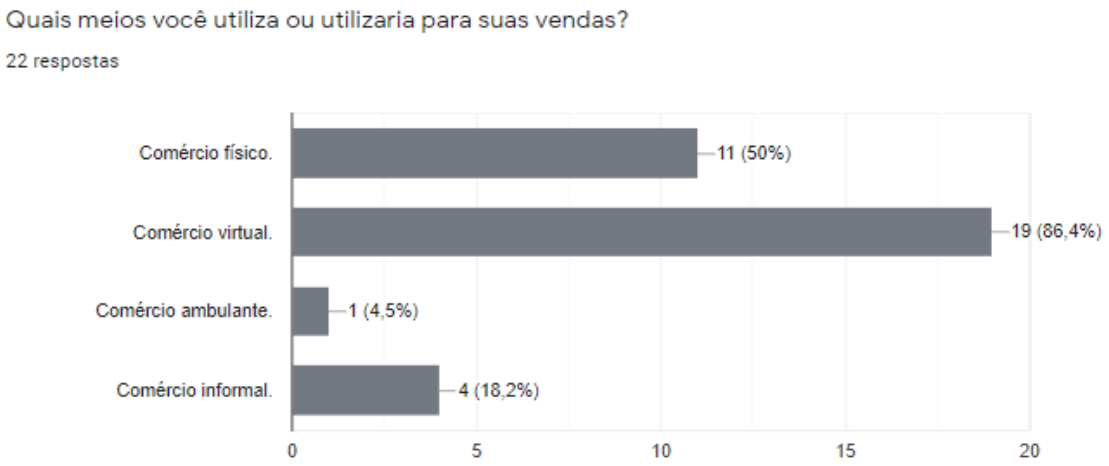


Gráfico 6 – Quais meios você utiliza ou utilizaria para suas vendas?

Sobre os meios de vendas, tratando-se de questões de múltipla escolha (Gráfico 6), 50% utilizam comércio físico, 86,4% utilizam comércio virtuais, 4,5% utilizam comércio ambulante e 18,2% utilizam o comércio informal.

5.3 Área, local de vendas e conhecimentos gerais comércios nos meios virtuais.

Neste bloco de questões, após uma análise geral, nota-se a parte principal da pesquisa. Os conhecimentos sobre a segurança em meios virtuais são abordados e é, a partir deles, montado a cartilha do microempreendedor.

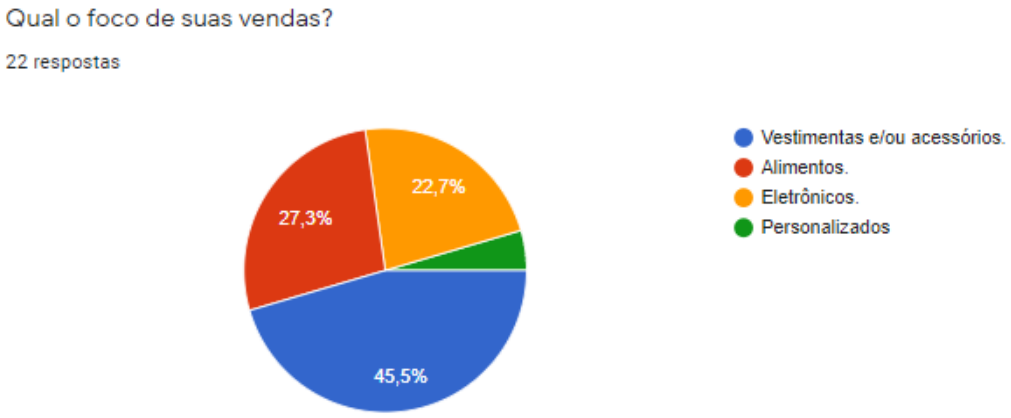


Gráfico 7 – Qual o foco de suas vendas?

Das áreas de atuação (Gráfico 7), 45,5% trabalham com vestimentas e/ou acessórios, 27,3% trabalham com alimentos e 22,7% trabalham com a venda de eletrônicos.

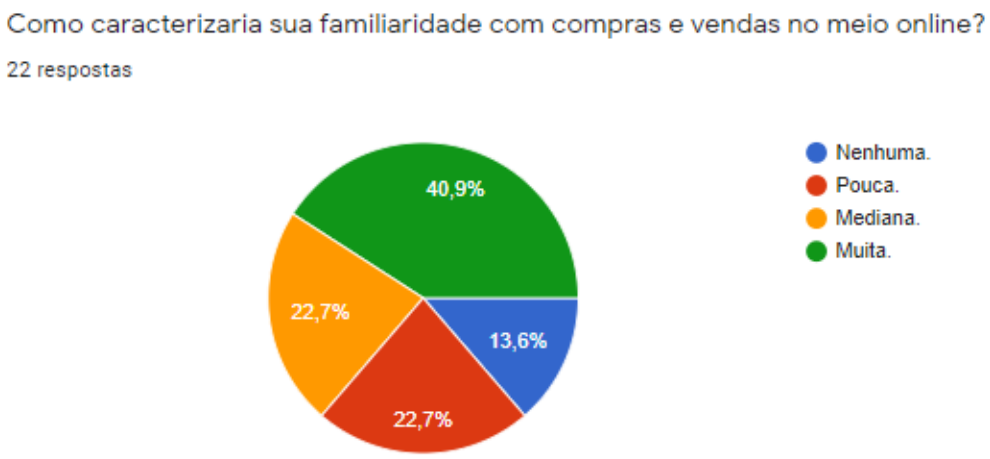


Gráfico 8 – Como caracterizaria sua familiaridade com compras e vendas no meio online?

Observando o Gráfico 8 temos 40,9% se consideram com muita familiaridade em compras e vendas no meio online, 22,7% consideram familiaridade mediana, 22,7% consideram pouca e 13,6% consideram nenhuma.

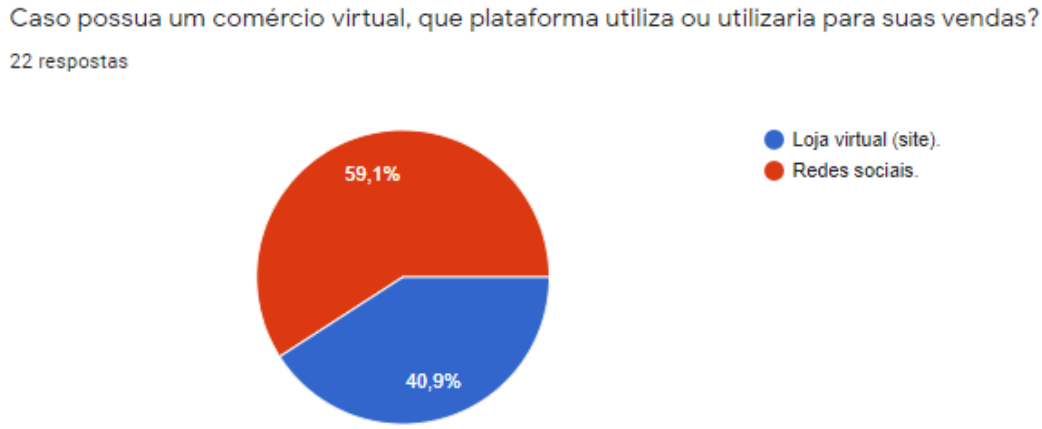


Gráfico 9 – Caso possua um comércio virtual, que plataforma utiliza ou utilizaria para suas vendas?

De acordo com os dados do Gráfico 9, 59,1% dos comerciantes trabalham ou trabalhariam com as redes sociais para a realização de suas vendas. Os 40,9% restantes, utilizam ou utilizariam sites.

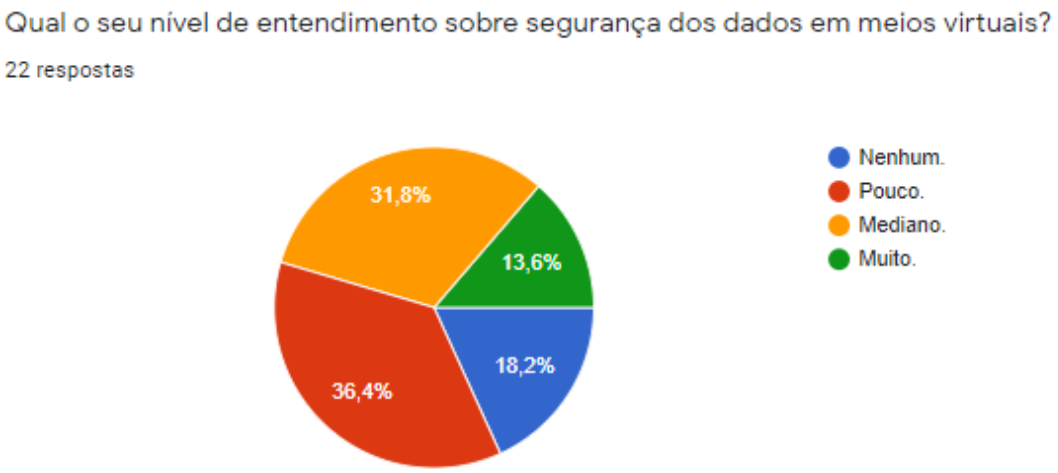


Gráfico 10 – Qual o seu nível de entendimento sobre segurança dos dados em meios virtuais?

A nível de entendimentos sobre segurança de dados (Gráfico 10), 36,4% possuem pouco conhecimento sobre segurança de dados, 31,8% possuem conhecimento mediano, 18,2% não possuem nenhum conhecimento e apenas 13,6% se consideram com muito conhecimento a respeito.

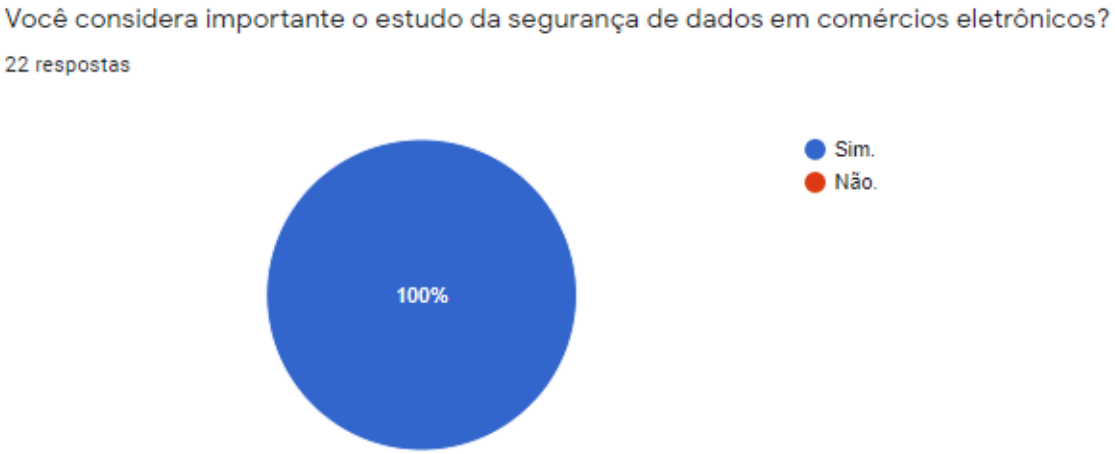


Gráfico 11 - Você considera importante o estudo da segurança de dados em comércios eletrônicos?

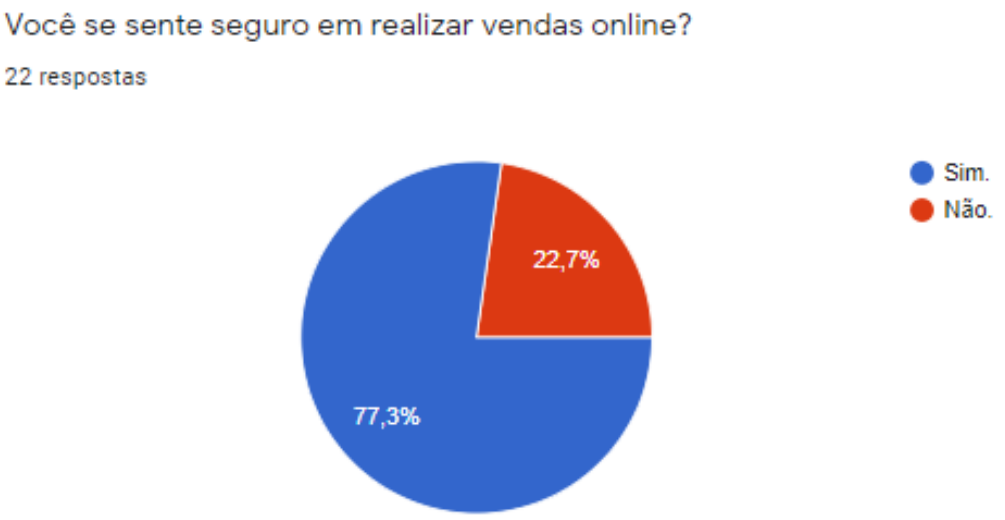


Gráfico 12 - Você se sente seguro em realizar vendas online?

Podemos verificar no Gráfico 11 que 100% das pessoas consideram o estudo da segurança de dados em comércios eletrônicos importante, em contra partida (Gráfico 12) 77,3% se sentem seguros na realização de vendas *online* e 22,7% não se sentem seguros.

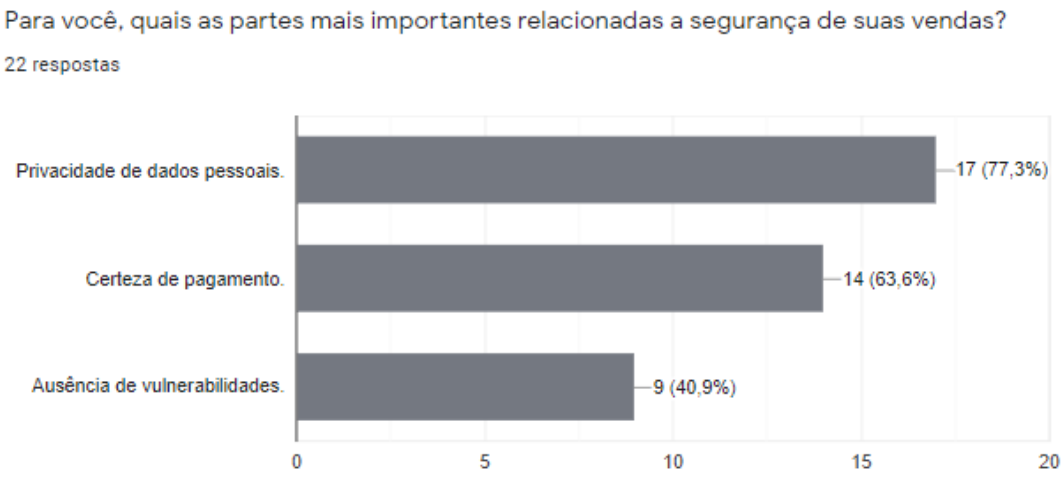


Gráfico 13 – Para você, quais as partes mais importantes relacionadas à segurança de suas vendas?

Com relação as partes mais importantes relacionadas à segurança das vendas *online* (Gráfico 13), sendo questões de múltipla escolha, 77,3% escolheram privacidade de dados pessoais, 63,6% escolheram certeza de pagamento e 40,9% escolheram a ausência de vulnerabilidades.

Gráfico 14 – Qual a maior ameaça ou preocupação deste meio, em sua opinião?

A maior ameaça ou preocupação deste meio, também se tratando de questões de múltipla escolha (Gráfico 14), para 54,5% seria ataques e/ou vírus, para 31,8% é o aumento na ocorrência de *phishing*, para 77,3% são as fraudes, para 54,5% é o roubo de dados dos usuários, para 13,6% é manipulação de preços e para 13,6% é o crescimento na elaboração de *pharming*.

5.4 Interpretação dos dados obtidos

De acordo com os resultados obtidos no estágio de interesse prévio, ou seja, a partir da eliminação dos participantes da pesquisa não interessados em qualquer meio virtual de vendas, tem-se o perfil de jovens e adultos graduados como os mais interessados neste meio, justificando os resultados obtidos da utilização do comércio eletrônico como principal fonte de vendas.

Ademais, no último estágio da pesquisa, constata-se que o conhecimento da segurança de dados em comércios eletrônicos é fundamental, apesar de a maioria dos entrevistados terem um nível de entendimento baixo ou mediano sobre o assunto.

Desse modo, os questionamentos finais podem ser utilizados como uma rota a ser seguida no desenvolvimento teórico acerca da falta de conhecimento dos assuntos mais importantes sobre segurança digital, levando em conta os resultados obtidos com os entrevistados e assim gerando uma orientação aos conhecimentos do que há de nocivo e elevando a compreensão dos leitores.

6. DESCRITIVO DO DESENVOLVIMENTO

Ao realizar um embasamento teórico para reunir informações pertinentes à área do conhecimento em contexto, assim como uma pesquisa de campo visando entender qual é o público-alvo da pesquisa, foi possível, por conseguinte, a elaboração de uma *checklist* como produto final do trabalho.

Durante a elaboração da *checklist*, a prioridade dos elementos a serem inseridos dependiam do nível de entendimento sobre o assunto, o qual, portanto, pode ser descrito como parcialmente técnico, uma vez que será direcionada a grupos de pessoas com pouco conhecimento sobre segurança de dados em meios virtuais.

Outro fator a ser considerado, são as principais medidas de segurança a serem abordadas, as quais foram destacadas por serem erros comumente realizados por indivíduos desprovidos de conhecimento técnico sobre o assunto.

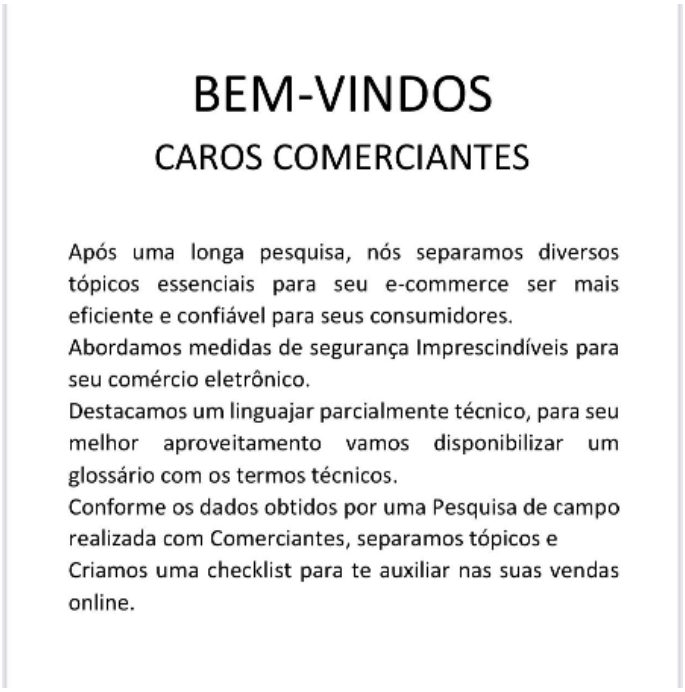
Dessa forma, podem ser apresentadas 11 medidas de segurança imprescindíveis na criação de um comércio eletrônico, as quais são:

- Seja criterioso ao escolher a plataforma de *e-commerce*;
- Conte com uma ferramenta de pagamento online confiável;
- Fique atento a comportamentos incomuns;
- Preste atenção às pequenas coincidências;
- Aposte na autenticação em duas etapas;
- Mantenha o *WordPress* atualizado;
- Filtre produtos mais cobiçados;
- Analise as compras mais caras;
- Configure perfis de usuários;
- Faça *backup* do *WordPress*;
- Crie senhas fortes.

7. MANUAL DO E-COMMERCCE

Segue as páginas do manual do e-commerce.

Página Manual 1 – Capa do Manual do E-commerce



Página Manual 2 – Introdução

Página Manual 3 – A checklist

COMO USAR?

1º SEJA CRITERIOSO AO ESCOLHER QUAL SITE IRÁ ULTILIZAR PARA REALIZAR SUAS VENDAS

Um site não confiável pode vender informações e dados de seus clientes. Hoje existem plataformas especializadas só para vendas como Ifood, Rappi, Shoppe, Mercado Livre etc;

2º ULTILIZE FORMAS DE PAGAMENTO ONLINE QUE SEJAM DE CONFIANÇA

Onde o cliente pode colocar dados importantes sem medo de ser clonados ou até mesmo enganados. Use também métodos de pagamento que você saiba que é seguro como PicPay, Mercado Pago;

3º FIQUE ATENTOS A COMPORTAMENTOS INCOMUNS

Se um cliente compra em excesso, ou em grande quantidade pode ser alguém querendo te enganar. Por exemplo se um cliente compra mais de cinco peças iguais, o porquê que ele iria usar cinco peças do mesmo modelo?

4º PRESTE ATENÇÃO NOS DETALHES

Se por algum acaso o local da entrega for longe da cidade, ou em lugares suspeitos, fique atento pois os golpistas gostam de realizar seus malefícios ao vendedor na hora da entrega, podendo perder carga e materiais, além de arriscar sua vida ou de quem entrega.

5º USE A AUTENTICAÇÃO EM DUAS ETAPAS

O que evita invasões em contas, faz com que seu cliente coloque a senha e um código de confirmação. Podemos prevenir muitos problemas, se alguém mal-intencionado tenta entrar na conta de uma pessoa cadastrada, ao exigir a confirmação em duas etapas, o seu cliente recebe a mensagem no celular

Página Manual 4 – Como usar a checklist

e só consegue entrar por aquele código, por fim, a entrada na conta não é realizada sem o comprador real, sem o próprio dono da conta.

6º ATUALIZE O WORDPRESS SEMPRE QUE POSSÍVEL

O WORDPRESS é um programa que permite você criar seu site, seu programa, sempre atualize as informações e o banco de dados. Não deixe que pessoas gerenciem sua página, tente manter a segurança sempre, se não tais pessoas podem inserir e retirar o que quiserem. Caso não atualizar suas informações e não aumentar sua segurança as pessoas de má índole podem tentar entrar e danificar seu site, ou roubar dados.

7º FAÇA UMA LISTA DOS PRODUTOS MAIS COBIÇADOS

Se houver alguma desconfiança, analise com cautela, pois são alvo dos fraudadores. Se um cliente que não tem muitos dados, não possui identificação confiável, e ele acaba pedindo um produto que está em alta, se atente a esse pedido;

8º ANALISE COMPRAS DE ALTO VALOR

Compras acima da média pode apresentar indício de fraude. Um comprador que faz sua primeira compra e acaba dando um valor acima do normal, pode-se desconfiar e analisar se é confiável o pedido ou não;

9º CONFIGURE PERFIS PARA OS USUÁRIOS

Isso impede que um único usuário possua vários métodos de pagamento, com poucos lugares para entrega, assim pode-se evitar fraudulências na hora da entrega. Quando um e-mail é cadastrado não permite que ele seja cadastrado novamente, assim a mesma pessoa não pode entrar novamente com outros dados.

10º SEMPRE QUE PUDER FAÇA O BACKUP DO WORDPRESS

Você evita a perca de dados e informações, pois fica armazenado no banco de dados. Atualizar o WORDPRESS como citei acima no item 6, os dados vão estar sempre atualizados e em segurança.

11º USE SENHAS FORTES

Página Manual 5 – Como usar a checklist

Assim evitamos problemas futuros, peça que os usuários usem senhas com números e letras. Por exemplo faça o usuário usar letras maiúsculas e minúsculas alternando, como Mg13hN, deixe ele ciente se sua senha é forte ou não.

AGRADECIMENTOS

Nós da equipe BOTS agradecemos a você, microempreendedor que chegou até aqui,
preparamos esse manual para te ajudar!
Use e abuse dessas dicas e sempre fique atento ao seu e-commerce.

Página Manual 6 - Agradecimentos

CONCLUSÃO

A internet mostrou-se algo indispensável na continuação satisfatória da realização de trabalhos, que antes eram estritamente feitos em locais físicos, agora num ambiente caótico que foi suscitado pela pandemia mundial de Covid-19.

Muitas microempresas não estavam preparadas para ocasiões deste porte, pois não possuíam conhecimentos suficientes a respeito, levando a falência de seus negócios. Por outro lado, algumas empresas que se arriscaram neste meio, se depararam com problemas causados pela falta de informações mais aprofundadas sobre vendas *online* e segurança da informação.

Neste universo, se propõem o trabalho de conclusão de curso, que visa explanar e alertar sobre os riscos nas realizações de vendas online, auxiliando na realização de vendagens remotas mais seguras e idôneas.

Portanto, é evidente que a segurança digital implica na confiabilidade de um negócio ao seu público, principalmente quando se está tratando de compras virtuais. Desse modo, é conclusivo que os conhecimentos a respeito da seguridade digital são fatores determinantes para a progressão de um comércio eletrônico.

Como resultado final, a elaboração de uma *checklist* com onze medidas de segurança imprescindíveis na criação de um comércio eletrônico, a qual reflete a fundamentação teórica desenvolvida durante o trabalho e adaptada para um público desprovido de conhecimentos técnicos na área da segurança digital.

Durante a pesquisa é notório o principal objetivo, que é conscientizar, principalmente, os microempreendedores de comércios eletrônicos para que se certifiquem de que estão seguros quanto aos diversos meios de tentativa de fraude ou invasão que podem ocorrer no sistema.

O manual do usuário terá por função, informar e conscientizar diversos microempreendedores das mais diversas áreas, buscando evitar futuros imprevistos relacionados à segurança.

Contudo, sugere-se que, com exceção da *checklist* produzida, os microempreendedores se atentem igualmente às suas próprias condutas quando sob a administração de um comércio eletrônico. Sem dúvidas, é imprescindível a criação de um ambiente ético que cumpra com os requisitos mínimos de segurança, para que assim suas empresas sejam hábeis a crescer financeiramente, sobretudo de maneira honesta e satisfatória.

REFERÊNCIA BIBLIOGRÁFICA

ABNT – Associação Brasileira de Normas Técnicas. NBR 14724: Informação e documentação. Trabalhos Acadêmicos - Apresentação. Rio de Janeiro: ABNT, 2002.

ABREU, Leandro Faria dos Santos. A SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS. 2011. 56 f. TCC (Graduação) – Curso de Tecnologia em Processamento de Dados, Faculdade de Tecnologia de São Paulo, São Paulo, 2011. Disponível em: http://www.fatecsp.br/dti/tcc/tcc0023.pdf. Acesso em: 21 Out. 2020.

ALBERTIN, Alberto Luiz; MOURA, Rosa Maria de. Comércio eletrônico: seus aspectos de segurança e privacidade. Ver. Adm. Empres., São Paulo , v. 38, n. 2, p. 49-61, jun. 1998. Disponível em http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-75901998000200006&lng=pt&nrm=iso. Acesso em 11 Set. 2020.

BELL, Simon; EISINGERICH, Andreas. (2007). The paradox of customer education : Customer expertise and loyalty in the financial services industry. European Journal of Marketing – EUR J MARK. 41. 466-486. 10.1108/03090560710737561.

COMMUNICATION TEAM. A importância de investir em segurança de aplicações continuamente. Conviso AppSec. Disponível em: <https://blog.convisoappsec.com/seguranca-aplicacoes/>. Acesso em: 6 Nov. 2020.

ECKERT, Alex; DAL BÓ, Giancarlo; MILAN, Gabriel Sperandio; et al. E-commerce: privacidade, segurança e qualidade das informações como preditores da confiança. Revista Pensamento Contemporâneo em Administração, v. 11, n. 5, p. 49, 2017. Disponível em: https://www.redalyc.org/pdf/4417/441753779004.pdf.

FARTO, Marcel. “As reinvenções do varejo no e-commerce”. Mercado Digital [02/07/2020]. Disponível em https://abcomm.org/noticias/as-reinvencoes-do-varejo-no-e-commerce/. Acesso em 16 Set. 2020.

FIORI, Diniz. “E-commerce cresce, mesmo durante a pandemia”. Mercado Digital [27/05/2020]. Disponível em: https://abcomm.org/noticias/e-commerce-cresce-mesmo-durante-a-pandemia/. Acesso em 16 Set. 2020.

FONSECA DA SILVA, Raquel; PEREIRA, Julio. IDENTIFICANDO VULNERABILIDADES DE SEGURANÇA COMPUTACIONAL. [s.l.: s.n., s.d.].

Disponível em: http://antigo.unipar.br/~seinpar/2013/artigos/Raquel%20Fonseca%20da%20Silva.pdf. Acesso em: 6 Nov. 2020.

FOROUZAN, Behrouz A.; FEGAN Sophia Chung. Protocolo TCP/IP. 3.ed. Porto Alegre: McGraw-Hill Brasil, 2009.

GUIMARÃES, Vinicius. “Os 7 principais desafios de segurança virtual para lojas brasileiras”. [31/03/2020]. Disponível em <https://www.escoladeecommerce.com/artigos/os-7-principais-desafios-de-seguranca-virtual-para-lojas-brasileiras/>. Acesso em 16 Set. 2020.

LATZE, Carolin. 2007. RVS Retreat 2007 at Quarten: Stronger Authentication in E-Commerce – How to protect even na¨ıve Users against Phishing, Pharming, and MITM attacks.

LINS, Bernardo. Câmara dos Deputados Praça dos 3 Poderes Consultoria Legislativa Anexo III -Térreo Brasília -DF PRIVACIDADE E INTERNET. [s.l.: s.n., s.d.]. Disponível em: https://www2.camara.leg.br/atividade-legislativa/estudos-e-notas-tecnicas/publicacoes-da-consultoria-legislativa/arquivos-pdf/pdf/001854.pdf.

LOTUFO, Larissa. “Tendências para o comércio digital em 2017” [11/04/2017]. Disponível em :https://www.ecommercebrasil.com.br/artigos/tendencias-e-commerce-2017/. Acesso em 21 Out. 2020.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. Segurança de Redes em Ambientes Cooperativos. São Paulo: Novatec Editora Ltda., Agosto 2007.

RAMOS, VASCONCELOS & TORRES, Luiz G. A. Cruz, Péricles D. O., Samuel N. D., Claudines T. Estudo de caso de Ataques de Negação de Serviço (DDoS). 2016, 19. Estudo de caso.

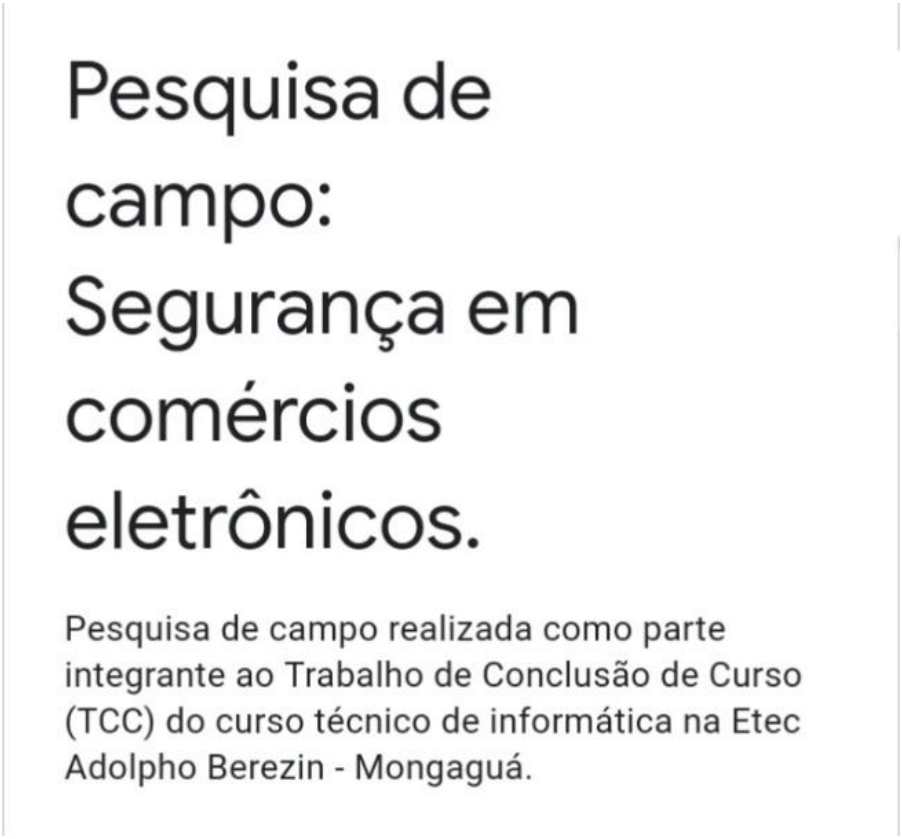
RHEE, Man Young. Internet Security: Cryptographic Principles, Algorithms and Protocols. Chichester: John Wiley & Sons, 25 Jul. 2003.

Segurança da Informação e sua Importância – NSB, NSB – Reduza custos com Gestão em Telecom, Facilities e TI, disponível em: https://nsb.com.br/seguranca-da-informacao-e-sua-importancia/, acesso em: 6 Nov. 2020.

VINÍCIUS, Jordan; ABBAS, Lorena. COOKIES DE COMPUTADOR E HISTÓRIA DA INTERNET: DESAFIOS À LEI BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS. Revista de Estudos Jurídicos UNESP, v. 22, n. 36, 2018.

Disponível em:
https://seer.franca.unesp.br/index.php/estudosjuridicosunesp/article/view/2767/2561.
Acesso em: 7 Nov. 2020.

APENDICE A


Pesquisa de campo: Segurança em comércios eletrônicos.
Pesquisa de campo realizada como parte integrante ao Trabalho de Conclusão de Curso (TCC) do curso técnico de informática na Etec Adolpho Berezin - Mongaguá.

Selecione sua idade: *

- 18 a 30 anos.
- 30 a 40 anos.
- 40 anos ou mais.

Insira sua região (estado e cidade): *

.....

cê *

- Tenho interesse em abrir um comércio eletrô...
- Não tenho interesse em abrir um comércio el...

Selecione seu nível de escolaridade: *

- ○ Ensino fundamental completo.
- ○ Ensino médio incompleto.
- ○ Ensino médio completo.
- ○ Ensino superior incompleto.
- ○ Ensino superior completo.
- ○ Outros...

Quais meios você utiliza ou utilizaria para suas vendas? *

- [ ] Comércio físico.
- [ ] Comércio virtual.
- [ ] Comércio ambulante.
- [ ] Comércio informal.

Qual o foco de suas vendas? *

- ( ) Vestimentas e/ou acessórios.
- ( ) Alimentos.
- ( ) Eletrônicos.
- ( ) Outros...

Como caracterizaria sua familiaridade com compras e vendas no meio online? *

- ◯ Nenhuma.
- ◯ Pouca.
- ◯ Mediana.
- ◯ Muita.

Caso possua um comércio virtual, que plataforma utiliza ou utilizaria para suas vendas?

- ◯ Loja virtual (site).
- ◯ Redes sociais.

Qual o seu nível de entendimento sobre segurança dos dados em meios virtuais? *

- ◯ Nenhum.
- ◯ Pouco.
- ◯ Mediano.
- ◯ Muito.

Você considera importante o estudo da segurança de dados em comércios eletrônicos? *

- ◯ Sim.
- ◯ Não.

Você se sente seguro em realizar vendas online? *

- ○ Sim.
- ○ Não.

Para você, quais as partes mais importantes relacionadas a segurança de suas vendas? *

- ☐ Privacidade de dados pessoais.
- ☐ Certeza de pagamento.
- ☐ Ausência de vulnerabilidades.

Qual a maior ameaça ou preocupação deste meio, em sua opinião? *

- [ ] Ataques e/ou vírus.
- [ ] Aumento na ocorrência de phishing (enganaç...
- [ ] Fraude.
- [ ] Roubo de dados dos usuários.
- [ ] Manipulação de preços.
- [ ] Crescimento na elaboração de pharming (info...
- [ ] Outros...