UNIVERSIDADE DE CAXIAS DO SUL
CAMPUS UNIVERSITÁRIO DA REGIÃO DOS VINHEDOS
ÁREA DO CONHECIMENTO DE CIÊNCIAS EXATAS E ENGENHARIAS
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

LEONARDO GUISSO

SEGURANÇA DIGITAL: AVALIAÇÃO DO NÍVEL DE CONHECIMENTO DA POPULAÇÃO SOBRE OS RISCOS DE SEGURANÇA ATRELADOS AO USO DA INTERNET NA REGIÃO DE BENTO GONÇALVES

BENTO GONÇALVES
2017

LEONARDO GUISSO

SEGURANÇA DIGITAL: AVALIAÇÃO DO NÍVEL DE CONHECIMENTO DA POPULAÇÃO SOBRE OS RISCOS DE SEGURANÇA ATRELADOS AO USO DA INTERNET NA REGIÃO DE BENTO GONÇALVES

Relatório do Trabalho de Conclusão apresentado ao curso de Sistemas de Informação como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação, no Campus Universitário da Região dos Vinhedos, da Universidade de Caxias do Sul.

Orientador: Prof. Me. Christian Zambenedetti

Bento Gonçalves

2017

RESUMO

A popularidade da Internet juntamente com a facilidade de acesso através da inclusão digital leva à tona um problema de proporções gigantescas, os chamados crimes cibernéticos. Como a população foi inserida nos meios digitais de forma desorientada e não possui cultura de acesso seguro praticado nas escolas e pelos pais, acabam se tornando alvos fáceis nas mãos de pessoas mal-intencionadas. O objetivo do presente trabalho é expor os perigos encontrados na Internet, demonstrar ferramentas de proteção atreladas às boas práticas de prevenção, assim como mensurar o nível de conhecimento da população da região de Bento Gonçalves sobre segurança digital, através de uma pesquisa quantitativa. Para uma abordagem completa do assunto, serão expostos fatos históricos sobre a Internet no Brasil e no mundo, assim como estatísticas sobre o crescimento da sua utilização. Também foi considerado de grande importância expor conceitos de inclusão digital, fator que contribui para o avanço contínuo no acesso à tecnologia. Comenta-se a importância de trabalhos relacionados com o tema, através de exemplos contendo seus objetivos e resultados obtidos. A metodologia escolhida foi a de apresentar conceitos técnicos de autores já conhecidos no assunto. Embora existam ferramentas que auxiliam na prevenção de ataques, elas não são suficientes perante as avançadas técnicas utilizadas pelos criminosos, por isso se faz necessário ter conhecimento sobre os riscos, e assim tomar medidas preventivas para evitá-los. Através da pesquisa de conceitos técnicos e da análise dos resultados da pesquisa quantitativa, foi possível desenvolver uma cartilha de orientação digital. Essa mesma cartilha será divulgada por meios digitais como uma forma de plano de ação para os problemas encontrados.

Palavras-chave: Internet. Crimes Cibernéticos. Inclusão Digital. Segurança Digital.

LISTA DE FIGURAS

LISTA DE SIGLAS

ARPANET - *Advanced Research Projects Agency Network*
CERN - Centro Europeu de Investigação Nuclear
CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CETIC.br - Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CGI.br - Comitê Gestor da Internet no Brasil
DDoS - *Distributed Denial of Service*
EUA - Estados Unidos da América
FAPESP - Fundação de Amparo à Pesquisa do Estado de São Paulo
FERMILAB - *Fermi National Accelerator Laboratory*
HTML - *Hyper Text Markup Language*
HTTP - *Hyper Text Transfer Protocol*
IBASE - Instituto Brasileiro de Análises Sociais e Econômicas
IBGE - Instituto Brasileiro de Geografia e Estatística
LNCC - Laboratório Nacional de Computação Científica
MCT - Ministério da Ciência e Tecnologia
MIT - *Massachusetts Institute of Technology*
NCP - *Network Control Protocol*
NSF - *National Science Foundation*
P2P - *Peer-to-peer*
PROCEMPA - Companhia de Processamento de Dados de Porto Alegre
PROCON - Programa de Proteção e Defesa do Consumidor
RNP - Rede Nacional de Pesquisas
SQL - *Structured Query Language*
TCP/IP - *Transmission Control Protocol/Internet Protocol*
TIC - Tecnologia de Informação e Comunicação
UFRJ - Universidade Federal do Rio de Janeiro
URL - *Uniform Resource Locator*
WEP - *Wired equivalent privacy*
WPA - *Wi-Fi protected access*
WWW - *World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

Segundo dados do Instituto Brasileiro de Geografia e Estatística (IBGE), em pesquisa realizada em 2014, a Internet já estava presente em mais de 50% das casas no Brasil, o que equivale a 32,3 milhões de lares. (CETIC.br, 2015). É inevitável dizer que a Internet se tornou um recurso indispensável no dia a dia das pessoas e grande parte dessa popularidade se deve às políticas de inclusão digital, além das facilidades com que computadores, *smartphones*, *tablets* e demais dispositivos são adquiridos e manuseados.

Dentre as inúmeras vantagens da Internet, é preciso salientar também os seus riscos, sendo o principal deles a criminalidade digital. Como a maioria da população foi inserida no universo digital de forma desorientada e sequer recebeu educação digital nas escolas, acabam se tornando alvos fáceis nas mãos de especialistas em crimes cibernéticos, os chamados *crackers*. (JESUS, 2016).

Hoje, toda a informação circula facilmente através da rede de Internet, mas em um passado não tão distante o acesso a esse recurso era algo muito restrito. Por muitos séculos, a informação foi transmitida por meio de papel ou apenas pessoalmente. O primeiro meio de transmissão de informação foi o telégrafo, que em 1844 transmitiu a primeira mensagem. (KLEINA, 2011 apud OMIZZOLO, 2013, p. 11).

Em agosto de 1969, foi criada a *Advanced Research Projects Agency Network* (ARPANET), primeiro conceito de rede que conectava três universidades e um centro de pesquisa. A ARPANET foi sendo aperfeiçoada e, por fim em 1991, o conceito do *World Wide Web* (WWW) foi criado no Centro Europeu de Investigação Nuclear (CERN), por Tim Berners-Lee. (KIOSKEA, 2012 apud OMIZZOLO, 2013, p. 11).

No Brasil, foi instalada a primeira rede conectada à Internet nas principais universidades brasileiras no ano de 1992. Na época, não existia interface gráfica e a única função realizada era a troca de e-mails, além de que o recurso era acessível a somente um grupo restrito de interessados. Em 1995, foi liberado o uso da Internet para fins comerciais, porém a velocidade de conexão era de 9,6 Kbps. (CHAGAS, 2003).

A Inclusão Digital tem por objetivo garantir a toda população o acesso às tecnologias de informação. No Brasil, essa inclusão teve destaque pela iniciativa do Instituto Brasileiro de Análises Sociais e Econômicas (Ibase), que vislumbrava a interação da sociedade civil com as Tecnologias de Informação e Comunicação (TIC).

Até o ano de 1994, a Internet brasileira estava restrita a iniciativas acadêmicas, porém ainda em 1989 o Ibase lançou um serviço de troca de e-mails voltado para a sociedade civil, chamado de Alternex. Por ser o único servidor WWW, o Ibase se tornou fundamental na propagação da Internet para uso geral da população. (FALAVIGNA, 2011 apud MARTINS, 2015, p. 51).

A propagação da Internet fez com que criminosos vissem nela um método fácil de se chegar a milhares de vítimas, dessa forma surgiu o cibercrime. No Brasil, não foi diferente, atualmente o país é o quarto do mundo com maior número de ameaças virtuais. Como se não bastasse, grande parte das fraudes mundiais são originadas no Brasil, ou seja, uma grande parcela dos criminosos está aqui no país. (JESUS, 2016).

Neste trabalho, são abordadas questões que cercam o uso da Internet, as ameaças atuais as quais os usuários são expostos, assim como formas para prevenção e boas práticas de utilização desse recurso. Também foi realizada uma pesquisa através de um questionário, com a intenção de mensurar o nível de conhecimento da população da região de Bento Gonçalves sobre os riscos de segurança que o uso da Internet de forma desorientada pode causar. Por fim, com o resultado da pesquisa em mãos, foi desenvolvida e divulgada uma cartilha com as boas práticas de uso da Internet e segurança digital.

A Internet sem dúvida é um espaço onde pode-se tirar inúmeros proveitos para o nosso dia a dia, é preciso somente estar atento para as armadilhas as quais os usuários são expostos, e para isso não há outra forma que não seja conhecer e saber identificar os riscos e dessa forma tirar o máximo proveito de algo que já é indispensável em nosso cotidiano.

1.1 PROBLEMA DE PESQUISA

Em tempos onde se fala muito da inclusão digital no Brasil, fator que sem dúvida é essencial para o desenvolvimento da nação, pouco é considerado sobre os riscos de segurança embutidos nessa temática.

As pesquisas sobre o uso das TIC’s nos domicílios brasileiros, realizada pelo Comitê Gestor da Internet no Brasil (CGI.br), apontou em 2014 que embora uma parcela significativa da população ainda se encontre digitalmente excluída em função de barreiras como custo de acesso, falta de cobertura e habilidades, houve um aumento considerável na utilização de dispositivos com acesso à Internet. O que mais

chama a atenção é o avanço no uso de telefones celulares, que triplicou nos últimos três anos: em 2011, a proporção era de 15% da população, chegando a 47% em 2014. O aumento foi visto em todas as classes sociais, embora ainda haja grande desigualdade nas áreas rurais e nas regiões Norte e Nordeste (CGI.br, 2015).

Com o aumento da conectividade, houve também uma elevação nos índices de ataques cibernéticos, assim como os meios utilizados para que esses crimes se concretizem. Basicamente, os cibercriminosos se aproveitam da fragilidade dos usuários, oferecendo serviços gratuitos, softwares falsos, links com assuntos polêmicos, jogos, pornografia, promoções, entre outros. Essas vulnerabilidades são exploradas através de e-mails com remetentes e links falsos, sites com códigos maliciosos infiltrados, softwares falsos de antivírus e download de aplicativos.

Recentemente, a ameaça cibernética mais comentada mundialmente é o chamado *Ransomware*, um *malware* que ao ser executado criptografa todos os arquivos do seu dispositivo solicitando um resgate financeiro para poder recuperá-los. Seu principal foco é roubar dados importantes de usuários desprotegidos, o que aumenta as chances de cederem às exigências de pagamento para poderem ter seus arquivos de volta.

Um dos principais focos dos ataques são as empresas, porém deve-se considerar que elas possuem, ou pelo menos deveriam possuir, ferramentas de proteção e detecção de ameaças, assim como o auxílio de profissionais. Partindo desse pressuposto, o foco desse trabalho será direcionado aos usuários domésticos que em sua maioria não possuem qualquer informação, auxílio ou proteção contra esses tipos de ataque.

Hoje, a inclusão digital já é uma realidade conhecida que vem cada vez mais cedo atraindo jovens para utilizarem as vantagens do mundo virtual. O governo federal possui programas de incentivo como o Projeto Cidadão Conectado – Computador para todos e o Programa Nacional de Inclusão Digital, que visam a facilitar a compra de computadores e instruir para sua utilização. O problema visto em cima disso é que não está havendo uma preocupação sobre os cuidados que se deve ter ao navegar na Internet. Não basta a população ter o acesso, é preciso também ensiná-la a utilizá-lo de forma segura, sabendo identificar sites com conteúdo impróprio, e-mails falsos, riscos sobre o envio de informações privadas, ou seja, estimular uma visão mais crítica sobre as informações que o cercam. Pais e professores precisam conhecer o assunto

para repassarem às crianças e adolescentes que por serem ingênuas são um alvo fácil para os criminosos.

Para que se saiba como agir é preciso primeiro perceber qual o nível de entendimento da população sobre o assunto, quais as suas expectativas e quais os seus receios referentes à utilização da Internet. Para isso, este trabalho de pesquisa se propõe a buscar formas de conscientizar a população no âmbito nacional, além de realizar uma pesquisa descritiva quantitativa na região de Bento Gonçalves para poder entender qual o seu nível de conhecimento no assunto.

1.1.1 Questão de Pesquisa

Que conhecimento a população da região de Bento Gonçalves tem a respeito dos riscos de segurança atrelados ao uso da Internet e quais as formas de conscientização para a utilização desse recurso de forma segura?

1.2 JUSTIFICATIVA

Os avanços tecnológicos interferem diretamente no comportamento humano, um exemplo disso é a Internet. São infinitos os benefícios que a *web* nos proporciona, porém junto a eles há também os riscos de segurança digital aos quais os usuários são expostos. Os ataques cibernéticos contra a honra, injúria, difamação e *bullying* são cada vez mais comuns e um dos principais facilitadores é a falta de conhecimento dos usuários.

Para Cassanti (2014, p. 22), “Não haverá o mínimo de possibilidade em obter êxito na luta contra os crimes virtuais se quem pretender vencê-lo primeiramente não puder entendê-lo.”

É de fundamental importância que os usuários conheçam os riscos e principalmente saibam identificá-los, só assim se conseguirá ser mais eficaz na luta contra os crimes cibernéticos. Uma das grandes preocupações relacionadas ao uso de Internet é que muitos usuários pensam que não estão correndo riscos, de que seu dispositivo é somente mais um entre milhares e dificilmente será alvo de invasores. É preciso estar ciente de que, mesmo ao estar navegando em um mundo virtual, tudo o que acontece lá é real, as informações são reais e os riscos também. (CERT.br, 2012).

O estudo deste trabalho se justifica pela necessidade do autor em auxiliar os usuários a identificarem com maior facilidade os riscos aos quais estão expostos, tornando-os aptos a prevenir os ataques. Também será possível mensurar qual o nível atual de conhecimento da população da região, e assim indicar aos governantes que ações de prevenção devem ser tomadas para disseminar a ideia de um comportamento seguro na Internet.

1.3 OBJETIVOS

A seguir, são apresentados os objetivos dessa pesquisa, divididos em geral e específicos.

1.3.1 Objetivo geral

Demonstrar conceitos de boas práticas de utilização da Internet e avaliar o nível de conhecimento da população da região de Bento Gonçalves a respeito dos riscos de segurança atrelados ao uso da Internet, assim como divulgar uma cartilha com orientações para a sociedade em geral.

1.3.2 Objetivos específicos

Este trabalho tem como objetivos específicos:

a) descrever os tipos de ataques da atualidade;
b) demonstrar formas de prevenção para esses ataques;
c) exemplificar quais as boas práticas de utilização da Internet;
d) desenvolver um questionário para avaliar o nível de conhecimento da população da região de Bento Gonçalves sobre os riscos de segurança digital;
e) analisar os resultados obtidos na pesquisa para poder entender e explanar quais as necessidades atuais para melhoria do conhecimento da população;
f) criar uma cartilha para expor as boas práticas de utilização da Internet e divulgar para os demais acadêmicos da UCS e sociedade em geral,

através de meios eletrônicos, para assim poder conscientizar um maior número de pessoas.

1.4 ESTRUTURA DO TRABALHO

No Capítulo 2, é apresentado o embasamento teórico utilizado para formulação do trabalho, o qual está dividido em seções representando cada tópico da pesquisa. As seções são, história da Internet, que inclui a história da sua origem, sua inserção no Brasil e estatísticas atuais, em seguida será visto a inclusão digital onde também será falado sobre a sua inserção no Brasil, os tipos de inclusão e a utilização de software livre. Após, será visto a origem dos crimes cibernéticos, os meios e tipos de ataques utilizados, assim como as formas de prevenção e dicas para utilização da Internet de forma segura. Concluindo o capítulo, são apresentados trabalhos com temas relacionados e suas contribuições na formulação do estudo.

No Capítulo 3, é exposto a metodologia utilizada no trabalho, que terá seu foco em uma pesquisa para avaliar o nível de conhecimento em segurança digital da população da região de Bento Gonçalves.

No Capítulo 4, são explicados os detalhes da pesquisa desenvolvida, assim como os resultados obtidos e analisados.

Por fim, no Capítulo 5, são demonstradas as conclusões obtidas, encerramento do assunto, assim como a divulgação de ideias para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica tem o objetivo de apresentar os conceitos e ideias que foram estabelecidos para o trabalho com base em estudos já realizados, dando sustentação ao tema.

2.1 HISTÓRIA DA INTERNET

A Internet nada mais é que uma rede mundial de dispositivos interligados com o propósito de servir usuários. É através dela que se pode, por exemplo, trocar *e-mails*, mensagens e visitar sites do outro lado do mundo.

A história da Internet teve início com a criação da *Advanced Research Projects Agency* (ARPA), formada em 1958 pelo Departamento de Defesa dos Estados Unidos. Sua principal missão era acelerar o desenvolvimento tecnológico do país, mobilizando recursos de pesquisa do mundo universitário para alcançar superioridade tecnológica militar em relação à União Soviética. (CASTELLS, 2003).

Com o objetivo de criar uma rede capaz de integrar computadores que estivessem distantes e que, por intermédio dela, fosse permitida a comunicação de dados, em 1969 foi criada a ARPANET, uma rede com tecnologia chamada de troca de pacotes para o transporte de informações. Essa mesma tecnologia é a base da Internet de hoje. (WENDT; JORGE, 2013).

Inicialmente, a ARPANET interligou a Universidade da Califórnia (Los Angeles e Santa Bárbara), a Universidade de Stanford (Santa Cruz) e a Universidade de Utah (Salt Lake City). Em 1972, foi organizada a primeira demonstração pública da rede, onde já era possível utilizar serviços como *login* remoto e correio eletrônico. Já no ano de 1973, foi possível realizar a primeira conexão internacional, que interligou a Inglaterra e a Noruega. Também no final dessa década, foi substituído seu protocolo de comunicação de pacotes, de *Network Control Protocol* (NCP) para *Transmission Control Protocol/Internet Protocol* (TCP/IP). (SIMON, 1997). A alteração de protocolo foi necessária para que se pudesse ter um padrão de comunicação, tornando a interligação de redes independentes mais fácil.

Outro ponto marcante da história foi a criação do WWW, no final da década de 1980, por Tim Berners-Lee, que também criou o protocolo *Hyper Text Transfer Protocol* (HTTP) e a linguagem *Hyper Text Markup Language* (HTML). Preocupados

com a segurança da rede, em 1984 a *National Science Foundation* (NSF) montou sua própria rede de comunicação, chamada NSFNET. Em 1990 a ARPANET foi desativada por ser considerada obsoleta. Nesse período, a NSFNET tentou comercializar sua tecnologia financiando fabricantes de computadores dos Estados Unidos da América (EUA), porém a maioria dos computadores já possuía capacidade de acesso à Internet e com isso em 1995 a NSFNET foi desativada dando origem à Internet privada comercializada por diversos provedores que montavam suas próprias redes. (CASTELLS, 2003).

2.2 A INTERNET NO BRASIL

No Brasil, o primeiro contato com a Internet foi realizado pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), em 1988, que realizou a primeira conexão à rede através de uma parceria com o *Fermi National Accelerator Laboratory* (FERMILAB), sendo considerado um dos mais importantes centros de pesquisa dos Estados Unidos. Seguindo a mesma onda, a Universidade Federal do Rio de Janeiro (UFRJ) e o Laboratório Nacional de Computação Científica (LNCC) também se conectaram. Em 1992, foi a vez do governo federal, com a criação da Rede Nacional de Pesquisas (RNP) que criou uma gigantesca infraestrutura para suportar a rede mundial de computadores que recebia o link internacional e o espalharia pelas principais capitais do país. (VIEIRA, 2003).

A utilização da Internet fora dos meios acadêmicos somente foi iniciada com a criação do Instituto Brasileiro de Análises Sociais e Econômicas (IBASE), através de um serviço de correio eletrônico chamado Alternex. Nos anos seguintes, houve uma expansão gradual no uso da Internet nos meios acadêmicos e, em 1994, o governo decide apoiar essa expansão, aliando a experiência e infraestrutura adquirida pela RNP com a exploração comercial por parte da Embratel, empresa que comandava unicamente o serviço de comunicação de dados no país. Ao que tudo indicava, a Embratel teria o monopólio da Internet, porém em 1995 o presidente Fernando Henrique Cardoso ao assumir o cargo declarou que as operadoras estatais não poderiam oferecer o serviço de Internet ao consumidor final, pois isso ficaria sob responsabilidade da iniciativa privada. As operadoras estatais, por sua vez, ficariam limitadas a proporcionar a infraestrutura necessária para o mercado corporativo. (VIEIRA, 2003).

> *O ano de 1995 pode ser considerado o marco-zero da Internet comercial no Brasil e no mundo. Foi quando surgiram nos Estados Unidos alguns dos mais importantes nomes da Internet, como o site de busca Yahoo! e a livraria virtual Amazon.com, além dos primeiros protagonistas da Web brasileira. (VIEIRA, 2003, p. 11).*

Já em 1996, foi criado o Comitê Gestor da Internet (CGI), formado por representantes do MCT, universidades, ONGs e provedores de acesso, sendo o principal órgão do governo até hoje, quando se fala em rede mundial de computadores. (VIEIRA, 2003).

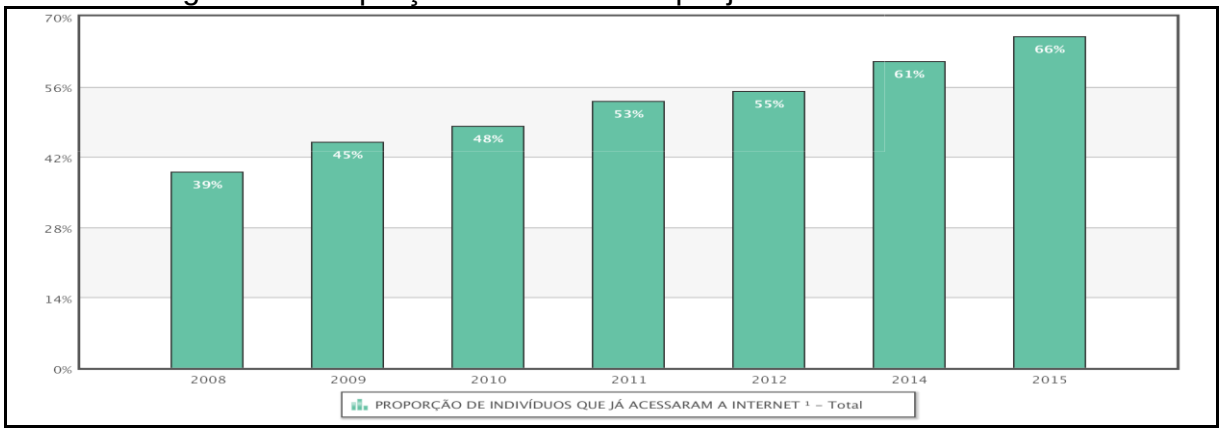
2.2.1 Estatísticas

O Brasil realiza anualmente pesquisas sobre a disponibilidade das TICs, sendo o órgão responsável o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.br).

A pesquisa TIC Domicílios 2014 demonstrou que o Brasil conta com mais de 94 milhões de usuários da rede, esse número está diretamente ligado à evolução tecnológica vivenciada ano após ano. Somente em 2011, o Brasil superou a marca de mais da metade da população sendo usuário de Internet. Com base nas pesquisas, é possível verificar uma evolução constante, que inclui por exemplo a disseminação dos dispositivos móveis e de fenômenos como o uso de redes sociais *on-line*. Também é possível verificar as barreiras que impedem que mais brasileiros possam usufruir dos benefícios proporcionados pela tecnologia. (CGI.br, 2015).

Na Figura 1, é possível identificar o crescimento da proporção de indivíduos que já acessaram a Internet entre os anos de 2008 e 2015.

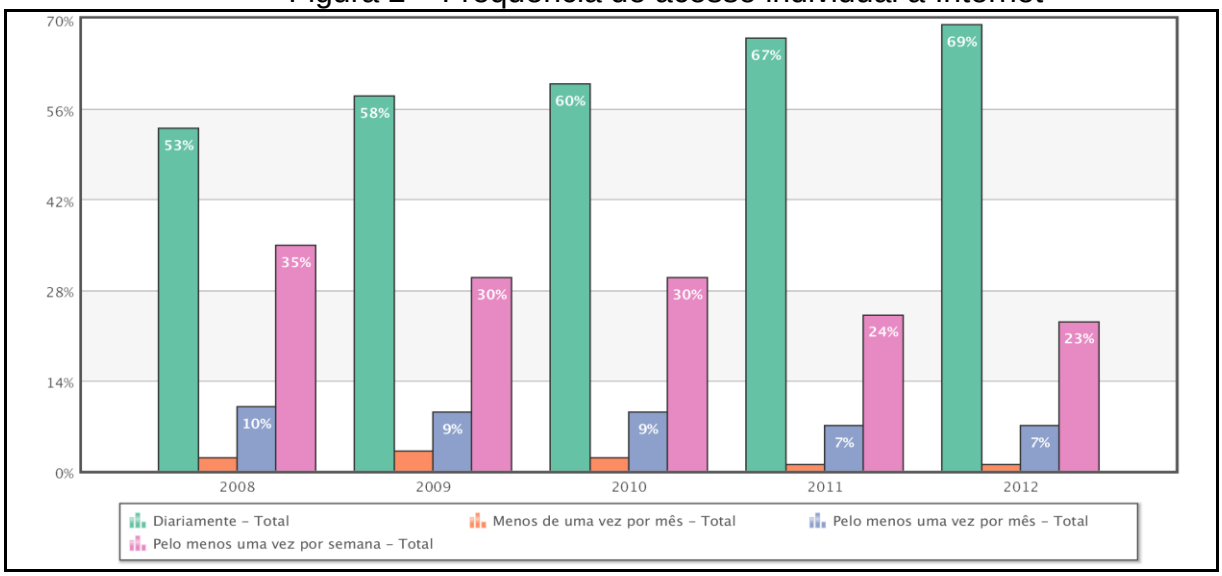
Figura 1 – Proporção de Indivíduos que já acessaram a Internet



Fonte: CETIC.br (2015).

Assim como a proporção de indivíduos que acessam a Internet aumentou, a frequência de utilização também seguiu a mesma tendência, como pode ser visto na Figura 2, em pesquisa comparativa realizada entre 2008 e 2012.

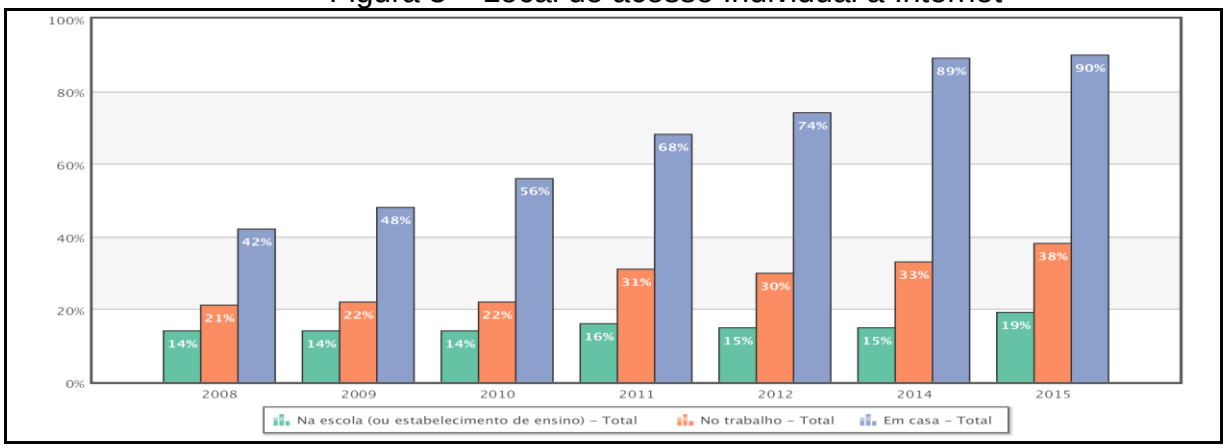
Figura 2 – Frequência de acesso individual à Internet



Fonte: CETIC.br (2015).

Em comparação ao local de acesso à Internet, tendo como critério de divisão, em casa, no trabalho e na escola, pode-se ver na Figura 3 um crescimento constante dos indivíduos que acessam a Internet a partir de seus lares, chegando a 90% em 2015. Entretanto, no quesito acesso nas escolas, percebe-se que não houve um crescimento significativo, o que aponta para um ponto crítico na sociedade, pois não está havendo aderência às metodologias de ensino através do computador e da Internet.

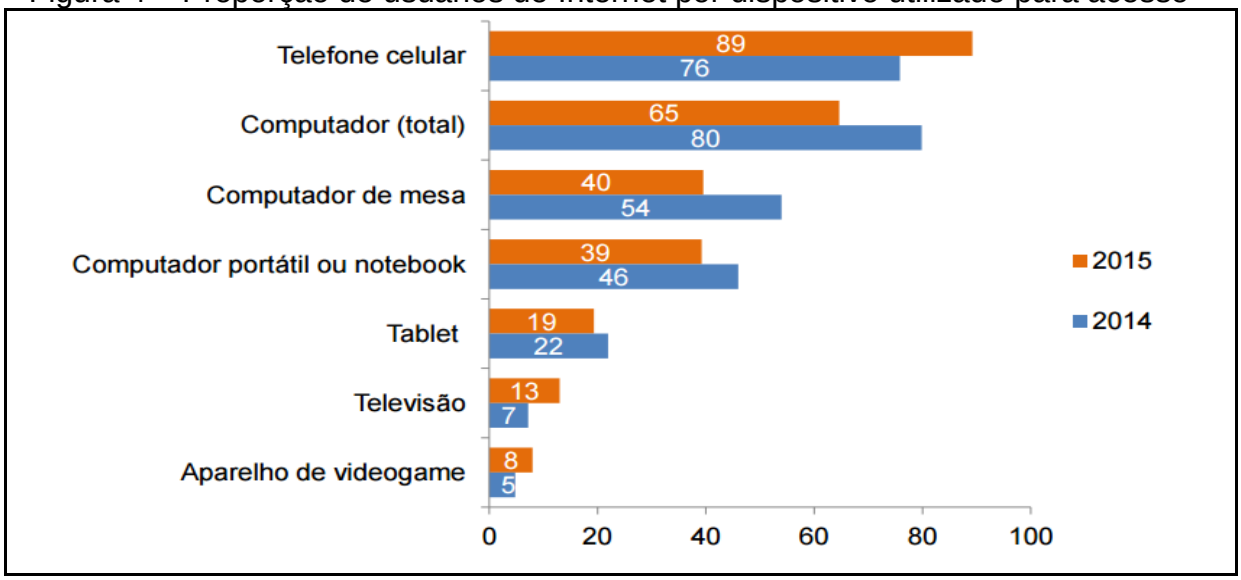
Figura 3 – Local de acesso Individual à Internet



Fonte: CETIC.br (2015).

À medida que a tecnologia evoluiu, foram abertos novos meios pelos quais pode-se acessar a Internet. Antigamente, o acesso era feito basicamente através de computadores de mesa, mas agora é comum a utilização de telefones celulares, notebooks, tablets e até mesmo televisões e aparelhos de videogame. Em 2015, foi atingida a marca histórica onde os telefones celulares ultrapassaram a proporção do total de computadores que acessam a Internet, como pode ser visto na Figura 4.

Figura 4 – Proporção de usuários de Internet por dispositivo utilizado para acesso



Fonte: CETIC.br (2015).

Com base nas pesquisas, conclui-se que houve uma evolução constante na utilização da Internet, isso se deve à grande gama de dispositivos e facilidades de aquisição, assim como os incentivos à inclusão digital, assunto que será abordado na próxima seção.

2.3 A INCLUSÃO DIGITAL NO BRASIL

A Internet pode ser considerada o principal meio de acesso e transmissão de informações, seja para estudo, entretenimento, negócios ou simplesmente para se comunicar com pessoas em qualquer lugar do mundo. O ponto fundamental do termo inclusão digital se refere a disponibilizar o acesso aos recursos digitais para a população, de forma ampla, indiferente de raça, classe social, região onde vive ou qualquer outro fator que possa ser considerado um empecilho ou fator de desigualdade.

Para que se possa entender o fator inclusão digital, é preciso conhecer também o seu oposto, a exclusão digital. A exclusão digital caracteriza-se por privar o cidadão do acesso a instrumentos básicos como computador, linha telefônica e provedor de acesso. (SILVEIRA, 2001 apud LEMOS, 2007, p.17). O abismo entre incluídos e excluídos digitais é grande no Brasil e, embora haja esforços do governo, o principal complicador é o alto índice de pobreza e analfabetismo. Para haver inclusão digital é preciso que além de computadores e internet, haja capacitação educacional, garantindo a construção da cidadania. (LEMOS, 2007).

No Brasil, o marco oficial de inserção da cultura da inclusão digital foi o Programa Sociedade da Informação, lançado em 15 de novembro de 1999. O programa era coordenado pelo Ministério da Ciência e Tecnologia (MCT) e tinha como objetivo estimular a utilização de tecnologias de informação para que a economia pudesse competir com o mercado global, além de contribuir para a inclusão social de todos os brasileiros. (LEMOS, 2007).

O segundo ponto importante na história da inclusão digital foi a criação dos primeiros espaços públicos, chamados de infocentros ou telecentros. Em 11 de julho de 2000, o então governador do estado de São Paulo, Mário Covas, inaugura o Infocentro na Casa de Cultura do Jardim São Luís, zona sul da capital. Três dias depois, também é inaugurado o projeto-piloto do Sampa.Org, já com seis telecentros, que dois meses depois chegariam a dez unidades. Também no ano de 2000, foi inaugurado pela prefeitura de Porto Alegre, em coordenação com a Companhia de Processamento de Dados de Porto Alegre (Procempa), os espaços de acesso gratuito à internet. Em 2001, a proposta avançou para a instalação de telecentros comunitários em todas as regiões do orçamento participativo, como tentativa de promover a inclusão digital por meio da apropriação comunitária desses espaços. (MARTINS, 2015).

Em 20 de setembro de 2005, foi decretado pelo presidente da república o Projeto Cidadão Conectado – computador para todos, com o objetivo de

> *[...] promover a inclusão digital mediante a aquisição em condições facilitadas de soluções de informática constituídas de computadores, programas de computador (software) neles instalados e de suporte e assistência técnica necessários ao seu funcionamento, observadas as definições, especificações e características técnicas mínimas estabelecidas em ato do Ministro de Estado da Ciência e Tecnologia. (Planalto.gov.br, 2005, sem paginação).*

Na época, havia grande discussão entre a população sobre o que significa incluir? Porquê? E para quem? Visto que havia diversos problemas considerados mais graves, como saúde, saneamento, moradia e segurança. O desafio era demonstrar à população que a inclusão lhes traria diversos benefícios, abrindo caminhos para a profissionalização e inserção em um mercado de trabalho cada vez mais necessitado de profissionais capacitados, além de promover a cultura do indivíduo. A inclusão digital sempre esteve diretamente ligada com as políticas de inclusão social, obtendo grande atenção do governo, que chegou a prever uma meta de ter seis mil telecentros no país até o ano de 2007. (LEMOS, 2007).

Existem duas formas distintas de inclusão digital, que são classificadas como espontânea e induzida, que serão explicadas, em detalhes, a seguir.

2.3.1 Inclusão digital espontânea

É desenvolvida através de processos comuns de evolução da sociedade na era da informação, não havendo necessidade de qualquer formação para seu uso. Atividades do dia-a-dia são cada vez menos analógicas e mais digitais, como por exemplo, o uso de caixas eletrônicos, urnas eletrônicas, terminais de autoatendimento, smartphones, câmeras digitais, entre outros, são vistos como formas de evolução natural e populares. (BONILLA; PRETTO, 2011).

2.3.2 Inclusão digital induzida

A inclusão digital induzida caracteriza-se por serem executadas por universidades, empresas privadas, instituições governamentais e/ou não governamentais, sendo necessário recursos e habilidades para sua execução. São divididas em três categorias: técnica, econômica e cognitiva, explicadas a seguir. (BONILLA; PRETTO, 2011).

A categoria técnica trata do estímulo do capital técnico para manuseio do computador, seus softwares e o acesso à Internet. Inclui-se nessa categoria os cursos básicos para atividades corriqueiras como mandar e-mails, formatar documentos, navegar na web e cursos em manutenção para reparo de peças e instalação de redes. Outro ponto importante é o tratamento de questões de acessibilidade para portadores de necessidades especiais, onde podem ser manipuladas ferramentas para melhor

desenvolver sua capacidade intelectual, como simuladores de teclado, emuladores de mouse e monitores sensíveis ao toque. (BONILLA; PRETTO, 2011).

Já a categoria econômica está relacionada com a capacidade financeira em adquirir e manter computadores e custeio para acesso à rede e softwares básicos, como por exemplo projetos que buscam a redução dos custos ou formas de parcelamento facilitado para a população de baixa renda, além de formas para baratear o custo do acesso à Internet. Também está vinculada a inclusão de micro e pequenas empresas, utilizando-se de formas para alavancar os negócios, como comércio eletrônico, integração de transações e facilidade de comunicação com fornecedores e clientes, mudando assim a forma de gerir a economia e proporcionando redução de custos. (BONILLA; PRETTO, 2011).

Por fim, a categoria cognitiva é a que se refere ao processo de aquisição de conhecimento, onde é analisado mais do que o ter ou não ter, e sim o que o processo poderá trazer de diferença na vida do indivíduo, analisando as capacidades e necessidades de cada um. O processo cognitivo se torna tão ou mais importante que o técnico, pois é a partir do conhecimento que o uso das novas ferramentas poderá ganhar o status de necessidade básica a todos, alterando assim a sua qualidade de vida. (BONILLA; PRETTO, 2011).

2.3.3 Utilização de software livre como meio de integração

Primeiramente é preciso entender o conceito de software livre e o seu oposto, o chamado software proprietário. O software livre caracteriza-se pela conceituação de quatro liberdades – (1) A liberdade de executar o programa, para qualquer propósito; (2) A liberdade de estudar como o programa funciona, e adaptá-lo para as suas necessidades; (3) A liberdade de redistribuir cópias de modo que você possa ajudar o seu próximo; (4) A liberdade de aperfeiçoar o programa, e liberar os seus aperfeiçoamentos de modo que toda comunidade se beneficie. (BONILLA; PRETTO, 2011). Já o software proprietário se refere a um programa de código-fonte fechado, de propriedade da empresa que o desenvolveu, não permitindo sofrer alterações além de ser cobrado por sua utilização.

Surgiram diversos desentendimentos sobre o uso de software proprietário para ações de inclusão digital, onde atores envolvidos nessas ações julgam que a pessoa fica “presa” na utilização desses softwares, não podendo haver alterações ou

adaptações para as suas reais necessidades, tornando-se assim clientes consumindo um produto. Além disso, essa questão remete a um problema ainda mais grave, onde existem países que produzem seus softwares e equipamentos, enquanto outros simplesmente os consomem, impossibilitando seu desenvolvimento, como é o caso do Brasil. (MARTINS, 2015).

A utilização de softwares livres em projetos de inclusão digital permite que a pessoa possa aprender como aquilo funciona, analisando os códigos e realizando alterações e testes conforme sua imaginação, gerando maior autonomia e aprendizagem. (MARTINS, 2015). Os softwares livres são, em sua maioria, gratuitos, possibilitando a utilização em sua casa sem ter que gastar para isso e diminuindo também a difusão de softwares “piratas”, que são programas proprietários sendo utilizados sem a devida autorização.

Em resumo, percebe-se que o uso de software livre está mais ligado ao tema de inclusão digital, pois possibilita ao indivíduo e ao coletivo uma autonomia e liberdade no aprimoramento do que está sendo utilizado, tornando o método inclusivo.

A inclusão digital se apresenta como uma metodologia capaz de incluir pessoas de diferentes classes sociais, tornando-as iguais perante o conhecimento do mundo digital. No Brasil, embora haja muita coisa a se fazer, pode-se verificar que houve um crescimento significativo na utilização de tecnologias como a internet, conforme visto na seção anterior, e grande parte dessa evolução se deve à utilização de práticas de inclusão digital, o que comprova a sua eficácia.

2.4 A INTERNET E SEUS RISCOS

O uso da Internet se tornou algo tão comum e indispensável que muitas vezes nem se nota que algumas atividades são realizadas através dela. A sua adesão é percebida em todas as faixas etárias, algo que não era capaz de ser imaginado, como idosos utilizando serviços de Internet *banking* e interagindo em redes sociais. Do lado oposto, e como já era imaginado, crianças também cada vez mais cedo utilizam a internet de forma cotidiana acessando redes sociais, jogos *on-line* e sites diversos. Toda essa expansão se deve à facilidade de adquirir e manusear esses equipamentos, mas em meio a toda essa informação que circula sem controle, o que se deve questionar é, será que a população está preparada para utilizar essa vasta gama de recursos que a internet nos proporciona de forma segura e consciente? Nas

seções a seguir, será falado sobre as origens dos ataques através da Internet, os meios utilizados pelos criminosos e também as precauções que devem ser tomadas para evitar qualquer tipo de problema durante sua utilização.

2.4.1 A história dos crimes cibernéticos

Antes mesmo do aparecimento dos primeiros códigos maliciosos, no final da década de 50, foi desenvolvido por um grupo de programadores um jogo chamado *Core Wars*, que era capaz de se reproduzir a cada vez que era executado, sobrecarregando a memória da máquina do oponente. Os mesmos criadores também inventaram um antivírus capaz de destruir as cópias geradas pelo jogo. Essas informações somente foram descobertas em 1983 através de um artigo escrito por um de seus criadores. (WENDT; JORGE, 2013).

Existem divergências quanto ao registro do primeiro delito informático. Para alguns autores, foi no âmbito do *Massachusetts Institute of Technology* (MIT), no ano de 1964, onde um aluno de 18 anos teria sido advertido por ter cometido um ato classificado como cibercrime. Outros autores referenciam um ato realizado na Universidade de Oxford, em 1978, onde um estudante invadiu e copiou uma prova de uma rede de computadores. (JESUS, 2016). Em 1982, Richard Skrenta, com apenas quinze anos, criou o *Elk Cloner*, que foi considerado por muitos como o primeiro vírus desenvolvido para infectar computador, embora o termo “vírus de computador” tivesse sido criado somente em 1984 por Fred Cohen. Em 1986, surgiu o vírus chamado *Brain*, criado por dois irmãos paquistaneses, que atingia o setor de inicialização de disco e tinha por finalidade detectar o uso não autorizado de um software médico de monitoramento cardíaco que haviam desenvolvido. O código sofreu alterações maliciosas e passou a espalhar um vírus causando lentidão nas operações de sistemas e ocupando espaço na memória. (WENDT; JORGE, 2013).

Nas décadas de 1980 e 1990 houve grande propagação de cibercrime, outro caso interessante foi o de John Draper, que conseguiu realizar ligações gratuitamente utilizando um apito para produzir o tom de 2.600 Hz, capaz de enganar o sistema telefônico americano. Nessa época, os atos mais comuns eram disseminação de vírus, pornografia infantil, invasão de sistemas e pirataria. Também foi nessa época que se iniciou um movimento para conscientização acerca da segurança de sistemas. (JESUS, 2016).

Já com a utilização do celular, em 2004 surgiu o seu primeiro vírus, oriundo das Filipinas. Chamado de *Cabir*, ele foi criado para infectar sistemas operacionais Symbian, com o objetivo de descarregar toda a bateria de celulares que eram infectados através do *Bluetooth*. (WENDT; JORGE, 2013).

O Brasil sempre teve altos índices de criminalidade digital e, no ano de 2002, chegou a ganhar o título de maior “exportador” de criminalidade via internet. Embora houvesse altos índices de delitos, a primeira condenação efetiva ocorreu somente em janeiro de 2004, onde um jovem de dezenove anos que aplicava golpes pela Internet no Brasil e Estados Unidos teve condenação de seis anos e quatro meses. (JESUS, 2016).

2.4.2 *Hackers X crackers*

Existem duas nomenclaturas utilizadas para definir *experts* em computadores, *hackers* e *crackers*, e embora ambos possuam habilidades avançadas em programação de computadores e sistemas, há uma diferença grande entre eles, que basicamente se caracteriza pela forma como utilizam seus conhecimentos.

O termo *cracker* é utilizado para identificar quem usa seus conhecimentos em informática de forma maléfica, ilegal ou sem ética. Esse nome foi criado em torno de 1985 com a finalidade de se diferenciar do termo já utilizado *hacker*. A palavra *cracker* deriva do verbo em inglês “*to crack*”, que significa quebrar. (CASSANTI, 2014).

Dentro dessa nomenclatura, existem subdivisões que definem outras habilidades dos *crackers*, sendo as principais o *Carder*, especialista em roubar informações bancárias como números de cartão de crédito, sites de movimentação bancária, saques em caixas eletrônicos, transferência para contas de laranjas, entre outros. O *Defacer*, especialista em pichar sites adicionando imagens e mensagens, geralmente de protesto quanto a alguma ação da empresa. Os principais alvos são órgãos governamentais e empresas de grande influência na mídia. O especialista *Spammer* é o que dissemina e-mails com correntes e vírus que podem danificar seu equipamento além de roubar suas informações. Já o *Phisher* é um profundo conhecedor de falhas de sistema, aplicando golpes diversos com esses conhecimentos. Por fim, o *Phreaker* é o especialista em sistemas de segurança de companhias telefônicas, que utiliza suas técnicas para fazer ligações de graça ou conseguir créditos. (CASSANTI, 2014).

Ao contrário do *cracker*, o *hacker* é um programador com amplo conhecimento sobre sistemas, mas que não tem a intenção de causar danos à sociedade. Suas habilidades são utilizadas por muitas empresas para desenvolver softwares de segurança e descobrir vulnerabilidades, utilizando seus conhecimentos para aplicar o método reverso ao utilizado por um *cracker*. Outra característica de um *hacker* é divulgar suas descobertas de forma que mais pessoas sejam beneficiadas e possam corrigir seus sistemas antes mesmo que os *crackers* descubram como o invadir.

2.4.3 Métodos de invasão utilizados pelos atacantes

Com a ampliação da disponibilidade de ferramentas de comunicação, integração e entretenimento, houve também um aumento nas vulnerabilidades exploradas por atacantes através dessas ferramentas. Embora poucos saibam, para o usuário ser atacado ele precisa permitir isso de alguma forma, seja ela indireta ou diretamente. (CASSANTI, 2014).

A invasão de forma indireta é feita através de vulnerabilidades de softwares, configurações incorretas ou falhas de segurança de *firewalls* de rede, que são exploradas pelos atacantes. Essas falhas são exploradas por invasores que ficam monitorando a rede à procura de brechas de segurança que, na maioria dos casos, é realizada através de softwares desatualizados ou até mesmo descontinuados pelo fabricante. (CASSANTI, 2014).

Já na forma direta, o atacante utiliza meios para implantar um software malicioso em seu dispositivo, sendo os principais meios através de e-mail, mensageiro instantâneo, redes sociais, sistema de compartilhamento de arquivos, sites falsos, engenharia social e arquivos com códigos maliciosos infiltrados. (CASSANTI, 2014).

O e-mail tornou-se um meio de comunicação indispensável tanto para usuários domésticos quanto para empresas, e é através dele que ocorre um dos meios mais eficazes de invasão, através de spam, vírus e golpe de roubo de identidade. Os ataques ocorrem através de anexos com arquivos maliciosos e links com redirecionamento para sites falsos. Os aplicativos de mensagens instantâneas como *Skype, WhatsApp, Google Hangouts*, assim como as redes sociais *Facebook, Twitter Youtube e Google+* são grandes disseminadores de links falsos, que são enviados por pessoas conhecidas que já foram infectadas, aumentando as chances de que outras pessoas também o cliquem. Os sistemas de compartilhamento de arquivos *peer-to-*

peer (P2P) são utilizados para download de programas, músicas, vídeos e *e-books*, sendo o seu principal atrativo a possibilidade de baixar arquivos com direitos autorais de forma gratuita, através da pirataria. Entre os milhares de downloads disponíveis, muitos deles são programas alterados e não confiáveis. A instalação de arquivos maliciosos também pode ser feita através de arquivos PDF, pois permitem a execução de *Javascript* e *flash object* embarcados no arquivo. (CASSANTI, 2014).

Outro método bem conhecido de invasão é a engenharia social, que consiste em ludibriar a vítima de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais nos quais os criminosos tenham interesse. Geralmente, os criminosos simulam fazer parte de instituições conhecidas como bancos, sites de grandes lojas e órgãos do governo, aumentando assim a sua credibilidade. Os pontos de ataque nesse tipo de situação não são falhas de software ou hardware, mas sim as próprias fragilidades humanas, que podem ser causadas por curiosidade, falta de conscientização, ingenuidade ou medo. Elas podem ser feitas através de e-mails, mensagens SMS ou até mesmo ligações, sempre solicitando informações pessoais como senhas, número de cartão de crédito, entre outros. A engenharia social não possui um procedimento definido, tudo vai depender da criatividade do atacante e da sua capacidade de persuasão. (WENDT; JORGE, 2013).

2.4.4 Principais tipos de ataque

A prática de crimes de Internet é explorada através de vulnerabilidades de segurança nos equipamentos, softwares ou até mesmo pela ingenuidade humana, conforme descrito anteriormente. Antigamente, todas as ameaças eram tratadas como vírus de computador, porém hoje há uma gama imensa de tipos de ataques cujos principais serão explicados a seguir.

2.4.4.1 Vírus

Vírus são programas com capacidade de alterar dados ou sistemas, destruir, alterar arquivos e programas, ou mesmo executar funções inesperadas em um sistema computacional ou dispositivo informatizado. (JESUS, 2016).

No início, os vírus eram transmitidos por programadores que queriam demonstrar suas habilidades e virar celebridades no mundo *hacker*, sem que isso

causasse qualquer dano a suas vítimas. Hoje, os vírus são utilizados por atividades criminosas com o objetivo de roubar dados ou danificar sistemas de outros usuários. Uma peculiaridade dos vírus é que eles não podem se auto executar, sendo necessário que o usuário o execute para dar início à contaminação. Dessa forma, se um vírus estiver em um HD, CD ou *pen drive*, ele não terá efeito algum até que o mesmo seja executado por alguém. Um mito popular é de que os vírus podem danificar o hardware do equipamento, o que é uma farsa já que o vírus é um software incapaz de queimar ou quebrar dispositivos físicos. Existem diversos tipos de vírus, sendo os principais explicados abaixo. (CASSANTI, 2014).

a) Vírus de arquivo: são anexados ao código de um programa, normalmente utilizam-se de arquivos executáveis como .EXE, .MSI, e seu efeito inicia quando os arquivos são executados. (CASSANTI, 2014).
b) Vírus de *boot:* são considerados os precursores de todos os demais vírus, eles se fixam na partição de inicialização de sistemas, impedindo-o de iniciar. Eles se espalham através de disquetes, CDs, DVDs e *pen drives*, e sua infecção ocorre quando estão conectados ao computador durante a sua inicialização. (WENDT; JORGE, 2013).
c) Vírus *time bomb*: caracteriza-se por sua ativação ser feita em determinada data e horário estipulado pelo programador que o desenvolveu. Dessa forma, a vítima não percebe nada na hora que o executou, dificultando a descoberta de sua real origem. Também é conhecido como bomba-relógio ou gatilho. (WENDT; JORGE, 2013).
d) Vírus de macro: são programas escritos na linguagem de macro de um aplicativo como por exemplo o Word e Excel da Microsoft. Para se tornarem ativos, eles precisam que a macro seja executada, alterando os componentes do programa e causando operações inesperadas ou se recusando a executá-las. Após a infecção, os demais arquivos abertos através desse programa também são afetados. (CASSANTI, 2014).

2.4.4.2 *Worm*

Também conhecido como verme, caracteriza-se por residir na memória ativa do computador e se replicar automaticamente, não sendo necessária nenhuma ação do usuário. Ele se instala geralmente em computadores e programas que possuem

vulnerabilidades, sendo a principal delas a de estar desatualizado. Os *Worms* consomem muitos recursos do computador, degradando a sua utilização e podendo também lotar o seu disco rígido, devido à quantidade de cópias geradas de si mesmo. (WENDT; JORGE, 2013).

2.4.4.3 Cavalo de troia ou *trojan*

O cavalo de troia é um arquivo aparentemente inocente entregue através de algo conhecido como por exemplo um cartão digital, um álbum de fotos, protetor de tela ou jogos. O elemento principal é executado normalmente enquanto o elemento malicioso trabalha de forma oculta ao usuário. (CASSANTI, 2014).

Após infectado, o invasor pode se tornar administrador da máquina e assim alterar outras configurações de segurança, deixando o computador ainda mais vulnerável. Também é possível que ele capture informações do usuário e as envie por e-mail para o criminoso. (JESUS, 2016).

2.4.4.4 *Keylogger* e *screenlogger*

O *keylogger* é uma técnica que consiste na captura dos caracteres digitados no teclado, armazenando-os em arquivo e enviando ao atacante. Os sites de bancos ao perceber o risco da captura de senhas dos usuários, desenvolveram a técnica de selecionar as letras e números que correspondem à senha através da seleção do mouse, isso fez com que os criminosos criassem o *screenlogger*, que captura as telas do usuário assim como pode filmar toda a utilização do mouse. (JESUS, 2016).

A utilização dessa ferramenta também é feita por organizações com a finalidade de monitorar seus usuários, por pais que querem saber o que seus filhos estão fazendo ou até mesmo pelo governo para fins de espionagem. (CASSANTI, 2014).

2.4.4.5 *Botnets*

Botnets são redes de computadores compostas por diversos *bots,* que são sistemas instalados por criminosos em estações servidores que respondem a comandos e funções enviados a ele. Os computadores se tornam “zumbis” e, devido

à grande quantidade de computadores invadidos, a descoberta da origem se torna difícil. (JESUS, 2016).

Uma das grandes utilidades das *Botnets* é para promover ataques *Distributed Denial of Service* (DDoS), em que diversos computadores encaminham solicitações para um determinado servidor, sobrecarregando-o e tornando o serviço indisponível. Para fins de investigação, a polícia primeiro identifica um computador utilizado para o ataque e depois aplica a engenharia reversa através da análise dos códigos maliciosos, descobrindo assim para onde estão indo as informações ou de onde elas vêm. (WENDT; JORGE, 2013).

2.4.4.6 *Deface*

A palavra *deface*, oriunda do inglês *defacing*, é utilizada para caracterizar aqueles que desfiguram sites, blogs ou perfis em redes sociais. Seus autores têm como propósito expor e defender suas ideias, dando destaque ao grupo que pertence. Suas convicções podem ser religiosas, filosóficas ou políticas e expressam a sua crítica através de mensagens e imagens. Em alguns casos, informações públicas são roubadas de sites conhecidos e divulgadas para a população com a finalidade de denegrir a imagem da organização. (WENDT; JORGE, 2013).

2.4.4.7 *Hijacker*

O significado da palavra inglesa *hijack* é sequestrar, e nesse caso os criminosos sequestram os navegadores de internet, direcionando-os para sites que não foram digitados, alteram sua configuração de página inicial, abrem *pop-ups* na tela que são novas janelas com propagandas, conteúdo pornográfico ou de sites fraudulentos. Eles utilizam-se de falhas de segurança em controles ActiveX e modificam registros do Windows para passar a responder da forma como desejam. (WENDT; JORGE, 2013).

2.4.4.8 *Spywares*

São programas espiões com a finalidade de coletar informações sobre o usuário, seus costumes de acesso e seus gostos. As informações são enviadas pela

Internet para fins de publicidade ou coleta de informações pessoais. São parecidos com os chamados *cookies* de sites que armazenam preferências dos usuários como idioma utilizado na página, fonte, cor, entre outros, porém os *spywares* utilizam essas ações de forma maliciosa. Os *spywares* tem ação de propagação semelhante a dos cavalos de troia, porém se difere por não ter o objetivo de que o sistema do usuário seja manipulado ou dominado por atacantes. (CASSANTI, 2014).

2.4.4.9 *Adwares*

São programas distribuídos de forma gratuita para download e patrocinados por anúncios de empresas. Quando instalado, além de ter o programa principal, é instalado um componente adicional que é alimentado por propaganda. Esse complemento pode surgir em forma de pop-up, adicionando uma nova barra de ferramentas ao navegador, alterando a página inicial ou redirecionando a vítima para outros sites. Em alguns casos, pode apresentar anomalias no sistema, incompatibilidades ou até mesmo atrapalhar o funcionamento do sistema operacional. (CASSANTI, 2014).

2.4.4.10 *Rootkits*

O termo *rootkit* vem da junção das palavras root, que significa usuário de computador que tem controle total sobre o computador nas plataformas Unix, e *kit* que se refere aos programas utilizados por usuários do sistema operacional Linux e que permitem o controle total sobre um sistema comprometido. Esses programas ficam ocultos no computador e podem ser instalados de forma local por alguém que tenha acesso ao computador ou remotamente através de outro computador. (CASSANTI, 2014).

A maioria dos antivírus não consegue detectá-lo pois suas chaves permanecem ocultas no registro e seus processos no gerenciador de tarefas não são localizados. No Windows, o arquivo malicioso pode gerar mensagens de erro geralmente acusando arquivo inexistente ao tentar abrir algum programa. Outro problema destes arquivos é que eles podem conter outros *malwares* infiltrados como *keylogger* e vírus. (WENDT; JORGE, 2013).

2.4.4.11 *Backdoor*

É um utilitário de administração remota que permite que o computador seja controlado através de uma rede ou internet. Um *backdoor* consiste de um cliente e um servidor, sendo o servidor a máquina atacada e o cliente o atacante. Alguns de seus recursos são permitir criar, apagar, executar comandos, alterar configurações do sistema e registros do Windows, alterar configurações de desligamento, roubar informações de *login*, captura de teclado e tela e até acionar a webcam para monitorar o que se passa na residência da vítima. (CASSANTI, 2014).

2.4.4.12 *Hoax*

São mensagens falsas divulgadas na internet geralmente relacionadas com fatos inexistentes e alarmantes como necessidade de ajuda financeira para entidades ou pessoas doentes, pessoas desaparecidas, projetos de lei que serão votados, notícias sobre conspiração, desastres, mensagens religiosas e programas de computador gratuito que se tornarão pagos. Muitas vezes, é oferecido um prêmio para quem encaminha a suposta mensagem para um certo número de pessoas, isso é chamado de corrente. Além de lotar as caixas de e-mail de usuários, causam transtornos e prejuízos para pessoas crédulas e denigrem a imagem de empresas com informações falsas. Esse tipo de mensagem também é comum em redes sociais e aplicativos de mensagens instantâneas. (WENDT; JORGE, 2013).

2.4.4.13 *Phishing*

O termo é originado do verbo inglês *to fish* que significa pescar e caracteriza a conduta de pesca de informações de usuários. Inicialmente, a palavra *phishing* era usada para definir a fraude de envio de e-mail não solicitado pela vítima, que era estimulada a acessar sites fraudulentos. Uma de suas características é que as mensagens estimulam ser de pessoas ou instituições legítimas como bancos, órgãos governamentais ou empresas. Hoje, a palavra também é utilizada para definir a conduta de pessoas que encaminham mensagens com a finalidade de induzir vítimas a enviar informações para os criminosos. (WENDT; JORGE, 2013).

A técnica de *phishing* já é bem conhecida e a sua conscientização é promovida por grandes provedores de e-mail como Google e Yahoo. As principais ações envolvendo *phishing,* utilizadas pelos atacantes, são mensagens com links para programas maliciosos, ofertas de grandes lucros, fotos de celebridades, notícias sobre tragédias, *reality* shows, orçamentos e cotações de preço, informações de cobrança em sites de comércio eletrônico, telefonia e provedores de acesso à internet, informações sobre inclusão do seu nome no SPC e Serasa, avisos de órgãos do governo e instalação de módulos de segurança para a realização de transações bancárias. (CASSANTI, 2014).

Um recurso bastante utilizado pelos criminosos para disfarçar suas ações é o uso de encurtadores de URL, onde o link com informações sobre o site é encurtado em poucas letras, evitando que o usuário saiba para onde realmente o link está apontando. (WENDT; JORGE, 2013).

2.4.4.14 DoS

O *Denial of Service* ou ataque de negação de serviço se caracteriza por sobrecarregar um serviço informático até que o mesmo fique indisponível. Esses ataques podem ser de diversas formas, como por inundação de pacotes, que consiste no envio de diversos pacotes de rede com o objetivo de congestionar o link e impossibilitando que usuários legítimos façam o acesso. O ataque por problemas de protocolo explora alguma deficiência no protocolo utilizado para comunicação com os seus clientes. Há também o ataque por problema de codificação que explora vulnerabilidades do software como por exemplo o *Buffer Overflow* que transborda de dados o software até ultrapassar os limites de memória configurados, isso ocorre por uma falha de desenvolvimento onde o programador não realizou nenhum tipo de checagem para evitar que isso ocorra. Já o ataque de disco consiste em enchê-lo de informações até que o faça parar de funcionar. Por fim, e não menos importante, existe o ataque de DDoS, muito utilizado atualmente e que consiste em utilizar diversas máquinas para realização de ataque simultâneo de inundação de pacotes, visto que o tráfego gerado por várias máquinas é muito maior do que se houvesse apenas uma. (JESUS, 2016).

2.4.4.15 Quebra de senhas

Existem três tipos conhecidos de ataques por quebra de senhas, um deles é o método de força bruta que consiste em tentar todas as combinações possíveis, havendo ferramentas que fazem isso de forma automatizada. Outro método é o ataque de dicionário que testa palavras de dicionário utilizadas com frequência. O terceiro método é o chamado *rainbow table,* destinado à quebra de senhas criptografadas, submetendo os *hashs* a uma tabela de *hashs* já calculados para realização de comparações. (JESUS, 2016).

2.4.4.16 *SQL injection*

Essa técnica consiste em alterar parâmetros ou instruções que são executadas sobre uma ou mais tabelas de um banco de dados, por meio da linguagem *Structured Query Language* (SQL), permitindo o acesso indevido, alteração ou destruição de informações. (JESUS, 2016).

2.4.4.17 *Sniffer*

Essa técnica tem a finalidade de monitorar todo o tráfego de rede TCP/IP, de modo que todos os dados transmitidos possam ser interceptados e analisados. Caso o usuário esteja navegando em sites sem criptografia (HTTP), todas as informações podem ser visualizadas, inclusive senhas de acesso. Essa captura é realizada por programas chamados *sniffers* e podem ser utilizados tanto por empresas para monitorar as atividades de seus funcionários como por criminosos interessados em informações como *logins*, senhas, sites acessados e conteúdos sigilosos trocados por e-mail. (WENDT; JORGE, 2013).

2.4.4.18 *Ransomware*

O *ransomware* é um dos *malwares* mais temidos pelos usuários, pela maneira que afeta suas vítimas. Em suas primeiras ocorrências, esse *malware* bloqueava a tela do computador deixando exposta uma mensagem exigindo pagamento para que o computador fosse liberado. Com o seu sucesso, surgiram diversas novas variantes

e, consequentemente, mais perigosas. As novas versões são capazes de criptografar os arquivos do seu dispositivo exibindo informações de como proceder para receber a chave de desbloqueio. O pagamento geralmente é solicitado através de *Bitcoins*, uma moeda eletrônica independente de qualquer autoridade central. É bom lembrar que o pagamento não garante que seus arquivos sejam desbloqueados, afinal como dificilmente é possível identificar o criminoso, também não há como cobrá-lo. (TREND MICRO, 2015).

O método mais comum de infecção é através de e-mails de *phishing,* onde o usuário é atraído a clicar em links que direcionam ao download do *ransomware*. Atualmente, também é comum o ataque através de sites populares que foram invadidos e tiveram seus códigos fonte e links alterados.

2.4.5 Crimes Virtuais

Ao contrário do que se imagina, os crimes virtuais não são praticados apenas por atacantes com conhecimento sofisticado em informática, a cada dia é mais comum os crimes através de e-mails e redes sociais. Os atacantes são estimulados pela falsa ideia de que ficarão impunes aos delitos por eles terem sido realizados pela internet, mas como qualquer outro crime, as penas são as mesmas independente do meio utilizado para a prática. A seguir, conforme CASSANTI (2014), são mencionados alguns exemplos de crimes e leis que podem ser utilizados nos meios eletrônicos:

a) Uso indevido de imagem: postar fotos de terceiros sem a autorização pode levar a processo. O artigo 5º Inciso X da Constituição Federal diz que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando direito à indenização pelo dano material ou moral”.
b) Insultos: falar mal ou insultar alguém numa rede social pode gerar processo com base no Artigo 140 do Código Penal, que pune “a injúria que ofende a dignidade ou decoro”.
c) Calúnia: inventar histórias nas redes sociais pode ser enquadrado no Artigo 138 do Código Penal.
d) Difamação: associar uma pessoa a um fato que ofenda a sua reputação. Artigo 139 do Código Penal.
e) Ameaça: intimidar ou amedrontar uma pessoa, seja por telefone, de forma escrita, e-mails ou redes sociais. Artigo 147 do Código Penal.

f) Divulgação de segredo: revelar segredos de terceiros na Internet, ou de documentos/correspondência confidencial que possam causar dano, pode levar a processo com base no Artigo 153 do Código Penal.
g) Furto: utilizar dados de conta bancária de outrem para desvio ou saque de dinheiro. Artigo 155 do Código Penal.
h) Dano: enviar vírus, realizar ataques de DoS e DDoS ou outro que destrua equipamentos ou seu conteúdo. Artigo 163 do Código Penal.
i) Cópia não autorizada: copiar ou plagiar obras de terceiros, violando seus direitos autorais. Artigo 184 do Código Penal.
j) Favorecimento da prostituição: Artigo 228 do Código Penal.
k) Apologia de crime: criar comunidades virtuais para ensinar como fazer “trambiques” ou divulgar ações ilícitas. Artigo 287 do Código Penal.
l) Falsa identidade: criar um perfil falso em uma rede social ou blog pode levar a processo judicial com base no Artigo 307 do Código Penal.
m) Preconceito ou discriminação: comentar em chats, e-mails, blogs e outros de forma negativa, sobre raças, religiões, etnias. Artigo 20 da Lei 7.716/89.
n) Pedofilia: troca de informações ou imagens envolvendo crianças ou adolescentes. Artigo 241-A/241-B/241-C/241-De/241-E da Lei nº 8.069/90 ECA.
o) Interceptação de comunicações de informática: monitoramento de rede sem aviso prévio. Artigo 10 da Lei 9.296/96.
p) Crimes contra software (“pirataria”): usar cópia de software sem licença. Artigo 12 da Lei 9.609/98.
q) Negligência: deixar os filhos navegarem na internet sem supervisão, sem criar regras para o uso consciente, seja dentro ou fora de casa. Artigos 932, Incisos I e IV e 1.634, Incisos I e V do Código Civil, assim como os artigos 3º e 4º do Estatuto da Criança e do Adolescente.

Dentre as diversas práticas de delitos informáticos, cabe salientar a importância de dois deles que vêm se propagando de forma descontrolada e causando grande preocupação para pais e educadores, são eles o *cyberbullying* e o *sexting*.

2.4.5.1 *Cyberbullying*

O *cyberbullying* é uma derivação do *bullying*, que consiste em insultos, intimidações, humilhação e violência entre crianças e adolescentes, mas que nesse novo formato é praticado de forma virtual. São utilizadas ferramentas tecnológicas como celulares e câmeras digitais em ambientes como Internet e redes sociais para disseminar tais conteúdos. Diferente do *bullying* que ocorre de forma presencial, o *cyberbullying* pode tomar proporções que nem mesmo o agressor imagina, pela rapidez com que esse tipo de conteúdo é espalhado na Internet. (NETICA.ORG.BR, 201-).

Embora esse seja um problema mundial, é pouco conhecido pelo grande público e muitas vezes subestimado pelos pais por acharem que se trata de uma brincadeira. (NETICA.ORG.BR, 201-). A justiça vem decidindo que a responsabilidade por esses delitos é dos pais por não terem educado seu filho de forma correta ou não terem acompanhado o que ele faz na Internet. (CASSANTI, 2014).

2.4.5.2 *Sexting*

O termo se originou da junção de duas palavras em inglês: “*sex*” (sexo) e “*texting*” (envio de mensagens). A prática consiste no envio de imagens ou vídeos com conteúdo sexual através do celular para grupos de redes sociais, e-mail ou salas de bate-papo e comunicadores instantâneos. O envio é feito pela própria pessoa, ou seja, a informação não é roubada da vítima, ela o envia com seu próprio consentimento. (CASSANTI, 2014).

Muitos jovens que praticam essa atividade sequer ouviram falar da expressão *sexting*. O *sexting* também está associado a práticas criminosas como extorsão, *cyberbullying*, danos à honra, intimidade e imagem, e pornografia infantil. Os danos gerados a uma pessoa que tenha suas fotos e vídeos expostos na Internet sem controle podem ser irreversíveis, gerando ansiedade, depressão, baixa autoestima, trauma, humilhação, isolamento social e, em alguns casos extremos, pode levar ao seu suicídio. (CASSANTI, 2014).

2.5 PREVENINDO ATAQUES NA INTERNET

Cientes de que é impossível evitar o uso de recursos providos pela Internet, resta estabelecer mecanismos de prevenção para assegurar uma utilização sadia e sem imprevistos. Para isso, a melhor forma é ter conhecimento sobre os recursos que estão sendo utilizados, como eles funcionam e de que forma é possível serem violados. Além disso, é possível contar com o uso de ferramentas que analisam e auxiliam em situações de risco, protegendo seus dados e equipamentos. A seguir, serão expostas algumas das ferramentas de prevenção disponíveis.

2.5.1 *Firewall*

O termo em inglês *firewall* significa “parede de fogo”, funcionando como uma defesa capaz de bloquear tráfego de dados indesejados e liberar acessos bem-vindos. Essa solução de segurança pode ser baseada em hardware, software ou em ambas, e a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas. As regras podem ser inicialmente baseadas em dois princípios, todo o tráfego é bloqueado, exceto o que está explicitamente autorizado, ou todo o tráfego é permitido, exceto o que está explicitamente bloqueado. (ALECRIM, 2013).

Para uso doméstico, existem os chamados *firewalls* pessoais, que são *firewalls* mais simples, mas que certamente ajudam a proteger seus dispositivos. A maioria dos sistemas operacionais já possuem um firewall nativamente instalado, como é o caso das distribuições Linux, Windows ou Mac OS, mas para que se possa ter uma configuração mais flexível e eficiente é necessário instalar um software de *firewall* externo, havendo versões disponíveis gratuitas e pagas. (ALECRIM, 2013).

2.5.2 Antivírus

O antivírus pode ser considerado o item mais básico de segurança em dispositivos de informática, e ao contrário do que muitos acreditam, eles são necessários também em sistemas operacionais Linux e Mac OS, embora a maioria dos ataques sejam específicos para o sistema operacional Windows. (WILLIAMS, 2014).

Antivírus é um programa de segurança capaz de proteger o sistema de infecções por *malwares*, incluindo vírus, *worms*, cavalos de troia, entre outros. Em geral, existem duas maneiras para o software identificar um *malware*: detecção de assinatura e detecção de comportamento. O método por detecção de assinatura faz uma varredura no computador em busca de características ou assinaturas de programas maliciosos conhecidos. Por isso, é muito importante ter o antivírus sempre atualizado pois diariamente surgem milhares de novas ameaças e os fabricantes disponibilizam atualizações assim que as mesmas são identificadas. Já no método de detecção por comportamento, o antivírus monitora os softwares instalados no computador e quando eles agem de forma suspeita tentando alterar arquivos protegidos do sistema ou modificar um programa, é gerado um alerta para o usuário, identificando dessa forma novos tipos de *malwares* que ainda não estão na biblioteca. O problema com esse tipo de alerta é sobre os falsos positivos, ou seja, aqueles comportamentos que o antivírus considera suspeito, mas que na verdade são legítimos. Com a geração de diversos alertas, o usuário pode se tornar insensível a eles, acabando por aceitar a execução de ataques. Além disso, geralmente quando o antivírus detecta o *malware,* ele já foi executado em seu equipamento e você não consegue saber quais ações ele já tomou. (WILLIAMS, 2014).

Recomenda-se usar antivírus de fabricantes conhecidos para não cair em golpes de antivírus falsos, os chamados *scareware*. Os *scarewares* se passam por antivírus reais simulando varreduras em seu dispositivo, informando sobre possíveis problemas e sugerindo a compra de seu software para solução. Outra observação importante é não ter mais de um antivírus instalado no equipamento pois eles podem entrar em conflito e deixá-lo em risco, além de comprometer o seu desempenho. (CASSANTI, 2014).

2.5.3 Antispyware

Embora muitos antivírus modernos já venham com funções antispyware integradas, existem também softwares específicos que em alguns casos podem trazer uma proteção maior. O que difere um antispyware de um antivírus é a classe de programas que eles removem, onde podem haver configurações específicas para cada tipo de ataque. (CASSANTI, 2014). O objetivo do antispyware é detectar e remover *spywares*, *adwares*, *keyloggers*, *trojans* entre outros *malwares*.

A medida que novas tecnologias de proteção são desenvolvidas, também novas formas de ataques são criadas, tornando impossível ter a garantia de um software de proteção 100% seguro. Dessa forma, o maior aliado na proteção de seus dados e equipamentos são os próprios usuários.

2.6 DICAS E BOAS PRÁTICAS

Existem diversas ferramentas que auxiliam na detecção e proteção de seus dados e equipamentos, porém conforme já mencionado, elas não garantem uma total segurança. A adoção de práticas conscientes, somadas a pequenas atitudes rotineiras, preservam nossas informações no mundo virtual. A seguir, serão demonstrados alguns exemplos dessas práticas.

2.6.1 Compartilhamento de informações

Todos possuem informações armazenadas online, mesmo que não saibam. A cada compra realizada, seja ela de forma online ou presencial, é disponibilizado para a empresa informações pessoais as quais são armazenadas em seus sistemas e que alimentam bancos de dados, para posteriormente gerarem relatórios sobre os históricos de compra, além de alimentar serviços de vendas e marketing. Um exemplo claro disso são os cartões de fidelidade disponibilizados por supermercados, que concedem descontos por sua utilização, mas que também armazenam todos seus hábitos de compras. (CHERRY, 2014).

É de fundamental importância saber quais informações são rastreadas pelas empresas para poder se proteger contra o roubo de dados e identidade, e assim poder decidir quais dessas informações devem ser passadas ou não. Em muitos casos, não é preciso passar informações reais, como por exemplo no processo de uma compra onde é solicitado o número do telefone, você pode preencher o campo com vários zeros, evitando assim o seu rastreamento. Outro exemplo é quando é solicitado o e-mail para cadastro em sites, nesses casos é possível gerar um e-mail temporário, evitando que seu e-mail real seja entregue a empresas que vendem assinaturas de revistas, produtos ou até mesmo ser inserido em listas de *Spam*. Em uma consulta simples em buscadores, é possível encontrar diversos sites que disponibilizam esse serviço. (CHERRY, 2014).

Existem duas razões principais pelas quais as empresas armazenam seu perfil de consumidor, a primeira delas é conhecer seu público-alvo e assim poder direcionar propagandas e ofertas que sejam de seu interesse. A segunda razão é para vender essas informações a outras empresas que têm a intenção de enviar propagandas. Um exemplo simples é o *Facebook*, onde são disponibilizadas diversas informações que facilitam aos anunciantes a exibição de anúncios no site da rede social. (CHERRY, 2014).

Muitas empresas demonstram os termos de proteção de informações do cliente em suas políticas, porém não há como garantir que essas informações não estejam sendo acessadas indevidamente por seus funcionários. Companhias de seguro, cartão de crédito, consultórios médicos, serviços de folha de pagamento, ou até o departamento de recursos humanos e financeiros da empresa onde você trabalha, possuem informações valiosas e de uso restrito, algumas inclusive são protegidas por leis de confidencialidade, como é o caso das informações médicas. (CHERRY, 2014).

A maioria dos sites hoje trabalha com o armazenamento de *cookies*, que são pequenos arquivos de texto armazenados em seu computador, contendo informações sobre o visitante. Através deles é possível, por exemplo, rastrear o usuário enquanto ele navega. Para evitar esse tipo de comportamento, todos os navegadores possuem configuração para desativá-las. Outra dica em relação à navegação é o uso do modo privativo dos navegadores, que quando habilitado desabilita a criação de *cookies*, arquivos temporários de Internet e histórico de navegação. (CHERRY, 2014).

2.6.2 Redes sociais

Existem regras básicas para o compartilhamento de informações nas redes sociais que, se não forem cumpridas, podem gerar transtornos muitas vezes irreversíveis. Segundo Cherry (2014, p.93), essas seriam algumas recomendações básicas sobre o que não deveria ser compartilhado na Internet:

> *Nenhuma informação pessoal.*
> *Nada que você não gostaria que seus avós vissem.*
> *Nada que você não gostaria que seus pais vissem.*
> *Nada que você não gostaria que seus filhos vissem.*
> *Nada que você não gostaria que seu chefe visse.*
> *Nada que você não gostaria que sua seguradora visse.*

Nada que você não gostaria que o governo visse.

Ao compartilhar informações em redes sociais, em questões de minutos não há mais nenhum controle sobre elas. Um exemplo são as publicações no *Facebook*, onde mesmo que após publicá-las haja um arrependimento e seja feita a exclusão, caso algum amigo tenha compartilhado a mesma informação, ela ficará disponível até que todos a excluam. Para auxiliá-lo a proteger as informações compartilhadas online, a maioria das redes sociais possuem configurações de privacidade onde é possível ajustar quem poderá vê-las. A configuração ideal é deixar que somente seus amigos possam ver tais informações e é claro que cabe a cada usuário selecioná-los e não adicionar ninguém que não conheça. (CHERRY, 2014).

2.6.3 Utilização de Senhas

Senhas são intransferíveis, particulares e sigilosas, sendo o principal meio de proteção contra o acesso não autorizado. Estudos indicam a lista de senhas mais utilizadas pelos usuários, sendo a primeira delas a palavra *password* (senha em inglês), seguida por 123456 e 12345678. Logo após aparecem senhas como abc123 e qwerty (a sequência das seis primeiras letras de qualquer teclado alfabético). (CASSANTI, 2014).

Existem quatro grupos de caracteres em um teclado padrão: letras maiúsculas, minúsculas, números e caracteres especiais como: !, @, #, $, %, &, *. Para que uma senha seja considerada segura, é necessário conter ao menos três desses quatro tipos de caracteres. Outro fator importante é a quantidade de caracteres utilizados na senha, sendo que o mínimo deve ser oito dígitos. Quanto maior for a senha mais tempo um atacante demora para conseguir quebrá-la pelos chamados ataques de força bruta, onde são utilizados scripts que testam todas as combinações possíveis. Mais uma dica sobre o uso de senhas é ter uma específica para cada site, dessa forma caso algum deles sofra um ataque por um *cracker*, não haverá a exposição das senhas de todos os sites navegados. (CHERRY, 2014).

Atualmente, a maioria dos sites estão disponibilizando o recurso de verificação em duas etapas, que consiste em primeiramente a digitação da senha e após uma verificação extra que pode ser um número gerado aleatoriamente por um *token*, aplicativo de celular, de computador ou uma mensagem de texto enviada para

o celular. O método é eficaz pois o número gerado só pode ser utilizado uma vez e tem um prazo curto de validade, geralmente um minuto. (CHERRY, 2014). Sistemas ainda mais modernos utilizam leitura biométrica, identificação facial e até leitura de íris em substituição à utilização de senhas.

2.6.4 Tornar o roteador e Wi-Fi mais seguros

Redes domésticas mal configuradas podem permitir que um cracker conecte em sua rede e instale algum vírus ou qualquer programa maléfico. Além disso, eles podem utilizar da sua conexão para invadir outras redes, acessar conteúdos proibidos, fazendo com que você responda por esses atos. (CHERRY, 2014).

Para tornar sua Wi-Fi mais segura, um fator obrigatório é a utilização de senha de acesso. Embora não pareça necessário, pois geralmente as redes sem fio tem um curto alcance, nada impede que alguém que esteja passando pela sua casa verifique uma rede aberta e utilize dessa conexão. Senhas complexas e longas dificultam ainda mais em tentativas de roubo. Existem três tipos de criptografia que podem ser configuradas nos roteadores, são elas a *Wired equivalent privacy* (WEP), que é considerada extremamente insegura, a *Wi-Fi protected access* (WPA) e a WPA2. Recomenda-se o uso do tipo de criptografia WPA2 por ser a mais segura. (CHERRY, 2014). Em regiões onde as casas são perto uma das outras, ou no caso de apartamentos, também é importante não identificar a pessoa ou a família através do nome da rede Wi-Fi, devendo-se colocar qualquer nome aleatório que não faça referência a você.

As configurações do roteador também devem ser alteradas a fim de garantir maior segurança pois caso alguém consiga conectar em sua rede, facilmente terá acesso ao endereço do roteador e caso não tenha sido feito a troca do usuário e senha padrão (admin/admin) o mesmo poderá alterá-la tornando a Wi-Fi inacessível. Caso isso ocorra, a única solução é reiniciar o roteador para a sua configuração de fábrica e configurá-lo novamente.

2.6.5 Criptografia

A prática de criptografia consiste em tornar os dados criptografados ilegíveis a uma pessoa que não possua a senha ou chave de acesso que foi previamente

configurada. As criptografias utilizadas hoje são praticamente indecifráveis, embora não exista nenhuma criptografia totalmente indecifrável. A segurança se dá pelo tempo necessário para poder quebrar a senha que pode ser incalculável. Essa é a melhor maneira de proteger dispositivos contra roubo ou perda pois, caso não haja essa configuração, os dados podem ser facilmente roubados removendo o disco rígido do dispositivo e o conectando em outro computador. (CHERRY, 2014).

Sistemas operacionais como o Windows da Microsoft e o Mac OS X da Apple possuem ferramentas nativas de criptografia com configurações específicas. No Windows, o nome da ferramenta é *BitLocker*, que criptografa os dados do disco rígido. Nas versões do Windows Vista e 7 é possível somente criptografar o disco inteiro, já a partir do Windows 8 é possível configurar a criptografia para pastas específicas. Ao ativar o *BitLocker* será solicitada a configuração da chave de recuperação, utilizada para acessar os arquivos caso o *BitLocker* apresente falhas na decriptografia dos dados, além da senha padrão que será necessária a cada acesso à unidade criptografada. É possível salvar a chave de recuperação em uma conta Microsoft, em arquivo ou até mesmo imprimir. O processo de criptografia para o sistema Mac OS X é bem semelhante, o nome do software responsável é o *FileVault*. Em ambos os sistemas, é importante lembrar de nunca salvar a chave de recuperação no próprio dispositivo pois se ela for perdida não será possível acessar seus dados e, consequentemente perderá tudo no computador. (CHERRY, 2014).

2.6.6 Sistemas operacionais e demais programas

É de extrema importância manter atualizado o sistema operacional e demais softwares instalados em seus dispositivos, isso garante que todas as atualizações de segurança estão instaladas, protegendo contra vírus e demais ataques. É comum as primeiras versões de programas conterem erros, que muitas vezes são vistos pelos próprios usuários, por isso é importante ter configurado as atualizações de forma automática, garantindo assim a sua instalação imediata. A utilização de softwares originais garante a obtenção de atualizações, algo que não ocorre quando se está usando um software “pirata”. (CASSANTI, 2014).

2.6.7 Compras pela Internet

Muitos são os atrativos em fazer compras pela Internet. Em apenas alguns minutos é possível pesquisar sobre produtos, comparar preços e comprar itens de todas as categorias imagináveis, tudo isso sete dias por semana, 24 horas por dia e sem enfrentar filas. (CASSANTI, 2014).

Este é um mercado que só cresce, tanto para consumidores quanto para golpistas, por isso é necessário ter alguns cuidados para fazer compras com segurança. Itens populares ou da moda são um grande atrativo e consequentemente são os mais utilizados pelos golpistas, por isso desconfie sempre de preços muito baixos e procure sempre pesquisar sobre a loja onde está comprando. (CASSANTI, 2014).

Evite utilizar *lan houses* para esse tipo de atividade e nunca forneça informações bancárias para outras pessoas. Antes de finalizar uma compra, sempre pesquise se existem reclamações sobre a loja, essas informações podem ser encontradas no site www.reclameaqui.com.br. Uma característica de site seguro é o que possui seu endereço iniciado por https://, isso indica que ele utiliza criptografia na troca de dados. Além disso, a existência do ícone de um cadeado no início da barra de endereços significa que o site utiliza certificado digital. É claro que somente isso não garante a segurança pois o certificado pode ser falso, por isso é necessário analisar a maior quantidade de informações possíveis a fim de tornar a compra mais segura. (WENDT; JORGE, 2013).

Outra dica é sempre verificar os termos de negociação, o prazo de entrega, o endereço físico da loja, as formas de pagamento, garantia e condições de troca. Em caso de devolução ou troca do produto, sempre peça antecipadamente quem deverá arcar com os custos. Sempre guarde todos os registros das transações on-line, e-mails trocados com o vendedor, descrição e valores a fim de poder comprovar o que estava sendo comprado. Em caso de problemas com a compra, tente o estorno do valor pago através da empresa de cartão de crédito ou intermediária de pagamento e lembre-se de registrar queixa contra a loja no Programa de Proteção e Defesa do Consumidor (Procon) de sua cidade. (CASSANTI, 2014).

2.6.8 Operações bancárias

Da mesma forma que as compras pela Internet, as operações bancárias também trazem agilidade, praticidade e comodidade, logo os mesmos cuidados devem ser tomados. Além dos cuidados já mencionados, são necessários alguns cuidados extras como, verificar o autor antes de instalar os módulos de proteção das instituições. Procurar sempre digitar o endereço do banco de forma manual na barra de endereços, nunca clicando em links enviados por e-mail, SMS ou redes sociais. Verificar se os links dentro do site do banco não estão direcionando para outros sites, para isso basta posicionar o cursor do mouse sobre o link e ver a informação na parte inferior do navegador antes de clicar. Digite a senha de acesso ao banco errada no primeiro acesso, se o erro for indicado o site está correto, caso contrário então o site é falso, visto que os golpistas não têm como conferir a informação pois querem apenas roubar sua senha. Lembre-se de clicar no botão sair sempre que concluir suas atividades no site, para garantir o encerramento de sua sessão. (CASSANTI, 2014).

2.6.9 Bloqueadores de anúncios e *pop-ups*

Essas ferramentas são basicamente complementos instalados nos navegadores que tem a finalidade de bloquear a exibição de anúncios e *pop-ups* nas páginas da web. Elas evitam que o usuário clique em links indesejados que podem apontar para páginas fraudulentas, além de tornar a exibição mais limpa e fluída. Alguns sites verificam a utilização da ferramenta e o impedem de visualizar o conteúdo da página até que o bloqueador seja desativado, isso ocorre pois elas necessitam que suas propagandas apareçam pois são sua fonte de renda. Por isso, é possível desativar o bloqueador para páginas específicas, adicionando os sites nas listas de exceções permitidas do bloqueador. O complemento mais utilizado no mundo é o *AdBlock*, que possui versões disponíveis para Chrome, Firefox, Android e Opera.

2.6.10 Links encurtados

Os links ou *Uniform Resource Locator* (URL) encurtados surgiram para solucionar o problema de que redes sociais como o Twitter, por exemplo, limitam o número de caracteres por postagem, e muitas vezes o link para um vídeo ou página

desejada pode ultrapassar esse limite. Além disso, URLs longas em e-mails e mensagens SMS podem ficar “quebradas”, caso não sejam corretamente inseridas, inviabilizando o acesso ao link. Para essa finalidade, surgiram os sites que encurtam a URL, abreviando-a em poucas letras e facilitando o acesso. Basicamente, o site fará o redirecionamento do link encurtado para o link real que foi configurado. (CRUZ, 2016). O grande problema na utilização desse recurso é que ele pode ser usado de forma maléfica, onde golpistas podem cadastrar endereços de sites inseguros ou até mesmo links diretos para download de programas maliciosos, sem que o usuário consiga identificar em o que está clicando.

É importante verificar se a URL encurtada realmente direciona para um site seguro, inclusive quando vierem de fontes seguras como amigos, parentes e colegas. Para esse tipo de verificação, é necessário utilizar sites que estendem o link para o seu formato original, um exemplo é o site http://unshorten.it/, onde basta colar o link encurtado para que ele retorne as informações necessárias para saber se é possível confiar no link ou não. Para links encurtados que começam com bit.ly e goo.gl basta colá-lo na barra de endereços e adicionar o sinal de “+” no final, assim você será direcionado a uma página que contém mais informações sobre o link. (CCM, 2016).

2.6.11 *Backups*

Uma das melhores práticas para proteger os dados de um sistema é através de *backups* ou cópias de segurança. Embora muitos achem que essa prática é uma preocupação somente de grandes empresas, ela deve ser considerada como item indispensável também para a proteção de dados pessoais. Através de um *backup,* é possível se proteger de falhas de *hardware*, como a pane de um disco rígido, falhas de *software*, como a invasão do sistema por *hackers*, ataque de vírus, perda acidental de arquivos, entre outros. (FIALHO, 2007).

Também é de fundamental importância manter cópias de segurança atualizadas, pois de nada adianta ter um *backup* com conteúdo defasado. A partir de um *backup* é possível remediar, por exemplo, o famoso ataque de um *Ransomware*, que criptografa os dados do sistema impossibilitando o acesso dos mesmos. Nestes casos, se não houver um *backup*, somente resta pagar ao atacante para ter seus dados de volta, prática essa que não é recomendada pois além de estar fortalecendo

o crime, não há como ter garantias da eficácia da ação. Ou, na pior das hipóteses, aceitar a perda dos arquivos.

Existem diversos meios de se realizar *backup* dos dados, entre as mais utilizadas estão o uso de discos rígidos externos, pen drive, CD/DVD/Blu-Ray, e os *backups* na nuvem. Para a solução de *backup* em nuvem, existem diversos provedores que inclusive disponibilizam um armazenamento inicial limitado gratuito. Entre eles estão o Drive da Google que disponibiliza até 15 Gb para uma conta gratuita, o OneDrive da Microsoft disponibilizando 5 Gb em seu modo gratuito, o Dropbox com 2 Gb de armazenamento gratuito, entre diversos outros. Para a utilização de planos com maior capacidade, há custos variados que podem ser cobrados mensal ou anualmente. Cabe ao usuário fazer uma análise de quão importante os seus dados são, para dessa forma poder dimensionar o investimento necessário para proteção.

2.7 TRABALHOS RELACIONADOS

Durante as pesquisas para formulação da proposta de trabalho e seu desenvolvimento, foram encontrados outros trabalhos que se relacionam com o tema e ajudaram a nortear as ideias expostas. Entre eles, pode-se citar o trabalho da Karine Cecagno Omizzolo (2013) que, em seu relatório de conclusão de curso chamado “Crimes Cibernéticos: análise dos crimes e aplicação de metodologias e ferramentas para detecção de pedofilia”, retratou o cenário da Internet no Brasil assim como os tipos de fraudes utilizados e como a polícia vem atuando para obtenção de provas. O foco do seu trabalho foram crimes de pedofilia pela Internet e na realização de testes através de ferramentas gratuitas da Computação Forense, para investigação de crimes de pornografia infantil.

Com o resultado dos seus testes, conclui-se que embora com a utilização de ferramentas gratuitas que demandem maior trabalho manual de um investigador Forense, é possível sim identificar e punir os responsáveis por esses atos. Existem também ferramentas que automatizam a busca de nudez em imagens, por exemplo, porém são pagas ou de uso exclusivo de forças da lei. Karine conclui também que a melhor forma de prevenir esses crimes é através do conhecimento e monitoramento de pais e educadores, aliado às novas leis específicas capazes de punir os criminosos.

Existem diversas monografias de cursos de direito que tratam do tema crimes cibernéticos, sendo dado foco maior ao aspecto criminal, como é o caso de Luis Guilherme de Matos Feitosa (2012) que, em sua monografia “Crimes Cibernéticos: o estelionato virtual”, conceituou os crimes aos quais os usuários estão expostos, a maneira como os criminosos agem e quais as aplicações penais utilizadas para reprimir essas fraudes. Seu foco principal foram os crimes de estelionato por intermédio da Internet, que se caracteriza por obter vantagem ilícita sobre um indivíduo que está sendo enganado. Sob seu julgamento, até a data de publicação do trabalho, não havia leis específicas para punir os autores, deixando muitas vezes os magistrados do direito sem ações que possam efetivamente condenar os envolvidos.

Sua principal contribuição foi a explicação de conceitos e práticas do estelionato virtual com o objetivo de apoiar pesquisadores e estudiosos a avançarem suas pesquisas, assim como apoiar novos estudos. Também serviu para enfatizar a urgente necessidade de modificações nas legislações que tangem ao direito informático, por estarem desatualizadas e favorecendo os criminosos a tratarem os crimes virtuais como uma forma de empreendimento “autorizado”.

3 METODOLOGIA

Após finalizada as pesquisas para elaboração do referencial teórico, foi desenvolvido um questionário estruturado, sendo distribuído de duas formas: através de formulário online com a ferramenta *Google Forms*, e impresso fisicamente para distribuição em turmas do ensino médio de algumas escolas da região, disponível no Apêndice A deste trabalho. Esse questionário tem por objetivo coletar informações para responder a questão principal da pesquisa, que é indicar qual o nível de conhecimento em segurança digital da população da região de Bento Gonçalves. O tipo de pesquisa utilizada será a descritiva quantitativa, também conhecida como pesquisa de levantamento ou *survey*. Para Baptista e Campos (2016), as pesquisas de levantamento são feitas principalmente para identificar comportamentos e atitudes e caracteriza-se pela coleta de dados fornecidos pelas próprias pessoas, geralmente através de questionários.

A estrutura do questionário foi dividida em sete blocos: explicação da pesquisa (bloco 1), identificação do respondente (bloco 2), questões próprias da pesquisa (bloco 3 a 6) e validação para respondentes com menos de 14 anos (bloco 7). As questões aplicadas são do tipo objetivas fechadas, onde o pesquisador define as alternativas e o respondente, por sua vez, assinala aquela que mais se ajusta às suas características, ideias ou sentimentos. Foram inseridas questões de múltipla escolha, algumas aceitando somente resposta simples e outras com múltipla escolha, além de perguntas em escala.

O método de amostragem será o não probabilístico por conveniência, que segundo Baptista e Campos (2016) caracteriza-se por não ser realizada de forma aleatória, pois nem toda a população terá a probabilidade de respondê-la. Foi de julgamento do autor definir a população como sendo usuários de internet com 14 anos ou mais e selecionando dentro destes os mais acessíveis. As respostas vindas de pessoas com menos de 14 anos foram invalidadas através da questão idade, que ao selecionar a opção até treze anos, eram direcionados automaticamente para o fim da pesquisa, havendo uma explicação de que o escopo do projeto não poderia incluí-las.

Ao término da aplicação do questionário, foi iniciado o processo de análise dos resultados, onde foi utilizado como ferramenta de auxílio para geração de gráficos e estatísticas o software *IBM SPSS Statistics*. A partir dos resultados obtidos, foi desenvolvida uma cartilha, disponível no Apêndice B, com boas práticas de uso da

Internet, com destaque para os pontos mais críticos que foram verificados. Essa cartilha foi divulgada de forma eletrônica para as pessoas que demonstraram interesse nos resultados, deixando seu e-mail de contato na pesquisa, além de redes sociais e blogs de TI.

4 PESQUISA DE AVALIAÇÃO SOBRE COMPORTAMENTOS EM SEGURANÇA DIGITAL

A pesquisa teve início na data de vinte e sete de abril de dois mil e dezessete, e foi concluída em vinte e três de maio de dois mil e dezessete, totalizando vinte e sete dias de duração. Num primeiro momento, ela foi compartilhada com amigos do *Facebook* e contatos do *Whatsapp*. Logo no primeiro dia, foi notado um problema que não havia sido mapeado, onde o *Facebook* bloqueou o envio de novas mensagens após ter sido feito para aproximadamente trinta amigos. O bloqueio durou em torno de quatro dias, e ao se tentar recomeçar o envio, logo houve o bloqueio novamente. Segundo pesquisas realizadas a respeito, isso ocorre, pois, o *Facebook* identificou uma atividade suspeita de envio de Spam, visto que o mesmo link estava sendo enviado para diversas pessoas. Por causa disso, resolveu-se mudar o método de envio, postando o link do questionário na linha do tempo ao invés de enviar particularmente para cada um dos contatos.

Em paralelo a isso, a pesquisa foi compartilhada também com colegas de trabalho e demais alunos de outros cursos da UCS, ambos através de e-mail. Também foram impressas 150 cópias da pesquisa, distribuídas em turmas do ensino médio de duas escolas públicas da região. Ao todo, foram registradas 511 respostas válidas.

As questões foram elaboradas com base no estudo realizado na primeira parte do trabalho, buscando identificar o nível de conhecimento da população sobre as principais questões de segurança vinculadas à Internet.

4.1 RESULTADOS DA PESQUISA

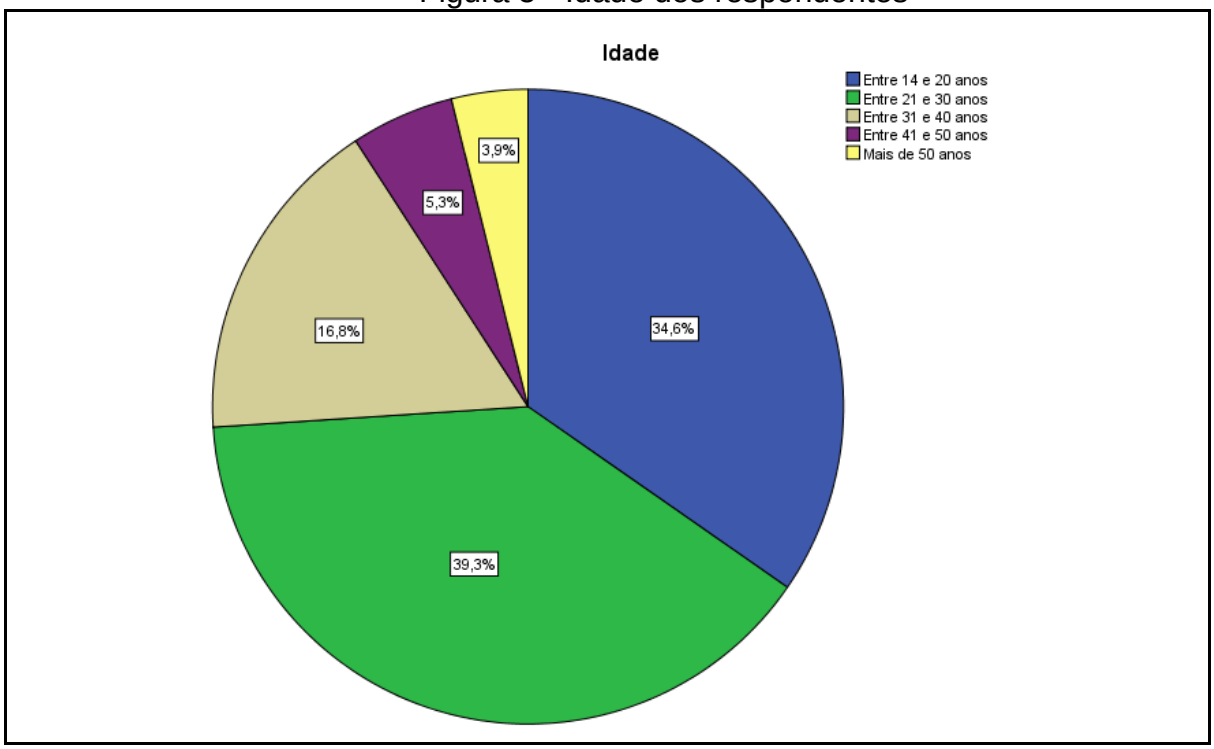
Conforme mencionado na metodologia, a pesquisa foi dividida em blocos para facilitar o entendimento dos respondentes e melhorar a organização.

4.1.1 Identificação do respondente

O primeiro bloco de perguntas tem por objetivo identificar o perfil do respondente e, para isso, foram feitas três perguntas de cunho socioeconômico: idade, sexo e escolaridade. Essas três questões também servem para identificar se há uma relação direta entre o conhecimento no assunto e o perfil do respondente.

No fator idade, a Figura 5 mostra que houve uma proximidade na proporção de respondentes das faixas etárias entre 21 e 30 anos (39,3%) e entre 14 e 20 anos (34,6%). Mostra também que nas faixas etárias acima de 30 anos houve uma diminuição gradativa na proporção de respondentes, tendo como valor mínimo a faixa com mais de 50 anos (3,9%).

Figura 5 - Idade dos respondentes

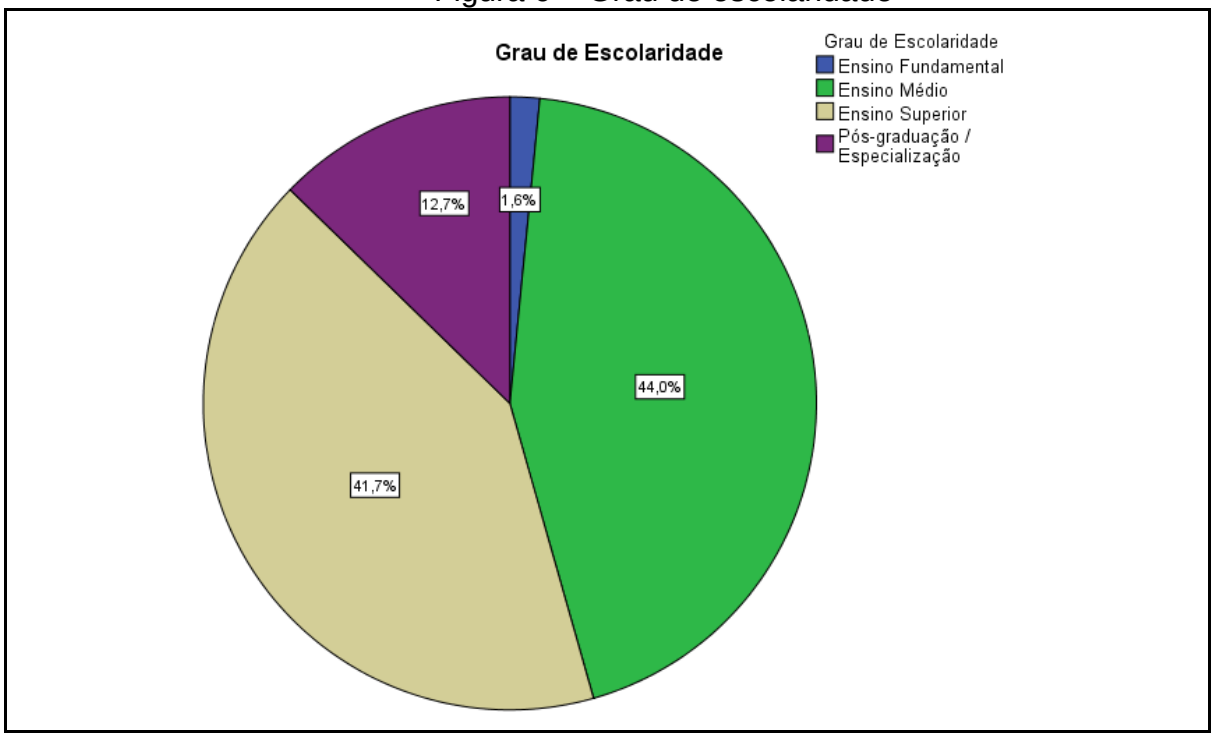


Fonte: Pesquisa direta (2017).

No quesito sexo, a pesquisa também obteve valores próximos entre homens e mulheres. Do total de entrevistados, 53,4% são homens e 46,6% são mulheres.

Analisando o quesito escolaridade, a Figura 6 mostra que o maior percentual encontrado está nos respondentes que possuem ensino médio (44%), seguido de perto dos que possuem ensino superior (41,7%). Já os que possuem somente o ensino fundamental foi a mais baixa (1,6%), como já era esperado, pois havia um limitador na pesquisa impedindo que pessoas com menos de 14 anos pudessem responder ao questionário.

Figura 6 – Grau de escolaridade

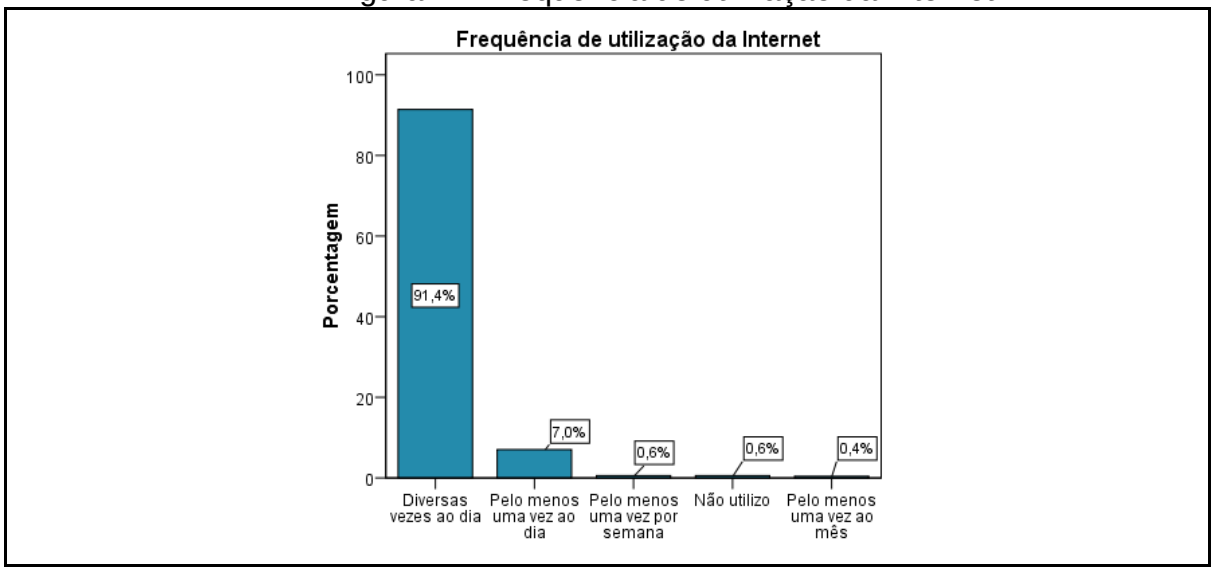


Fonte: Pesquisa direta (2017).

4.1.2 Questões técnicas com respostas simples

O segundo bloco do questionário é composto por perguntas de múltipla escolha, aceitando somente respostas simples. A primeira delas questiona a frequência de utilização da Internet dos respondentes, cujo resultado é apresentado na Figura 7.

Figura 7 – Frequência de utilização da Internet



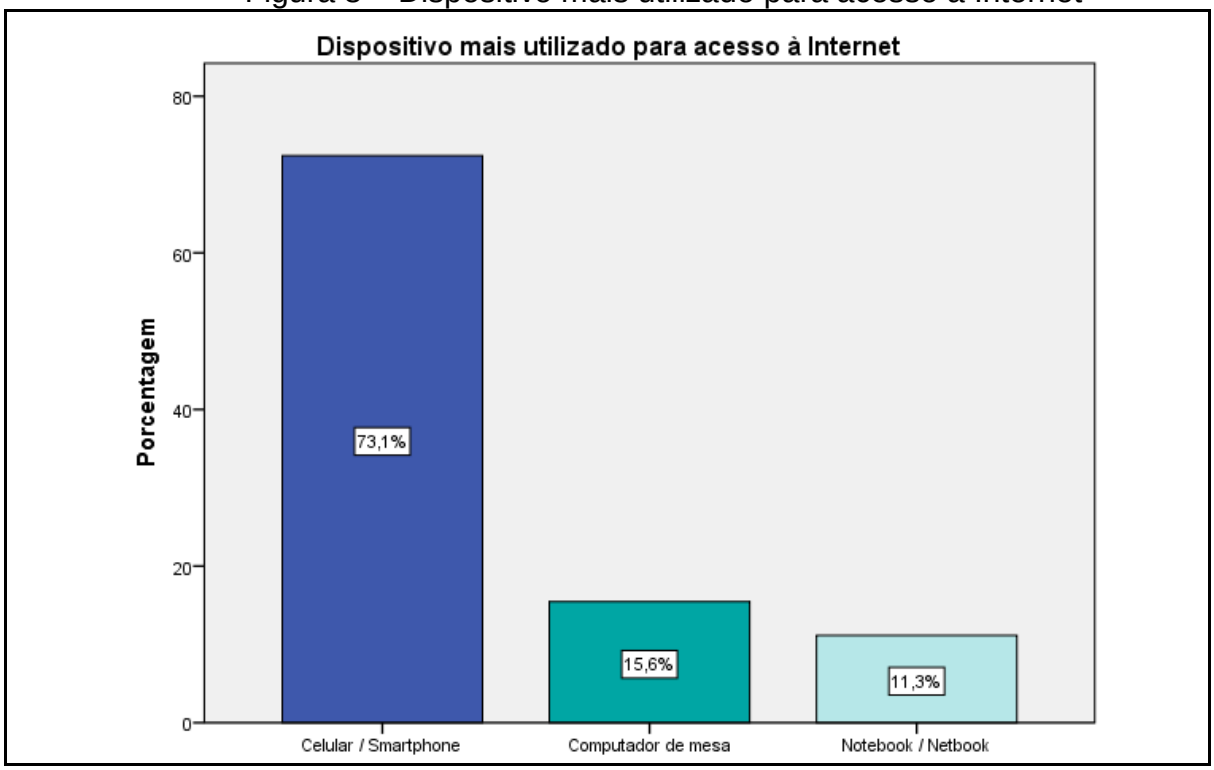
Fonte: Pesquisa direta (2017).

A Figura 7 mostra que, independente da faixa etária, sexo ou escolaridade, a grande maioria dos respondentes acessa a Internet diversas vezes ao dia, opção representada por 91,4% do total de respostas.

As pesquisas realizadas pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.br), também apontam que desde 2008 esse número já se destaca dos demais, havendo elevação considerável ano após ano.

Há uma relação direta entre a frequência de acesso e o método pelo qual este acesso é feito. Isso pode ser notado em conjunto com a Figura 8, que mostra qual o dispositivo mais utilizado para acesso à Internet pelos respondentes.

Figura 8 – Dispositivo mais utilizado para acesso à Internet



Fonte: Pesquisa direta (2017).

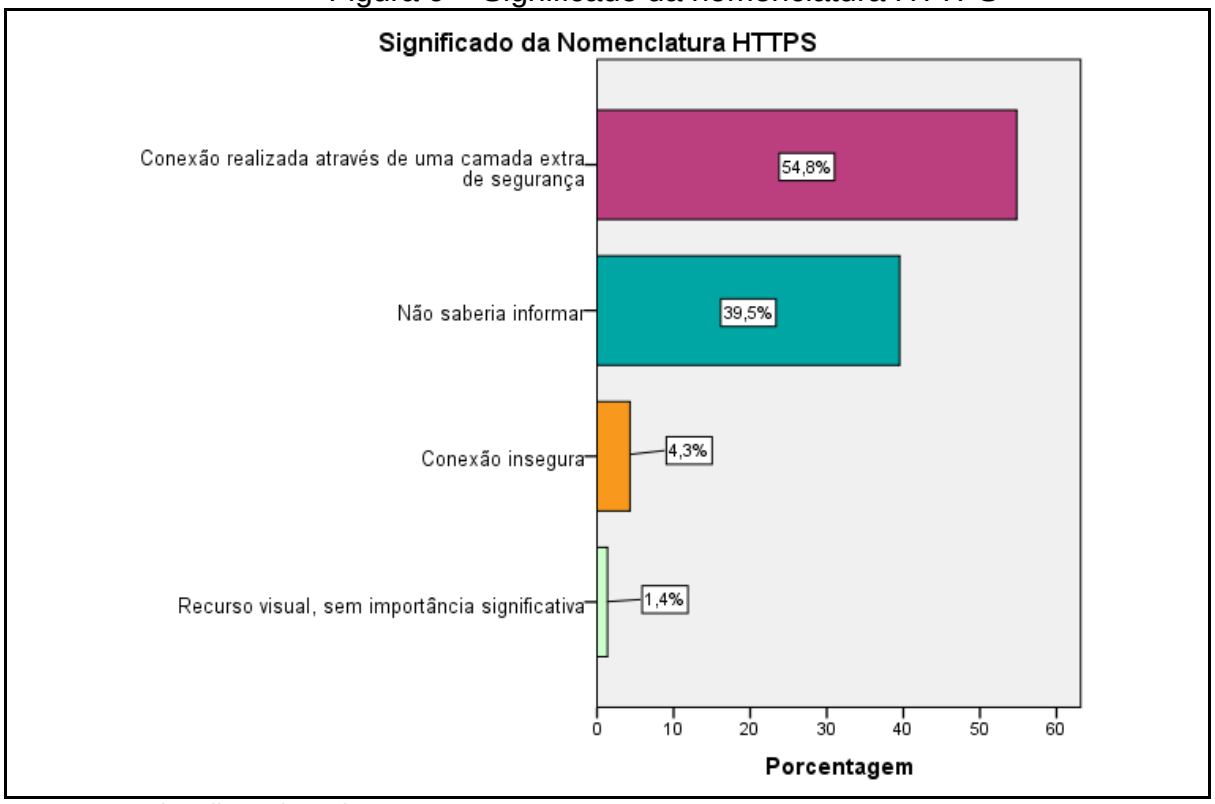
O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.br) revelou em suas pesquisas que, em 2015, pela primeira vez os *smartphones* haviam ultrapassado os computadores, em proporção de acesso à internet. Essa discrepância vem aumentando nos últimos anos e nesta pesquisa o uso do celular/smartphone como principal dispositivo para acesso à Internet chegou a 73,1%, já os computadores de mesa e notebooks/netbook chegaram a 15,6% e 11,3%, respectivamente.

Esses números confirmam a teoria de que a Internet está cada vez mais acessível para todos e, entre os principais fatores para isso estão os preços dos dispositivos mais baixos, acesso fácil a Internet, além da facilidade de aprendizagem para seu manuseio.

A partir deste ponto, as perguntas foram feitas com o propósito de identificar o nível de conhecimento dos respondentes sob a análise de segurança digital. Para isso, foram utilizadas questões de teor técnico, mas que deveriam ser aplicadas no dia a dia dos usuários e, portanto, de comum conhecimento.

Quando questionados sobre o significado da nomenclatura HTTPS, a intenção foi de saber se os usuários conseguem identificar quando um site utiliza protocolos de segurança ou não. A Figura 9 apresenta as respostas obtidas.

Figura 9 – Significado da nomenclatura HTTPS



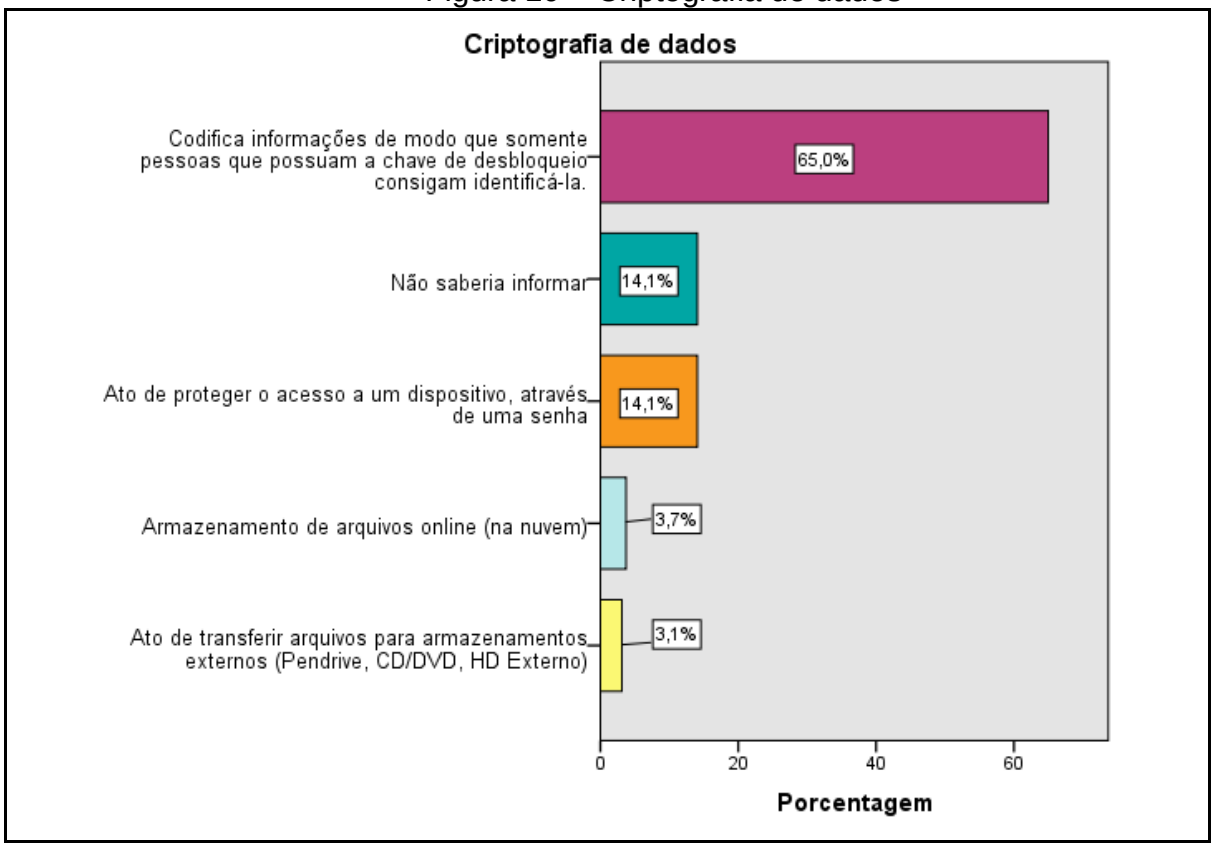
Fonte: Pesquisa direta (2017).

Percebe-se, através da Figura 9, que pouco mais da metade dos respondentes, 54,8%, assinalaram a resposta correta para a definição de HTTPS. A soma dos demais grupos, 45,2% representam os usuários que não saberiam informar ou assinalaram respostas incorretas.

Embora haja uma parcela considerável de usuários que sabem identificar a utilização desse recurso de segurança, a porção de “desorientados” é significativa. Estes usuários realizam diariamente acessos a sites bancários e compras pela Internet sem saber que seus dados podem estar sendo interceptados ou violados.

Analisando a questão sobre criptografia de dados, quando questionados para assinalarem a opção que caracteriza a criptografia, obteve-se os percentuais representados pela Figura 10.

Figura 10 – Criptografia de dados



Fonte: Pesquisa direta (2017).

O resultado demonstrado pela Figura 10 foi bastante positivo pois, 65% dos entrevistados assinalaram a opção correta, informando que criptografia é o ato de codificar informações de modo que somente pessoas que possuam a chave de desbloqueio consigam identificá-la. A soma das demais respostas, 35%, representa a parcela que não saberiam informar ou a responderam de forma incorreta.

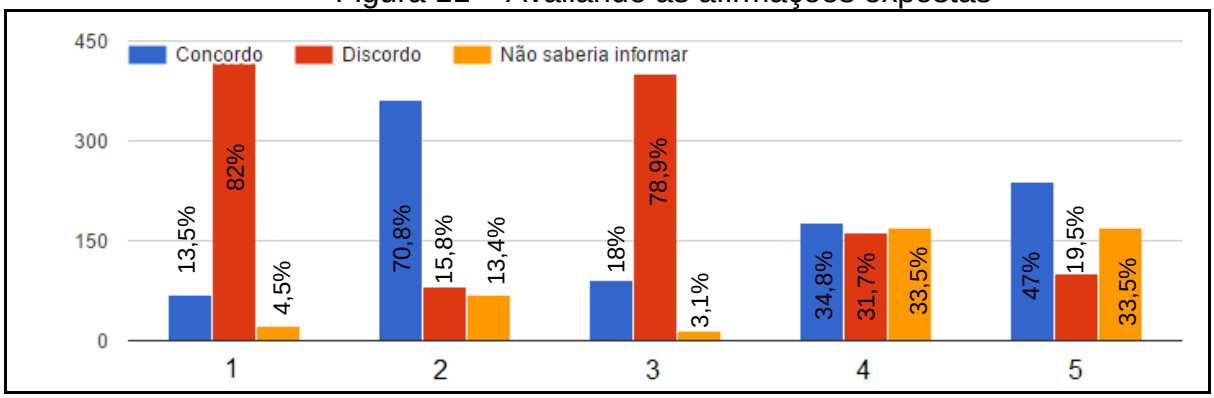
Embora a prática de criptografia seja mais conhecida no mundo corporativo, ela pode ser facilmente adotada e manuseada também em dispositivos domésticos. Vale também ressaltar que a porcentagem de respondentes que sabem o que significa

criptografia de dados não necessariamente implica em dizer que utilizam essa prática em seu dia a dia.

4.1.3 Questões técnicas com respostas em escala

Na primeira questão do terceiro bloco foram expostas afirmações e solicitado que fossem avaliadas em: concordo, discordo ou não saberia informar. A Figura 11 expõe os resultados obtidos.

Figura 11 – Avaliando as afirmações expostas



Fonte: Pesquisa direta (2017).

A afirmação 1 compreende “Criminosos da Internet possuem maior interesse em atacar computadores de grandes empresas, por isso os usuários domésticos estão protegidos”. Onde 82% dos respondentes acertaram a resposta ao discordar desta afirmação.

Sabe-se que atualmente os criminosos da Internet não escolhem a quem irão atacar, portanto usuários domésticos estão tão expostos às vulnerabilidades quanto os usuários corporativos.

Na afirmação 2, "Uma empresa legítima não solicitará informações pessoais em uma mensagem de e-mail. Apesar de parecerem convincentes, mensagens que solicitam informações pessoais com urgência provavelmente são falsas", 70,8% dos respondentes também acertaram a resposta em concordar com a afirmação.

Uma das táticas mais comuns para coleta de informações pessoais é através de e-mail, onde o atacante se passa por uma empresa legítima e lhe solicita dados para confirmar alguma operação ou corrigir algum suposto problema. Por mais que estes e-mails despertem curiosidade e pareçam ser verdadeiros, uma empresa

legítima jamais solicitará esse tipo de informação, seja por e-mail, mensagem SMS, redes sociais ou por telefone.

A afirmação 3 diz que, "Redes Wi-Fi domésticas possuem sinal de curto alcance, logo não é necessário a utilização de senhas difíceis". Do total de respondentes, 78,9% discordaram da afirmação e, portanto, acertaram a resposta.

Ainda é comum encontrar redes Wi-Fi configuradas sem nenhum tipo de segurança. Isso além de comprometer a qualidade do seu sinal, já que pessoas não autorizadas podem a estar utilizando, possibilita que pessoas mal-intencionadas capturem informações dos demais dispositivos conectados e também distribua conteúdo impróprio na Internet sem poderem ser identificados.

A afirmação de número 4, "Durante operações bancárias realizadas pela Internet, uma prática de segurança comum é digitar a senha incorretamente no primeiro acesso, para validar se o site é legítimo", foi a que mais causou dúvida entre os respondentes. Apenas 34,8% acertou a questão, marcando a opção concordo. A soma das respostas não concordo e não saberia informar, representam 65,2% do total e indicam o não conhecimento dessa prática.

Pessoas mal-intencionadas podem criar sites e aplicativos com layout idêntico ao de um banco, com a finalidade de capturar as senhas dos usuários. Uma prática extremamente simples, porém pouco conhecida, é digitar a senha errada durante o primeiro acesso, pois caso o site seja falso ele não conseguirá validar essas informações e você logo saberá que se passa de uma farsa.

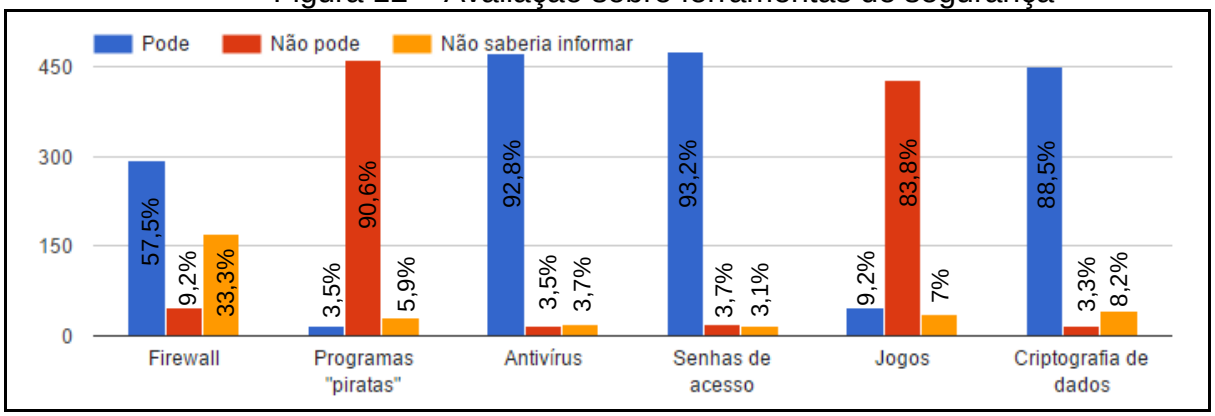
Na quinta e última afirmação, "Links de sites encurtados, exemplo: "goo.gl/Rio8fT", são utilizados para fraudes pois dificultam a identificação do site que estamos sendo direcionados", houve semelhança entre respostas corretas e incorretas, 47% concordaram com a afirmação e acertaram a resposta, enquanto 53% discordaram ou não souberam informar.

O grande problema dos links encurtados é que eles não informam corretamente o endereço do site que será aberto, e isso pode ser utilizado como direcionamento para sites indevidos. Nesses casos, o cuidado deve ser redobrado e, para evitar incômodos, é importante verificar a fonte de quem enviou o link ou verificar qual o direcionamento dele, através de sites que fazem essa tradução.

Na segunda pergunta deste bloco, foi solicitado a avaliação dos itens sobre poderem ou não serem considerados ferramentas de segurança. Os resultados estão expostos na Figura 12.

A grande maioria dos respondentes identificou quais eram as ferramentas de segurança com facilidade, e discordou das opções programas “piratas” e jogos, que não podem ser. O item que mais gerou dúvida foi o firewall, onde 42,5% dos respondentes informaram que não pode ser considerado uma ferramenta de segurança ou não souberam responder, e isso é incorreto.

Figura 12 – Avaliação sobre ferramentas de segurança

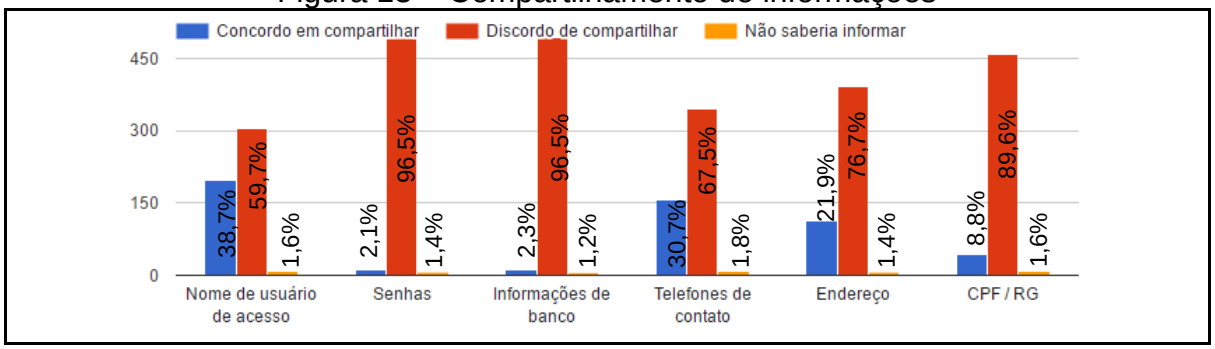


Fonte: Pesquisa direta (2017).

O objetivo de um firewall é filtrar o tráfego de rede de entrada e saída de um dispositivo. O termo firewall não é tão conhecido em usuários domésticos pois muitas vezes ele já vem atrelado a outras ferramentas como ao antivírus, por exemplo.

A terceira e última questão deste bloco faz a seguinte afirmação: "Todos possuem informações pessoais compartilhadas online, que são obtidas principalmente através de cadastros. Dentre os itens, avalie se você concorda ou não em compartilhá-los”. Os resultados obtidos estão expostos na Figura 13.

Figura 13 – Compartilhamento de informações



Fonte: Pesquisa direta (2017).

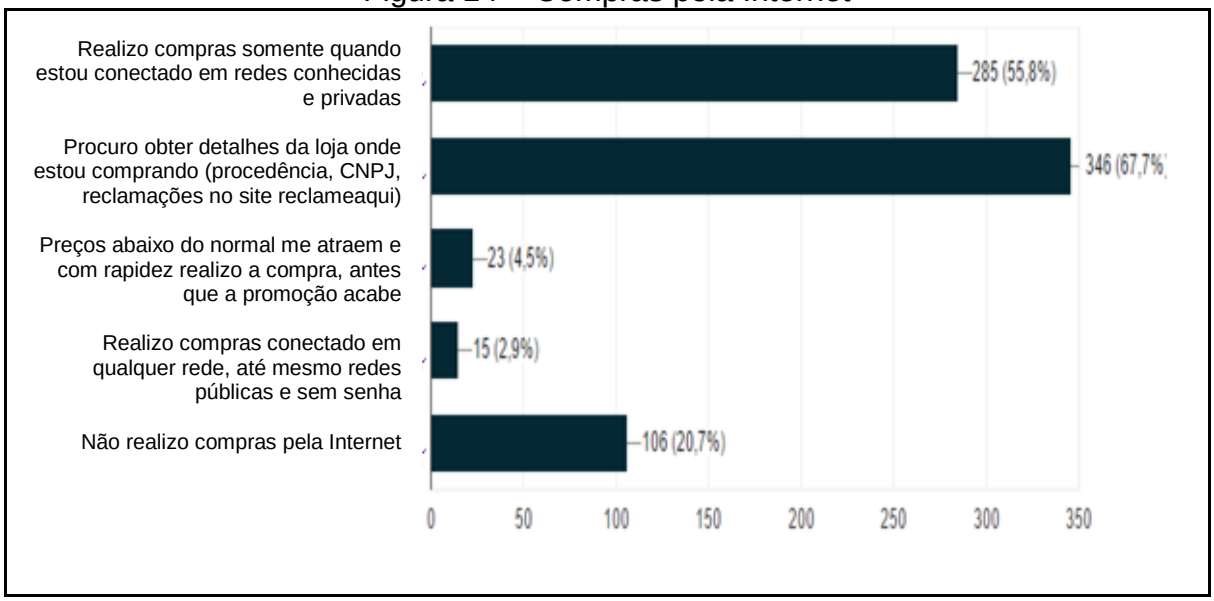
Observa-se que há divergências entre quais informações se pode ou não compartilhar. Em geral, deve-se evitar ao máximo expô-las, por mais simples que elas

sejam, como por exemplo: endereço, telefone, CPF ou RG. Isso pois, uma informação simples pode ser o primeiro passo para uma análise aprofundada de seu cotidiano e assim haver o planejamento de um ataque. Obviamente, algumas informações são públicas e podem ser facilmente adquiridas de outras formas, mas o aconselhável é evitar isso ao máximo. Quanto aos itens senha e informações bancárias, obviamente, elas devem ser sigilosas e nunca devem ser compartilhadas. O item que mais obteve respostas incorretas foi o nome de usuário de acesso, onde 38,7% dos respondentes concordaram em compartilhá-lo. Este item, por mais que pareça insignificante, representa a primeira informação que o atacante precisa saber para acessar, por exemplo, o seu e-mail. Não sabendo disto, um atacante terá dois trabalhos, descobrir o seu usuário e após a sua senha, dificultando ou pelo menos retardando o tempo necessário para que essa informação seja descoberta.

4.1.4 Questões técnicas com respostas de múltipla escolha

O quarto bloco do questionário é composto por perguntas de múltipla escolha, podendo ser selecionada mais de uma resposta em cada questão. Iniciou-se pela questão compras pela Internet, onde os resultados estão na Figura 14.

Figura 14 – Compras pela Internet



Fonte: Pesquisa direta (2017).

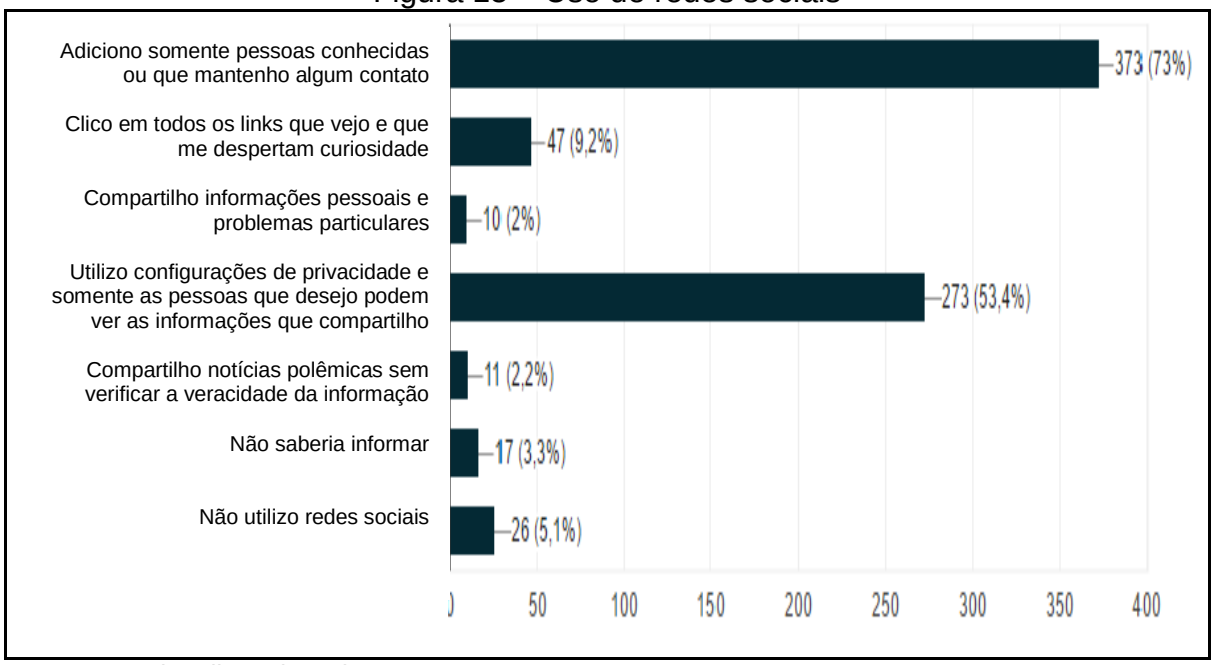
Nota-se, analisando a Figura 14, que a grande maioria dos respondentes é cauteloso e tem como prática realizar compras somente quando conectado em redes

conhecidas, além de obter detalhes da loja onde está comprando. Isso é representado por 55,8% e 67,7% dos respondentes, respectivamente. Outro número relevante é o de respondentes que não realizam compras pela Internet, representando 20,7%.

Embora a pesquisa tenha indicado o uso de boas práticas, sabe-se que o número de clonagem de cartões de crédito em sites e problemas na entrega dos produtos adquiridos são grandes, por isso é importante ter cautela e analisar bem antes de finalizar uma compra.

A Figura 15 representa os comportamentos na utilização de redes sociais. Percebe-se que boa parte dos respondentes adicionam somente pessoas conhecidas ou que mantem algum contato, 73%, além de utilizar configurações de privacidade para que somente as pessoas que desejam possam ver as informações compartilhadas, 53,4%. Em contrapartida, 9,2% informaram que clicam em qualquer link que os desperta curiosidade, e cerca de 2% compartilha informações pessoais ou notícias polêmicas sem verificar sua veracidade. Outro fato curioso para os dias de hoje é que 5,1% dos entrevistados não utilizam redes sociais.

Figura 15 – Uso de redes sociais



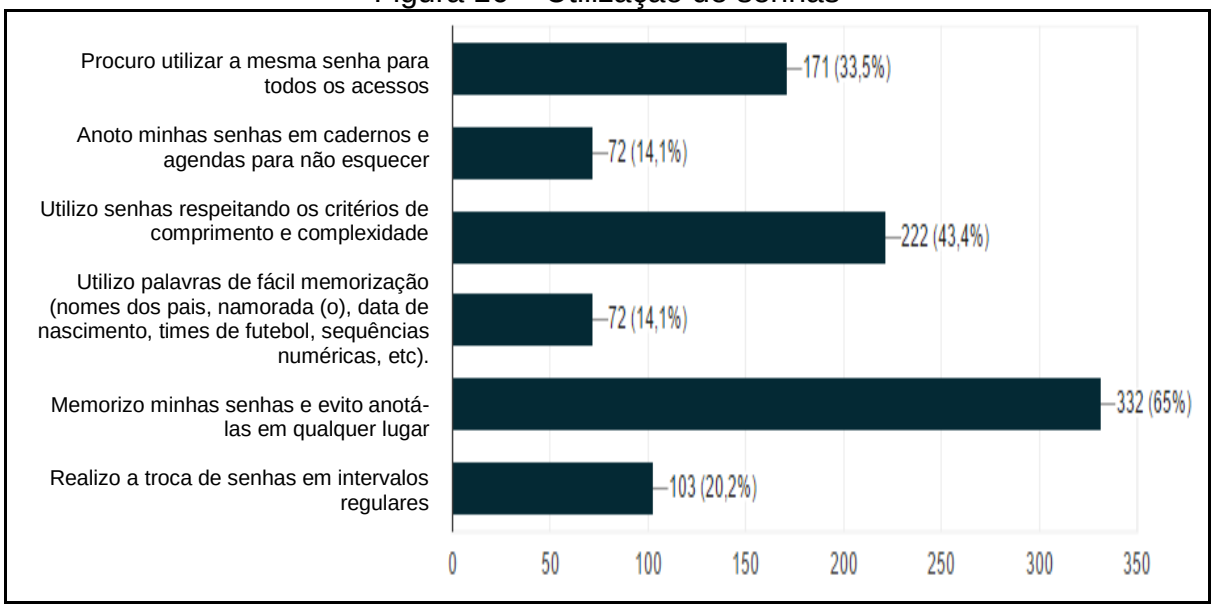
Fonte: Pesquisa direta (2017).

Grande parte do tempo gasto na Internet se resume em utilização de redes sociais, e com elas um enorme fluxo de informações dos tipos mais variados. Muitas dessas informações que circulam são falsas ou adulteradas para promover algo que seja de interesse do publicador. O compartilhamento de informações falsas faz com

que ela seja promovida cada vez mais e atingindo assim mais pessoas, além de se enquadrar no crime de calúnia, previsto no Artigo 138 do Código Penal. Além disso, algumas propagandas são utilizadas para lhes direcionar a um endereço fora da rede social, e este endereço pode não ter relação nenhuma com o propósito informado.

A questão sobre o comportamento na utilização de senhas, representado pela Figura 16, tem por objetivo identificar o percentual de respondentes que praticam ações corretas, além de apontar as práticas indevidas e que necessitam de um reforço na aprendizagem.

Figura 16 – Utilização de senhas



Fonte: Pesquisa direta (2017).

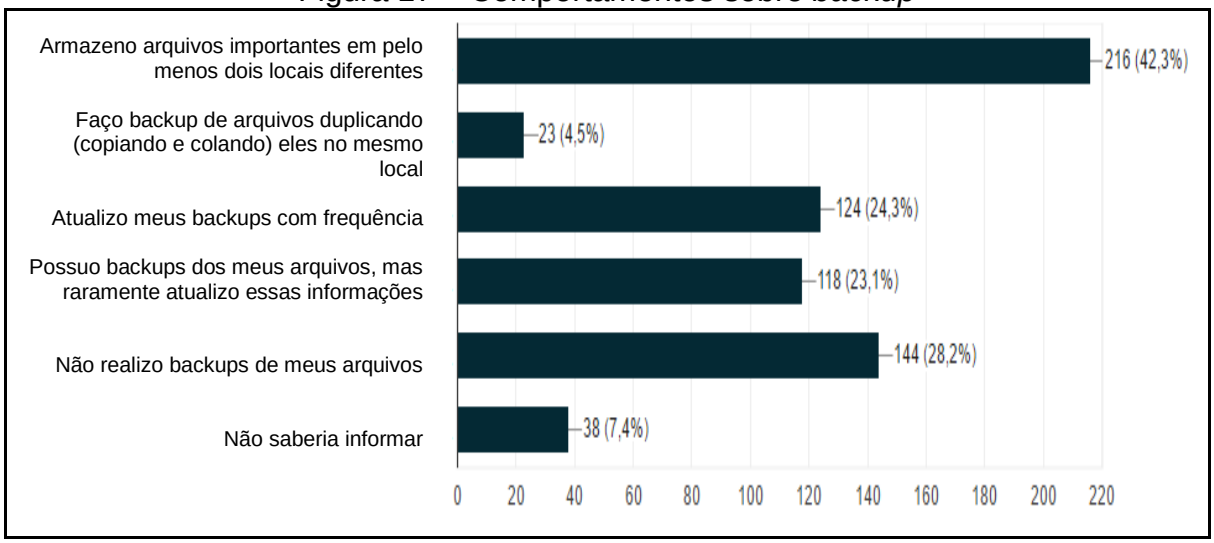
Sobre o item “utilizo senhas respeitando os critérios de comprimento e complexidade”, 43,4% afirmam adotar essa prática. No quesito memorizar senhas e não as anotar em qualquer lugar, 65% utiliza essa prática, e sobre a troca de senhas em intervalos regulares, é representado por 20,2%. Todos esses números são sobre as práticas corretas na utilização de senhas. Por outro lado, 33,5% afirmam utilizar a mesma senha para todos os acessos, 14,1% anotam suas senhas para não se esquecer, e outros 14,1% utilizam senhas de fácil memorização.

Percebe-se algumas práticas muito perigosas e que são praticadas com frequência, como por exemplo a utilização da mesma senha para todos os acessos, isso significa que caso alguém descubra essa senha, todos os seus acessos estarão comprometidos. Já a utilização de senhas fáceis implica em poderem ser quebradas rapidamente, até mesmo sob uma análise do seu cotidiano exposto nas redes sociais.

Para encerrar o bloco de perguntas técnicas, comenta-se sobre o assunto *backup*, demonstrado na Figura 17. Essa questão auxilia a identificar se existe a utilização dessa prática e, em caso afirmativo, saber se está sendo feito de forma correta.

Nota-se, na Figura 17, que 42,3% dos respondentes armazenam seus arquivos importantes em pelo menos dois locais diferentes, e 24,3% atualizam seus *backups* com frequência. Porém, um dado alarmante é que 28,2% afirmam não realizar qualquer tipo de *backup*, e 7,4% não sabe nem o que isso significa. Algumas práticas incorretas de realização do *backup* também foram identificadas, como a não atualização frequente das informações (23,1%), e a realização de *backup* através da duplicação dos arquivos e pastas no mesmo local (4,5%).

Figura 17 – Comportamentos sobre *backup*



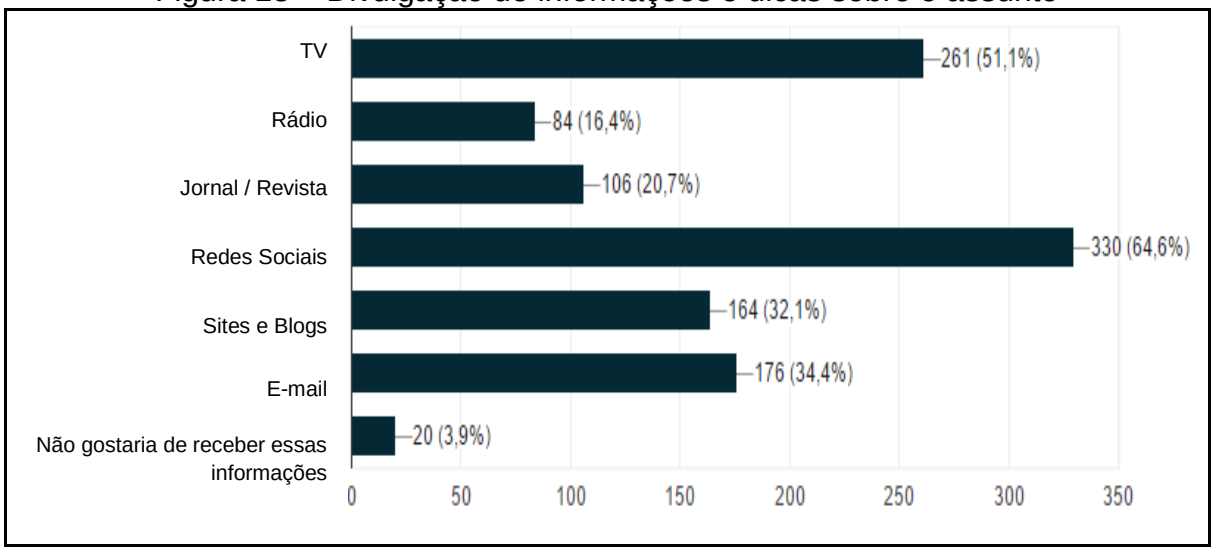
Fonte: Pesquisa direta (2017).

Backups devem ser considerados itens básicos de segurança e prevenção. Eles são a melhor forma de contornar, por exemplo, o ataque pelo famoso *ransomware,* que criptografa os dados do dispositivo. Além disso, através deles é possível recuperar dados perdidos ou corrompidos.

4.1.5 Fechamento da pesquisa

Já na fase final da pesquisa, foi solicitado que os respondentes marcassem de quais formas gostariam de receber orientações sobre segurança digital, visto que no Brasil pouco se fala sobre o assunto. Os resultados estão expostos na Figura 18.

Figura 18 – Divulgação de informações e dicas sobre o assunto

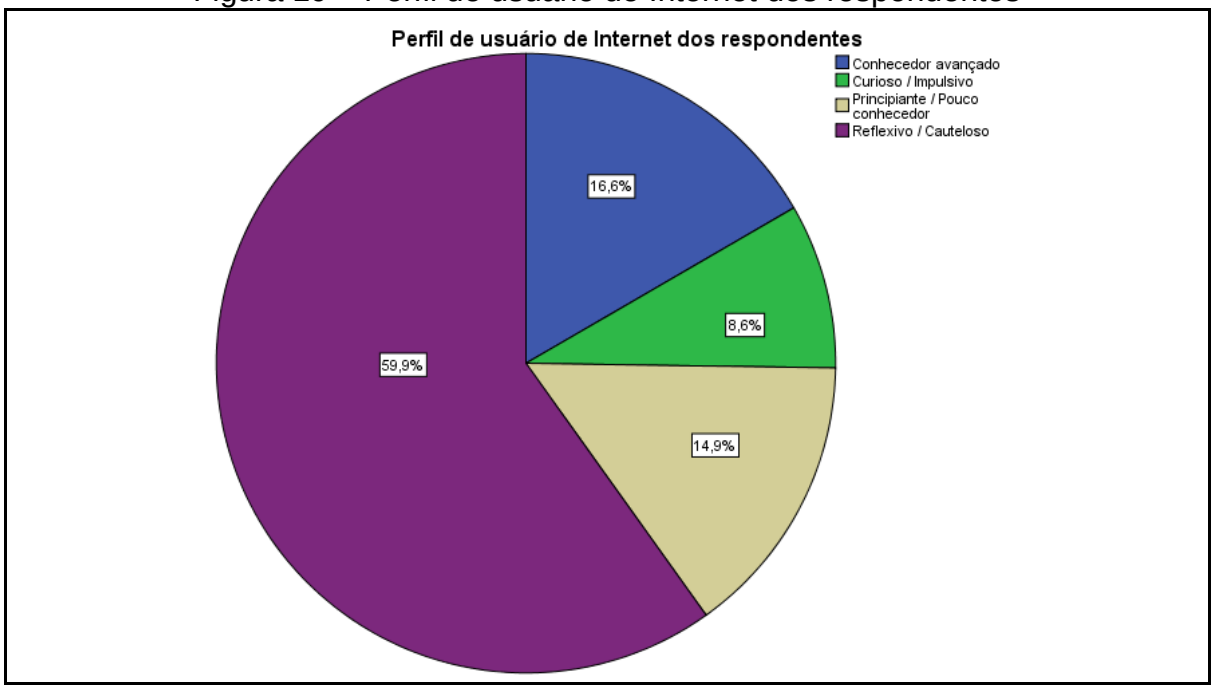


Fonte: Pesquisa direta (2017).

O interesse da divulgação nas redes sociais ficou em destaque, com 64,6%, e em segundo lugar a TV, com 51,1%. Apenas 3,9% do total prefere não receber este tipo de informação.

Embora nem todos os meios de comunicação sejam facilmente atingidos, os resultados desta pesquisa assim como a cartilha de boas práticas serão divulgados na finalização do trabalho, como forma de plano de ação para os problemas encontrados, através de e-mail, redes sociais e blogs de TI.

Figura 19 – Perfil de usuário de Internet dos respondentes



Fonte: Pesquisa direta (2017).

Para auxiliar nessa divulgação, foi disponibilizado um campo para que os interessados preenchessem com seus e-mails. Este campo era opcional e obteve 150 respostas, entre os 511 respondentes.

Finalizando a pesquisa, a última questão solicitava que os respondentes se classificassem no quesito usuários de Internet. O objetivo dessa pergunta é despertar a autoavaliação dos respondentes, para que possam refletir e responder com a sua análise sobre o assunto abordado. Os resultados obtidos estão divulgados na Figura 19.

4.2 CONSIDERAÇÕES FINAIS

A pesquisa tinha por objetivo atingir ao menos uma amostra de 400 respostas, e este foi alcançado, já que foram recolhidas 511. Os meios de comunicação atuais, como redes sociais e e-mail, facilitaram a divulgação da pesquisa, e isso também demonstra como as notícias publicadas na Internet se espalham rapidamente.

Cabe também destacar que foi de fundamental importância o auxílio das professoras e diretoras das escolas nas quais foram distribuídos os questionários de forma impressa.

A população atingida pela pesquisa mostra que estes não estão totalmente desinformados, havendo um conhecimento básico nos assuntos que foram tratados. Porém em grande parte dos questionamentos, houveram pontos nos quais o conhecimento deve ser melhorado. Para tal, a análise dos resultados serviu como base para criação da cartilha de orientação digital, que foi desenvolvida para esclarecer as dúvidas sobre os pontos mais críticos identificados.

5 CONCLUSÃO

Diante dos avanços tecnológicos vistos diariamente, um dos que mais proporcionou novos recursos e funcionalidades foi, sem dúvida, a Internet. A mesma evolução que traz benefícios também abre portas para que pessoas mal-intencionadas usem esses recursos para enganarem pessoas, roubarem informações e dinheiro. Diante do objetivo principal de apresentar conceitos de boas práticas de utilização da Internet e avaliar o nível de conhecimento da população da região de Bento Gonçalves, o trabalho tratou de questões técnicas que norteiam os tipos atuais de crimes e quais as ferramentas e práticas adequadas para prevenir essas situações, além da análise realizada sobre a pesquisa, apontando os pontos de menor conhecimento e que necessitam de ações de aprendizagem.

A Internet no mundo teve início em 1969 pela ARPANET, já no Brasil tudo começou em 1988, quando a FAPESP realizou a primeira conexão à rede. De lá para cá os avanços foram constantes e o que em um primeiro momento era disponibilizado apenas para algumas entidades educacionais, agora pode ser encontrado em qualquer lugar do mundo para os fins mais variados possíveis.

É fato que a inclusão digital exerceu e ainda exerce um papel fundamental na expansão do uso da Internet. O objetivo de inserir conhecimentos digitais para as diferentes classes sociais é capaz de quebrar barreiras entre a população e servir como um incentivo à educação moderna, diminuindo assim a exclusão digital.

A facilidade com que crianças, adolescentes, adultos e até mesmo idosos interagem com a Internet incentiva cada vez mais aos criminosos desenvolverem técnicas cada dia mais surpreendentes para enganar as pessoas. Os crimes cibernéticos não são algo recente, contudo foi nos últimos anos que o número de ataques e prejuízos digitais aumentou consideravelmente, fazendo com que o assunto fosse visto com maior cuidado por especialistas, governos e educadores.

Sabe-se que os crimes de Internet evoluíram no mesmo ritmo que as demais tecnologias, e hoje não se pode tratar um ataque como sendo um simples vírus de computador, pois existe uma gama imensa de novos tipos de ataques. Os especialistas que desenvolvem meios de combater esses ataques sempre estão um passo atrás dos criminosos, pois esses desenvolvem novas tecnologias diariamente, onde o objetivo é o mesmo, fraudar o usuário. Atualmente, esses conceitos estão

sendo revistos pois foi percebido que é necessário prever e combater fraudes antes mesmo que elas possam trazer prejuízos para a sociedade em geral.

Verificou-se que as ferramentas de proteção de equipamentos podem evitar diversos tipos de ataques que os usuários não têm conhecimento, mas como visto, isso não é o bastante. A utilização de práticas rotineiras e visões mais críticas perante o uso da Internet são de grande auxílio nesse combate. Muitas dessas questões devem ser tratadas pelos próprios usuários, pois não há outra forma de fazer isso e, para que isso seja eficaz, o ponto de partida é o conhecimento no assunto, seja por educadores nos meios de ensino, seja por programas de incentivo do governo ou até mesmo pelas próprias pesquisas realizadas na Internet para entender quais são os riscos e como evitá-los.

Diante dos resultados obtidos na pesquisa sobre segurança digital, foi possível perceber que a sociedade da região de Bento Gonçalves possui conhecimento em alguns assuntos, porém também foram identificados muitos pontos frágeis que demandam uma atenção maior. A falta de conhecimento atinge todas as faixas etárias e níveis de escolaridade, portanto esses critérios não podem ser considerados como um fator relevante. Essa falta de conhecimento é percebida também pelos criminosos, e isso influencia no aumento de atos ilícitos. A melhor forma de evitar esses atos é a prevenção, e isso só é possível através da educação e do conhecimento. A mobilidade de acesso foi adquirida principalmente com o uso de *smartphones*, onde as pesquisas apontam como sendo o dispositivo mais utilizado para acesso à Internet.

Acredita-se que a divulgação dos resultados obtidos nesta pesquisa, assim como a cartilha de boas práticas, será de grande valia, auxiliando na conscientização da população. A própria sociedade apontou interesse em se aprofundar no assunto, indicando como principal meio de divulgação as mídias como TV, redes sociais, e-mail, blogs, sites, revistas e jornais.

Contudo, como dica para trabalhos futuros sobre o assunto, pode ser criado um aplicativo para dispositivos móveis que divulgue a cartilha de boas práticas de forma dinâmica, interagindo com o usuário, e até mesmo atuando na identificação de fraudes e conteúdo impróprio. Além disso, a comparação dessa pesquisa para usuários domésticos com uma pesquisa em ambiente corporativo também pode ser válida para verificar de que formas estão sendo tratados esses problemas de segurança digital.

REFERÊNCIAS

ALECRIM, Emerson. **O que é firewall?** – Conceito, tipos e arquiteturas. Disponível em: <http://www.infowester.com/firewall.php>. Acesso em: 14 nov. 2016.

BAPTISTA, Makilim Nunes; CAMPOS, Dinael de. **Metodologias de pesquisa em ciências** - análise quantitativa e qualitativa, 2. ed. Rio de Janeiro: LTC, 2016. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788521630470/>. Acesso em: 06 set. 2016.

BONILLA, Maria Helena Silveria; PRETTO, Nelson de Lucca. **Inclusão Digital:** polêmica contemporânea. Salvador: EDUFBA, 2011. Disponível em <https://play.google.com/books/reader?id=kEM8CwAAQBAJ&printsec=frontcover&output=reader&hl=pt_BR&pg=GBS.PP1>. Acesso em: 20 out. 2016.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014. Disponível em: <https://play.google.com/books/reader?printsec=frontcover&output=reader&id=ribyAgAAQBAJ&pg=GBS.PP1>. Acesso em: 07 set. 2016.

CASTELLS, Manuel**. A Galáxia da Internet:** Reflexões sobre a Internet, os negócios e a sociedade. Brasil: Zahar, 2003. Disponível em: <https://play.google.com/books/reader?id=jrJZCwAAQBAJ&printsec=frontcover&output=reader&hl=pt_BR&pg=GBS.PA1>. Acesso em: 11 out. 2016.

CCM. **Como visualizar uma URL encurtada com segurança.** Disponível em: <http://br.ccm.net/faq/29928-como-visualizar-uma-url-encurtada-com-seguranca>. Acesso em: 16 nov. 2016.

CERT.BR. **Cartilha de segurança para Internet.** Disponível em: <http://cartilha.cert.br/>. Acesso em: 28 ago. 2016.

CETIC.BR. **TIC Domicílios**. Disponível em: <http://data.cetic.br/cetic/explore?idPesquisa=TIC_DOM>. Acesso em: 10 out. 2016.

CGI.BR. **TIC domicílios 2014**: pesquisa sobre o uso de tecnologias de informação e comunicação nos domicílios brasileiros. São Paulo. 2015. Disponível em: <http://cgi.br/media/docs/publicacoes/2/TIC_Domicilios_2014_livro_eletronico.pdf>. Acesso em: 23 ago. 2016.

CHAGAS, Carolina. **Túnel do tempo** (cronologia da Internet no Brasil). Folha de São Paulo. Disponível em: <http://www1.folha.uol.com.br/folha/sinapse/ult1063u275.shtml>. Acesso em: 06 set. 2016.

CHERRY, Denny. Tradução de Christiane Leonor Simyss Moreira. **Fundamentos da privacidade digital:** Ferramentas para proteger suas informações pessoais e sua identidade na internet. 1 ed. Rio de Janeiro: Elsevier, 2014. Disponível em: <https://play.google.com/books/reader?id=hFkaBQAAQBAJ&printsec=frontcover&output=reader&hl=pt_BR&pg=GBS.PP1>. Acesso em: 16 nov. 2016.

CONFEDERAÇÃO NACIONAL DAS EMPRESAS DE SEGUROS GERAIS, PREVIDÊNCIA PRIVADA E VIDA, SAÚDE SUPLEMENTAR E CAPITALIZAÇÃO. **Estudo lista tendências de riscos cibernéticos**. Disponível em: <http://www.cnseg.org.br/cnseg/servicos-apoio/noticias/estudo-lista-tendencias-de-riscos-ciberneticos.html>. Acesso em: 21 de ago. 2016.

CRUZ, Lucas. **O que é o um encurtador de url.** Disponível em: <http://expertdigital.net/o-que-e-o-um-encurtador-de-url-link-veja-os-mais-populares/>. Acesso em: 16 nov. 2016.

FEITOZA, Luis Guilherme de Matos. **Crimes cibernéticos:** estelionato virtual. 2012. 70 p. Monografia de Conclusão (Bacharel em Direito) - Universidade Católica de Brasília, Brasília, 2012.

FIALHO Jr., Mozart. **Guia essencial do backup.** São Paulo: Digerati Books, 2007. Disponível em: <https://books.google.com.br/books?id=RP8R90IysJQC&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>. Acesso em: 24 maio. 2017.

GOMES, Helton Simões. **Internet chega pela 1º vez a mais de 50% das casas no Brasil, mostra IBGE**. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/04/Internet-chega-pela-1-vez-mais-de-50-das-casas-no-brasil-mostra-ibge.html>. Acesso em: 06 set. 2016.

JESUS, Damásio de. **Manual de crimes informáticos**, 1. ed. São Paulo: Saraiva, 2016. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502627253/>. Acesso em: 06 set. 2016.

LEMOS, André. **Cidade Digital.** Portais, Inclusão e Redes no Brasil. Salvador: EDUFBA, 2007. Disponível em: <http://docplayer.com.br/storage/33/16466288/1477014718/vUyDHaUiTSVuU1U6PgUFlw/16466288.pdf>. Acesso em: 20 out. 2016.

MARTINS, Jéssica Maiara Rodrigues. **Inclusão digital para a inclusão social:** o papel das tecnologias da informação e comunicação no campo dos direitos sociais. 2015. 192 f. Dissertação (Mestrado em Desenvolvimento, Sociedade e Cooperação Internacional) - Universidade de Brasília, Brasília, 2015. Disponível em: <http://repositorio.unb.br/handle/10482/19209>. Acesso em: 24 de ago. 2016.

NETICA.ORG.BR. **Orientações para Educadores**. [201-]. Disponível em: <http://new.netica.org.br/educadores/orientacoes/orientacoes/>. Acesso em: 14 de nov. 2016.

OMIZZOLO, Karine Cecagno. **Crimes cibernéticos:** análise dos crimes e aplicação de metodologias e ferramentas para detecção da pedofilia. 2013. 95 p. Relatório do Trabalho de Conclusão (Bacharelado em Sistemas de Informação) – Universidade de Caxias do Sul, Curso de Bacharelado em Sistemas de Informação, Bento Gonçalves, 2013.

PLANALTO.GOV.BR. **DECRETO Nº 5.542.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5542.htm>. Acesso em: 17 out. 2016.

SIMON, Imre. **A ARPANET**. 1997. Disponível em: <http://www.ime.usp.br/~is/abc/abc/node20.html#SECTION00052000000000000000>. Acesso em: 05 out. 2016.

TREND MICRO. **Ransomware:** o que é e como se proteger? 2015. Disponível em: <http://blog.trendmicro.com.br/ransomware-o-que-e-e-como-voce-pode-se-proteger>. Acesso em: 03 nov. 2016.

VIEIRA, Eduardo. **Os Bastidores da Internet no Brasil.** 1. ed. Barueri, São Paulo: Manole, 2003.

WENDT, Emerson; JORGE, Higor Vinicius Nogueria. **Crimes Cibernéticos:** Ameaças e Procedimentos de Investigação. 2. ed. Rio de Janeiro: Brasport, 2013. Disponível em: <https://play.google.com/books/reader?printsec=frontcover&output=reader&id=iGY-AgAAQBAJ&pg=GBS.PP1>. Acesso em: 11 out. 2016.

WILLIAM, Jake. **O que é um antivírus?** Disponível em: < https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201412_pt.pdf>. Acesso em: 14 nov. 2016.

APÊNDICE A – PESQUISA DE AVALIAÇÃO SOBRE COMPORTAMENTOS EM SEGURANÇA DIGITAL

Essa pesquisa foi desenvolvida como parte do trabalho de conclusão do curso de Sistemas de Informação da UCS de Bento Gonçalves e tem por objetivo identificar o nível de conhecimento da população da região sobre os riscos de Segurança Digital, aos quais estão expostos na utilização da Internet.

Evite buscar as respostas para suas dúvidas na Internet neste momento, respondendo as questões de forma sincera e com base em seus conhecimentos e comportamentos atuais.

A pesquisa leva em torno de 10 minutos para ser respondida.

Saliento que a pesquisa não possui qualquer vínculo que possa comprometer o respondente, por isso não serão solicitadas informações como nome, telefone ou e-mail.

1 - Informações sobre o respondente:

Idade:

☐ Até 13 anos
☐ Entre 14 e 20 anos
☐ Entre 21 e 30 anos
☐ Entre 31 e 40 anos
☐ Entre 41 e 50 anos
☐ Mais de 50 anos

Sexo:

☐ Masculino
☐ Feminino

Grau de Escolaridade:

☐ Ensino Fundamental
☐ Ensino Médio
☐ Ensino Superior
☐ Pós-graduação / Especialização

2 - Questões da Pesquisa:

*** Nesta seção você deve assinalar somente uma das respostas para cada pergunta.**

Com que frequência você utiliza a Internet?

☐ Diversas vezes ao dia
☐ Pelo menos uma vez ao mês

☐ Pelo menos uma vez ao dia ☐ Não utilizo

☐ Pelo menos uma vez por semana

Qual o dispositivo que você mais utiliza para acessar a Internet?

☐ Computador de mesa ☐ Tablet

☐ Notebook / Netbook ☐ Outro: _____

☐ Celular / Smartphone

Qual o significado da nomenclatura HTTPS, inserida no início do endereço de alguns sites?

☐ Conexão Insegura

☐ Recurso visual, sem importância significativa

☐ Conexão realizada através de uma camada extra de segurança

☐ Não saberia informar

Assinale a alternativa que caracteriza a criptografia de dados:

☐ Ato de transferir arquivos para armazenamentos externos (Pendrive, CD/DVD, HD Externo)

☐ Armazenamento de arquivos online (na nuvem)

☐ Codifica informações de modo que somente pessoas que possuam a chave de desbloqueio consigam identificá-la.

☐ Ato de proteger o acesso a um dispositivo, através de uma senha

☐ Não saberia informar

3 - Questão da Pesquisa:

*** Nesta seção você deve avaliar cada uma das afirmações ou itens selecionando uma das opções.**

Avalie cada umas das afirmações abaixo:

"Durante operações bancárias realizadas pela Internet, uma prática de segurança comum é digitar a senha incorretamente no primeiro acesso, para validar se o site é legítimo".

☐ Concordo ☐ Discordo ☐Não saberia informar

"Links de sites encurtados, exemplo: "goo.gl/Rio8fT", são utilizados para fraudes pois dificultam a identificação do site que estamos sendo direcionados".

☐ Concordo ☐ Discordo ☐ Não saberia informar

"Criminosos da Internet possuem maior interesse em atacar computadores de grandes empresas, por isso os usuários domésticos estão protegidos".

☐ Concordo ☐ Discordo ☐ Não saberia informar

"Uma empresa legítima não solicitará informações pessoais em uma mensagem de e-mail. Apesar de parecerem convincentes, mensagens que solicitam informações pessoais com urgência provavelmente são falsas".

☐ Concordo ☐ Discordo ☐ Não saberia informar

"Redes Wi-Fi domésticas possuem sinal de curto alcance, logo não é necessário a utilização de senhas difíceis".

☐ Concordo ☐ Discordo ☐ Não saberia informar

Dentre os itens abaixo, avalie se podem ou não ser classificados como ferramentas de segurança:

	Pode	Não pode	Não saberia informar
Jogos	☐	☐	☐
Firewall	☐	☐	☐
Criptografia de dados	☐	☐	☐
Programas “piratas”	☐	☐	☐
Antivírus	☐	☐	☐
Senhas de acesso	☐	☐	☐

"Todos possuem informações pessoais compartilhadas online, que são obtidas principalmente através de cadastros". Dentre os itens abaixo, avalie se você concorda ou não em compartilhá-los:

	Concordo em compartilhar	Discordo de compartilhar	Não saberia informar
Telefones de contato	☐	☐	☐
Informações de banco	☐	☐	☐
CPF / RG	☐	☐	☐
Endereço	☐	☐	☐
Senhas	☐	☐	☐
Nome de usuário de acesso	☐	☐	☐

4 - Questão da Pesquisa:

*** Nesta seção você pode marcar uma ou mais respostas, de acordo com sua necessidade.**

Sobre o assunto compras pela Internet, marque a (as) opções que caracterizam a sua utilização:

☐ Realizo compras somente quando estou conectado em redes conhecidas e privadas

☐ Procuro obter detalhes da loja onde estou comprando (procedência, CNPJ, reclamações no site reclameaqui)

☐ Preços abaixo do normal me atraem e com rapidez realizo a compra, antes que a promoção acabe

☐ Realizo compras conectado em qualquer rede, até mesmo redes públicas e sem senha

☐ Não realizo compras pela Internet

Sobre o uso de redes sociais, qual (is) dos comportamentos abaixo você utiliza em seu dia a dia?

☐ Adiciono somente pessoas conhecidas ou que mantenho algum contato

☐ Clico em todos os links que vejo e que me despertam curiosidade

☐ Compartilho informações pessoais e problemas particulares

☐ Utilizo configurações de privacidade, onde somente as pessoas que desejo podem ver as informações que compartilho

☐ Compartilho notícias polêmicas sem verificar a veracidade da informação

☐ Não saberia informar

☐ Não utilizo redes sociais

Marque a (as) opções que caracterizam o seu comportamento na utilização de senhas:

☐ Realizo a troca de senhas em intervalos regulares

☐ Utilizo palavras de fácil memorização (nomes dos pais, namorada (o), data de nascimento, times de futebol, sequências numéricas, etc).

☐ Memorizo minhas senhas e evito anotá-las em qualquer lugar

☐ Procuro utilizar a mesma senha para todos os acessos

☐ Anoto minhas senhas em cadernos e agendas para não esquecer

☐ Utilizo senhas respeitando os critérios de comprimento e complexidade

"Backups ou cópias de segurança podem ser utilizados para restaurar dados que foram perdidos, apagados, roubados ou corrompidos". Marque a (as) opções que definem seu comportamento sobre backups:

☐ Armazeno arquivos importantes em pelo menos dois locais diferentes

☐ Faço backup de arquivos duplicando (copiando e colando) eles no mesmo local

☐ Atualizo meus backups com frequência

☐ Possuo backups dos meus arquivos, mas raramente atualizo essas informações

☐ Não realizo backups de meus arquivos

☐ Não saberia informar

"No Brasil assuntos sobre segurança digital são pouco divulgados nas mídias". Marque de qual ou quais formas você gostaria de receber informações e dicas sobre o assunto?

☐ TV

☐ Rádio

☐ Jornal / Revista

☐ Redes Sociais

☐ Sites e blogs

☐ E-mail

☐ Não gostaria de receber essas informações

5 - Finalização:

Caso tenha interesse em receber os resultados dessa pesquisa, assim como um manual de boas práticas de utilização da Internet, deixe seu e-mail de contato abaixo. (Não é obrigatório)

_____

Marque a opção que melhor define você como usuário de Internet:

☐ Principiante / Pouco conhecedor

☐ Curioso / Impulsivo

☐ Reflexivo / Cauteloso

☐ Conhecedor avançado

Obrigado!

Agradeço imensamente o tempo dedicado para responder a pesquisa. Sua avaliação será de fundamental importância no desenvolvimento de meu trabalho de conclusão de curso.

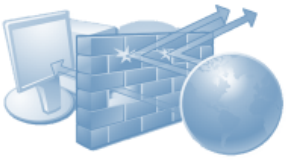
APÊNDICE B – CARTILHA DE ORIENTAÇÃO DIGITAL

Esta cartilha tem por objetivo divulgar as boas práticas de uso da Internet e segurança digital, destacando itens do nosso cotidiano que muitas vezes não damos a atenção necessária.

FERRAMENTAS DE SEGURANÇA

FIREWALL

O termo em inglês firewall significa "parede de fogo", e funciona como uma defesa capaz de bloquear tráfego de dados indesejados e liberar acessos bem-vindos. A maioria dos sistemas operacionais já possuem um firewall nativamente instalado, basta você lembrar de nunca o desativar e sempre manter as atualizações do sistema em dia.



ANTIVÍRUS

O antivírus pode ser considerado o item mais básico de segurança em dispositivos de informática. Embora a maioria dos ataques sejam específicos para o sistema operacional Windows (sistema mais utilizado no mundo), os demais sistemas incluindo o de dispositivos móveis também podem estar vulneráveis. Recomenda-se a utilização de antivírus de fabricantes conhecidos para não cair em golpes de programas falsos e sempre que possível utilizar um antivírus pago, pois são mais eficientes.

COMPARTILHAMENTO DE INFORMAÇÕES

A regra geral é evitar ao máximo a sua exposição. Por mais simples que as informações pareçam, podem ser usadas contra você por pessoas mal-intencionadas. Uma dica para não haver rastreamento de informações em sites é o uso da navegação privativa, que quando habilitada desativa o armazenamento do histórico de navegação.

REDES SOCIAIS

É preciso entender que ao compartilhar informações nas redes sociais assim como na Internet em geral, em questões de minutos não temos mais controle algum sobre elas. Por isso, evite o compartilhamento de informações pessoais, comentários ofensivos contra pessoas e empresas. Adicione somente pessoas conhecidas e utilize configurações de privacidade, selecionando quem pode ou não ver suas publicações. Verifique a veracidade de uma informação antes de compartilhá-la, pois o compartilhamento de informações falsas faz com que elas sejam promovidas cada vez mais.

SENHAS

Senhas são intransferíveis, particulares e sigilosas, sendo o principal meio de proteção contra o acesso não autorizado. Não utilize a mesma senha para os acessos, pois caso alguém a descubra, todos seus acessos serão comprometidos.

- Nunca anote suas senhas, sempre as memorize.
- Crie senhas complexas utilizando letras maiúsculas, minúsculas, números e caracteres especiais, e com no mínimo 8 dígitos.
- Realize a troca das senhas em períodos regulares.
- Jamais forneça suas senhas a ninguém, lembre-se que uma empresa legítima nunca solicita esse tipo de informação, seja por e-mail, telefone, SMS ou redes sociais.

REDES Wi-Fi

Utilize senhas seguras em sua rede Wi-Fi doméstica e evite a navegação em redes desconhecidas. Essas redes podem estar sendo monitoradas com o objetivo de capturar seus dados pessoais. Na dúvida, não utilize.

CRIPTOGRAFIA

A prática de criptografia consiste em tornar os dados ilegíveis a uma pessoa que não possua a senha ou chave de acesso que foi previamente configurada. Essa é a maneira mais segura de proteger seus dados contra roubo, perda ou acesso indevido.

ATUALIZAÇÕES

É de fundamental importância manter atualizado o sistema operacional assim como os softwares instalados em seus dispositivos. As atualizações garantem que você esteja protegido de falhas e vulnerabilidades descobertas no sistema. A utilização de softwares originais garante o fornecimento de atualizações, algo que geralmente não ocorre com produtos "piratas".

COMPRAS PELA INTERNET

Procure sempre obter detalhes completos sobre a loja antes de finalizar a compra. Verifique se a loja realmente existe e qual a sua reputação. Desconfie de preços muito baixos, essa prática desperta a curiosidade e geralmente é utilizada para direcionar a sites falsos. Para realização de compras com cartão de crédito, verifique sempre se o site utiliza HTTPS no início do endereço no navegador, isso significa que ele utiliza criptografia na troca de dados. Guarde o registro e detalhes do item comprado, dessa forma você poderá provar o que havia sido comprado em caso de algum problema.

OPERAÇÕES BANCÁRIAS

Evite o acesso bancário através de links que você recebe por e-mail, SMS ou redes sociais, sempre digite o endereço do site na barra do navegador para garantir estar acessando o site correto. Uma prática pouco conhecida, mas de grande valia é digitar a senha incorreta no primeiro acesso, se o erro for indicado o site está correto, caso contrário então o site é falso. Os golpistas não têm como conferir se a informação é válida, pois querem apenas roubar sua senha. Lembre-se de clicar no botão sair sempre que concluir suas atividades no site, para garantir o encerramento de sua sessão.

BACKUP

Backups devem ser considerados itens básicos de segurança e prevenção. Eles são a melhor forma de contornar, por exemplo, o ataque pelo famoso ransomware, que criptografa os dados do dispositivo.

Além disso, através dele é possível recuperar dados perdidos ou corrompidos. O ideal é armazenar seus arquivos importantes em pelo menos dois locais diferentes, disco externo e na nuvem, por exemplo, e é claro manter sempre esses backups atualizados. Lembre-se que duplicar arquivos e pastas no mesmo local não se configura backup, essa é uma prática incorreta e insegura.

Essas dicas nos direcionam para um uso seguro da Internet, além de comentar itens gerais de segurança digital. Porém é importante destacar que nunca estaremos 100% seguros e não há ferramentas que consigam nos garantir isso. Aliado as boas práticas, precisamos ter bom senso para determinar quais informações podem ser úteis ou não.

Fiquem à vontade para compartilhar o material e assim fazer com que essa informação possa auxiliar outras pessoas.