CENTRO UNIVERSITÁRIO LUTERANO DE PALMAS
Recredenciado pela Portaria Ministerial nº 1.162, de 13/10/16, D.O.U nº 198, de 14/10/2016
ASSOCIAÇÃO EDUCACIONAL LUTERANA DO BRASIL

Jarbas Lopes Sousa Pereira

GUIA DE USO SEGURO DA INTERNET PARA USUÁRIOS LEIGOS

Palmas – TO

2016

Jarbas Lopes Sousa Pereira

GUIA DE USO SEGURO DA INTERNET PARA USUÁRIOS LEIGOS

Trabalho de Conclusão de Curso (TCC) I e II elaborado e apresentado como requisito parcial para obtenção do título de bacharel em Sistemas de Informação pelo Centro Universitário Luterano de Palmas (CEULP/ULBRA).

Orientador(a): Prof.ª M. Sc. Madianita Bogo Marioti.

Palmas – TO

2016

Jarbas Lopes Sousa Pereira

GUIA DE USO SEGURO DA INTERNET PARA USUÁRIOS LEIGOS

Trabalho de Conclusão de Curso (TCC) I e II elaborado e apresentado como requisito parcial para obtenção do título de bacharel em Sistemas de Informação pelo Centro Universitário Luterano de Palmas (CEULP/ULBRA).

Orientador(a): Prof.ª M. Sc. Madianita Bogo Marioti.

Aprovado em: _____/_____/_____

BANCA EXAMINADORA

_____

Prof.ª M. Sc. Madianita Bogo Marioti

Orientador

Centro Universitário Luterano de Palmas – CEULP

_____

Prof.º M. Sc. Fabiano Fagundes

Centro Universitário Luterano de Palmas - CEULP

_____

Prof.º M. Sc. Fernando Luiz de Oliveira

Centro Universitário Luterano de Palmas - CEULP

Palmas – TO

2016

Por sofrer nas minhas derrotas e rejubilar nas minhas conquistas, dedico este trabalho à minha mãe, dona Adalgisa. Além de mãe, é conselheira, amiga, confidente e por isso dedico. Dedico ainda, à minha filha Heloísa por ter sido a fonte de inspiração para esta conquista.

AGRADECIMENTOS

Nem sempre é fácil vencer, graças a Deus tive a ajuda de algumas pessoas às quais gostaria de agradecer.

Neste primeiro momento gostaria de agradecer a Deus pela minha vida, por me manter saudável a maior parte do tempo, pelas condições financeiras que me proporcionou concluir os estudos e pelas pessoas que cruzaram meu caminho nesta etapa da graduação, pois todas de alguma forma contribuíram para este momento de conquista e felicidade.

Quero neste momento agradecer os meus irmãos Marceone, Carlito, Gedeão, meu pai o senhor Josias e Minha Mãe dona Adalgisa, pelas ajudas financeiras quando necessitei.

Agradecer aos meus professores pelo melhor que puderam ser em sala como profissionais e pessoas para que eu pudesse levar o conhecimento, a ética, o profissionalismo na minha vida e colegas da faculdade que em algum momento ajudaram com as dúvidas em disciplinas diversas. Em particular, a professora Mádia, minha orientadora neste Trabalho de Conclusão de Curso, com paciência de mãe, conhecimento de um bom profissional, que é, soube me orientar, a fim de que superasse as dificuldades durante todo o desenvolvimento do trabalho, obrigado.

“Uma rede é um conjunto de nós interconectados” Manuel Catells.

RESUMO

Este trabalho tem por objetivo desenvolver um guia de uso seguro da Internet para usuários leigos, que apresenta boas práticas de segurança para navegação na Internet. Uma das justificativas deste trabalho é o fato da Internet ser um ambiente em que há muitas ameaças que exploram vulnerabilidades e invadem os equipamentos e redes de usuários. Como muitos dos usuários são leigos ou simplesmente estão iniciando a experiência de utilização da Internet, o guia pode auxiliar estes usuários a terem experiência satisfatória, fazendo uso de boas práticas de segurança e evitando contratempos. Assim, o presente documento apresenta os principais riscos encontrados na Internet, bem como as suas consequências, dicas de prevenção, como realizar ações de segurança e como as leis brasileiras tratam essa questão.

Palavras-chave: Segurança da Informação, Internet, usuário.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

API – *Application Programming Interface*

ARPANET – *Advanced Research Projects Agency Network*

CF – Constituição Federal do Brasil

C&C – *Command and Control*

CGI.BR – Comitê Gestor da Internet no Brasil

CNPJ – Cadastro Nacional de Pessoa Jurídica

CPF – Cadastro de Pessoa Física

CPB – Código Penal Brasileiro

DNS – *Domain Name System*

DOS – *Disk Operating System*

DoS – *Denial of Service*

DDoS – *Distributed Denial of Service*

EUA – *United States of America*

HTTP – Hiper Text

HTTPS – Hiper Text

HD – *Hard Disk*

ISP – *Internet Service Provider*

IP – *Internet Protocol*

ISO – *International Organization Standardization*

MCI – Marco Civil da Internet

PGP – *Pretty Good Privacy*

SMS – *Short Message Service*

TCP – *Transmission Control Protocol*

SUMÁRIO

1 INTRODUÇÃO

A Internet é um universo virtual recheado de informações e possibilidades, que pode ser usado para disponibilizar serviços, acesso a plataformas sociais, compartilhamento, integração e negócios diversos. Utilizando a Internet um usuário pode, por exemplo, estudar à distância, entregar o imposto de renda, realizar uma compra em uma loja virtual, fazer pesquisas, comunicar-se com outras pessoas, fazer uma transação bancária, participar de redes sociais. Logo, o uso da Internet é amplo e a rede de opções e possibilidades é gigantesca.

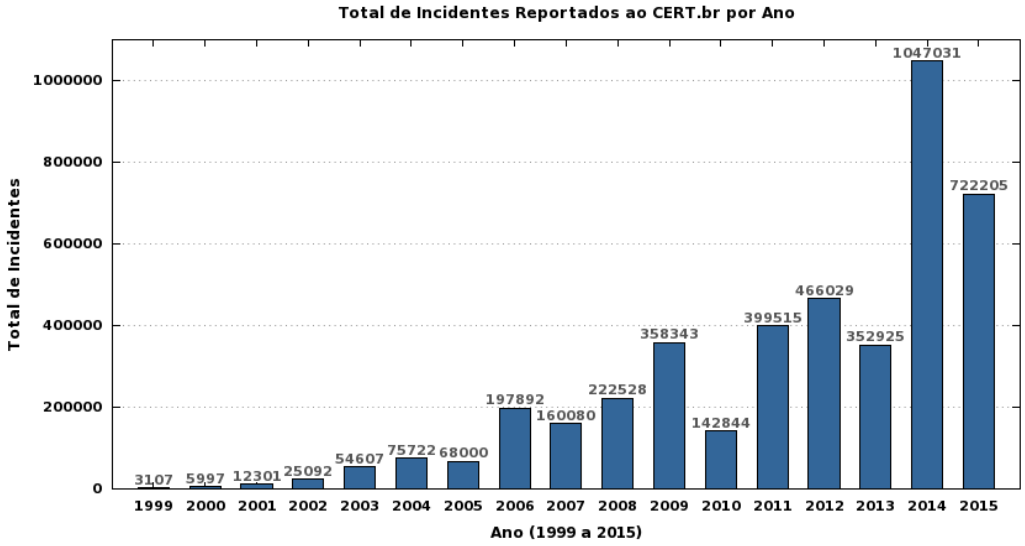
Segundo o IBGE (2014, p. 49) em o uso da Internet por atividade principal, destaca-se a área da "educação, saúde e serviços sociais em segundo lugar" no *ranking*, ficando em "primeiro lugar o uso da Internet para outras atividades".

Ao utilizar a Internet, os usuários devem estar cientes que, a maioria do que existe no virtual é real, seja uma empresa ou pessoa, logo, os problemas do uso refletem na vida real dos usuários. Por exemplo, uma compra mal sucedida em um *site* eletrônico gera prejuízo real ao usuário. Acessar um *e-mail* comprometido, que trás consigo um código malicioso, pode expor o computador e todas as informações nele armazenadas.

Não é incomum notícias de pessoas que tiveram fotos e/ou vídeos comprometedores disponibilizados na Internet, causando sérias consequências na vida pessoal e profissional. Um dos casos mais conhecidos no Brasil é o da atriz Carolina Dieckmann, que teve seu computador invadido por "*Hackers* de Minas e São Paulo", e suas fotos íntimas roubadas, que posteriormente foram divulgadas na Internet. Esses indivíduos enviaram-lhe "*Spam* via *e-mail*". A função do *Spam* era de abrir caminho para que os indivíduos instalassem ferramentas adequadas para esse tipo de delito (REDE GLOBO DE TELEVISÃO, 2012, *on-line*).

No entanto, este não é um caso isolado. Por ano ocorrem dezenas de milhares de incidentes relacionados à segurança na Internet. Conforme dados do CERT.br entre os anos de 1999 a 2015 o número desse tipo de ações cresceu significativamente, como ilustra a Figura 1.

Figura 1: Incidentes reportados ao CERT.BR (CERT.BR, 2015, *on-line*).



Entre os incidentes apresentados no gráfico da Figura 1, a fraude é o tipo de incidente em evidência. Fraude caracteriza-se como qualquer ato de má fé, ou seja, tentativa de enganar a vítima para obter vantagem/lesar. Segundo Michaelis (2016, *on-line*) a fraude é "ato de má fé que tem por objetivo fraudar ou ludibriar alguém... ato de falsificar documentos e produtos... mentira ardilosa".

Assim, independente do equipamento utilizado, do tipo de rede e da necessidade para acesso à Internet, usuários devem atentar-se para a qualidade de uso da rede. Isso inclui cuidados com a segurança do *hardware*, do *software*, experiência do usuário e até a maturidade de vida.

O acesso à Internet cresce a cada ano. No *ranking* de países que passam mais tempo navegando o "Brasil se destaca em terceiro lugar no mundo" de acordo com (ECOMMERCEBRASIL, 2015, *on-line*). A faixa etária de pessoas que mais utilizam a Internet no Brasil segundo o IBGE (2015, p. 47) é "pessoas entre 15 a 17 anos", confirmando os dados da análise por ocupação principal, quando se destaca a educação, nesta faixa de idade os estudantes utilizam bastante a Internet como fonte de pesquisa, comunicação, armazenamento e confecção de trabalhos. Muitos desses usuários agem por curiosidade, e não tem noção do perigo real de uso da Internet.

Neste contexto, o presente trabalho tem como objetivo apresentar um guia para uso seguro da Internet para usuários leigos, pois é evidente o quanto a rede pode ser útil se usada de maneira segura, da mesma forma, pode levar a consequências indesejadas quando se está vulnerável aos incidentes de segurança. Neste guia, o usuário leigo pode conhecer as principais vulnerabilidades que existem no mundo virtual, atentar-se para riscos, bem como encontrar dicas de como navegar de forma segura e proteger suas informações.

Para a realização deste trabalho fez-se necessário um estudo detalhado sobre os assuntos relacionados. O resultado deste estudo está apresentado neste trabalho da seguinte forma: Referencial Teórico (capítulo 2), onde são apresentados os conceitos relacionados à Internet (seção 2.1); Além dos conceitos de utilização da Internet (2.1.1), os Usuários da Internet (2.1.2) e principais tipos de Fraudes Eletrônicas (2.1.3); Aborda, também, conceito de Segurança da Informação (2.2). O trabalho ainda apresenta Materiais e Métodos (capitulo 3) utilizados durante a realização do trabalho; Resultados e Discussão (capitulo 4), apresentando um guia seguro para navegação na Internet confeccionado com a aplicação dos conceitos estudados; Considerações Finais (5), informando as conclusões obtidas durante o desenvolvimento do trabalho; Referências Bibliográficas (capitulo 6), que apresentam as referências dos trabalhos utilizados durante a confecção deste trabalho.

2 REFERENCIAL TEÓRICO

Esta seção apresenta os conceitos necessários para a compreensão do contexto do trabalho, que são: Internet (seção 2.1), que abrange: utilização (subseção 2.1.1), usuários (subseção 2.2.1) e fraudes eletrônicas (subseção 2.1.3); Segurança da Informação (seção 2.2).

2.1 INTERNET

Segundo o CGI.BR (2013, p. 61), "conectar as redes por pacotes de rádio e satélite com o ARPANET (*Advanced Research Projects Agency Network*) foi o ponto de partida para a Internet de hoje como um conjunto mundial de redes interligadas". Para que estes diferentes equipamentos tecnológicos interagissem entre si de forma eficiente fez-se necessário criar regras específicas de comunicação, conhecidas como protocolos.

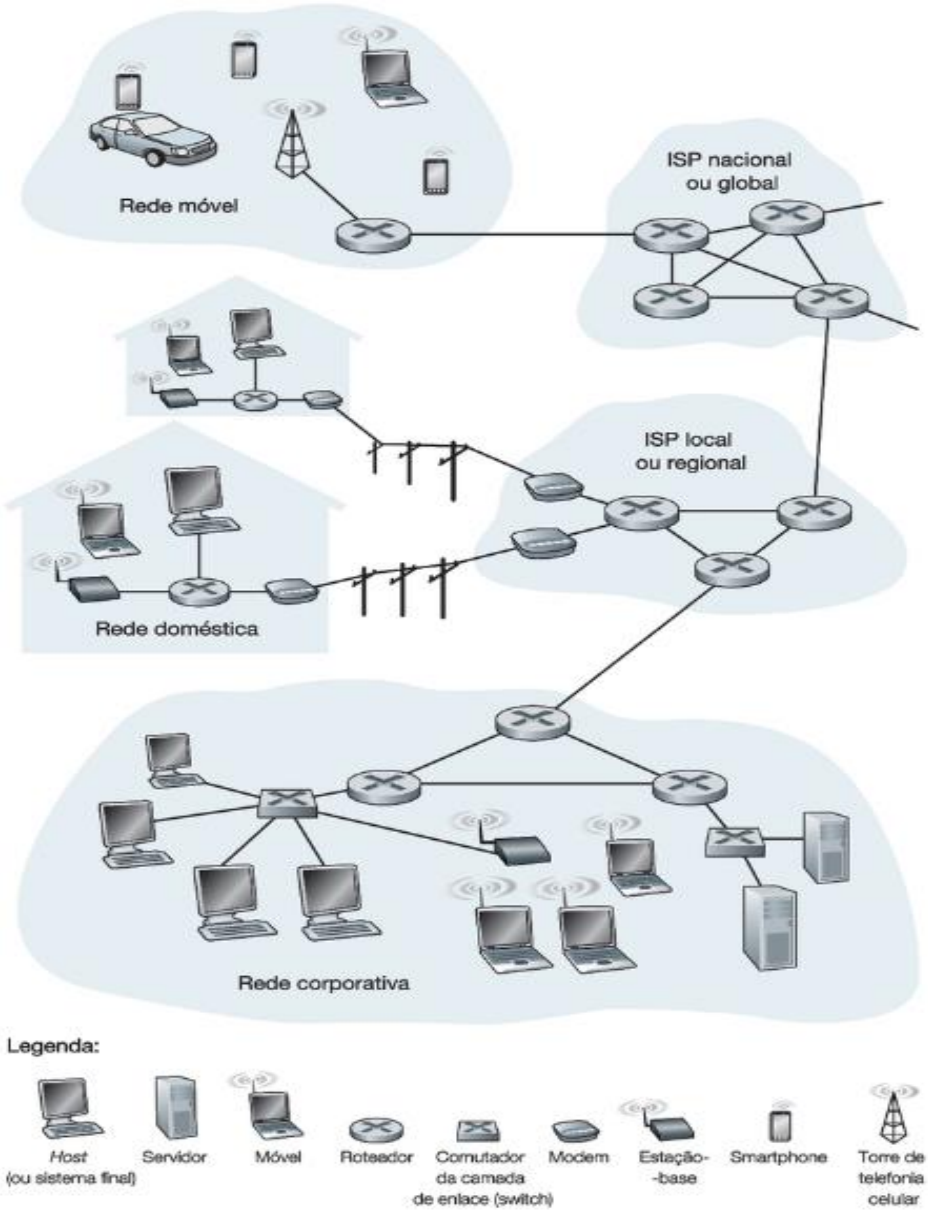
Os protocolos permitem a comunicação entre equipamentos e meios de comunicação heterogêneos, por exemplo, o grupo TCP/IP (*Transmission Control Protocol* / *Internet Protocol*) torna possível a comunicação de computadores em redes distintas (SOCOLOFSKY; KALE, 1991). Assim, a Internet deslanchou podendo ser acessada de lugares e equipamentos diferentes, através de tecnologia fixa ou móvel, usando redes cabeadas ou sem fio.

Desde que foi criada, a rede mundial de computadores cresce de forma exponencial, trazendo novos horizontes para a economia e comunicação. É quase impossível imaginar um mundo sem *E-Mail*, redes sociais, *sites* de compras e tantos outros recursos disponíveis no ambiente virtual.

Para Kurose e Ross (2013, p. 1) a Internet da atualidade "é provavelmente o maior sistema de engenharia já criado pela humanidade, com centenas de milhões de computadores conectados, enlaces de comunicação e comutadores; bilhões de usuários...", a ela já está presente em todas as áreas de trabalho, por exemplo, no campo integrando equipamentos de precisão utilizados na lavoura. E mais recente em objetos domésticos, conhecida por a Internet das coisas.

A Figura 2 ilustra de forma parcial componentes da Internet.

Figura 2: Alguns componentes da Internet (KUROSE; ROSS, 2013, p. 3, *on-line*).



A Figura 2 ilustra alguns equipamentos da Internet, como pode ser observado na legenda da esquerda para a direita: o *Host*, Servidor, Móvel, Roteador. *Switch*, Modem, Estação-base, *Smartphone* e Torre de telefonia celular.

O *Host* é qualquer tipo de equipamento ligado à Internet; o Servidor é o computador que disponibiliza um serviço ou compartilhamento, por exemplo; móvel são todos os equipamentos que acessam a rede de maneira não física, por exemplo, o *notebook* e o *Smartphone*; roteador tem a função de encaminhar os dados ou pacotes de um ponto a outro, geralmente usado entre redes distintas; comutador tem a função decodificar os pacotes que chegam e identificar o endereço exato do destinatário; o modem é um modulador e

demodulador de sinais, de analógico para digital e digital para analógico; a Estação-base conecta equipamentos a um ponto, no exemplo ao comutador ou *Switch*; a Torre de telefonia celular, a qual recebe o sinal de Internet de um ISP (*Internet Service Provider*) e transmite o sinal de Internet, distribuindo aos consumidores. A ilustração ainda apresenta o provedor de serviço de Internet (ISP), que pode ser global ou regional, e tem a função fornecer o sinal de Internet.

No entanto, apesar da importância da utilização da Internet, chamam a atenção as vulnerabilidades e riscos que ela proporciona em especial para usuários. Toda essa estrutura da Internet estreita o caminho entre um ponto de origem e o destino numa comunicação e, na maioria das vezes, o usuário nem faz ideia da complexidade que envolve uma simples troca de mensagem. Toda essa logística, envolve tecnologia desde *hardwares* e *softwares*, políticas de segurança, autenticações, controle de acesso, sistemas de detecção, filtros, barreiras de segurança, regras, leis e profissionais. Mas, tanto equipamentos, *softwares*, quanto a pessoas são passíveis de fraudes eletrônicas que colocam a segurança do tráfego em risco.

2.1.1 UTILIZAÇÃO

A utilização da Internet no Brasil cresce a cada ano, para diversas finalidades e por usuários das várias áreas de atuação. “A Internet se tornou o terceiro maior veículo de alcance no Brasil, atrás apenas de rádio e TV”, sendo que, 87% dos usuários buscam por produtos e serviços (TO BE GUARANY, 2015). A Figura 3 ilustra o percentual de pessoas que utilizam a Internet, segundo os grupamentos de atividade do trabalho principal no Brasil.

Figura 3: uso da Internet segundo os grupamentos de atividade do trabalho principal (IBGE, 2014, p.49).

A Figura 3 apresenta o uso da Internet, ficando óbvio que seu uso não se restringe a uma área, mas que é utilizada para várias áreas de atividade. Outras atividades possuem o maior percentual de uso em relação às demais atividades de ocupação. Estão incluídas nessa categoria as redes sociais como, o *Facebook*.

Na educação a Internet está presente nos cursos à distância, em bibliotecas virtuais, nas pesquisas escolares, na qualificação dos profissionais, assim, quebrando paradigmas e instigando a curiosidade e motivando o aprendizado.

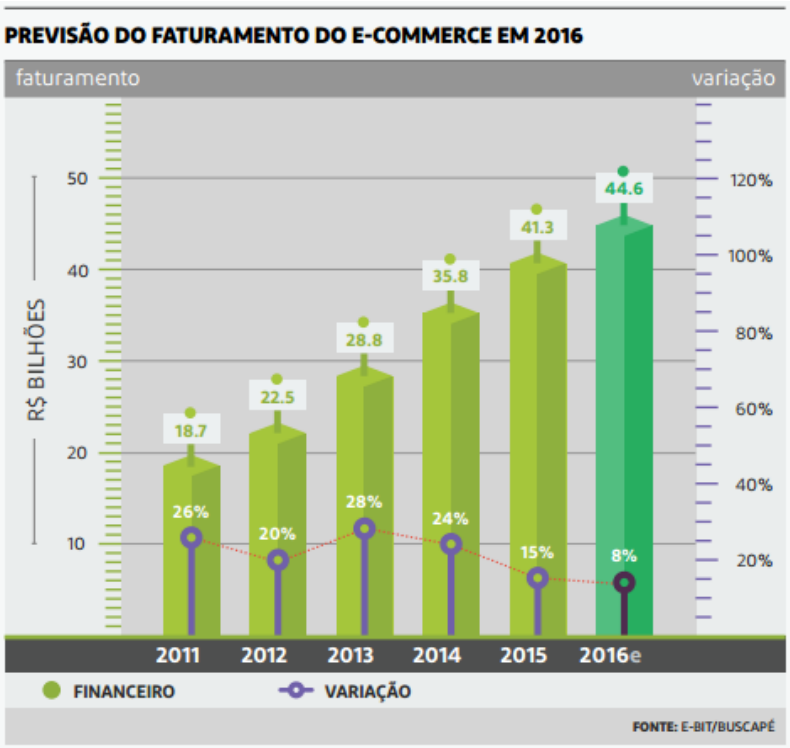
As indústrias tiveram que reorganizar as formas de produção e distribuição, para atender as exigências do mercado consumidor, por produtos com interação com a Internet, por exemplo, hoje em dia é possível encontrar TV's que rodam filmes direto da rede.

Venda não presencial é uma utilização da Internet para o comércio, expandindo de forma grandiosa o número de clientes, esse ramo de atividade tem aos poucos ganhado a confiança dos usuários da rede.

Na construção, a Internet está presente na troca de informações entre profissionais, compartilhamento e uso de dados estatísticos do mercado da construção, para aprendizado e como vitrine.

A Internet proporciona um ambiente muito chamativo para realizar compras, pois a concorrência é acirrada e os comerciantes virtuais tentam atrair o consumidor com promoções e preços menores do que no mundo real. Dados estatísticos apontam crescimento contínuo do *e-commerce* no Brasil, a Figura 4 ilustra essa evolução e a previsão para 2016.

Figura 4: previsão do faturamento do e-commerce em 2016 (E-BIT/BUSCAPÉ, 2016, *on-line*).



A Figura 4 ilustra o crescimento contínuo do comércio eletrônico no Brasil entre os anos de 2011 e 2015, com uma previsão variável para 2016 em torno de 8%. No entanto, na mesma medida que o este segmento cresce, junto a ele cresce também o número de fraudes associadas.

2.1.2 USUÁRIOS

Dezenas de milhares de pessoas usam a Internet todos os dias, quanto mais aprendem a usá-la mais dependentes ficam dela. A seguir, é apresentada a Tabela 1 com dados que apresentam estatísticas de usuários da Internet. A parte superior apresenta o percentual da população, com 10 anos ou mais, que utiliza a Internet. A parte inferior apresenta a quantidade de usuários da Internet, em milhões.

Tabela 1: usuários de Internet no Brasil (TELECO, 2016, *on-line*).

Usuários da Internet (% da POP com 10 ou mais anos)	2011	2012	2013	2014	2015
Fonte: PNAD	46,5%	49,2%	49,4%	54,4%	-
Fonte: TIC Domicílios	46%	49%	51%	55%	58%

Usuários de Internet (Milhões)	2011	2012	2013	2014	2015
Fonte: PNAD	77,7	84,2	85,6	95,4	-
Fonte: TIC Domicílios	76,6	80,9	85,8	94,2	102,0

Como pode ser observado na tabela 1, pode-se perceber que o uso da Internet cresce muito anualmente e que mais de 50% da população tem acesso à mesma. Além disso, em números, de 2011 para 2015 a Internet teve mais de 25 milhões de novos usuários.

Na Tabela 2, são apresentados dados sobre a quantidade de pessoas que nunca acessam a Internet e os usuários de Internet. São considerados usuários de Internet aqueles que acessaram nos últimos três meses.

Tabela 2: usuários de Internet no Brasil (TELECO, 2016, *on-line*).

	2010	2011	2012	2013	2014	2015
Usuário de Internet	41%	46%	49%	51%	55%	58%
Nunca Acessou	52%	47%	45%	42%	39%	34%

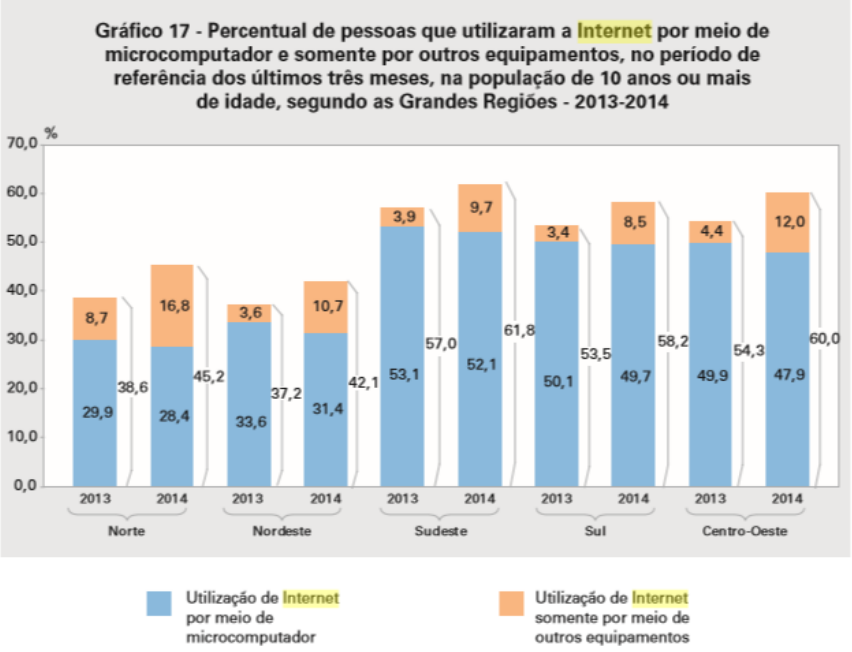
Observando a Tabela 2, é possível perceber uma evolução no número de usuários de Internet, que cresceu muito. Percebe-se que está ocorrendo inclusão digital no país de forma gradual, mas constante a cada ano. No entanto, 34% é um número bem relevante de pessoas que não tiveram experiência com a Internet.

O motivo que leva algumas pessoas a não usurem a rede são variados, boa parte tem receio com os perigos da rede, outra com a falta de privacidade e, ainda, com a falta

segurança nas transações (CETIC.BR, 2015, *on-line*). As pessoas têm a consciência que precisam da Internet, mas, muitos não a usam por falta de habilidades ou por não saber como usar de forma segura e, na dúvida, acabam por não acessarem.

O acesso a Internet é originado de diversos equipamentos como computadores *desktops*, *notebooks*, *tablets*, *smatphones* e celulares, através de redes públicas, privadas e pessoais, em *lan house*s, *cyber* cafés, no trabalho, nas escolas e residências. O uso do celular para navegar teve um crescimento surpreendente, superando inclusive o uso do microcomputador. A Figura 5 ilustra o crescimento do uso de outros equipamentos para acesso à Internet em relação ao microcomputador, segundo as grandes regiões brasileiras.

Figura 5: uso da Internet pelo microcomputador e somente por outros equipamentos (IBGE, 2014, p. 45).



Como ilustrado na Figura 5, o *mobile* é de fato um diferencial na inclusão digital, onde o celular, entre os outros equipamentos, é o que se destaca no uso da rede mundial de computadores, no Brasil há mais celulares do que brasileiros (ECOMMERCEBRASIL, 2015, *on-line*). A Figura 5, ainda ilustra que as regiões brasileiras mais desenvolvidas são as que mais utilizam a Internet e, por fim, que o uso do microcomputador ficou abaixo do uso de outros equipamentos pela primeira vez nos anos de referência.

Independente do tipo de usuário, do equipamento, da rede, do lugar a experiência com o uso da Internet deve ser satisfatório, positivo, que possa de fato contribuir para atender as

necessidades das pessoas e entidades, contudo, é necessário cuidado com as fraudes eletrônicas, que colocam em risco o usuário.

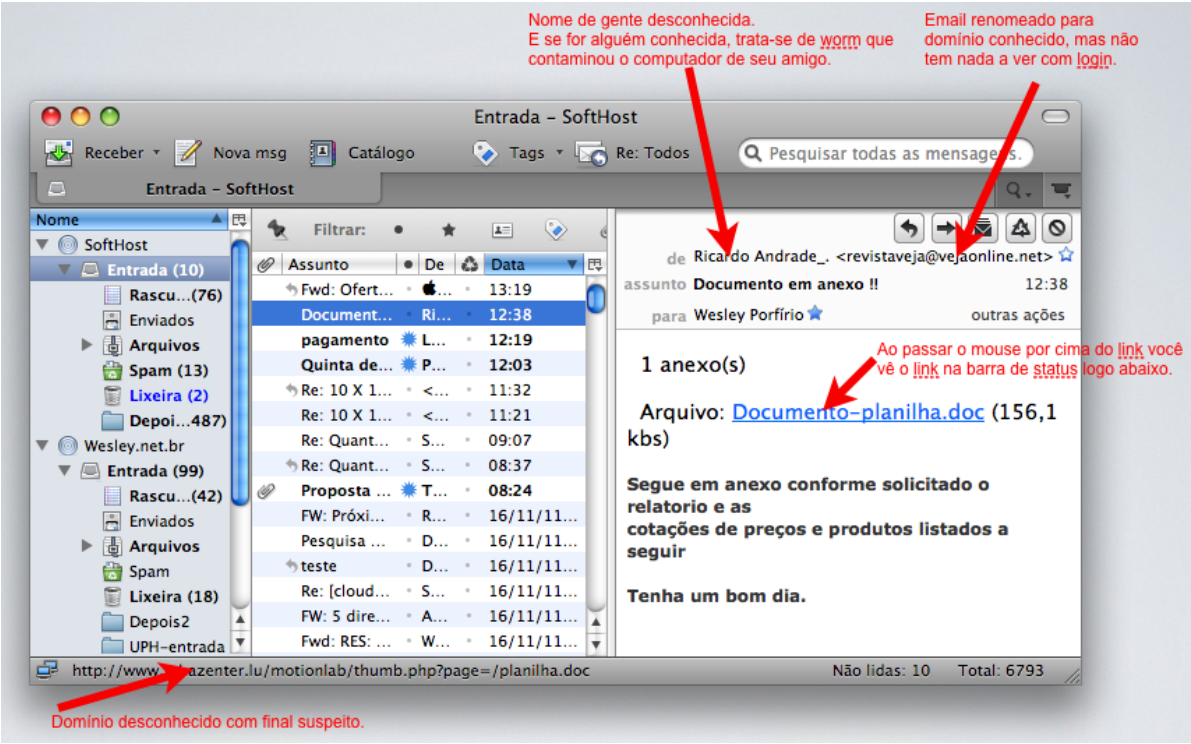
2.1.3 FRAUDES ELETRÔNICAS

Apesar de ser extremamente útil, a Internet esconde muitos riscos, geralmente, associados aos serviços mais utilizados. Estes serviços podem possuir falhas, as quais podem ser exploradas por indivíduos com conhecimento avançado em rede, Internet e programação, mais conhecidos como *crackers* (*hackers* mal intencionados) ou, ainda, pessoas de má índole que utilizam programas criados por esses indivíduos para tentar prejudicar usuários da Internet. Assim, esta seção apresenta as principais fraudes ocorridas na Internet.

2.1.3.1 SPAMS

Na utilização do serviço de *e-mail* é pertinente o risco de *Spam*, que são mensagens que o usuário não pediu para receber. Elas podem conter código malicioso com objetivos bem direcionados como, por exemplo, abrir porta no computador que posteriormente pode ser utilizada para instalar ferramentas específicas para roubar informações e/ou arquivos, senhas e redirecioná-las ao mau elemento via *e-mail*, tudo isso sem o usuário conceder ou perceber. A Figura 6 ilustra um exemplo de um *Spam*.

Figura 6: exemplo de *Spam* (PORFÍRIO, 2011, *on-line*).



Para adquirir endereços de *e-mails*, os *spammers* (quem envia o *Spam*) compram bancos de dados ou criam as próprias listas. Para tanto, usam técnicas como: ataques de dicionário, códigos maliciosos e *Harvesting*. Um código malicioso pode agir coletando endereços de *e-mail* no equipamento em uso e posteriormente enviá-los ao *spammer*; no ataque de dicionário a forma de coleta é baseada em listas de nomes e combinações de caracteres alfanuméricos; já na ação por *Harvesting*, a coleta ocorre por varredura em páginas da *Web* e em listas de discussão.

2.1.3.2 GOLPE PHISHING

O *phishing* é outro problema constantemente encontrado no uso do correio eletrônico, pois é a forma utilizada pelos golpistas para chegar até os usuários. Trata-se de uma fraude em que o remetente tenta de alguma forma convencer o usuário a clicar em um *link* que ele disponibiliza junto com a mensagem de texto. Essa fraude tem a ideia de lesar financeiramente o usuário (SYMANTEC, 2016, *on-line*).

Com a finalidade de atrair a atenção do usuário e forçá-lo a fornecer dados pessoais, os golpistas usam vários temas, com nomes de instituições importantes, intimidação,

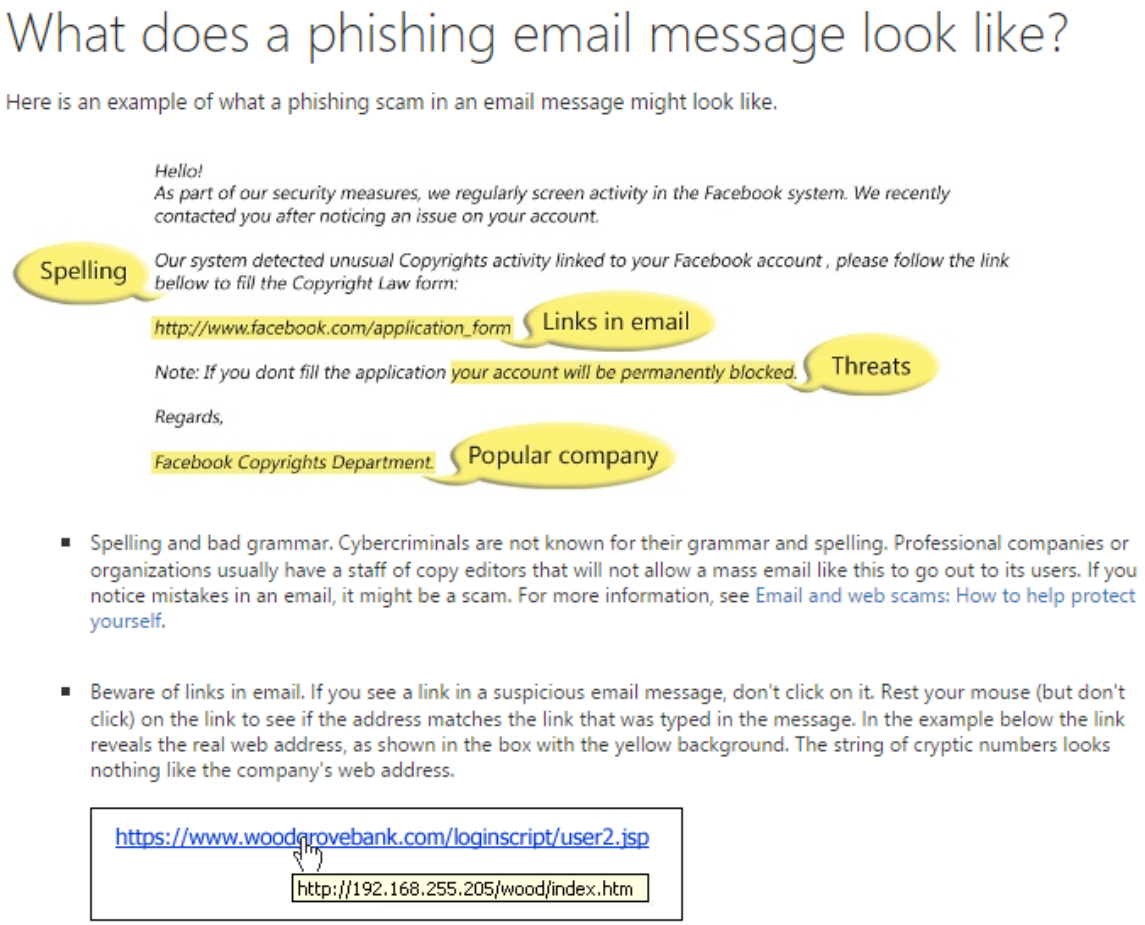
oferecimento de oportunidades de vantagem financeira, entre outros. Por exemplo, envia um e-mail que afirma que um usuário foi selecionado para algum evento ou programa de televisão, mas que para garantir a vaga, a pessoa deve imediatamente fornecer alguns dados pessoais.

Este golpe está presente em vários serviços oferecidos na Internet como: páginas de comércio eletrônico, redes sociais, páginas de serviços bancários e outros. No comércio *online*, a situação pode ser semelhante ao seguinte exemplo: uma mensagem recebida de uma empresa que tem *site* de vendas oferece ao usuário a chance de comprar um produto por um preço muito bom, neste caso, é disponibilizado um *link* para o usuário clicar, o qual redireciona a uma página falsa na Internet onde a vítima efetua a compra, paga por ela e nunca recebe o produto.

O redirecionamento ocorre devido ao fato do serviço de DNS (*Domain Name System*) estar comprometido, ou seja, alterado por um código malicioso ou por meio da ação de um invasor, por exemplo. O *Phishing* com as características de redirecionamento por alteração no serviço de DNS é conhecido, também, por *Pharming* (AVAST, 2016, *on-line*).

Porém, há casos em que a ideia é instalar códigos maliciosos no equipamento da vítima que, ao clicar no *link* fornecido pelo golpista, visualiza uma mensagem de erro pedindo que o usuário instale uma dependência, ou ainda, pedindo para salvar um arquivo que, ao ser aberto, instala o código malicioso. A Figura 7 ilustra um exemplo de um falso link, onde a pessoa vê um nome, mas acessa um endereço diferente.

Figura 7: *phishing* no *e-mail* (MICROSOFT, 2016, *on-line*)**.**



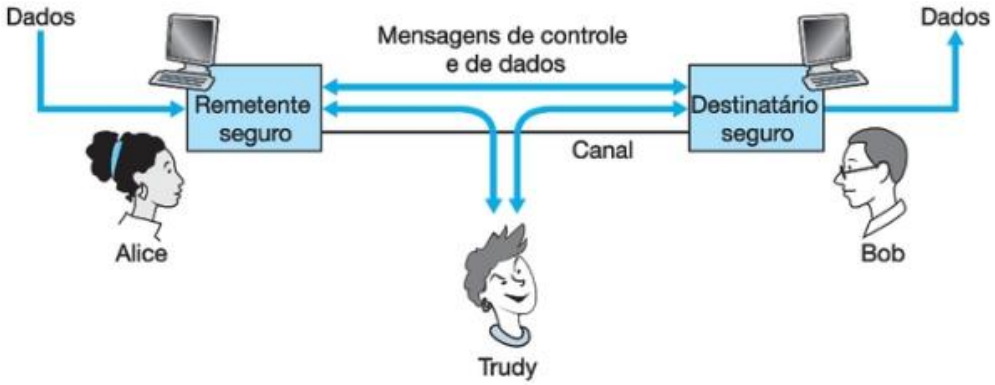
A Figura 7 ilustra uma mensagem típica de *phishing* que disponibiliza um *link* falso. A mensagem dá um aviso ao usuário para que ele regularize a sua situação junto a uma determinada companhia, neste exemplo, o *Facebook*. Logo após informar o caso, pede educadamente ao usuário que clique no *link* e que preencha o formulário. No final da mensagem, faz uma última observação de intimidação, informando que, caso não realize a ação, a conta será bloqueada permanentemente. Por fim, apresenta um *link* com o nome de uma companhia, no entanto, ao descansar o *mouse* sobre o *link* observa-se que um endereço diferente aparece, este endereço trata-se de um IP (*Protocol Internet*), logo, o nome apresentado difere do anterior, esta é uma situação suspeita.

Outra situação semelhante seria aparecer em vez de um nome diferente, no final a extensão apresentar-se executável com terminações como: .com, .exe, .bat, DOS (.src, .cmd (.lnk, .vbx, .pif)). O que seria péssimo para o usuário que clicar sobre o *link*, pois um código malicioso se instalaria ao clicar sobre este *link*.

2.1.3.3 INTERCEPTAÇÃO DE MENSAGENS

Quando se utiliza a Internet, as mensagens em trânsito podem ser interceptadas por terceiros com os mais variados objetivos. O interceptador (pessoa ou programa) pode querer roubar senha e dados, sequestrar uma sessão em curso, tentar ler, alterar e reenviar mensagens ou disfarçar-se de uma das partes comunicantes (KUROSE; ROSS, 2013, p 497). A Figura 8 ilustra a representação gráfica de uma comunicação entre duas partes, onde um intruso (Trudy) está presente.

Figura 8: remetente, destinatário e intruso (KUROSE; ROSS, 2013, p 497, *on-line***)**.



Como ilustra a Figura 8, o invasor pode captar a comunicação de ambos os lados, podendo orquestrar diversos tipos de ataques contra remente e/ou destinatário Assim, uma ou ambas as partes podem ter algum serviço interrompido ou pode ter suas informações roubadas. Por exemplo, a comunicação entre um *Browser* e um servidor *Web* onde ocorre uma transação eletrônica (compra *on-line*) pode ser interceptada, de forma que uma pessoa mal intencionada pode ter os dados do cartão de crédito do usuário.

Para uso seguro de uma comunicação, o usuário deve usar recursos que ofereçam os princípios básicos de segurança, são eles: confidencialidade, integridade e autenticação, detalhados na seção Segurança da Informação.

Uma forma de garantir segurança é usando o PGP (*Pretty Good Privacy*). Segundo Kurose e Ross (2013, p. 522) “o PGP é um esquema de criptografia para *e-mail* que se tornou padrão de fato”, a técnica de uso de criptografia é mencionada na norma ISO 17.799 como um mecanismo de segurança (LYRA, 2008, p.33). Com o uso do PGP o usuário pode garantir o sigilo da mensagem em toda sua trajetória até o destinatário, de igual forma, pode assinar digitalmente esta mensagem, comprimi-la, e garantir que somente a parte interessada terá acesso a ela.

O PGP possibilita ao usuário criar um par de chaves, sendo uma pública e a outra privada, cuja chave deve ser protegida por senha, é utilizada para assinar digitalmente a mensagem do remetente. A chave pública pode ser alocada em servidores de chaves públicas, no entanto, o uso de um certificado emitido por uma entidade legítima de certificação dá maior segurança à chave, pois ocorrem problemas com falsificação e redundância de chaves públicas nos servidores, esta chave serve para verificar a assinatura do remetente no destinatário. O software PGP permite ao usuário criptografar a mensagem antes de enviá-la, logo, esses procedimentos podem ser feitos juntos ou separados, juntos garantem maior segurança.

2.1.3.4 GOLPE NO COMÉRCIO ELETRÔNICO

O comércio eletrônico é uma opção de compra atraente, crescente e que atrai pela diversidade de ofertas, por exemplo. Crescente, também, estão os golpes associados às transações decorrentes do comércio virtual, este ramo de atividade é alvo de diversas fraudes (FAST COMMERCE, 2016, p. 1, *on-line*).

Apesar de existir variações como, a autofraude, quando um indivíduo efetua a compra e diz ser vítima, e a fraude amigável, quando uma pessoa usa o cartão de crédito do titular para realizar uma compra, sem o consentimento dele, usando de má fé ou não, o trabalho focará na Fraude efetiva que é quando um indivíduo ou quadrilha especializada em fraude usa dados obtidos sem o consentimento do proprietário para a prática de golpe na Internet.

Nesse tipo de golpe é explorada, principalmente, a relação de confiança existente entre as partes envolvidas e sempre com o objetivo de obter vantagem financeira. Por exemplo, numa compra *on-line*, quando o usuário cliente confia que está fornecendo seus dados pessoais e de cartão a um *site* confiável, o qual lhe enviará a mercadoria comprada, pode estar passando os dados para um terceiro elemento. Dessa forma, o fraudador, de posse de dados reais obtidos ilicitamente, efetua compras reais gerando prejuízos ao consumidor e ao lojista.

Os golpistas captam dados criando *sites* falsos, usam dados obtidos ilegalmente, envia *Spam*, *links* com códigos maliciosos, propagandas em outros *sites*, promoções muito atraentes de produtos mais comprados e compram os dados de outros golpistas e pessoas associadas a eles. Agem muito em *sites* de compra coletiva, nos quais o usuário tem pouco tempo para

decidir comprar, assim podem atingir uma grande quantidade de vítimas em curto espaço de tempo.

Outro exemplo de golpe ocorre em *sites* de leilão, pode acontecer de ambos os lados da transação comercial tentarem enganar o outro, de um lado o comprador afirma a efetivação do pagamento e exige a mercadoria, enquanto do outro lado o vendedor tenta receber o pagamento sem a intenção de fazer a entrega da mercadoria.

2.1.3.5 FURTO DE IDENTIDADE

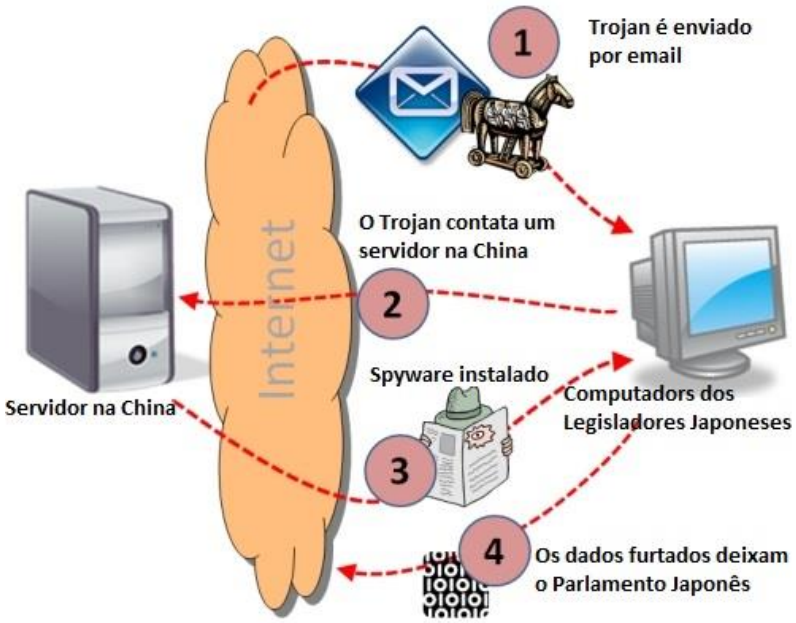
O furto de identidade ocorre quando uma pessoa assume a identidade de outro usuário perante entidades reais ou virtuais, serviços na Internet e terceiros (MCAFEE, 2010, p. 4, *on-line*). Um exemplo clássico é a conhecida página "*fake*" nas redes sociais. Geralmente usada para divulgação, espalhar códigos maliciosos e, de alguma forma, obter vantagens. Nesse caso, o fraudador assume uma falsa identidade para agir indevidamente em nome do verdadeiro proprietário da identidade. A Figura 9 ilustra um exemplo de página falsa na rede social *Facebook*.

Figura 9: página falsa na rede social *Facebook* (TVI24, 2014, *on-line*).

A Figura 9 ilustra uma página *fake* (ou falsa) do Facebook, que enviou diversos convites a fiéis. Nela, o fraudador tenta se passar pelo patriarca de Lisboa. A fraude ficou clara, pois a fotografia utilizada era de um patriarca anterior e não do cardeal José Policarpo (patriarca até julho de 2013) (TVI24, 2014, *on-line*).

Para conseguir as informações, os criminosos usam técnicas através dos meios de comunicação atingindo os principais serviços usados pelos internautas, vasculham lixeiras e caixas de correspondência para captar os dados, enviam *spams* em busca de informações, entre outros recursos. A Figura 10 ilustra um esquema de roubo de dados.

Figura 10: furto de dados **(**MARIANO, 2011, *on-line*).



A Figura 10 ilustra o roubo de dados através do uso de correio eletrônico, onde o usuário acessou uma correspondência infectada por um código malicioso chamado '*Trojan'*, que se instala na máquina e executa ações para as quais fora programado, por exemplo, abre portas deixando o equipamento vulnerável, avisando ao invasor em outra localidade (China). Ao receber os dados, o golpista instala outro programa, chamado '*Spyware*', o qual captura os dados do computador da vítima e os envia de volta.

2.1.3.6 BOATO

Boatos, ou *Hoaxs* (trote, engano, pregar uma peça), são notícias ou mensagens falsas, geralmente trazem temas alarmantes com pessoas, órgãos e entidades conhecidas, notícias apelativas ou que oferecem oportunidades imperdíveis (UOL, 2016, *on-line*). A Figura 11 ilustra um exemplo de boato.

Figura 11: Boato que diz que o *Facebook* será cobrado (LOPES, 2013, *on-line*).

A Figura 11 ilustra o boato de que a rede social *Facebook* será taxada, que é 'oficial' e está 'na mídia', no entanto, não tem a fonte da notícia, pede para divulgar 'colar isto...' o texto e faz intimidação 'caso contrário...', estas são características desse boato, que é muito comum nesse tipo de fraude. Na página inicial ou de *login* do *Facebook* está escrito que "É gratuito e sempre será" (FACEBOOK, 2016, *on-line*). Infelizmente, há boatos mais perigosos que podem levar o usuário a ter prejuízo financeiro, à morte, difamação e expor a segurança de equipamentos em risco.

As redes sociais e *e-mails* são bastante explorados para disseminação de falsos conteúdos, pois atingem um grande número de usuários em curto tempo e, assim, as chances de se tornar viral na rede é maior. Os golpistas podem usar essa oportunidade para espalhar códigos maliciosos e aplicar diversas fraudes.

2.1.3.7 FRAUDE DE ANTECIPAÇÃO DE RECURSOS

Na fraude de antecipação de recursos o golpista tenta receber quantias em dinheiro adiantado, ou captar o máximo de informações sobre a vítima, como dados pessoais e empresariais, bancários, bens, atividade profissional, entre outras.

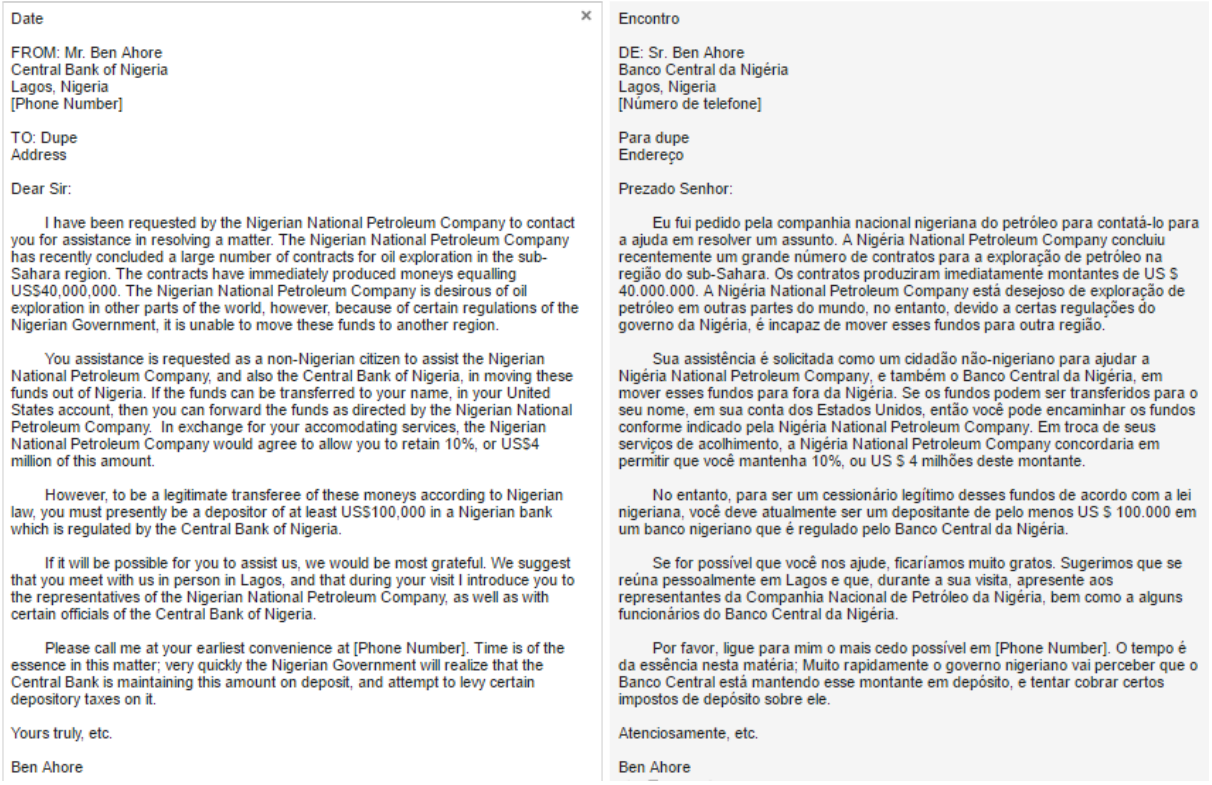
Neste tipo de golpe, geralmente, há oferta de dinheiro, algum tipo de benefício, vantagem financeira, até romance ou chance única ao usuário, valores sempre altos, intermediações fora do país e, para compensar o trabalho da vítima, ela recebe num futuro próximo uma parte que varia entre 10% a 25%.

Porém, antes que a pessoa ponha realmente a mão no dinheiro, os golpistas inventam algum problema, onde e somente, a vítima pode ajudar, sendo que o usuário precisa antecipar algum dinheiro para gastos administrativos, com advogados, subornar alguém. Porém, depois do usuário depositar a grana para os golpistas, eles somem e se reaparecem algum tempo depois é para tentar pegar mais grana.

Outros casos mais perigosos ocorrem quando encontros pessoais são marcados, no país da vítima ou no país que originou o golpe. Quando o encontro ocorre no país do golpista a vítima é ‘depenada’ de seus recursos, através de mentiras e ameaças. “Já ocorreram casos em que vítimas, tentando descobrir o esquema ou obter seus recursos de volta, foram encontradas mortas tempo depois” (QUATLOOS, 2016, *on-line*).

Apesar de ser apenas um exemplo de carta desse tipo de golpe, a Figura 12 ilustra o texto na sua forma original e traduzido para o português.

Figura 12: texto de uma carta da fraude de antecipação de recursos (QUATLOOS, 2016, *on-line*).



Date

FROM: Mr. Ben Ahore
Central Bank of Nigeria
Lagos, Nigeria
[Phone Number]

TO: Dupe
Address

Dear Sir:

I have been requested by the Nigerian National Petroleum Company to contact you for assistance in resolving a matter. The Nigerian National Petroleum Company has recently concluded a large number of contracts for oil exploration in the sub-Sahara region. The contracts have immediately produced moneys equalling US$40,000,000. The Nigerian National Petroleum Company is desirous of oil exploration in other parts of the world, however, because of certain regulations of the Nigerian Government, it is unable to move these funds to another region.

You assistance is requested as a non-Nigerian citizen to assist the Nigerian National Petroleum Company, and also the Central Bank of Nigeria, in moving these funds out of Nigeria. If the funds can be transferred to your name, in your United States account, then you can forward the funds as directed by the Nigerian National Petroleum Company. In exchange for your accomodating services, the Nigerian National Petroleum Company would agree to allow you to retain 10%, or US$4 million of this amount.

However, to be a legitimate transferee of these moneys according to Nigerian law, you must presently be a depositor of at least US$100,000 in a Nigerian bank which is regulated by the Central Bank of Nigeria.

If it will be possible for you to assist us, we would be most grateful. We suggest that you meet with us in person in Lagos, and that during your visit I introduce you to the representatives of the Nigerian National Petroleum Company, as well as with certain officials of the Central Bank of Nigeria.

Please call me at your earliest convenience at [Phone Number]. Time is of the essence in this matter; very quickly the Nigerian Government will realize that the Central Bank is maintaining this amount on deposit, and attempt to levy certain depository taxes on it.

Yours truly, etc.

Ben Ahore

Encontro

DE: Sr. Ben Ahore
Banco Central da Nigéria
Lagos, Nigeria
[Número de telefone]

Para dupe
Endereço

Prezado Senhor:

Eu fui pedido pela companhia nacional nigeriana do petróleo para contatá-lo para a ajuda em resolver um assunto. A Nigéria National Petroleum Company concluiu recentemente um grande número de contratos para a exploração de petróleo na região do sub-Sahara. Os contratos produziram imediatamente montantes de US $ 40.000.000. A Nigéria National Petroleum Company está desejoso de exploração de petróleo em outras partes do mundo, no entanto, devido a certas regulações do governo da Nigéria, é incapaz de mover esses fundos para outra região.

Sua assistência é solicitada como um cidadão não-nigeriano para ajudar a Nigéria National Petroleum Company, e também o Banco Central da Nigéria, em mover esses fundos para fora da Nigéria. Se os fundos podem ser transferidos para o seu nome, em sua conta dos Estados Unidos, então você pode encaminhar os fundos conforme indicado pela Nigéria National Petroleum Company. Em troca de seus serviços de acolhimento, a Nigéria National Petroleum Company concordaria em permitir que você mantenha 10%, ou US $ 4 milhões deste montante.

No entanto, para ser um cessionário legítimo desses fundos de acordo com a lei nigeriana, você deve atualmente ser um depositante de pelo menos US $ 100.000 em um banco nigeriano que é regulado pelo Banco Central da Nigéria.

Se for possível que você nos ajude, ficaríamos muito gratos. Sugerimos que se reúna pessoalmente em Lagos e que, durante a sua visita, apresente aos representantes da Companhia Nacional de Petróleo da Nigéria, bem como a alguns funcionários do Banco Central da Nigéria.

Por favor, ligue para mim o mais cedo possível em [Phone Number]. O tempo é da essência nesta matéria; Muito rapidamente o governo nigeriano vai perceber que o Banco Central está mantendo esse montante em depósito, e tentar cobrar certos impostos de depósito sobre ele.

Atenciosamente, etc.

Ben Ahore

A Figura 12 ilustra um modelo básico do golpe, pois a variedade é muito grande, abordando vários assuntos, mas possível de ser identificados. O conteúdo da carta fala de vantagem financeira para a vítima, oferecendo uma porcentagem alta, desde que a pessoa concorde com os termos apresentados. Mas, o problema é que, normalmente, a vítima nunca chega a receber o que foi prometido e, ainda, pode perder os recursos e expor os dados críticos e a própria segurança em risco.

Os golpistas utilizam o telefone, correio eletrônico e falsas páginas para disseminar na Internet esse tipo de golpe, na sua maioria tem origem na Nigéria (QUATROCANTOS, 2016, *on-line*), porém, outros exemplos já foram registrados como, a noiva russa, loteria federal e crédito fácil.

2.1.3.8 GOLPE BANCÁRIO NA INTERNET

O *Internet Banking* ou Banco *Online* é utilizado há algum tempo e essa utilização vem crescendo em todo o mundo, inclusive no Brasil. Segundo dados da FEBRABAM este “canal foi o responsável pelo maior número de transações em 2015” (CIAB FEBRABAM, 2016, *on-line*).

A instituição financeira é a responsável por garantir a segurança em seus sistemas de transações bancárias, por isso, as instituições brasileiras investem pesado em segurança. No entanto, a transação segura tem outro personagem, o usuário cliente e suas ações podem determinar, também, a segurança das transações.

O usuário deve fazer o acesso de um equipamento seguro, em uma rede segura e usar conexão segura, ainda assim, é preciso estar atento a detalhes de cada passo realizado para não cair em golpes como, o "falso boleto bancário" (IDEC, 2016, *on-line*).

Figura 13: boleto legítimo (à esquerda) e boleto alterado por vírus (à direita) (PUCCINELLI, 2014, *on-line*).

A Figura 13 ilustra um exemplo de boleto de pagamento alterado por ação de um vírus. Neste exemplo, o código de barras passou por mudanças, mas dificilmente o internauta vai perceber a modificação, exceto se já estiver informado e atento.

Para conseguir executar uma ação desse tipo, o golpista primeiro teve que invadir a segurança do equipamento do usuário e instalar código malicioso. Para isso, usa de diversas técnicas como: telefonemas, mensagens via celular ou *e-mail*, *links*, cartas pedindo para acessar falsas páginas.

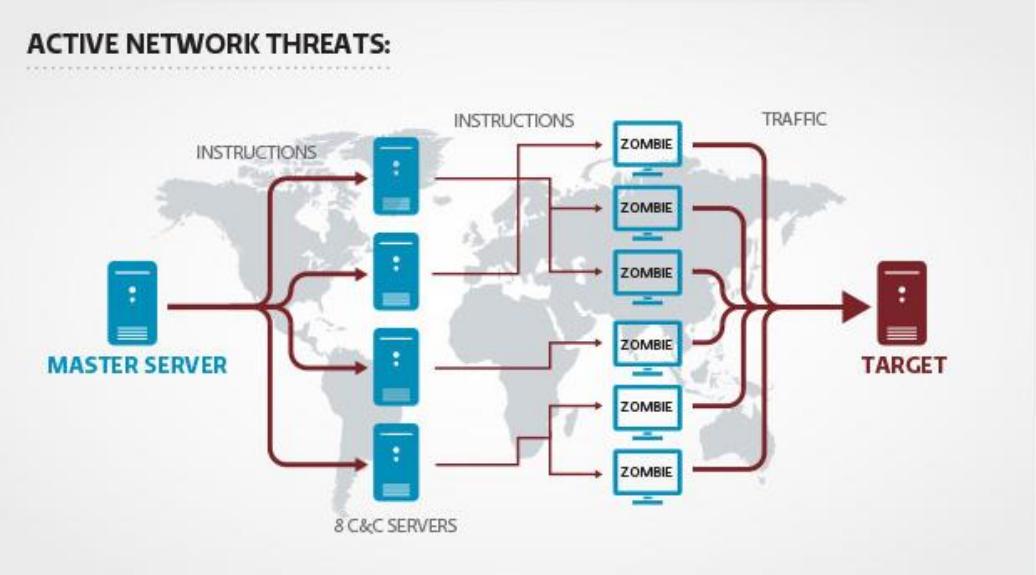
Outro golpe é a transferência *on-line* entre agências, na qual se retira dinheiro da conta da vítima através de transferência *on-line*, praticado com a participação de ex-funcionários do banco ou funcionários legítimos e ativos, pois estes indivíduos têm todo o conhecimento do funcionamento da agência e seus sistemas. Apoderam-se de dados dos clientes e realizam saques e transferências. Vírus também podem alterar os sistemas de segurança da vítima, de

forma que os golpistas podem realizar transações da própria máquina da vítima. Por isso, é importante os programas estarem atualizados e possuir mais de um tipo instalado.

2.1.3.9 ATAQUE DE NEGAÇÃO DE SERVIÇO

Negação de Serviço, DDoS (*Distributed Denial of Service*), trata-se de um ataque em que não ocorre roubo, alterações ou acesso não autorizado. Sua principal ação é tirar de funcionamento um serviço, como uma conversa entre duas pessoas, uma transação comercial ou um servidor *Web*. A Figura 14 ilustra um diagrama do modelo desse ataque.

Figura 14: remetente, destinatário e intruso (KUROSE; ROSS, 2013, p 497, *on-line*).



A Figura 14 ilustra um modelo de ataque de negação de serviço, no qual um servidor mestre coordena outros servidores, os quais são controladores de máquinas *zombies*, ou seja, as máquinas controladas para atacarem juntas a máquina vítima, com o objetivo de sobrecarregá-la a ponto de parar o serviço que provê.

O atacante pode fazer isso de duas formas, “ataque por inundação” ou “ataque por vulnerabilidade” (RNP, 2000, *on-line*). Ataque por inundação consiste em consumir os recursos disponíveis, como processamento e memória, solicitando muitas conexões. Enquanto no segundo tipo, em vez de exaurir os recursos da vítima, procura por vulnerabilidades (DoS) nos *softwares*, usando esta para torná-los indisponíveis.

2.1.3.10 ATAQUE DE VARREDURAS EM REDE

Todo equipamento conectado à Internet fica escutando, ou seja, aguardando requisição de conexão, para isso, deve estar ativo na rede (STALLIVIERE, 2011, *on-line*). No ataque de varredura de rede, primeiro descobre-se que máquinas estão ativas, em seguida é feita uma verificação de atividades do alvo. Na sequência, registram-se as informações coletadas, tais como: portas abertas, fechadas e associadas a um serviço. Assim, o atacante pode associar uma possível vulnerabilidade ao serviço.

A varredura de uma rede pode ocorrer com objetivos legítimos ou não. O administrador de um equipamento pode querer usá-la para descobrir as vulnerabilidades visando corrigir as falhas. Em caso oposto, um mau elemento pode realizar a varredura para descobrir a máquina com conexão aberta, usando-a para distribuir códigos maliciosos.

2.1.3.11 ATAQUE DE FORÇA BRUTA

O ataque de força bruta consiste em tentar adivinhar o nome de usuário e senha através de tentativas e erro. Pode ocorrer pela Internet ou fisicamente caso tenha acesso ao equipamento.

Para ter maior chance de adivinhar os dados corretos, os atacantes usam, entre outras, técnicas como: informações pessoais encontradas nas redes sociais, dicionário de nomes em vários idiomas, trocas de caracteres óbvios, sequências numérica ou de teclado e número de telefone.

Este tipo de ataque pode provocar uma sobrecarga no serviço devido ao grande número de tentativas em curto espaço de tempo, logo, pode se tornar um DoS por inundação. Nesse tipo de ataque, quanto mais simples ou intuitiva for a senha, mais rápido ela será descoberta. A Tabela 3 apresenta um confronto entre o formato de senha, seu comprimento e tempo de decodificação usando um ataque de força bruta.

Tabela 3: formato de senha e comprimento, afeta o tempo de decodificação (CHEETAH MOBILIE, 2014, *on-line*).

Formato de Senha	Comprimento	Tempo Decodificação
Apenas Números	6	1 segundo
Letras: Maiúscula e Minúscula	6	33 minutos
Letras: Maiúscula e Minúscula	8	62 dias
Números + Letras: Maiúscula e Minúscula	8	253 dias
Números + Letras: Maiúscula e Minúscula + Símbolos	8	23 anos

A Tabela 3 deixa claro que uma senha mais forte leva mais tempo para ser decodificadas e que as senhas fáceis demandam pouco tempo.

2.2 SEGURANÇA DA INFORMAÇÃO

Em segurança da informação existe o conceito de "ativo da informação" (LYRA, 2008, p. 5), este engloba desde a própria informação, passando pela tecnologia que a suporta/mantém até quem se utiliza dela. Estes ativos possuem vulnerabilidades que podem ou não ser exploradas por pessoas mal intencionadas ou que desejam apenas testar suas habilidades.

Um ativo que merece destaque é a pessoa, pois, segundo Lyra (2008, p. 19), "pessoas são os elementos centrais de um sistema de segurança da informação", seja do lado ativo ou passivo de um problema ou ataque, estão sempre presentes.

Segundo Lyra (2008, p. 3), três aspectos se destaca e devem ser garantidos quando se trata de segurança na troca de informações, são eles:

- **Confidencialidade**: a informação é acessível somente à parte que é devida. Analogamente em um sistema administrativo todos os usuários podem está ativos, no entanto, as informações do administrador geral devem ser restritas somente a este papel e não a outro qualquer. Em uma comunicação segundo Kurose e Ross (2013, p. 495) "o fato de intrusos conseguirem interceptar a mensagem exige, necessariamente, que esta seja cifrada". Ou seja, o conteúdo da comunicação mesmo sendo capturado, este estará de uma forma não compreensível, embaralhado.

- **Integridade**: a informação no destino deve ser a mesma da origem, sem alterações, compreensível. É possível garantir a integridade, para tanto, torna-se necessário o uso de “extensões das técnicas de soma de verificação que encontramos em protocolos de transporte e de enlace confiáveis” (KUROSE; ROSS, 2013, p. 495).

- **Disponibilidade**: deve estar sempre disponível para ser usada com as devidas finalidades.

Para garantir a segurança das informações, outros aspectos podem ser aplicados, são eles Lyra (2008, p. 4):

- **Autenticação**: garantir que o usuário deve ser quem diz ser. Visualmente pode-se acreditar que uma mensagem recebida por um amigo ou *e-mail*, seja daquela pessoa, mas afirma Kurose e Ross (2013, p. 495) que “quando entidades comunicantes trocam mensagens por um meio pelo qual não podem ver a outra parte, a autenticação não é tão simples”. Esta afirmação alerta para a segurança numa comunicação, ou seja, se não houver como ter certeza que o remetente é de fato quem diz ser, pode ser um intruso.

- **Não-repúdio**: capacidade de provar que um certo usuário fez determinada ação no sistema.

- **Legalidade**: garantir que o sistema esteja de acordo com as leis específicas e atuais.

- **Privacidade**: garantia de anonimato ao usuário, não fazendo relações dele com ações no sistema.

- **Auditoria**: capacidade de registrar todas as ações ocorridas em um sistema, fraudes e tentativas de ataque.

Os mecanismos para garantir a segurança existem, no entanto, usuários devem habituar-se em usá-los. Um usuário atento pode se proteger de muitos perigos, mas não deve excluir a necessidade dos mecanismos de segurança disponíveis. Tais mecanismos precisam de configurações adequadas, corretas e para que seja possível, o

usuário deve conhecê-los, portanto, tem papel fundamental para garantir segurança às informações.

3 MATERIAIS E MÉTODOS

Nesta seção são apresentados os recursos e métodos utilizados durante o desenvolvimento deste trabalho.

3.1 MATERIAIS

Dos materiais, para que fosse possível a realização deste trabalho foram utilizados recursos próprios e da instituição de ensino. Recursos próprios como: computador pessoal e *softwares*; Recursos da instituição como: laboratório de informática e a Internet.

Dentre os materiais utilizados no referencial teórico estão: artigos científicos, teses de mestrado e doutorado, trabalhos de conclusão de curso, livros que abordam o assunto, vídeos sobre configurações e segurança, filmes sobre segurança e invasão, entrevistas informais com profissionais da área de segurança, conversas informais com usuários leigos, dados estatísticos nacionais e internacionais sobre o uso da internet, vulnerabilidades, riscos *on-line*, tipos de usuários e o que eles acessam.

3.2 METODOLOGIA

Da metodologia, a princípio fez-se revisão de literatura e aprofundamento dos conceitos necessários. Em seguida, a confecção do conteúdo teórico, na sequência o desenvolvimento do guia com base nos conhecimentos adquiridos.

Em primeiro momento buscou-se um aprofundamento referente aos conceitos relacionados ao trabalho em questão, como: Internet, a qual abrange assunto de sua utilização, tipos de usuários e fraudes eletrônicas, e ainda Segurança da Informação.

Nesta etapa a dificuldade fora tentar limitar a quantidade de informações e classifica-las. Portanto, as informações selecionadas foram as que mais tinham haver com o contexto do

trabalho e a classificação se deu pela importância da fonte e conteúdo. Com as informações necessárias deu-se início a segunda etapa do trabalho.

Num segundo momento iniciou-se a confecção da parte teórica, a qual daria a base necessária para o desenvolvimento do guia.

Nesta etapa, ao passo que andava a produção do texto, riscos de detalhar/testar bastante um assunto ou outro foi pertinentes, solucionado somente na qualificação, quando a orientação apresenta uma opção a ser seguida para se checar a conclusão do projeto. Só então, a confecção da parte teórica ganhou sentido. Após a parte teórica ter avançado, inicia-se a parte prática do trabalho.

E finalmente deu-se início a confecção do guia, o qual ganhou uma estrutura que favorece a compreensão do usuário e ao mesmo tempo o estimule a continuar. A estrutura definida para o guia está ilustrado na Figura 15.

Figura 15: estrutura do guia.

A Figura 15 apresenta a estrutura definitiva do guia, intuitiva e hierárquica, primeiro destaca-se o serviço em uso, seguido do risco associado a este serviço, logo na sequência os temas correlatos ao risco em questão. Assim, o usuário chega rapidamente ao ponto de seu interesse e consegue as informações que necessita para uma navegação segura.

4 RESULTADOS E DISCUSSÃO

Os usuários de Internet no Brasil iniciam suas experiências bem cedo, órgãos de estatísticas registram dados de acesso a partir dos 10 anos de idade, destacando-se os jovens, seguido por usuários mais velhos (IBGE, 2014, p.47). Entre os iniciantes existem pessoas de toda faixa de idade, as quais justificam suas ausências na rede por falta de habilidade, receio de perigos, falta de privacidade e segurança. Logo, muitos são leigos na área de informática e, pensando em ajudar esses usuários, decidiu-se fazer um manual que os ajude a se prevenir e obter boas práticas na utilização da Internet, que é apresentado a seguir.

4.1 SERVIÇOS: RISCOS E PREVENÇÃO

As seções a seguir compõem um guia rápido de consulta, que apresenta os serviços *web* mais acessado e, para cada um deles, o tipo de risco associado, suas consequências, como se prevenir, forma prática de agir e, ainda, como as leis brasileiras tratam cada um deles.

4.1.1 E-MAIL

O serviço de correio eletrônico é um dos serviços mais utilizados na Internet, pois encurta distância, aproximada pessoas e é eficiente na troca de informações. Entre outras opções, com o serviço de *e-mail* é possível compartilhar textos, imagens e vídeos. Este serviço está disponível em duas modalidades livre e pago, nas versões pagas é possível ter opcionais e mais segurança.

Torna-se importante a utilização do e-mail de maneira segura, uma vez que os dados transmitidos através de seu uso podem ser interceptados, alterados ou infectados por códigos maliciosos. Usando este serviço de modo seguro é possível saber a sua origem real e destino, Por exemplo, um *e-mail* assinado digitalmente por uma certificadora credenciada pode ser usado como prova judicial, pois sua autenticidade pode ser comprovada.

Assim, esta subseção apresenta riscos associados ao serviço de correio eletrônico, as consequências que estes riscos podem causar ao usuário, meios de prevenção, como realizar as ações necessárias para usar o serviço de forma segura e o como as leis brasileiras tratam essas questões. A Figura 16 ilustra o serviço de *e-mail* na estrutura definida para o guia, de igual forma os riscos associados.

Figura 16: serviço de *e-mail* e riscos associados apresentados no guia.

- Risco 1
  - *Spam.*

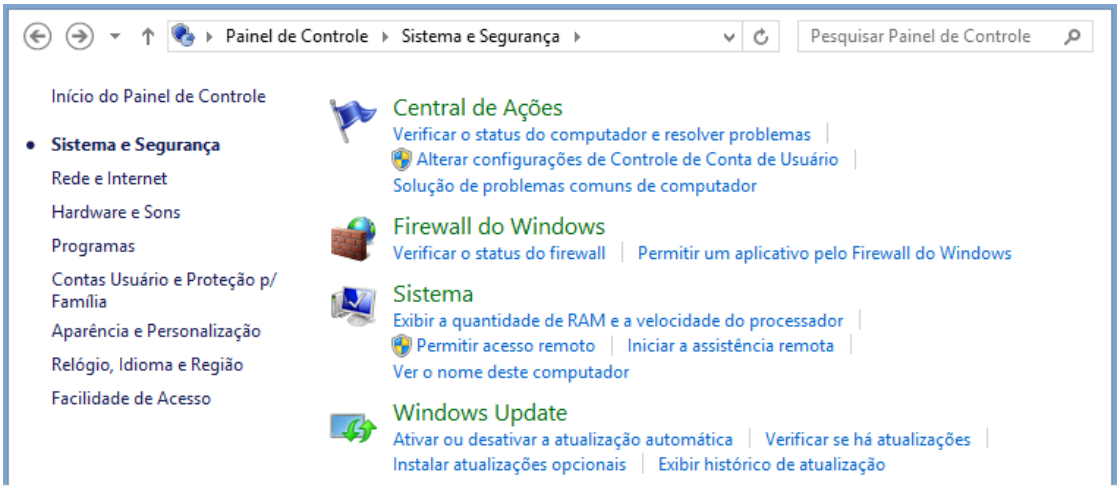
    - Consequência:
      - classificação errada de mensagens;
      - perda de mensagens;
      - não recebimento de correspondência;
      - perda de tempo;
      - se deparar com conteúdo agressivo, ofensivos e de má fé;
      - infectar o sistema e/ou equipamento em uso.

    - Prevenção:
      - analisar a correspondência (remetente, assunto, texto, *link* e anexo);
      - desconfiar de texto que promete, sugere, fala de leis, tentam convencer a comprar ou fornecer dados de cartões e/ou pessoais. Nesse caso, é aconselhável excluir e classificar como *Spam*;
      - usar *software* especializado, como *antispam* e *firewall* pessoal;
      - usar filtros do serviço;
      - verificar as marcações pré-habilitadas nos formulários e *logins*;
      - ao encaminhar mensagens, retirar os antigos destinatários;
      - criar e usar *e-mails* diferentes e não intuitivos, como joao@gmail.com;
      - não fornecer o *e-mail* sem realmente haver necessidade;
      - nunca fornecer dados pessoais e senhas por *e-mail*;
      - desabilitar execuções automáticas de códigos, como Java *Script*.
      - nunca clicar ou seguir *link* de *e-mails* que não tenha certeza que é confiável;
      - nunca abrir anexo sem antes examinar com um bom programa antivírus;
      - manter os *softwares* atualizados e com validação atualizada;
      - verificar certificado, campos como: validade, requerente e quem emitiu.

    - Como fazer:
      - no endereço http://www.spamfighter.com/SPAMfighter/Lang_PT/Product_Info.asp é possível adquirir um programa *antispam* de fácil instalação e execução. Após a instalação, é disponibilizada uma página contendo todas as explicações para usar o *software*;
      - no endereço http://pc-tools-firewall-plus.softonic.com.br/ é possível fazer o *download* de um programa de *firewall* pessoal de fácil instalação e uso;
      - no endereço https://www.avira.com/pt-br/free-antivirus-windows, o usuário poderá fazer o *download* da versão mais recente de um antivírus. E, no endereço https://www.youtube.com/watch?v=DiryeRxJPjU são disponibilizadas informações de configuração. Sempre antes de executar um antivírus é importante atualizá-lo, assim, ele poderá detectar códigos maliciosos mais recentes na sua lista interna de programas maliciosos;
      - o endereço https://www.youtube.com/watch?v=CQhuffVH5cE ensina o passo a passo para configurar filtro em um serviço de *e-mail*, assim, dando ao usuário informações possibilitam compreender e utilizar o serviço de forma correta;

- neste endereço https://www.youtube.com/watch?v=CQhuffVH5cE o usuário encontra um vídeo que o ajudará a com marcadores, criar e gerenciar pastas e ainda a configurar filtro no serviço de *e-mail*;
- para ativar as atualizações do *Windows*, abra o Painel de controle, em seguida escolha a opção Sistema e Segurança, de forma que será apresentada a tela da Figura 16. Em *Windows Update*, ative a atualização automática. É interessante, também, verificar se há atualizações disponíveis e, caso haja, deve-se realizar sua instalação. Para isso, clique sobre o resultado da verificação para iniciar o procedimento de *download*, caso já não tenha ocorrido, e se sim, na sequência deve ser selecionado quais devem ser instaladas, e por fim, seleciona opção instalar, poderá ocorrer mensagens pedindo o reinicio do equipamento.

Figura 17: *firewall* e *Update* no *Windows* 8**.**



- ainda na tela ilustrada na Figura 16, para configurar adequadamente o *firewall*, abra o Painel de controle, em seguida escolha a opção Sistema e Segurança, de forma que será apresentada a tela da Figura 16. Em Verificar o status do *firewall*, várias ações podem ser realizadas, que o antivírus instalado no equipamento já gerencia. Ao retornar à tela da Figura 16, em Permitir um aplicativo pelo firewall do *Windows*, é possível permitir ou negar aplicativos na lista do *firewall*. Logo, se a intenção é remover um aplicativo da lista do *firewall*, abra clicando sobre Alterar configurações, pode ocorrer de pedir senha de administrador ou para confirmar uma escolha, desmarque a caixa de seleção ao lado do nome do aplicativo que deseja remover e confirme em remover;

- ainda sobre *firewall*, devido possuir várias ações de configuração, no endereço https://www.youtube.com/watch?v=65li5-b2X1c, tem um vídeo sobre como executar configurações avançadas no *firewall*, neste outro endereço https://www.youtube.com/watch?v=G4CzdQ9nvj0, o vídeo ensina sobre como habilitar e desabilitar regras no *firewall*. No site da Microsoft no endereço https://technet.microsoft.com/pt-br/library/cc646023(v=sql.100).aspx, é possível conhecer outras ações sobre o *firewall* relacionadas a programas de banco de dados e na própria

área de configuração, após a etapa Permitir um aplicativo, entre em Quais são os riscos de permitir que um aplicativo se comunique? Para mais detalhes de risco e configuração e por fim, o endereço http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml, possui a lista completa de todas as portas e serviços correlatos;

- para verificar os certificados selecione o executável do programa desejado, em seguida com o botão direito do *mouse* selecione propriedades, na janela que abrir selecione a aba Assinaturas Digitais, selecione a linha desejada e escolha o botão detalhes, logo em seguida Exibir Certificado, assim a janela contendo dados do certificado será exibida. Na aba geral, parte inferior será apresentada a validade, na aba detalhes pode-se verificar várias opções, ver, por exemplo, o requerente e na aba caminho de certificação encontra-se a emissora do certificado, a qual se pode verificar sua idoneidade.

- Leis:
  - na legislação brasileira não há uma lei específica contra a prática de *Spam*, ou seja, o envio de mensagens não solicitadas não é crime no Brasil. No entanto, se ocorrer a invasão de privacidade, através do uso ou não do *Spam*, com roubo de dados do usuário, a Constituição Federal (CF) no Art. 5º/X trata como crime a invasão de privacidade.

- Risco 2
  - *Phishing*

- Consequência:
  - páginas falsas criadas com os dados pessoais fornecidos;
  - *e-mails* falsos criados com os dados fornecidos;
  - prejuízo financeiro por compras efetuadas com seus dados de cartões;
  - endividamento devido fornecer dados de cartões ou os dados pessoais;
  - problemas com a justiça;
  - aborrecimentos e desgaste durante o processo de limpeza do nome e provar a idoneidade, que foi vítima de golpe;
  - Ter o nome ou o CPF (Cadastro de Pessoa Física) bloqueado nos órgãos de crédito;
  - Infectar o equipamento em uso, comprometendo a segurança.

- Prevenção:
  - o usuário deve estar atento às suas correspondências, suspeitar e questionar-se;
  - desconfiar de mensagens de remetente que desconhece, do assunto, da insistência no fornecimento de dados pessoais, de cartão de crédito, do favorecimento em troca de alguma coisa, exageros no conteúdo e erros gramaticais;
  - utilizar ferramenta *antiphishing* que, geralmente, já estão integradas ao navegador;

- manter aplicativos e sistema operacional atualizados;
- verificar o tipo de conexão, pois bancos e *sites* de compras sempre utilizam *antiphishing*;
- instalar um *Firewall* pessoal;
- utilizar ferramenta *antimalware*, as quais detectam códigos maliciosos;
- usar uma conta de usuário sem privilégios de administrador no computador;
- configurar o nível básico de segurança recomendado pela empresa do *software*, no programa *SmartScreen* do *Windows*, assim, para executar um aplicativo desconhecido da Internet será exigida a aprovação do administrador. Assim, as páginas visitadas serão analisadas e comparadas com uma lista dinâmica de *sites* de *Phishing* e mal-intencionados. Os arquivos de *download* serão comparados com uma lista de *sites* de *softwares* mal-intencionados;
- configurar a opção *Download* do navegador para perguntar onde salvar cada arquivo antes de fazer o *download*. Isso dá uma chance de cancelar a ação, pois há *sites* que disparam *downloads* automáticos caso esta opção esteja desmarcada;
- consultar o endereço do *site* que deseja acessar antes de acessá-lo, através do *site* vírus total (https://virustotal.com/) é possível fazer uma varredura na página a ser visitada em busca de ameaças;
- analisar o endereço fornecido, pois os golpistas tentam enganar utilizando nomes de grandes empresas com credibilidade no mercado;
- verificar junto à instituição remetente a sua política de privacidade ou segurança, quanto ao uso indiscriminado de mensagens;
- verificar o certificado digital, com a finalidade de saber se pertence mesmo ao *site* verdadeiro;
- se digitar um dado endereço e for redirecionado para outro, o qual pode requerer alguma instalação, não execute a instalação e saia imediatamente do *site*. Pode ocorrer, ainda, de ficar abrindo janelas sem parar até a máquina travar ou reiniciar. O computador deve ser executado em modo de segurança e examinado com as ferramentas de segurança (antivírus, antispam, antimalware), deve-se limpar o histórico de pesquisa do navegador com opção de *cookies*, *cache* e senhas marcadas;
- reportar as tentativas de *Phishing* é importante, pois a partir de dados estatísticos torna-se viável a criação de ações e políticas de combate.

- Como fazer:
  - no Painel de controle, escolher a opção Sistema e Segurança, selecionar *Windows Update* e optar por ativar ou desativar a atualização automática, a Figura 16, apresentada no sub item como fazer do Risco 1 ilustra como chegar até esta etapa;
  - verificar se no campo de endereço do navegador aparece um cadeado no lado esquerdo. Esse cadeado indica que o endereço usa conexão segura (https). Ao clicar no cadeado, são apresentadas, entre outras, informações de certificado digital da página.
    - o cadeado pode ocorrer de aparecer, também, na parte inferior direita da página;
  - criar um usuário sem privilégios de administrador no *Windows*, assim, quando navegar e algum programa mal-intencionado tentar se instalar o

privilégio não será suficiente. Para isso, acesse o Painel de controle, selecione a opção Contas de Usuário e Proteção p/ família, escolha Contas de Usuário, na sequência Gerenciar Contas, opção adicionar uma conta de usuário;

- verificar se o filtro *SmartScreen* está ativado e, caso não esteja, ativá-lo. Para isso, acesse o Painel de controle, Sistema e Segurança, opção Central de Ações e selecione Alterar as configurações do *Windows SmartScreen*;
- nas configurações do navegador, selecionar opção mostrar configurações avançadas, pois nela é possível configurar uma opção que dá ao usuário a chance de escolher salvar ou cancelar e o local que deseja colocar um arquivo baixado da Internet. Para isso, localize a opção *Download* e marque a caixa de seleção onde está escrito "Perguntar onde salvar cada arquivo antes de fazer *download* ";
- no endereço: https://pplware.sapo.pt/microsoft/windows/top-5-ferramentas-anti-malware-para-windows/, são apresentadas algumas das melhores ferramentas no mercado para combater *malwares*, onde é possível baixar exemplar gratuito. Após o *download* segue-se com a instalação a partir do executável do programa;
- para reportar as tentativas de fraudes eletrônicas, acessa-se a página no endereço: https://www.ftccomplaintassistant.gov/#crnt&panel1-1, escolhe-se uma categoria e preenche o formulário de reclamação. Outra opção está no endereço: http://www.antifraudcentre-centreantifraude.ca/index-eng.htm, e ainda, à disposição tem-se: http://www.fraudes.org/.

- Leis:
  - Não há lei específica para o *Phishing* na legislação brasileira. Porém, há leis que podem ser associadas a crimes decorrentes do *Phishing:*
    - a lei nº 72.738/RS associa o *Phishing* ao furto qualificado, enquanto o projeto de lei nº 5485/2013 associa ao estelionato. Logo, não há normalização;
    - na lei 12.737/12 está previsto que dados de cartões de crédito ou débito obtidos de forma indevida equipara-se ao crime de falsificação de documento particular;
    - no Art. 307 do código penal brasileiro quem atribuir a si mesmo ou a outrem falsa identidade para obter vantagem, em proveito próprio ou alheio, tem punição;
    - no Art. 155 do código penal brasileiro tratam da questão furto qualificado por fraude, onde há punição.

- Risco 3
  - Intercepção de mensagens

- Consequência:
  - perda de dados pessoais ou de cartão, para um interceptador;
  - prejuízo financeiro, quando os dados são utilizados para compras;
  - comprometer a própria segurança, pois os hábitos do usuário podem ser conhecidos por um intruso;
  - ter a privacidade invadida;

- comunicar-se com o invasor sem saber;
- ter problemas com a justiça, se os dados pessoais forem utilizados para abertura de contas falsas, por exemplo.

- Prevenção:
  - uso de criptografia;
  - uso de certificado digital;
  - usar ferramenta de segurança para comunicação;
  - assinatura digital.

- Como fazer:
  - nos endereços eletrônicos https://www.gnupg.org/download/index.html ou https://www.gpg4win.org/download.html, o usuário encontra arquivo do PGP compatível com o sistema operacional desejado. Este é um programa capaz de garantir uma comunicação segura, para isso deve ser feito o *download* do arquivo do programa PGP, na sequência executar a sua instalação. Alguns procedimentos devem ser realizados após a instalação para de fato começar a usar o *software* PGP, tais procedimentos estão presentes na documentação que o acompanha, no entanto, no endereço http://www.blog.iz.inf.br/2015/06/voce-ja-enviou-um-e-mail-confidencial.html é disponibilizado um passo a passo de como configurá-lo simples de ser seguido.

- Lei:
  - a interceptação de *e-mail* pessoal ou empresarial está prevista como crime no Código Penal Brasileiro no Art. 10 da lei 9.296/96;
  - está prevista na Constituição Federal 1988, Art. 5, XII, que trata da inviolabilidade da correspondência;
  - prevista no Marco Civil da Internet Lei 12.965 de 23 de Abril de 2014, Art. 7º, II e III, trata da inviolabilidade e sigilo do fluxo de comunicação pela Internet e comunicação privada armazenada, com exceção em caso de pedido judicial.

- Risco 4
  - Fraude de Antecipação de Recursos

- Consequência:
  - prejuízo financeiro;
  - perigo à segurança física;
  - fornecer dados críticos a estranhos;
  - ser vítima de estelionatário.

- Prevenção:
  - não responder *e-mail* com promessas de ganho fácil, que sejam apelativos, que tentem convencer de um par romântico, entre outros temas, pois pode confirmar que está ativo;
  - ser cuidadoso, duvidar da situação, averiguar se trata de mais um golpe;

- observar se o *e-mail* demonstra ser confidencial, se pede sigilo, que tem urgência, se tem erros gramaticais ou sem sentido. Essas situações são pistas de fraude;
- comentar com outros usuários sobre o recebimento de *e-mails* que desconfie, com temas de enriquecimento rápido, por exemplo, pois há uma grande chance dele ter recebido algo semelhante.

- Como fazer:
  - visitar os endereços https://www.truthorfiction.com e http://www.quatloos.com, para se informar dos vários modelos de *e-mails* suspeitos e assistir vídeos sobre o assunto. Isso deve ser feito com frequência, pois podem surgir novas fraudes a qualquer momento;
  - no endereço http://abcnews.go.com/International/story?id=82716&page=1, o usuário encontra noticia sobre o golpe e, ainda, um telefone de contato do oficial de mesa nigeriano no Departamento de Comércio dos EUA (*United States of America*), onde pode receber orientações sobre golpes 4-1-9.

- Lei:
  - Art. 171 do CPB (Código Penal Brasileiro) trata essa fraude como estelionato.

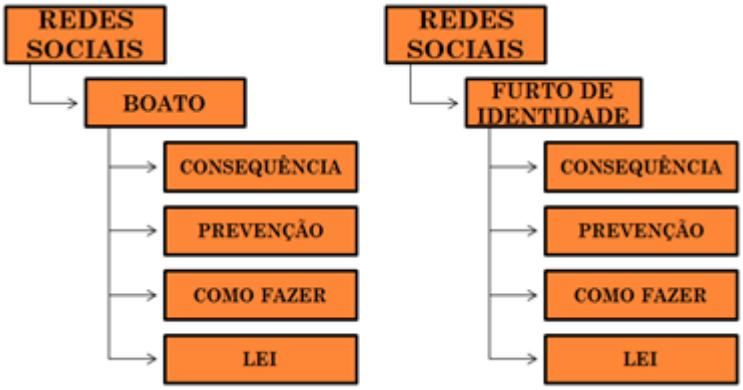
4.1.2 REDES SOCIAIS

As redes sociais é outro serviço da Internet muito utilizado pelos brasileiros, com ela é possível comunicar-se com outras pessoas, fazer amizades, comprar, vender, compartilhar fotos e endereços eletrônicos, notícias e vídeos. No entanto, todo este uso deve ser resguardado com segurança, para que a experiência em seu uso seja satisfatória e positiva.

Assim como, qualquer serviço na Internet, este exige cuidados seja com um *link* ou um comentário compartilhado, é importante a atenção do usuário. O usuário deve atentar-se a analisar as informações que acessam que estão de alguma forma disponível para uso, pois nem tudo que ocorre na rede parte de fontes seguras, ou está ali para ajudar.

Assim, esta subseção apresenta riscos associados a este serviço, como eles afetam a vida das pessoas, como podem evitar perigos ligados a estes riscos, como agir para se assegurar e o que as leis do Brasil dizem sobre o assunto. A Figura 18 ilustra a estrutura do serviço definida no guia, tal como, os riscos associados.

Figura 18: redes sociais e riscos associados apresentados no guia.



- Risco 1
  - Boato

    - Consequência:
      - prejuízo financeiro para a vítima;
      - difamação da pessoa ou empresa;
      - perda da credibilidade da pessoa ou empresa;
      - perigo à própria segurança quando o usuário é a vítima e a de terceiros quando a vítima é alguém que o usuário ajuda a espalhar o Boato, por exemplo, o caso da dona de casa Fabiane Maria de Jesus (BARBOSA, 2014, *on-line*);
      - perigo de códigos maliciosos que podem comprometer o equipamento, deixando-o vulnerável;
      - disseminação de desinformação, ou seja, ao repassar uma notícia sem ter certeza da veracidade;
      - comprometimento do desempenho e espaço nos serviços da rede. Por exemplo, consumo de banda de rede e aumentar a carga de servidores de *e-mail*;
      - induzir o usuário a fornecer seus dados pessoais e de cartões, que poderão ser usados em fraudes.

    - Prevenção:
      - checar a veracidade da informação, não acreditando em tudo o que lê na Internet;
      - checar se trata de golpe em páginas especializadas;
      - observar com atenção o texto, procurar por erros de grafia, exageros, referências, contradições , as frase clássica como: “URGENTE”. Mas, não é uma regra, pode vir de outra forma, com novidades, o melhor é ficar atento. Só vira Boato se o leitor acreditar, então, duvide.

    - Como fazer:
      - em muitos casos uma verificação no *Google* resolve, por exemplo, no caso de Fabiane anteriormente citado, fora verificado pela polícia que o mesmo fato ocorria em São Paulo e Rio de Janeiro com isso constatou-se que se tratava de Boato;
      -

- acesse os endereços https://www.aosfatos.org ou http://www.boatos.org/, para verificar a veracidade da informação, para isso, procure ou pesquise pela notícia no *site*; acesse *sites* especializados em fraudes, para verificar se o Boato está associado a golpes. Os endereços http://www.fraudes.org ou http://www.symantec.com/avcenter/hoax.html, são exemplos desse tipo de *site.*

- Lei:
  - na legislação brasileira não existe lei específica para o Boato, mas o CPB trata de questões associadas nos Arts. 139, 141/III, 142, 143 e 144.

- Risco 2
  - Furto de Identidade

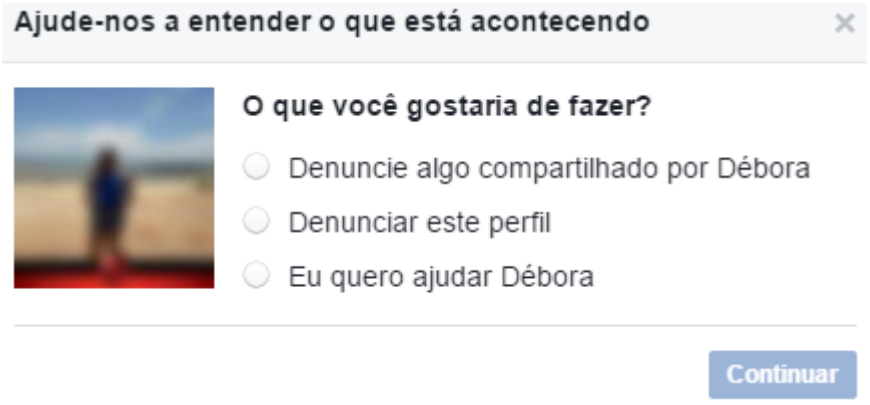
- Consequência:
  - prejuízo financeiro, se os dados forem usados em empréstimos;
  - problemas com a justiça, pois os dados podem ser usados para abrir uma firma que pede empréstimos e não paga;
  - problemas junto aos órgãos de crédito;
  - entrar em listas negras por espalhar códigos maliciosos;
  - comprometer a reputação devido difamação de mau pagador, ou por está envolvido em fraudes;
  - comprometer a credibilidade junto a órgãos financeiros
  - desgaste, pois pode levar muito tempo até sanar todos os problemas.

- Prevenção:
  - proteger os dados particulares e privados, pois mesmo sem possuir uma página legítima numa rede social o usuário pode ser vítima de uma página *Fake*;
  - se o usuário já for uma vítima precisa guardar o máximo de provas como, telas do perfil falso, mensagens eletrônicas, bate-papos e vídeos;
  - registrar a ocorrência em órgãos competentes, como cartórios, delegacia especializadas e a empresa que detêm a página falsa;
  - ter cuidado com o que vai para o lixo, pois um simples *e-mail* pode servir para o mau elemento enviar um código malicioso, como mostra o filme Invasores – nenhum sistema está à salvo;
  - cuidar da segurança das correspondências;
  - ter cuidado com a exposição de dados críticos e *e-mail*;
  - verificar junto a órgãos competentes seu CPF como, receita federal;
  - ter cuidado com *sites* falsos, *Spam*, *Phishing* e ligações pedindo dados pessoais;
  - manter os programas em uso atualizados;
  - usar um sistema ou mais de proteção do equipamento e de *softwares*;
  - manter sua senha secreta e protegida;
  - em redes públicas ou *lan house*, nunca faça transações de pagamento ou transferência e nem forneça seus dados;

- seja ágil em caso de problemas, pois quem rouba dados pretende usá-los rapidamente;
- ao criar perfis, informe somente o necessário e adicione aos amigos somente quem realmente conhece;
- use programas como gerenciador de arquivos e diretórios confiáveis para proteger seus dados sensíveis;
- ficar atento, a situações como: receber *e-mail* como se fosse um retorno, mas que o usuário não tem contato, pessoa ou empresa afirmando resolver problemas de crédito ou empréstimos e por isso está entrando em contato;
- acompanhar diariamente a movimentação da conta bancária;
- se certificar de que seus dados não serão repassados ou vendidos a terceiros;
- ao repassar ou vender equipamentos de armazenamento como, por exemplo, HD (*Hard Disk*) os quais tenha salvo informações críticas, ter certeza que foram apagados definitivamente;
- não pedir a ajuda de desconhecidos para usar o caixa eletrônico, ou outro meio onde tenha que fornecer os dados pessoais e de cartões.

- Como fazer:
  - localizar o perfil falso e reclamar junto à entidade que o promove na Internet. Para isso, após localizar a página falsa, na foto da capa, selecione um ícone de uma reticência dentro de um retângulo, e marque a opção ”Denunciar este perfil”, Figura 17. Após essa ação, será realizada uma verificação de identidade.

Figura 19: área de denúncia de falso perfil (FACEBOOK, 2016).



- no endereço http://www.iobit.com/pt/password-protected-folder.php o usuário encontra um programa muito aceito pelos internautas para proteção de arquivos, sua instalação e utilização é simples e intuitiva;
- o programa ‘*Jihosoft Free Eraser*’ é capaz de apagar definitivamente arquivos do dispositivo de armazenamento, no endereço http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2014/01/como-excluir-arquivos-do-computador-sem-deixar-chance-de-recuperacao-no-hd.html o usuário encontra um passo a passo e *link* para efetuar o *download*.

- Lei:
    - o Marco Civil da Internet (MCI) da Internet lei 12.965 de 23 de abril de 2014, Art. , Art. 7º/I,II,III, Art. 21 trata dos deveres de entidade que detém dados produzidos por terceiros;
    - CF de 1988 Art. 5º/X trata dos direitos invioláveis;
    - CPB lei 2.848 de 7 de dezembro de 1940, Arts. 298 trata da falsificação de documentos, 304 trata do uso de papeis falsos ou adulterados, 154-A, 138 trata da calunia e 153 trata da divulgação dados sensíveis, 307 trata da atribuição a terceiro de falsa identidade, 308 trata do uso próprio de identidade alheia.

4.1.3 E-COMMERCE

Comércio eletrônico ou e-commerce, segundo Ascensão (2016, *on-line*) "é um conceito aplicável a qualquer tipo de negócio ou transação comercial que implique a transferência de informação através da Internet". As transações ocorrem por meio de equipamentos e plataformas eletrônicas. Este serviço é bastante utilizado na Internet, por exemplo, lojas virtuais com venda no varejo.

Devido essas características do comércio eletrônico, golpistas exploram este serviço com objetivo de lesar os usuários, para tanto, usam várias técnicas e códigos maliciosos. Os usuários devem se resguardar com o uso dos mecanismos de segurança disponíveis e ficar sempre alerta.

Nesta subseção são apresentados riscos associados ao serviço de comércio eletrônico, as consequências aos usuários, maneiras de se prevenir, como realizar as configurações de prevenção e como as leis brasileiras tratam o assunto. A Figura 20 ilustra a estrutura do serviço definida no guia, tal como, os riscos associados.

Figura 20: serviço de *e-commerce* e riscos associados apresentados no guia.

- Risco 1
    - *Sites* fraudulentos

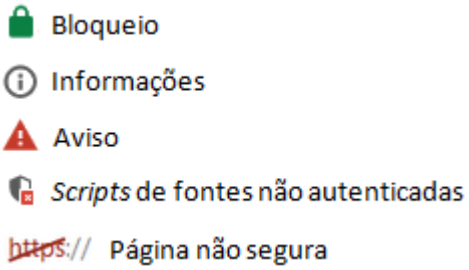
        - Consequência:
            - fornecer os dados pessoais e de cartão a desconhecidos, uma vez que o *site* não é verdadeiro;
            - prejuízo financeiro caso venha, o usuário a comprar no falso *site* ;
            - problemas com a justiça, caso os dados roubados sejam usados por estelionatários para novas fraudes;
            - nome sujo em órgãos de crédito, caso compras tenham sido feitas com dados de cartões roubado do usuário;
            - problemas com a receita federal, caso uma empresa tenha sido aberta com os dados roubados e usada de faixada em outros golpes.

        - Prevenção:
            - não comprar por impulso;
            - observar o tipo de conexão com o *site*, “https” em vez de “http”, a apresentação de um cadeado, o qual, afirma ser uma conexão segura;
            - verificar o certificado digital se corresponde à empresa, que garante que os dados dos clientes irão trafegar de maneira segura;
            - verificar a existência de selo de segurança;
            - consultar em *sites* de reclamação do consumidor sobre a empresa;
            - procurar alguém que já tenha comprado no *site* da empresa para saber como foi a experiência;
            - procurar efetuar os pagamentos via sistemas de gerenciamento de pagamento como, o PagSeguro;
            - observar sempre a reputação da empresa e do vendedor, para tanto ir direto ao *site* digitando o endereço, nunca em *links*;
            - não responda e nem clique em *links* vindos da empresa ou vendedor afirmando ser para agilizar a venda, retirada e acompanhamento;
            - só efetue o pagamento mediante o recebimento ou opte pelo cartão de crédito;
            - verificar a política de segurança da empresa, tal como, o funcionamento de troca e devolução;

- consultar o CNPJ (Cadastro Nacional de Pessoa Jurídica) da empresa no *site* da receita federal, pois as empresas legítimas tem a obrigação de fornecer alguns dados à receita;
- verificar os meios de contato (*chat*, telefone, e-*mail*) com a empresa e se consegue contatá-los com facilidade;
- observar os prazos, pois costumam ser alterados em épocas de maior venda;
- para realizar a compra procurar sempre redes e equipamentos seguros, nunca fazer compras em redes públicas, pois isso aumenta as chances de uma golpista conseguir os seus dados;
- guardar os elementos envolvidos na comunicação e na transação da compra como, *e-mail*, códigos, confirmações, telas, pois podem ser úteis em caso de problemas;
- atentar-se em quem está ouvindo os números do seu CPF, por exemplo, agora em supermercados o caixa pede o número para sair na nota fiscal;
- consultar o CPF no *site* do Serasa por hábito, pois assim é possível saber se está sendo usando em alguma fraude.

- Como fazer:
  - verificar se a conexão a um *site* é segura, assim, dados pessoais e de cartão estarão assegurados ao trafegar na rede, para isso, deve-se analisar seus símbolos como ilustrado na Figura 18.
    - O cadeado indica que o certificado digital é válido e que a conexão entre o navegador e o *site* foi estabelecida com segurança.
    - Já o símbolo de informações, indica que a conexão não foi estabelecida com segurança, portanto, não é recomendável fornecer dados críticos neste ambiente;
    - enquanto o símbolo de aviso alerta para perigo, se possível não usar este *site*;
    - E por último o escudo, alerta que a página está tentando executar s*cripts* (códigos) não autenticados, neste momento o navegador está protegendo o usuário de possíveis ameaças;
    - Porém, se o usuário decide autorizar executar os *scripts* mesmo sendo inseguros, na barra de endereços, aparecerá o símbolo de https:// na cor vermelho com um traço cortando, a Figura 18 ilustra esses símbolos.

Figura 21: símbolos do navegador chrome.



- clicar sobre o cadeado ou sobre o símbolo de informações, em seguida selecionar a opção detalhes, para verificar informações do certificado, seguir passos da seção 4.1.1 / Risco – *Spam* / como fazer. O cadeado pode assumir cores como, verde ou amarelo, pode está, também, inferior, do lado esquerdo ou direito, seguindo padrões de desenvolvimento de cada navegador.
- no *site* do Procon *on-line* é possível verificar uma lista negra de aplicações consideradas inseguras para comprar ou navegar, para isso, acesse o endereço http://sistemas.procon.sp.gov.br/evitesite/list/evitesites.php;
- no endereço https://www.receita.fazenda.gov.br/ pessoajuridica/cnpj/ cnpjreva/cnpjreva_solicitacao.asp, o usuário pode consultar os dados da empresa junto à receita federal, pois este órgão armazena informações obrigatórias de empresas devidamente registradas. Para obter as informações, informe no campo indicado (CNPJ) o número do cadastro jurídico da empresa, o qual pode ser encontrado no próprio *site* da empresa;
- acesse o endereço http://www.reclameaqui.com.br/ para verificar a reputação da empresa ou fazer uma reclamação quando tiver problemas. Na página, basta informar o nome da empresa no campo indicado (pesquisar ou reclamar);
- no teclado tem um botão com uma abreviação 'Prt Scr', chamado de '*print screen'*. Ele captura tudo que aparece na tela do computador em forma de imagem. Use-o para capturar a tela da sua transação, pois esta tela pode vir a ser útil em caso de problemas, servindo como prova. Para salvar a cópia o usuário pode abrir um programa de imagens como, por exemplo, o *Paint*, colar esta imagem e em seguida salvá-la;
- localizar o selo de segurança, se o *site* possuir um, pois este garante que a página é segura e protegida. Ao clicar sobre o selo, logo o usuário será redirecionado a uma página que garante a verificação da credibilidade do selo, caso este seja verdadeiro. No endereço https://www.siteblindado.com/consumidor/verifique/ é possível verificar, também, se um *site* é protegido ou está vulnerável. Na página, basta informar, no campo 'nome da URL', o nome do domínio da empresa, por exemplo, http://www.empresatal.com.br, e confirmar a ação no botão de verificação. Caso a empresa seja segura aparecerá uma caixa de diálogo em cor azul. Caso não seja segura, aparecerá uma caixa de diálogo com informações na cor vermelha.
    - A Figura 19 ilustra um exemplo de página resultante da ação de clicar sobre um selo de segurança, na qual o usuário pode verificar campos como, "*Site"* do certificado, '*Status'* onde aparece a data atual (obrigatoriamente), "Razão Social" da empresa, ainda é possível verificar o tipo proteção da página, por exemplo: ataques de hackers, roubo de informações e clonagem de cartões;

Figura 22: página de verificação de veracidade do selo do site blindado (SITE BLINDADO, 2016, *on-line*).

- Lei:
  - no Código Penal Brasileiro (CPB), os Art. 307 e 308 tratam da falsa identidade, quando passada a terceiros para obter vantagem, e do uso dela, como própria. Pode ocorrer detenção de, no mínimo, três meses e, no máximo, de dois anos, se não constituir crime mais grave;
  - o CPB, ainda trata da questão de falsificação de cartão e documentos de identificação Art. 298, pena com reclusão de um a cinco anos e multa;
  - CPB, Art. 175 trata sobre a venda de mercadoria falsificada ou deteriorada.

- Risco 2
  - Ataque de Negação de Serviço

    - Consequência:
      - indisponibilidade do que se provê, devido o ataque interromper o serviço prestado ou a aplicação da *Web*;
      - ter a credibilidade afetada, por não conseguir manter a disponibilidade;
      - prejuízos financeiros, pois se o serviço ou aplicação gerar receita ao usuário, fora de funcionamento, não gerará.

    - Prevenção:

- se possível usar ferramentas capazes de monitorar o uso da CPU (*Central Processing Unit*), memória, disco rígido, conexões (servidor) e tráfego de interfaces;
- somente ações de prevenção podem realmente funcionar, para isso, deve haver a colaboração de usuários, mantendo seu *hardware* e *softwares* atualizados e com as manutenções preventivas em dias, de desenvolvedores de APIs (*Application Programming Interface*) para mitigarem ou aniquilarem as falhas, administradores dos computadores, serviços e todo *hardware* envolvido;
- manter um bom nível de segurança nos equipamentos, através dos mecanismos disponíveis;
- proteger os dados sensíveis;
- ter disponível o contato de um bom profissional ou empresa especialista em segurança, para saber como reagir ou mitigar em caso de problemas;

- Como fazer:
  - Programas, geralmente no *site* do fabricante de softwares, têm os procedimentos para configuração, novas versões e uma área de suporte, em alguns casos por *chat on-line*;
  - para atualizar, *firewall* e antivírus seguir instruções apresentadas na seção 4.1.1 – e-*mail* / Risco 1 - *Spam* / como fazer;
- Lei:
  - Lei 12.737 de 30 de novembro de 2012 trata, no Art. 3º, sobre a interrupção ou perturbação de serviço informático.

- Risco 3
  - Ataque de Varredura em Rede;

  - Consequência:
    - comprometimento da rede, serviço ou programa;
    - códigos maliciosos, uma vez que o atacante descobre como penetrar no serviço ou aplicação, ele pode querer usar com má fé ;
    - falhas de segurança, devido segurança fraca;
    -

  - Prevenção:
    - configurar adequadamente serviços e programas;
    - configurar adequadamente o *firewall*, pois portas podem está abertas;
    - manter sistema, serviços e programas atualizados e com as últimas versões;
    - proteger senhas e arquivos, pois dados críticos são sempre ao alvos;
    - usar criptografia sempre que envolver informações críticas;
    - adquirir conhecimento sobre o assunto.

  - Como fazer:
    - para antivírus ver seção 4.1.1 – *e-mail* / Risco 1 - *Spam* / como fazer;
    - para atualização ver seção 4.1.1 – *e-mail* / Risco 1 - *Spam* / como fazer;

- configurar adequadamente o *firewall*, ver seção 4.1.1 – *e-mail* / Risco 1 - *Spam* / como fazer;
- no endereço https://www.youtube.com/watch?v=i26OKlNK-ks, o usuário encontra um vídeo ensinando como fazer varredura, pode acompanhar dúvidas de outras pessoas em sala virtual, para isso acessar o endereço diretamente do navegador;
- neste outro endereço http://rodrigolira.eti.br/nmap-30-exemplos-de-comandos-para-administradores-de-rede/, o usuário encontra um tutorial ensinando a fazer varredura, passos que levam a prática .

- Lei:
  - Art. 3º / II e Art. 11 da Lei 12.965 de 23 abril de 2014 trata da privacidade;

4.1.4 SERVIÇOS BANCÁRIOS

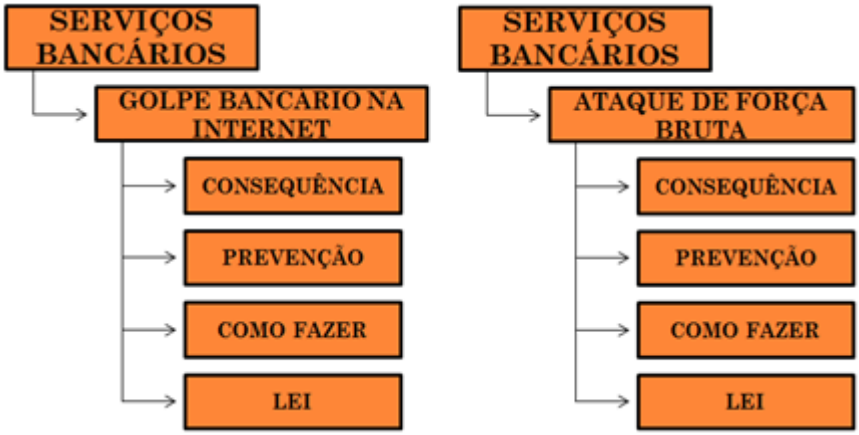
Internet *banking* ou banco *on-line* é o banco convencional de forma virtualizada. Significa que os serviços oferecidos de forma tradicional passam a ser, também, disponibilizados na Internet.

A virtualização dos bancos permite que os usuários executem serviços bancários de qualquer lugar com acesso a Internet, usando um computador ou um smartphone, por exemplo. É possível fazer transferência bancária entre contas, executar pagamentos de boletos, e muitos outros serviços.

Apesar da praticidade, conveniência e segurança envolvida nos serviços bancários, muitos problemas podem ocorrer, de forma que o prejudicado venha a ter prejuízo financeiro. Tais problemas podem acontecer por motivos como, códigos maliciosos e dados roubados.

Assim, esta subseção apresenta riscos associados aos serviços bancários, suas reais consequências às vítimas, formas de prevenção, como fazer para ter mais segurança e como as leis brasileiras tratam o fato. A Figura 23 ilustra a estrutura do serviço definida no guia, tal como, os riscos associados.

Figura 23: serviços *bancários* e riscos associados apresentados no guia.



- Riscos 1
    - Golpe bancário na Internet

    - Consequência:
        - dados roubados por estelionatários;
        - prejuízo financeiro, pois com os dados em mãos golpistas retiram dinheiro da vítima ou ainda, compram em nome dela como se fossem ela própria;
        - aborrecimento e desgaste até resolver os problemas decorrentes do golpe;
        - crédito bloqueado junto aos bancos;
        - credibilidade e reputação podem ser abalada;
        - invasão de privacidade;
        - violação do sigilo bancário;
        - rotulado por partição em esquemas de fraude.

    - Prevenção:
        - observar erros de digitação como: “bancodovrasil” em vez de banco do brasil;
        - usar conexões e equipamentos seguros, uma conexão segura dados trafegam seguros e quanto a equipamentos bem configurados e atualizados defendem contra falhas de segurança mais recentes;
        - nunca usar rede pública, *lan-house* para transações bancárias, pois não há garantias de segurança, por exemplo, no computador a ser usado;
        - Se possível usar um computador pessoal e exclusivo para acesso a banco;
        - conferir sempre os documentos a serem pagos, todos os campos, inclusive para quem vai o pagamento;
        - ao ser instalado um módulo de segurança, primeiro verificar se pertence a entidade a qual pretende usar;
        - sob qualquer dúvida entrar em contato com o banco e averiguar;
        - usar programas que aumentem a segura como, *Firewall* pessoal e antivírus;
        - acessar o banco sempre digitando-o a partir da barra de endereços do navegador;
        - verificar o certificado digital, campos como: requerente, validade e emissor do certificado;
        - habituar-se a sair pela opção correta, para encerrar a sessão com o servidor em uso, geralmente trás descrição “sair”, “encerrar” ou “*logout*”;
        - ter cuidado, suspeitar de página com erros ou indisponibilidade;

- elaborar senhas mais difíceis e não intuitivas como, próprio nome, nome do cachorro e número do telefone;
- fazer uma verificação antecipada ao *site* que deseja acessar;
- adquirir o hábito de trocar a senha de vez em quando;
- em caso de acesso indevido, desconectar a Internet pode atrapalhar a não concretizar o golpe, dessa maneira ajudando a vítima;
- boa prática é excluir os arquivos temporários como, cookies no seu navegador;
- informar o banco quando for vítima de um golpe, pois eles poderão orientar;
- registrar ocorrência;
- não mexer no equipamento, pois provas ou pistas importantes podem está nele;
- verificar junto ao banco outras opções de notificação de movimentação da conta, por exemplo, SMS (*Short Message Service*);
- acompanhar notícias sobre golpes e segurança;
- fazer um teste de "falso positivo", informe dados não reais de *login* , se acessar pode ser fraude.

- Como fazer:
  - ao acessar o seguinte endereço https://www.youtube.com/watch?v=xBkQm3KNOAs, o usuário acompanha um teste de "falso positivo", realizado por um cliente de um banco que gravou o procedimento de tentativa de fraude no momento que estava tentando acessar o *site* da empresa, desconfiado informou dados aleatórios, para ver isso, basta editar o endereço no navegador e prosseguir;
  - no endereço https://virustotal.com/, o usuário pode testar a segurança de uma página que deseja acessar, para isso, basta editar o endereço desejado no campo adequado do *site* de teste e executar a ação;
  - seguir os procedimentos descritos na seção 4.1.3 – E-COMMERCE / *sites fraudulentos* / prevenção / como fazer, ao que tange à segurança;
  - acessar os endereços http://www.fraudes.org, http://cartilha.cert.br/glossario/, para manter-se informado sobre fraudes e outros perigos da Internet;
  - ir até o local indicado no *site* para encerrar uma sessão de acesso, garante ao usuário a saída efetiva do sistema, para isso, deve-se procurar por nomes em botões ou menu como: "encerrar a sessão", "terminar", "sair", "*logout*", logo em seguida uma mensagem de aviso do encerramento deve surgir.

- Lei:
  - Art. 171 do CPB trata de estelionato que é como se configura esses tipos de crimes.

- Risco 2
  - Ataque de Força Bruta.

- Consequência:
  - falha na segurança;
  - perda de dados;

- dependendo do serviço afetado e o que ele representa, pode ser desastroso.

- Prevenção:
  - criar senhas fortes, elas sempre são acima de oito caracteres e os misturam de forma aleatória, entre eles tem-se, por exemplo: números, letras (maiúscula e minúscula) e símbolos;
  - proteger dados críticos como, as senhas, dados de cartões e dados pessoais;
  - usar *firewall* pessoal, antivírus, *antispam* e *antimalware*.

- Como fazer:
  - no endereço http://www.cmcm.com/blog/pt/security/2014-11-12/460.html, o usuário encontra dicas interessantes sobre confecção de senha e um testador de senha, com avaliação de outras entidades da Internet. Para isso, o usuário pode copiar e colar a senha citada na Seção 2.1.3.13 / Ataque de Força Bruta e recriar semelhante, ou ainda, informar os dados na área reservada de teste e verificar os resultados;
  - no endereço https://sourceforge.net/projects/keepass/, o usuário encontra um gerenciar de senhas, assim elas não serão facilmente esquecidas, para isso, acessar o endereço e fazer o *download*, neste outro endereço https://www.youtube.com/watch?v=-fXERLsJ5Cc, é possível aprender como baixar, instalar, configurar, criar as senhas, ou seja, os passos necessários para usar a ferramenta Keepass;
  - outra opção segura é anotar dados críticos e proteger no cofre, criptografar ou ainda, editadas em arquivo ".txt" e proteger de alguma forma, ocultando ou informando o nome do arquivo sem ligação com o conteúdo;
  - programas de segurança ver seção 4.1.1 / Risco 1 – *Spam* / Como fazer;
  - no endereço https://www.youtube.com/watch?v=WmRHB15aLts, o usuário tem acesso ao vídeo explicativo sobre o Ataque de Força, para isso, acessar o endereço digitando-o na área de endereço do navegador;

- Lei:
  - a Lei 12.737 de 30 de novembro de 2012 trata da questão privacidade, o qual este delito pode ser caracterizado;

Este capítulo apresentou os principais serviços utilizados pelos usuários na Internet, assim como os principais riscos associados a cada um deles, para cada risco as consequências que podem ocasionar ao usuário, formas de prevenção, como realizar ações práticas e como as leis brasileiras trata cada um deles. O guia rápido de consulta é viável, pois orienta o usuário a obter boas práticas de navegação, assim utiliza a rede e ao mesmo tempo se previne das ameaças.

5 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo criar um guia para uso seguro da Internet para usuários leigos, a partir do uso das informações contidas no guia o usuário poderá utilizar serviços na Internet com segurança como, por exemplo, em serviços de *e*-mail: reconhecer um *e-mail* suspeito de conter código malicioso, no serviço de Internet *Banking* realizar um teste de "falso positivo", ou ainda, como confeccionar uma senha forte.

O guia tem uma estrutura intuitiva, de fácil leitura, para que o usuário possa rapidamente aprender a usá-lo. Possui informações separadas por uma hierarquia, onde o usuário identifica com facilidade o tema de maior relevância e os temas correlatos. Considera-se importante esse padrão, pois possibilita ao usuário leigo rapidez, compreensão e segurança tudo ao mesmo tempo. Acredita-se ainda, que o guia possa estimulá-los a fazer uso de boas práticas de segurança e desenvolver o hábito seguro de navegação.

O usuário tem papel importante para manter a segurança da informação, ele deve estar atento e se cercar de cuidados. Existem diversos mecanismos de segurança, mas as pessoas precisam se acostumar a usá-los, pois o mau hábito pode resultar em sérias consequências como, por exemplo, exposições, prejuízos financeiros e infecção de equipamentos por códigos maliciosos.

Considera-se que independente da idade do usuário, desde que saiba ler, que o guia será útil para a experiência com a Internet. O usuário leigo a partir do uso do guia descobrirá diversos mecanismos de segurança e aprenderá a usá-los, pois o guia contém o necessário para o usuário leigo instalar, configurar e usar estes mecanismos.

Quanto às leis brasileiras, acredita-se que precisem ser regularizadas com maior rapidez, melhoradas e que sejam mais específicas, caso o contrário, favorece a prática indiscriminada de golpes na Internet. Há certa urgência para regularização e adaptações das leis sobre crimes na rede mundial de computadores, pois a quantidade de crimes é grande e suas modalidades se diversificam rápido.

Para trabalho futuro, seria interessante adicionar novos serviços como, Telnet e comunicação remota, fóruns de discussão e serviços de telefonia. Além disso, poderia ser criado um manual *on-line* para usuários leigos, que contivesse instruções em textos, imagens e vídeos com explicações de configurações e uso seguro. Seria interessante que, no manual *on-line*, fosse disponibilizada uma avaliação do conhecimento do usuário, dando-lhe uma noção do seu grau de conhecimento no que se refere à acesso seguro.

REFERÊNCIAS

ASCENSÃO, Carlos Pinto. **O que é e-commerce?.** 2016. Disponível em: <http://www.gestordeconteudos.com/e-Commerce/Artigose-Commerce/Oqueée-Commerce /tabid/3850/Default.aspx>. Acesso em: 17 nov. 2016.

AVAST SOFTWARE (Us). **Pharming.** California, 2016. Disponível em: <https://www.avast.com/pt-br/c-pharming>. Acesso em: 15 nov. 2016.

BARBOSA, Caio. **Perigo na rede social: boatos no Facebook levaram à morte de dona de casa:** Fabiane Maria de Jesus foi linchada após ser vítima de boatos que diziam que ela sequestrava crianças para fazer magia negra. 2014. Disponível em: <http://odia.ig.com.br/noticia/brasil/2014-05-10/perigo-na-rede-social-boatos-no-facebook-levaram-a-morte-de-dona-de-casa.html>. Acesso em: 20 nov. 2016.

CERT.BR. **Estatísticas dos Incidentes Reportados ao CERT.br.** Br, 2015. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 03 out. 2016.

CETIC.BR. **TIC DOMÍCILIOS E USUÁRIOS 2015.** Br, 2015. Disponível em: <http://cetic.br/tics/usuarios/2015/total-brasil/C15/>. Acesso em: 27 out. 2016.

CGI.BR. **Marco Civil.** 5. ed. Br, 2013. Disponível em: <http://www.cgi.br/media/docs/publicacoes/3/cgibr-revistabr-ed5.pdf>. Acesso em: 19 ago. 2016.

CHEETAH MOBILIE (China). **Redefinindo suas senhas, aumentando a sua segurança.** Beijing, 2014. Disponível em: <http://www.cmcm.com/blog/pt/security/2014-11-12/460.html>. Acesso em: 19 nov. 2016.

CIAB FEBRABAM. **Transação com mobile banking cresce 138% em 2015.** Sp, 2016. Disponível em: <http://www.ciab.com.br/pt/noticia/2016/05/transacao-com-mobile-banking-cresce-138-em-2015#>. Acesso em: 17 nov. 2016.

E-BIT/BUSCAPÉ. **Webshoppers.** 33. ed. Sp: E-bit/buscapé, 2016. 77 p. Disponível em: <http://img.ebit.com.br/webshoppers/pdf/33_webshoppers.pdf>. Acesso em: 15 nov. 2016.

ECOMMERCEBRASIL. **Pesquisa mostra dados da internet no Brasil em 2015.** Br, 2015. Disponível em: <https://www.ecommercebrasil.com.br/noticias/pesquisa-mostra-dados-da-internet-no-brasil-em-2015/>. Acesso em: 01 out. 2016.

FAST COMMERCE. **Manual anti-fraude para comércio eletrônico.** Sp, 2016. Disponível em: <https://www.fastcommerce.com.br/dnload/ManualAntiFraude.pdf>. Acesso em: 11 out. 2016.

FACEBOOK. **Abra uma conta.** Disponível em: <https://www.facebook.com/>. Acesso em: 17 nov. 2016.

IBGE (Rj). **Pesquisa Nacional por Amostra de Domicílios: Acesso à Internet e à Televisão e Posse de Telefone Móvel Celular para Uso Pessoal.** 2014. Disponível em: <http://biblioteca.ibge.gov.br/index.php/biblioteca-catalogo?id=295753&view=detalhes>. Acesso em: 13 set. 2016.

IDEC. **Dicas & Direitos:** dicas para evitar o golpe do falso boleto bancário. 2016. Disponível em: <http://www.idec.org.br/con sultas/dicas-e-direitos/dicas-para-evitar-o-golpe-do-falso-boleto-bancario>. Acesso em: 03 set. 2016.

KUROSE, James F.; ROSS, Keith W.. **Redes de computadores e a Internet:** uma abordagem top-down. 6. ed. São Paulo: Pearson Education do Brasil, 2013. 634 p.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna Ltda, 2008. 253 p.

LOPES, Gilmar Henrique. **5 boatos mais comuns no Facebook!** 2013. Disponível em: <http://www.e-farsas.com/5-boatos-mais-comuns-no-facebook.html>. Acesso em: 17 nov. 2016.

MARIANO. **Cyber Crimes Delegado Mariano:** Parlamento japonês é atingido por cyber-ataque. 2011. Disponível em: <http://mariano.delegadodepolicia.com/parlamento-japones-e-atingido-por-cyber-ataque/>. Acesso em: 17 nov. 2016.

MCAFEE. **O que você precisa saber para evitar o roubo de identidade.** 2010. Disponível em: <https://promos.mcafee.com/pt-BR/PDF/BR_ID_Theft_E_Guide.pdf>. Acesso em: 05 out. 2016.

MICROSOFT. **Safety & Security Center:** How to recognize phishing email messages, links, or phone calls. 2013. Disponível em: <https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx>. Acesso em: 03 nov. 2016.

PORFÍRIO, Wesley. **Veja dois exemplos de um spam com link malicioso e como se prevenir de vírus e outras pragas que chegam em seu e-mail.** 2011. Disponível em: <https://wporfirio.wordpress.com/2011/11/17/veja-um-exemplo-de-um-spam-com-link-malicioso-e-como-se-prevenir-de-virus-e-outras-pragas-que-chegam-em-seu-email/>. Acesso em: 14 nov. 2016.

PUCCINELLI, Maurilio. **SAIBA COMO IDENTIFICAR UM BOLETO MODIFICADO POR VÍRUS.** 2014. Disponível em: <http://agencia.yesbr.com.br/dicas-e-tutoriais/saiba-como-identificar-um-boleto-modificado-por-virus/>. Acesso em: 17 nov. 2016.

QUATLOOS. **Nigerian 4-1-9 Scam**. Disponível em: <http://www.quatloos .com/scams/nigerian.htm>. Acesso em: 17 nov. 2016.

QUATRO CANTOS. **Lendas e folclore Internet. As pulhas virtuais**. Disponível em:< http://www.quatrocantos.com/lendas/58_419_scam_nigeria.htm >. Acesso em: 07 out. 2016.

REDE GLOBO DE TELEVISÃO. **Suspeitos do roubo das fotos de Carolina Dieckmann são descobertos.** 2012. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html>. Acesso em: 20 ago. 2016.

RNP. **Tudo que você precisa saber sobre os ataques DDoS.** 2000. Disponível em: <https://memoria.rnp.br/newsgen/0003/ddos.html>. Acesso em: 02 set. 2016.

SYMANTEC, Norton By. **Fraude on-line:** phishing. 2016. Disponível em: <https://br.norton.com/cybercrime-phishing>. Acesso em: 10 out. 2016.

SITE BLINDADO S. A. (Sp). **Site Blindado Contra Hackers.** São Paulo, 2016. Disponível em: <https://s3-sa-east-1.amazonaws.com/cdn.siteblindado.com/lp_aw/verifica-pt-br.html?url=www.siteblindado.com>. Acesso em: 17 nov. 2016.

SOCOLOFSKY, T.; KALE, C.. **RFC1180:** A TCP/IP Tutorial. Network Working Group. 1991. Disponível em: <https://tools.ietf.org/html /rfc1180>. Acesso em: 28 nov. 2016.

STALLIVIERE, Cristiane del Sávio. **Técnicas de invasão:** Entendendo para se proteger. 2011. Disponível em: <http://micreiros.com/tecnicas-de-invasao-entendendo-para-se-proteger/>. Acesso em: 03 out. 2016.

TELECO. **Internet no Brasil:** Statísticas. 2016. Disponível em: <http://www.teleco.com.br/internet.asp>. Acesso em: 27 out. 2016.

TO BE GUARANY. **Dados, Estatísticas e Projeções sobre a Internet no Brasil.** 2015. Disponível em: <http://tobeguarany.com/internet-no-brasil/>. Acesso em: 27 out. 2016.

TVI24. **Cardeal José Policarpo alvo de roubo de identidade no Facebook.** 2014. Disponível em: <http://www.tvi24.iol.pt/tecnologia/patriarcado-de-lisboa/cardeal-jose-policarpo-alvo-de-roubo-de-identidade-no-facebook>. Acesso em: 17 nov. 2016.

UOL. **Fraudes na Internet:** Boatos. 2016. Disponível em: <https://sac.uol.com.br/info/cartilha/fraudes/sec3.jhtm>. Acesso em: 09 out. 2016.