UNIVERSIDADE FEDERAL DO PARÁ

INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS

FACULDADE DE COMPUTAÇÃO

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ODIRLEY PINHEIRO DE MATOS

UM ESTUDO SOBRE ATAQUES DE PHISHING E SUAS MEDIDAS DE CONTENÇÃO

BELÉM

2017

ODIRLEY PINHEIRO DE MATOS

UM ESTUDO SOBRE ATAQUES DE PHISHING E SUAS MEDIDAS DE CONTENÇÃO

Trabalho de Conclusão de Curso apresentado no curso de Bacharelado em Sistemas de Informação da Universidade Federal do Pará como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

Orientado: Prof. Dr. Roberto Samarone dos Santos Araújo.

BELÉM

2017

ODIRLEY PINHEIRO DE MATOS

UM ESTUDO SOBRE ATAQUES DE PHISHING E SUAS MEDIDAS DE CONTENÇÃO

Trabalho de Conclusão de Curso apresentado no curso de Bacharelado em Sistemas de Informação da Universidade Federal do Pará como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

Aprovada em: _____/_____/_____

BANCA EXAMINADORA

_____

Prof. Dr. Roberto Samarone dos Santos Araújo
Universidade Federal do Pará
Orientador

_____

Profª. Drª. Marcele Mota Pereira
Universidade Federal do Pará

_____

Profª Drª Regiane Silva Kawasaki Frances
Universidade Federal do Pará

Agradecimentos

Dedico meus sinceros agradecimentos para:

O professor Doutor Roberto Samarone dos Santos Araújo, pela orientação e incentivo;

Aos meus colegas de curso;

E, principalmente, a minha família.

Resumo

Dados estatísticos indicam um número cada vez maior de pessoas acessando a rede mundial de computadores no Brasil. Essas pessoas, consequentemente, também estão expostas às ameaças da Internet. Uma dessas ameaças é o ataque de *phishing*, golpe em que o usuário da Internet é ludibriado a executar determinadas ações que podem lhe trazer enormes prejuízos. Nesse sentido, este trabalho apresenta um estudo com as principais características dos ataques de *phishing*, bem como os métodos psicológicos e tecnológicos utilizados pelos atacantes para torná-lo mais efetivo. São mostradas, também, algumas medidas de proteção que os internautas podem utilizar contra o phishing. Por fim, é apresentado o resultado de uma avaliação feita em ferramentas *anti-phishing* disponíveis no mercado.

Palavras-chave: *Phishing*, *Anti-phishing*, Segurança na Internet.

Abstract

Statistical data indicate an increasing number of people accessing the worldwide computer network in Brazil. These people, therefore, are also exposed to Internet threats. One such threat is the phishing attack, a scam where the Internet user is deceived into performing certain actions that can bring him or her huge losses. In this sense, this work presents a study with the main characteristics of the phishing attacks, as well as the psychological and technological methods used by the attackers to make it more effective. Also shown are some protection measures that Internet users can use against phishing. Finally, the results of an evaluation of the anti-phishing tools available on the market are presented.

Keywords: Phishing, Anti-phishing, Internet Security.

Lista de Figuras

Lista de Tabelas

Sumário

Capítulo 1

Introdução

A internet disponibiliza aos seus usuários um conjunto de serviços, desde os mais simples como blogs, até os mais complexos, como sites de bancos, que possibilitam a realização de transações financeiras. Todos esses serviços, no entanto, exigem algum tipo de atenção por parte do internauta, seja com o conteúdo que estes sites exibem, seja com as informações que neles são inseridas.

A grande rede mundial de computadores pode ser um ambiente hostil, propício para a aplicação de golpes. Existem golpistas experientes ou amadores; existem as potenciais vítimas, indivíduos que não acreditam que podem ser enganados no ambiente virtual; e existem as oportunidades que podem ser exploradas pelos golpistas, como ofertas de emprego, dinheiro fácil, promoções tentadoras, cobranças de multa, entre outras.

Características favoráveis a golpes vão ser utilizadas com maior ou menor intensidade dependendo da época do ano e/ou do perfil do alvo. No Natal, por exemplo, a probabilidade de um golpista obter sucesso pedindo doações em dinheiro alegando ser para crianças carentes é bem maior, já que está sendo explorada nesta situação a sensibilidade das pessoas na época natalina. “Os hackers muitas vezes tiram proveito de acontecimentos recentes e determinadas épocas do ano, como as Olimpíadas de 2016, desastres naturais, epidemias de doenças, preocupações econômicas, eleições políticas, etc.” (EL PESCADOR, 2015).

Os golpes citados no parágrafo anterior, assim como outras atividades ilícitas que exploram vulnerabilidades humanas, são cada vez mais praticados na Internet. São inúmeros os riscos com os quais os internautas se deparam: acesso a conteúdos impróprios ou ofensivos, roubo de identidade, furto e perda de dados, invasão de privacidade, divulgação de boatos, dificuldade de exclusão e dificuldade de manter sigilo (CERT, 2012).

1. INTRODUÇÃO

Atividades ilícitas na Internet podem ser relacionadas a programas maliciosos e/ou pessoas mal intencionadas. Um internauta pode ter seus dados copiados toda vez que acessa a página de uma instituição financeira por um destes programas, por exemplo. Estes programas maliciosos podem vir escondidos em outros programas, maliciosos ou não, que podem ser "adquiridos" pelo internauta durante o acesso a um site falso. No entanto, para que o ataque descrito tenha sucesso e os programas maliciosos em questão sejam instalados, é preciso "fisgar" o usuário, isto é, o atacante precisa convencer a potencial vítima a tomar uma decisão da qual acredita que se beneficiará, mas que só dará ganhos ao golpista.

Os atacantes, que neste trabalho também serão denominados de hackers, cibercriminosos, *phishers* (que realizam ataques de *phishing*) ou *scammers* (que praticam fraudes *online*), procuram por brechas de segurança em computadores ou sistemas e, principalmente, por usuários da Internet, também, com algum tipo de vulnerabilidade, tais como: desatenção, displicência, desinformação, desmotivação ou insatisfação com o trabalho.

Quando encontram uma ou mais das vulnerabilidades citadas, os atacantes aumentam suas chances de êxito durante a execução dos golpes mencionados. Usuários da Internet desinformados, por exemplo, podem se tornar vítimas de cibercriminosos iniciantes que buscam apenas senhas fáceis em serviços de webmail ou redes sociais.

Os internautas não estão 100% imunes contra as ameaças da Internet. Estes, contudo, podem diminuir a probabilidade de serem os próximos alvos. Internautas que costumam baixar programas da Internet e não os configuram de maneira adequada depois de instalados, isto é, não modificam senhas padrões, por exemplo, podem ser alvos fáceis para os atacantes que procuram por estas falhas e ter, assim, dados sigilosos roubados.

Outros usuários vão precisar de um pouco mais de cuidado na Internet ao digitar suas senhas ou outras informações sensíveis, pois podem se deparar com hackers que combinam conhecimentos técnicos na área da computação com o conhecimento de algumas fraquezas humanas. Essa combinação permite ao golpista realizar ataques mais elaborados e, consequentemente, com maior taxa de sucesso. Esses ataques são mais conhecidos por *phishing* e são predominantemente usados por cibercriminosos para roubar dados e executar fraudes *online* (PHISHLABS, 2016).

Não só indivíduos estão suscetíveis a ataques de *phishing*, empresas, organizações, órgãos públicos, entre outros, também estão. Quando uma instituição é alvo de ataques, é natural que esta invista mais em segurança. O aumento do número de ataques de *phishing*, principalmente aqueles direcionados a grandes empresas, provoca o aumento do nível de segurança dos alvos. Isso faz com que os atacantes busquem constantemente novas modalidades de golpes ou busquem alvos mais fáceis.

Empresas pouco suscetíveis a ataques de *phishing*, por exemplo, passam a ser mais visadas, enquanto que empresas que sofreram muitos ataques começam a ser menos visadas em detrimento das medidas de segurança que são obrigadas a implementar. A Tabela 1.1 apresenta os tipos de empresas que tiveram um aumento no número de ataques de *phishing* e as que conseguiram diminuir esses ataques no período de 2013 a 2015.

Tabela 1.1: Tipos de empresas alvos de ataques de *phishing* (2013 - 2015).

	Aumentando				Diminuindo	
Ano	Armazenamento na Nuvem / Hospedagem de Arquivos	Webmail / Serviços Online	E-Comerce	Redes Sociais	Financeiro	Serviços de Pagamento
2015	19.9%	17.7%	11.9%	3.9%	30.6%	10.3%
2014	14.6%	13.6%	11.4%	0.6%	35.7%	19.4%
2013	7.7%	10.2%	5.1%	0.6%	41.0%	26.3%

Fonte: Adaptado de PHISHLABS (2016).

É importante ressaltar que nem sempre os atacantes precisam cometer crimes para adquirir informações valiosas de seus alvos, eles podem fazer uso de táticas seguras para adquirir informações relevantes para um possível planejamento de ataque. Os atacantes podem reunir dados do alvo acessando páginas de redes sociais ou o site da empresa onde a potencial vítima trabalha, em busca de pistas que possam aumentar as chances de sucesso quando o ataque for executado, sem o risco de ser pego.

Neste contexto de crimes na Internet, este trabalho objetiva realizar um estudo sobre ataques de *phishing* e suas respectivas medidas de contenção. São apresentados temas correlatos como ataques cibernéticos, programas maliciosos e, principalmente, Engenharia Social. Testes em navegadores Web, em programas antivírus com extensões *anti-phishing* e

em extensões *anti-phishing* para navegadores Web também serão realizados, visando identificar a relevância que estas ferramentas têm na proteção do internauta durante o acesso a sites fraudulentos e na abertura de e-mails falsos.

1.1 Motivação

Dados de 2015 mostram um aumento no número de pessoas que têm acesso à Internet. Segundo pesquisa realizada pelo Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (CETIC), 50% dos domicílios brasileiros possuem acesso à Internet, tanto pelo computador pessoal quanto por dispositivos móveis. Usuários da Internet já são 55% em relação ao total da população de 10 anos de idade ou mais. E os que usam a Internet pelo celular correspondem a 47%, também sobre o total da população de 10 anos de idade ou mais (CETIC, 2015).

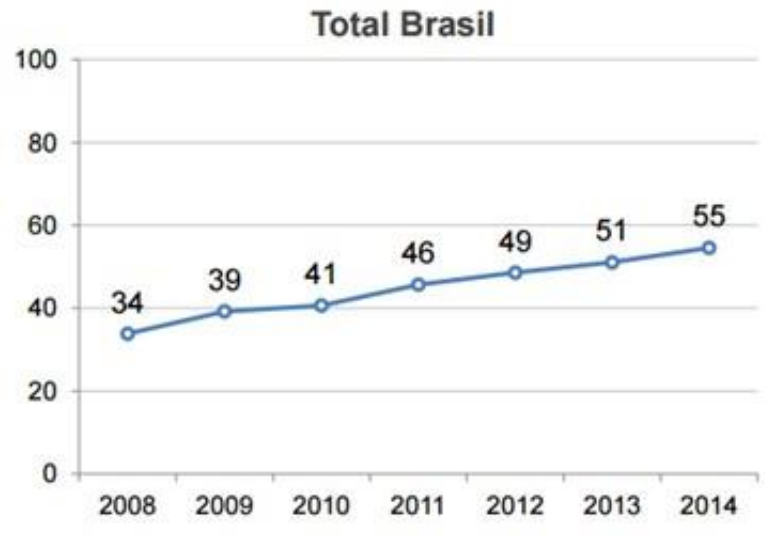


Figura 1.1: Percentual de usuários de Internet sobre o total da população de 10 anos ou mais. Fonte: CETIC, 2015.

Com o aumento do número de usuários da Internet, mais pessoas ficam expostas a ataques cibernéticos. Esses ataques, por sua vez, podem ser reportados a empresas, instituições e órgãos especializados em segurança na Web. Um desses órgãos é o Centro de Estudos, Pesquisa, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT). O CERT também divulga dados estatísticos sobre incidentes na Internet como ataques de negação de serviço, acesso não autorizado a um computador ou rede, ataques a servidores, fraude, entre outros, conforme a Figura 1.2.

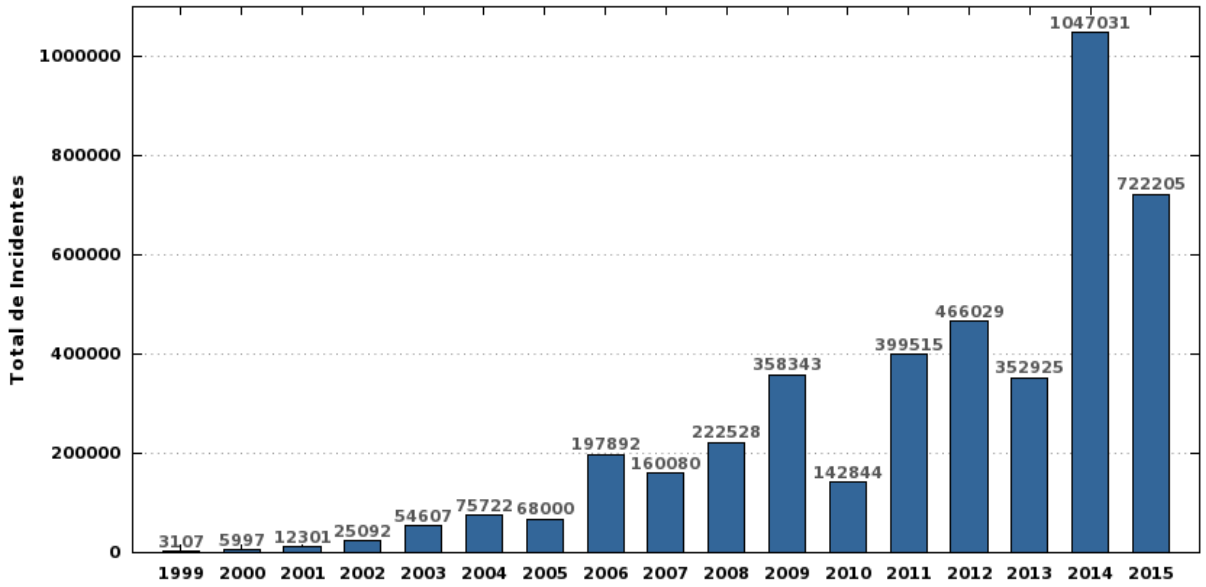


Figura 1.2: Total de incidentes reportados ao CERT por ano - 1999 a 2015.
Fonte: CERT, 2015.

Mesmo com a queda acentuada no número de incidentes de 2014 a 2015, observada na figura acima, o crescimento percebido nos últimos 17 anos não pode ser ignorado. A Figura 1.2 apresenta, ainda, um padrão interessante: os incidentes crescem por um ou mais anos, caem por um ano, depois tornam a crescer. Ou seja, assim como cresce o número de usuários da Internet e o número de incidentes reportados, cresce também a batalha entre atacantes (que também aumentam em número e aperfeiçoam suas técnicas proporcionando-lhes sucesso por um período) e seus alvos, que vão se adaptando e ficando menos suscetíveis aos ataques.

Existem ainda, grupos internacionais que têm uma área de atuação mais específica, como é o caso do *Anti-Phishing Working Group* (APWG). De acordo com alguns relatórios publicados trimestralmente por esta organização, o Brasil aparece como um dos dez países que mais hospedam sites de *phishing* (APWG, 2016). Em um relatório publicado no quarto trimestre de 2015, por exemplo, o Brasil aparece na oitava colocação no mês de outubro, como pode ser visto na Tabela 1.2. É preciso levar em consideração, no entanto, que o APWG coleta dados de ataques de *phishing* reportados diretamente ao site da organização ou por e-mail, ou seja, membros das empresas precisam relatar os ataques. O que se tem, então, é apenas uma pequena amostra dos ataques cibernéticos no Brasil.

Tabela 1.2: Países/Territórios que hospedam sites de *phishing* - 4º trimestre de 2015.

Outubro		Novembro		Dezembro	
Belize	42.75%	USA	50.90%	USA	83.58%
USA	42.56%	Belize	27.22%	Holanda	1.95%
Bélgica	2.58%	Europa	4.65%	Reino Unido	1.51%
Europa	2.38%	Hong Kong	4.57%	Alemanha	1.26%
Alemanha	0.99%	China	1.14%	Austrália	1.12%
Reino Unido	0.81%	Canadá	1.09%	Hong Kong	0.86%
Canadá	0.71%	Itália	0.88%	China	0.82%
Brasil	0.63%	Alemanha	0.86%	França	0.73%
Hong Kong	0.60%	Reino Unido	0.81%	Rússia	0.60%
França	0.50%	Austrália	0.76%	Islândia	0.57%

Fonte: APWG (2016).

Nos relatórios publicados pelo APWG o Brasil também aparece relacionado algumas vezes entre os dez países que relatam *trojans* à base de *phishing* e hospedagem do arquivo malicioso. Em fevereiro e abril de 2014, o país aparece na nona posição e em junho atinge a quinta posição no ranque com 2.39% dos relatos registrados (APWG, 2016). No quarto trimestre de 2014 o Brasil só sai do ranque no mês de dezembro. Em 2015, mais precisamente no último trimestre, o Brasil não aparece ranqueado na categoria que relata *trojans* (APWG, 2016).

Com o Brasil frequentemente figurando nos relatórios do APWG que mostram os países que sofrem ataques de *phishing*, ainda que não englobe todas as empresas e, levando-se em consideração os dados coletados pelo CERT (Figura 1.2), torna-se necessário estudar e testar formas de se defender contra ataques de *phishing* e disponibilizar os resultados obtidos para a comunidade em geral.

1.2 Objetivos

O objetivo geral deste trabalho é realizar um estudo sobre ataques de *phishing* e suas respectivas medidas de contenção.

Os objetivos específicos são:

- Estudar os principais tipos de ataques de *phishing*;
- Estudar as principais medidas de contenção contra ataques de *phishing*;
- Apresentar as principais medidas de contenção contra ataques de *phishing*;
- Realizar testes nos principais navegadores de Internet quanto à capacidade de detectar ataques de *phishing*;
- Realizar testes em programas antivírus e extensões *anti-phishing* para os navegadores de Internet Chrome e Firefox.

1.3 Trabalhos Relacionados

O trabalho aqui apresentado está relacionado com outros trabalhos no que concerne a ataques de *phishing*, medidas de contenção contra golpes na Internet e Engenharia Social.

PEREIRA (2012), em seu trabalho "*Phishing*: Conceitos e ações preventivas aplicadas à empresa", demonstrou o funcionamento da fraude online *phishing* e propôs a redução da incidência desse tipo de ameaça de forma a não impactar na continuidade dos negócios da empresa. Ele elenca os tipos de fraude envolvendo *phishing* e também propõe, através do uso das melhores práticas de segurança da informação, uma forma de treinamento e conscientização do usuário de TI de uma empresa. Por fim, o autor destaca como aspectos positivos a disponibilidade de novas ferramentas no mercado no combate ao *phishing*.

ALENCAR et al. (2013), baseados em estudos teóricos e pesquisa aplicada a empresas da Grande Recife, Estado de Pernambuco, Brasil, elaboraram um artigo intitulado "O efeito da conscientização de usuários no meio corporativo no combate à engenharia social e *phishing*", cujo objetivo é mensurar a eficiência obtida através do processo contínuo de conscientização e treinamento de funcionários de empresas privadas de áreas externas à tecnologia da informação sobre os temas engenharia social e *phishing*. Segundo os autores, a pesquisa demonstra que engenharia social e *phishing* continuam sendo um meio eficiente para se conseguir dados de funcionários em meio corporativo.

No artigo "*Individual processing of phishing emails: How attention and elaboration can protect against individual phishing victimization*", HARRISON et al. (2016), exploram a

susceptibilidade de usuários ao *phishing* pela abertura de mecanismos que podem influenciar em sua vitimização, focando nas características da mensagem de e-mail. Segundo os autores, usuários foram expostos a um ataque real de *phishing* para avaliar o conhecimento, a experiência com *phishing* e como eles processam cognitivamente e-mails de *phishing*.

No artigo "*Experimental Analysis of Browser Based Novel System Tool at Educational Level*", GUPTA e SHUKLA (2016), propõem uma extensão para navegador de Internet batizada de "ePhish" e comparam sua performance com ferramentas *anti-phishing* existentes. A performance das ferramentas *anti-phishing* foram checadas em computadores de uma escola particular. Neste artigo são citadas algumas técnicas de identificação de *phishing* como número de pontos (.) e arrobas (@) na URL; a existência de endereço IP com ou sem porta na URL; entre outros.

No trabalho de PEREIRA (2012), as ferramentas de combate ao *phishing* citadas são voltadas para empresas, assim como o estudo de ALENCAR at al. (2013), restringe-se ao meio corporativo. Neste trabalho as ferramentas que ajudam a conter ataques de *phishing* estão voltadas tanto para empresas como para indivíduos.

Já no trabalho de HARRISON et al. (2016), não são abordados os principais tipos de ataques de *phishing*, tampouco as respectivas técnicas de contenção. Já no trabalho de GUPTA e SHUKLA (2016), a proteção oferecida contra ataques de *phishing* pelos navegadores de Internet foi menciona, no entanto, nenhum resultado de teste nestas ferramentas foi exposto pelos autores, diferentemente do trabalho aqui apresentado.

Os trabalhos de PEREIRA (2012) e de ALENCAR at al. (2013) se relacionam a este no que concerne à apresentação de técnicas de prevenção ao *phishing* e táticas de Engenharia Social. Já o trabalho de HARRISON et al. (2016), apresenta as principais características de das mensagens de e-mail. E o trabalho de GUPTA e SHUKLA (2016), mostra algumas técnicas de identificação de *phishing*.

1.4 Organização do Trabalho

O restante do documento está dividido seguindo o ordenamento descrito abaixo:

- Capítulo 2 – Trata de ameaças cibernéticas com ênfase em programas maliciosos e na técnica de Engenharia Social.

- Capítulo 3 – Apresenta os principais tipos de ataques de *phishing*. Ele também mostra dois exemplos de ferramentas utilizadas por atacantes e discute medidas de proteção contra ataques de *phishing*.

- Capítulo 4 – Apresenta testes realizados em navegadores de Internet, programas antivírus e extensões *anti-phishing*; mostra, também, o ambiente, o objetivo, a metodologia e o resultado dos testes.

- Capítulo 5 – Apresenta as considerações finais e os trabalhos futuros.

Capítulo 2

Ameaças Cibernéticas

A Internet, com milhões de computadores interconectados, assim como proporciona aos seus usuários facilidade na realização de muitas tarefas, também pode gerar muitos transtornos. Estes transtornos podem ser pequenos, quando decorrentes de um simples roubo de senha e posterior mudança de perfil em uma rede social qualquer, ou incalculáveis, quando decorrentes da perda de dados sigilosos, como, por exemplo, segredos industriais.

Com a expansão e evolução da Internet, passando de simples compartilhamento de arquivos HTML entre algumas universidades aos atuais serviços bancários online, novas possibilidades de se cometer delitos surgiram. Estas possibilidades fazem com que os internautas fiquem expostos a muitas ameaças. Estas ameaças muitas vezes se originam de brechas em sistemas computacionais ou falhas humanas que podem ser exploradas por golpistas. Brechas ou vulnerabilidades, por sua vez, quando exploradas pelos atacantes, geram incidentes de segurança, causando, não raramente, transtornos psicológicos e/ou financeiros.

Pelo exposto, este capítulo, então, apresentará conceitos relativos à segurança na Internet. Para isto, ele foi organizado da seguinte forma: na seção 2.1, são descritos os conceitos iniciais de ameaça, vulnerabilidade e incidentes de segurança; na seção 2.2, são mostrados os principais programas maliciosos que podem ser utilizados em ataques de *phishing*; na seção 2.3, é discutida a técnica de Engenharia Social; e, finalmente, na seção 2.4, têm-se a conclusão deste capítulo.

2.1 Conceitos Iniciais

Na Internet, o que é seguro hoje, pode não ser seguro amanhã. Programas de computador, principalmente os mais famosos, e equipamentos de rede, por exemplo, frequentemente são alvos de hackers buscando por algum tipo de falha. Essa busca, muitas

vezes, resulta na identificação de erros de programação, falha de desenvolvimento, entre outros. O internauta que utiliza *softwares* e/ou *hardwares* que apresentam algum tipo de vulnerabilidade, está sob constante ameaça de ter seu computador violado, podendo assim tornar-se vítima de um incidente de segurança. A seguir são apresentados os conceitos de vulnerabilidade, ameaça e incidente de segurança no contexto da Internet.

Vulnerabilidade

Vulnerabilidade está relacionada a falhas de programação ou até mesmo ao que os cibercriminosos consideram fraquezas humanas, como cobiça e ganância, por exemplo. Vulnerabilidade é uma "Condição que, quando explorada por um atacante, pode resultar em uma violação de segurança" (CERT, 2012).

> Por meio da exploração de vulnerabilidades, um computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados e ser usado para a propagação de códigos maliciosos. Além disto, equipamentos de rede (como modems e roteadores) vulneráveis, também podem ser invadidos, terem as configurações alteradas e fazerem com que as conexões dos usuários sejam redirecionadas para sites fraudulentos (CERT, 2012).

Para encontrar e explorar as vulnerabilidades descritas, os atacantes utilizam muitas vezes programas maliciosos específicos quando visam explorar falhas de programação ou de configuração. Ou ainda, no caso em que objetivam explorar algumas fraquezas humanas, os atacantes fazem uso de táticas de persuasão.

Uma vulnerabilidade é um ponto fraco que permite que uma ameaça seja concretizada ou que tenha efeito sobre um bem, afirmam KIM e SOLOMON (2014) apud MOREIRA (2016). Por fim, FRAGA (2016), define vulnerabilidade como um vetor, uma porta de entrada para um atacante.

Ameaça

A Natureza, de um modo geral, apresenta riscos com os quais os seres vivos têm de lidar a todo o momento. Com a Internet, componente recente desta Natureza, não podia ser

diferente. A rede mundial de computadores e seus usuários estão suscetíveis aos mais diversos riscos, que vão desde desastres naturais como terremotos, enchentes e queimadas, até os que são provenientes diretamente da ação humana, como roubo de dados, congestionamento da rede, entre outros.

O risco, ou a possibilidade de que algo aconteça, pode ser entendido como uma ameaça. De acordo com KIM e SOLOMON (2014) apud MOREIRA (2016), "uma ameaça é qualquer ação que possa danificar um bem". Já FRAGA (2016), explica que ameaça é um agente, uma ação que se aproveita de uma vulnerabilidade. Então, se um ataque cibernético pode danificar um bem como um arquivo confidencial, uma rede de computadores, ou torna possível a realização de transações financeiras fraudulentas, por exemplo, então um ataque cibernético pode ser considerado uma ameaça tanto para os internautas, quanto para a própria Internet.

Incidentes de Segurança

Crimes cibernéticos estão intimamente interligados com incidentes de segurança na Internet. Para o CERT (2012), "um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores".

CERON et al. (2009) classificam um incidente de segurança em duas categorias: incidentes internos e incidentes externos. O primeiro pressupõe que o atacante possui prévio conhecimento do alvo, ou seja, pode ser o funcionário de uma empresa, por exemplo, tentando ganhar acesso a informações confidenciais de seus colegas. O segundo se caracteriza por ser praticado por um agente de fora do sistema alvo, como por exemplo, um hacker na Rússia tentado invadir servidores nos Estados Unidos.

São exemplos de incidentes de segurança: tentativa de uso ou acesso não autorizado a sistemas ou dados, tentativa de tornar serviços indisponíveis, modificação não autorizada em sistemas e o desrespeito à política de segurança de uma empresa (CERT, 2012).

2.2 Programas Maliciosos

Programa malicioso, código malicioso, *software* malicioso, ou simplesmente *malware* são expressões que se referem a um programa de computador que é inserido em um sistema, normalmente de forma encoberta (MELLO et al., 2011). Estes programas têm, entre outras finalidades, o objetivo de roubar dados da vítima, ou ainda, bloquear ou destruir arquivos de seus alvos.

Com a existência de muitos programas antivírus, acarretando em uma maior capacidade de identificação de ameaças da Internet, e com uma maior preocupação por parte dos desenvolvedores com "*bugs*" em sistemas operacionais e em outros *softwares* mais ou menos robustos, infectar computadores com programas maliciosos não é uma tarefa tão simples, mas ainda ocorre, e um dos principais motivos pode estar relacionado à variedade de tipos de *malware* existentes.

Os principais tipos de *malware* existentes incluem vírus, *spyware*, *adware*, *trojan*, e *ransomware*. Esses programas maliciosos chegam ao computador alvo geralmente pela Internet, via e-mail, sites fraudulentos ou violados por um atacante, demonstração de jogos, arquivos de música; ou mídias removíveis como *pen-drives*, CDs e DVDs.

Programas maliciosos instalados no computador da vítima, como os citados no parágrafo anterior, podem causar desde pequenos transtornos como a perda de alguns arquivos até enormes prejuízos financeiros como o que vitimou a Etna Industrie em Paris – França, onde o atacante, fingindo ser o diretor executivo da empresa, solicitou e obteve a transferência de milhares de Euros através de e-mails falsos (KEYWORTH; WALL, 2016).

De acordo com o APWG (2016), no segundo trimestre de 2016 foram identificados 18 milhões de novas amostras de *malware*, em média 200.000 por dia. Dessas ameaças detectadas, 71,53% eram de *trojans* (incluindo *ransomware*), 12, 36% eram de vírus, 10,05% eram *worms*, 2,01 eram de *adware*/*spyware*, e o restante, 4,05%, eram de PUPs (Potentially Unwanted Programs – Programas Potencialmente Indesejáveis). Ainda segundo o APWG (2016), no primeiro trimestre de 2016 o Brasil era o décimo país em seu ranque de taxa de infecção, no segundo trimestre figurou em nono. Estes dados estão resumidos na Tabela 2.1.

Tabela 2.1: Ranque de infecção por *malware* por país.

Ranking	1º trimestre de 2016		2º trimestre de 2016	
	País	Taxa de infecção	País	Taxa de infecção
1	China	51.35%	China	49.02%
2	Turquia	48.02%	Taiwan	47.34%
3	Taiwan	41.24%	Turquia	40.99%
4	Equador	39.59%	Rússia	38.95%
5	Guatemala	38.01%	Guatemala	37.56%
6	Rússia	37.98%	México	36.89%
7	México	36.32%	Peru	36.23%
8	Peru	36.02%	Guatemala	36.22%
9	Polônia	35.55%	Brasil	34.68%
10	Brasil	34.00%	Polônia	33.01%

Fonte: APWG (2016).

*** Guatemala aparece duas vezes no relatório original.**

Para um maior entendimento das ameaças que acometem usuários da Internet, a seguir são apresentados os tipos mais comuns de *malware*.

Vírus

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas ou de arquivos (CERT, 2012).

> Para que um código malicioso seja considerado um vírus ele deve ter a capacidade de auto-replicação, ou seja, fazer uma cópia de si mesmo e distribuir essa cópia para outros arquivos e programas do sistema infectado (MELLO et al., 2011).

Os principais tipos de vírus são:

Vírus de e-mail – Arquivo anexo a um e-mail que além de contaminar o computador da vítima, pode enviar cópias de si para todos os contatos disponíveis no serviço de e-mail.

Isso significa que um usuário pode receber um código malicioso de um amigo sem que este saiba que está sendo usado como ponte para novos ataques;

Vírus de script – Escrito em linguagem de script como VBScript e Javascript. Pode ser executado automaticamente caso as configurações do navegador de Internet ou do programa leitor de e-mails do usuário permita (CERT, 2012);

Vírus de macro – Escrito em linguagem de macro. Segundo SMITH (2016), é escrito de forma a explorar vulnerabilidades de aplicativos que utilizam macro, que é uma sequência de passos necessários para imprimir um documento como a orientação de retrato e utilizando a escala de cores em tons de cinza, por exemplo. O arquivo que contém o vírus de macro precisa ser aberto para executar uma série de comandos automaticamente e infectar outros arquivos no computador.

Principais danos causados por vírus:

Os principais danos causados por esta ameaça são a perda de arquivos ou a formatação do computador, tornar o computador infectado vulnerável a outros tipos de ataques e *malwares*, e a lentidão do computador.

Spyware

Spyware é um tipo de programa malicioso construído para monitorar as atividades de um sistema, coletar dados sensíveis e enviar estes dados para o atacante. Os dados coletados vão desde informações sobre o histórico de navegação da vítima até informações confidenciais como número de cartão de crédito e senhas.

Os principais tipos de *spyware* são:

Keylogger – Programa malicioso que monitora as teclas do computador infectado. A ativação do *keylogger* é, em muitos casos, condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de *Internet Banking* (CERT, 2012);

Screenlogger – Programa malicioso que armazena a posição do cursor e a tela do site no instante em que o mouse é acionado.

Adware – Programa gratuito mantido por propagandas que aparecem como janelas de *pop-up*[*] ou como barra de ferramentas no computador ou navegador. Podem ser usados para coletar informações pessoais e rastrear os sites que o usuário costuma acessar (AVAST, 2016). Com as informações coletadas por *adware* é possível elaborar um ataque mais eficaz.

Principais danos causados por *spyware*:

Os principais danos causados por essa ameaça são o roubo de senhas, a captura de informações relativas à navegação da vítima e outros dados sensíveis.

Worm

Worm é um tipo de *malware* que ataca redes de computadores. A propagação desse tipo de ameaça ocorre automaticamente em redes locais e na Internet, seja por anexos de e-mail, FTP ou até mesmo por TCP/IP graças à capacidade do programa em fazer cópias de si próprio. Desta forma, computador a computador, vulnerável ao programa malicioso, vai sendo infectado.

Worms podem produzir brechas de segurança nos computadores, fazendo com que fiquem expostos a outros *malwares*. Por outro lado, *worms* podem auxiliar na descoberta de vulnerabilidades de sistemas de corrigi-las com a instalação de pacotes de atualização.

Os principais tipos de *worm* são:

Worm de e-mail – Infecta computadores por meio de mensagens de e-mail contendo *links* e/ou anexos maliciosos;

[*] Janela que aparece automaticamente e sem permissão, sobrepondo a janela do navegador Web, após o acesso a um site.

Worm de bate-papo – Compromete a segurança do computador por meio de canais IRC (*Internet Relay Chat*), isto é, redes de servidores que hospedam canais de bate-papo;

Worm de Internet – Infecta computadores por meio da própria rede mundial de computadores, principalmente, durante o acesso a sites fraudulentos ou que tiveram sua segurança comprometida.

Principais danos causados por *worms*.

Este tipo de programa malicioso causa lentidão na rede, podendo até mesmo pará-la completamente. Algumas variações de *worm* podem apagar arquivos em um sistema e também enviar documentos por e-mail.

***Trojan* (Cavalo de Tróia)**

Trojan é um tipo de programa malicioso que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas (CERT, 2012).

É considerado um vírus inteligente por hackers já que pode ser controlado à distância pelo atacante que o utiliza. "Esse tipo de *malware* é o mais comum quando se trata do cenário da Internet brasileira" (MELLO et al., 2011).

Os principais tipos de *trojans* são:

Trojan Backdoor[*] – Instala *backdoors* possibilitando o acesso remoto do atacante ao computador da vítima;

Trojan DoS (*Denial of Service* – Negação de Serviço) – Instala ferramentas de negação de serviço e as utiliza para desferir ataques. É um dos ataques mais comuns a servidores. Nesse tipo de ataque o alvo dos atacantes é exposto a uma quantidade muito grande de requisições

[*] Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim (CERT, 2012).

tornando seus recursos indisponíveis por minutos ou até dias. Muitos usuários participam desses ataques mesmo sem saber, tornando-os parte de *botnets*[*];

Trojan Proxy – Instala um servidor *Proxy*, possibilitando que o computador da vítima, atuando como intermediário entre a rede local e a Internet depois da infecção, seja utilizado para navegação anônima do atacante e para envio de *spam*[**];

Trojan Spy – Instala programas *spyware* e os utilizam para coletar informações sensíveis como senhas e números de cartão de crédito. Existem muitos outros tipos de *trojans* que, segundo o CERT (2012), são classificados de acordo com uma coletânea de nomes mais comumente utilizados pelos programas *antimalware*.

Principais danos causados por *trojans*.

O computador infectado por esse programa malicioso pode ser monitorado e até mesmo controlado, possibilitando que a vítima tenha senhas ou outros dados sigilosos roubados, além de permitir que o computador seja utilizado como ponte para outros ataques, sem o conhecimento da vítima, dificultando o rastreamento do atacante.

Ransomware

Ransomware é um *malware* desenvolvido para criptografar arquivos do HD da vítima. A chave para descriptografar os arquivos pode ou não ser fornecida depois que ocorrer o pagamento de um resgate. Daí o nome do programa malicioso (*ransom* – resgate). De acordo com o US-CERT (2016), variantes de *ransomware* têm sido observadas por vários anos e muitas vezes são programadas para extorquir dinheiro das vítimas exibindo alertas na tela do computador.

[*] *Botnet*, segundo o CERT (2012), é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots*, que por sua vez são programas que dispõem de mecanismos de comunicação com o invasor que permitem que eles sejam controlados remotamente.

[**] Termo usado para se referir aos e-mails não solicitados que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é chamado de UCE (*Unsolicited Comercial E-mail*).

Os alertas normalmente afirmam que o sistema da vítima foi bloqueado ou que seus arquivos foram criptografados. As vítimas são informadas de que a menos que um resgate seja pago, o acesso não será restaurado. O pagamento se dá principalmente na forma de *bitcoin* (moeda virtual), e dificilmente será rastreado já que os golpistas podem impossibilitar a descoberta de sua localização utilizando, por exemplo, a rede TOR, que provê conexões anônimas (REE; SYLVERSON; GOLDSCHLAG, 1996 apud DA SILVA; XAVIER, 2015).

Ransomware é conhecido também como *rogueware* (*rogue* – trapaceiro) ou *scareware* (*scare* – medo). Esse *malware* pode ser oferecido ao alvo como programa de segurança (antivírus ou *antispyware*), vir anexado a e-mails ou ainda pelo navegador de Internet, quando o usuário acessa um site infectado.

Os principais tipos de *ransomware* são:

CryptoLocker – Infecta o usuário por meio da abertura de e-mails que contêm anexos maliciosos que se instalam no computador da vítima, que por sua vez baixam o *CryptoLocker*;

Samas – Variação de *ransomware* que se propaga por meio de servidores Web vulneráveis;

Locky – Tipo de *ransomware* que se propaga através de e-mails *spam* que incluem documentos maliciosos do Microsoft Office ou anexos compactados (rar, zip) (US-CERT, 2016).

Principais danos causados por *ransomware*.

Os principais danos causados por esta ameaça são o bloqueio ou a perda de dados e, em caso de pagamento de resgate, prejuízo financeiro.

2.3 Engenharia Social

Para fazer com que os usuários da Internet sejam infectados por *malware*, os atacantes lançam mão de táticas de manipulação de fraquezas humanas, aplicando o que os estudiosos chamam de Engenharia Social.

Persuadir pessoas a executar determinadas ações é uma prática antiga. Essa prática, ou melhor, essa técnica é usada indistintamente tanto por crianças quanto por adultos. Um bebê quando chora tentando conseguir leite, um garoto fazendo "cara de triste" para ter a permissão de jogar videogame, ou um advogado manipulando informações para um júri com a finalidade de obter uma sentença favorável são alguns exemplos da utilização de Engenharia Social.

Engenharia Social, então, é uma técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações explorando a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas (CERT, 2012).

O medo ou o respeito que algumas pessoas têm por autoridades também pode ser explorado pelo engenheiro social, pessoa que utiliza essa técnica. Em empresas, por exemplo, o engenheiro social pode parecer modesto e respeitável, possivelmente afirmando ser um novo funcionário, um técnico ou pesquisador, oferecendo até mesmo credenciais para apoiar sua identidade (US-CERT, 2016), reunindo, desta forma, informações que lhe darão acesso à empresa.

HADNAGY (2011), define Engenharia Social como a arte de manipular uma pessoa para que ela tome alguma ação sendo ou não sendo o melhor alvo para o atacante, isso inclui obter informação ou ganhar acesso. Se um atacante não for capaz de reunir informações suficientes a partir de uma fonte, ele pode entrar em contato com outra fonte e confiar na informação da primeira fonte para ganhar mais credibilidade (US-CERT, 2016). Os golpistas podem, portanto, atacar mais de um alvo dependendo das fraquezas das pessoas que vão abordar e do objetivo a ser alcançado.

No contexto da Internet, a técnica da Engenharia Social ocorre principalmente com a manipulação de mensagens de e-mails ou na construção de sites falsos. Essa manipulação, por sua vez, tem como objetivo ludibriar pessoas e, assim, conseguir delas informações confidenciais como senhas, números de cartões de crédito ou, ainda, acesso a computadores ou sistemas por meio da instalação de programas maliciosos. A Figura 2.1 exemplifica a manipulação descrita.

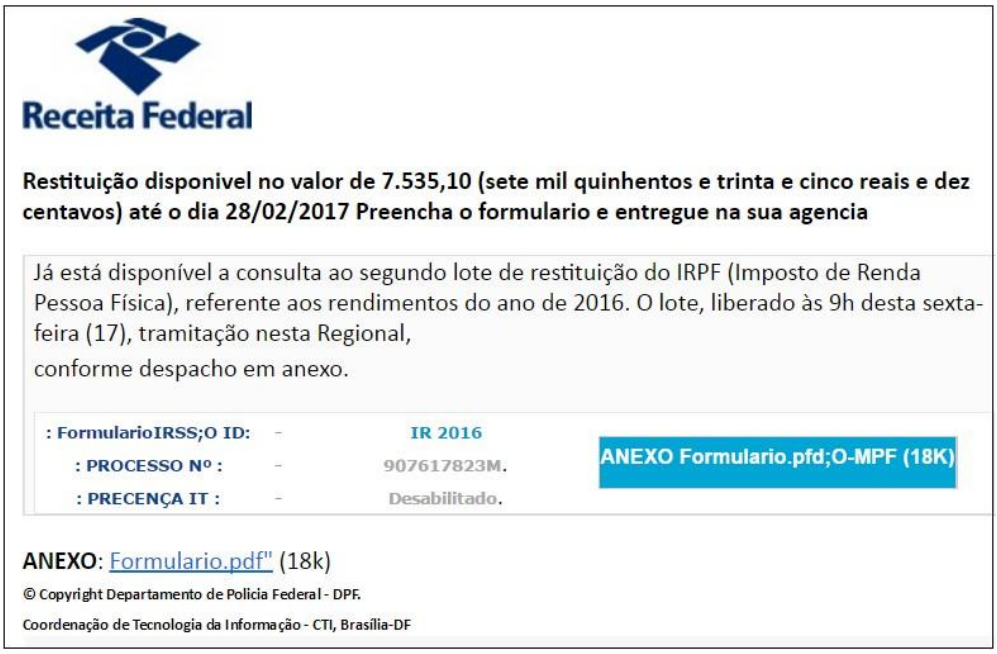


Figura 2.1: E-mail falso que induz o destinatário a clicar em *links* potencialmente maliciosos. Fonte: Elaborado pelo autor.

A técnica da Engenharia Social permite ao golpista induzir seus alvos a tomar uma decisão ou executar uma ação que lhes trará grandes prejuízos de tal maneira que não ofereçam nenhuma resistência e ainda assim acreditem que foi a coisa certa a ser feita. As vítimas, então, podem ter a sensação de dever cumprido e de que foram úteis para algo importante.

Para REINALDO FILHO (2006), Engenharia Social é um método de ataque onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do internauta para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores e outras informações. “Os criminosos e fraudadores usam Engenharia Social porque com ela é mais fácil de enganar alguém a revelar suas senhas do que com hackeamento do PC” (AVAST, 2016).

Alguns métodos de Engenharia Social podem ser evidenciados na Internet em sites fraudulentos de lojas que oferecem produtos com preços muito abaixo do que é praticado pelo mercado. Neste caso, os golpistas exploram principalmente fraquezas como a ganância, a cobiça e a ingenuidade da vítima fazendo com que ela pague por um produto que não vai receber e, em muitos casos, tenha seu cartão de crédito utilizado para efetuar outras compras ou para realizar novos golpes. LASZKA, VOROBEYCHIK e KOUTSOUKOS (2015),

explicam que o atacante procura o que há de mais atual circulando na mídia e provoca sua potencial vítima a acionar *links* falsos, instalar programas maliciosos, ou visitar diretamente sites igualmente falsos.

Outro golpe bastante utilizado ocorre quando o atacante, por meio de mensagens de *spam*, informa que identificou um problema no computador do alvo e que para "consertá-lo" há a necessidade de instalação de um programa para que o reparo seja realizado. A fraqueza que o atacante explora, neste caso, é o sentimento de confiança que o alvo deposita em um suposto serviço técnico de ajuda. A Figura 2.2 ilustra a tentativa de um atacante ludibriar seu alvo com um e-mail promocional.

Figura 2.2: E-mail falso utilizando técnicas de Engenharia Social.
Fonte: (BRADESCO, 2016).

No e-mail acima, Figura 2.2, o atacante explora o sentimento de cobiça (prêmio de R$ 120.000,00), e ao mesmo tempo, de confiança que as pessoas têm em relação aos bancos, para que o usuário clique no botão "INSCREVA-SE". Este clique pode descarregar no computador

da vítima um programa malicioso que vai monitorar suas ações em sites predefinidos pelo atacante, ou, ainda, redirecioná-la para um site falso que está programado para capturar os dados do alvo.

Engenharia Social não é um programa malicioso. No contexto da Internet, é uma técnica de persuasão, como a utilizada para elaborar o e-mail exemplificado na figura anterior, muito usada por *scammers* para ludibriar internautas a instalar programas maliciosos, acessar sites falsos ou mesmo sites legítimos que precisam melhorar sua posição nos ranques dos motores de busca da Web.

2.4 Conclusão

Neste capítulo foi possível observar que muitas vezes os usuários da Internet se tornam vítimas de criminosos que não utilizam pistolas ou facas, mas sim computadores, programas maliciosos e/ou métodos persuasivos para cometer seus crimes explorando vulnerabilidades de sistemas computacionais e/ou das pessoas que operam esses sistemas.

Por fim, Foram mostrados os principais programas maliciosos utilizados pelos golpistas: vírus, *spyware*, *worm*, *trojan* e *ransomware*. E foram discutidas as principais táticas de Engenharia Social. Nesse sentido, foi possível concluir que a combinação de programas maliciosos com Engenharia Social oferece subsídios ao golpista para manipular suas vítimas a fornecerem informações sensíveis, ou até mesmo realizarem transferências bancárias.

No próximo capítulo será mostrado um tipo de golpe que é, em sua essência, composto de táticas de Engenharia Social e que pode ser combinado com a utilização de programas maliciosos: o ataque de *phishing*.

Capítulo 3

Ataques de Phishing

Phishing, alusão a palavra inglesa *fishing* (pescaria), é o tipo de fraude por meio da qual os golpistas tentam obter dados pessoais e financeiros de um usuário da internet pela utilização combinada de meios técnicos e de engenharia social (CERT, 2012). Combina psicologia com tecnologia (ROSS, 2008). A taxa de sucesso desse tipo de ataque chega aos 20% (PHISHLABS, 2016).

E-mails com mensagens apelativas contendo *links* para sites falsos de empresas ou instituições consolidadas, sites maliciosos ou telefonemas solicitando atualização de dados cadastrais são alguns dos meios técnicos utilizados pelos golpistas para "pescar" informações sensíveis de seus alvos. Já o contexto criado para ludibriar o usuário a fornecer o número do seu cartão de crédito, *login*, senha, ou outro dado sigiloso é mérito da Engenharia Social.

O termo "*phishing*" foi criado por hackers que estavam conduzindo o roubo das contas da América Online (AOL) no ano de 1995 (ROSS, 2008). De posse do nome de usuário e de senhas das vítimas, os atacantes conseguiam novas informações sigilosas em outros tipos de serviços que a vítima pudesse ter, ou seja, era uma forma de "pescaria de informação".

Pescar informações na Internet foi, e ainda é, possível devido ao fato de que muitas pessoas têm o hábito de repetir suas senhas por comodidade quando vão realizar algum tipo de cadastro. Este comportamento arriscado no mundo real, replicado no mundo virtual, contribui para o sucesso dos atacantes.

O ataque de *phishing* evoluiu. Esse tipo de ataque é o principal vetor de ameaças dos atacantes e continua sendo o meio mais atrativo e eficaz para explorar vulnerabilidades (PHISHLABS, 2016). Conhecer seu funcionamento, como são construídos e as respectivas

contramedidas tornam-se necessário para a diminuição dos prejuízos causados na Internet. Para isto, este capítulo foi organizado da seguinte forma: a seção 3.1 discute as formas de uso do *phishing*; a seção 3.2 mostra a elaboração de um ataque de *phishing*; a seção 3.3 discute os tipos de ataques de *phishing*; a seção 3.4 mostra ferramentas para ataques de *phishing*; a seção 3.5 apresenta medidas de proteção contra ataques de *phishing* e, por fim, a seção 3.6 mostra a conclusão do capítulo.

3.1 Formas de Uso do *Phishing*

O ataque de *phishing* é usado para obter ilegalmente dados sigilosos de usuários. Contudo, existem duas formas na qual esses dados podem ser obtidos.

Forma Ativa

A forma ativa de *phishing* se dá quando o atacante envia e-mails, aleatórios ou não, aos seus potenciais alvos. Os e-mails utilizados podem vir de listas adquiridas de forma ilícita ou de listas elaboradas por programas específicos como o *TheHarvester*[*]. A vítima dessa forma de ataque é persuadida pelo atacante a entrar em um site de *phishing* ou a clicar em *links* ou botões para instalar programas maliciosos ou acessar sites fraudulentos.

A forma ativa de se obter dados sensíveis é a mais comum, pois requer menos esforço por parte do atacante. Com uma simples mensagem de e-mail o *phisher* pode conseguir informações valiosas da vítima ou até mesmo a transferência de dinheiro para uma conta bancária que está sob seu controle.

E-mails fraudulentos, bem elaborados ou não, são conhecidos como e-mails de *phishing* e também se enquadram na forma ativa de *phishing*, pois precisam ser disparados para seus alvos. Esses e-mails possuem algumas "armadilhas", que são recursos de programação ou construção de páginas em HTML com os quais se consegue o redirecionamento de um site para outro. Por exemplo, tem-se o caso da marcação <a> (*anchor* – âncora), responsável pela renderização de *hiperlinks* em documentos HTML.

[*] Ferramenta que possibilita a coleta de informações de um host, como e-mails relacionados, portas abertas, entre outras informações sensíveis.

OLIVO (2010), cita várias técnicas utilizadas por golpistas visando à captura de informação por meio de *hiperlinks*:

> Hiperlink com texto visível em formato de URL, mais apontando para uma URL diferente; hiperlink com um texto visível qualquer, mas apontando diretamente para um endereço IP como URL; e-mail com o corpo codificado em formato HTML; URL muito extensa; domínio do remetente do e-mail diferente do domínio de alguma URL no corpo da mensagem; imagem carregada a partir de domínio externo diferente das URLs do corpo da mensagem; descarga de uma imagem a partir de um endereço IP; número de domínios e subdomínios da URL; hiperlink com imagem ao invés de texto visível e URL da imagem baseada em endereço IP; e texto âncora do hiperlink não fornece informações sobre o seu destino.

Os exemplos acima se referem apenas a formas de ludibriar o usuário por meio da manipulação de *hiperlinks* HTML. No entanto, existem outras táticas utilizadas pelos atacantes que se enquadram na forma ativa de *phishing*. Um dos mais utilizados é o golpe da autoridade.

No golpe da autoridade os golpistas podem elaborar mensagens de e-mails de tal modo que assumem a identidade de pessoas com cargo de chefia (presidente, diretor) dentro de grandes organizações. Os alvos desses golpistas geralmente são gerentes ou funcionários do departamento de recursos humanos que podem, respectivamente, fazer movimentações financeiras ou enviar relatórios detalhados de outros funcionários. Mensagens bem elaboradas solicitando sigilo na comunicação fazem com que a vítima realmente acredite que esteja participando de algo importante e, ao mesmo tempo, impossibilitando que outras pessoas detectem o golpe, cedendo, então, a qualquer pedido dos golpistas.

Em resumo, a forma ativa de *phishing* requer uma participação mais efetiva do golpista.

Forma Passiva

Na forma passiva, o comportamento da vítima é que vai determinar o sucesso do atacante. Nesta forma o atacante pode simplesmente construir um site de *phishing* semelhante ao site de uma grande empresa e aguardar o acesso da vítima.

O acesso da vítima a sites de *phishing* pode ser induzido por meio de técnicas como a *BlackHat*[*]. Como exemplo PINHEIRO (2017), afirma que os fraudadores podem usar documentos PDF falsos com palavras chaves, *links* e imagens para destacarem-se nos motores de busca. O autor explica, também, que a manipulação de motores de busca forjando palavras chaves gera tráfego legítimo para páginas maliciosas que, quando acessadas, podem buscar por vulnerabilidades no navegador de Internet da vítima ou atacar diretamente seu roteador.

PINHEIRO (2017), afirma, por fim, que o diferencial da técnica *BlackHat* é que o pescador (atacante) é passivo, pois o mesmo não executa uma ação mais intrusiva, ele espera o acesso do seu alvo, garantindo, assim, mais sucesso nas infecções.

As duas formas de ataque de *phishing* apresentadas podem, contudo, não surtir o efeito desejado pelo golpista se seu ataque não for bem elaborado.

3.2 A Elaboração de um Ataque de *Phishing*

Estudos realizados sobre a efetividade dos ataques de *phishing* mostram quando e em que contexto um ataque de *phishing* é mais eficaz. O que provoca medo ou o que oferece ganhos financeiros. (ROGERS, 1983 apud HARRISON et al., 2016, tradução do autor) afirma que:

> Ataques de *phishing* baseados em medo são mais prováveis de resultar na diminuição e na elaboração da mensagem do que os ataques baseados em recompensa. Ataques baseados em medo são mais prováveis de resultar em vitimização que ataques baseados em recompensa.

Golpes em que o atacante utiliza e-mails contendo botões e/ou *links* para sites fraudulentos ou sites que descarregam *trojans* são os mais citados no material de referência pesquisado. Estes são também os mais difíceis de prevenir, pois a mensagem que estes e-mails possuem geralmente trata de um assunto com forte apelo emocional ao destinatário.

[*] Técnica capaz de pôr um site nas primeiras posições dos motores de busca. Ela pode ser utilizada tanto por webmasters quanto por golpistas.

A Figura 3.1 exemplifica o que ROGERS (1983) apud HARRISON et al. (2016) constatou em seu estudo: uma mensagem em tom de ameaça enviada por um atacante tentando induzir o alvo a clicar no botão “Iniciar Atualização”. A seta na figura abaixo destaca para onde o alvo será redirecionado caso acione o botão.

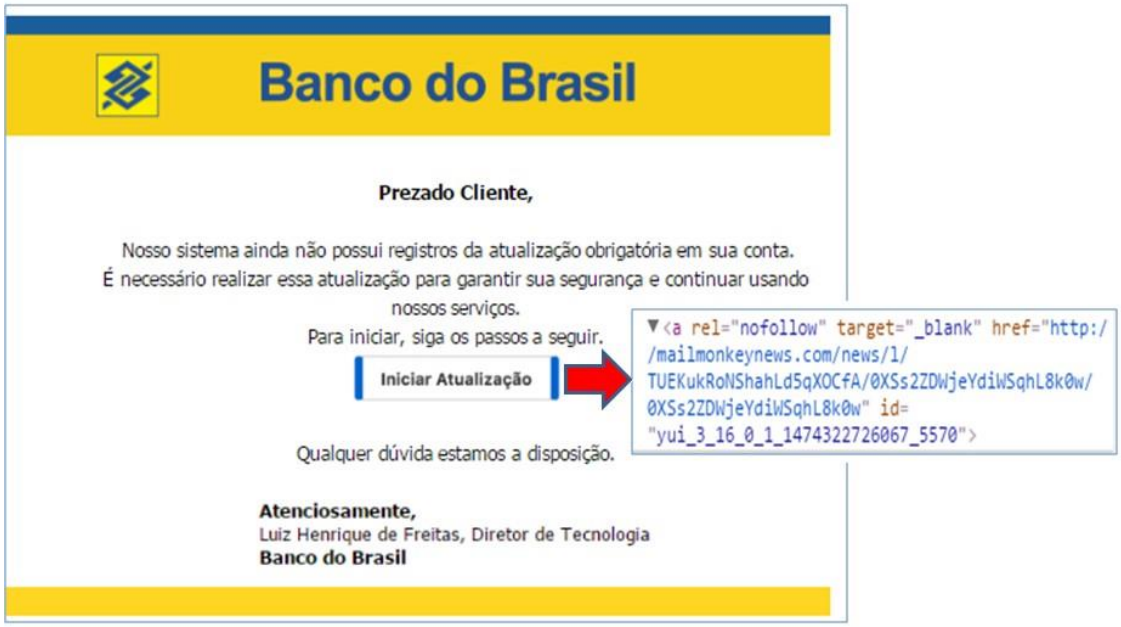


Figura 3.1: Exemplo de e-mail falso solicitando atualização de conta.
Fonte: Elaborado pelo autor.

O conteúdo de uma mensagem de e-mail de *phishing* tende a ser breve, como na figura anterior, mas também pode invocar urgência quando usar expressões como “Perigo” ou “Fim da linha” conjuntamente com frases como “Encerramento iminente de conta” ou “Restituição de impostos não reclamados” (ROGERS, 1983 apud HARRISON et al., 2016).

As mensagens com conteúdo apelativo do parágrafo anterior podem ser encontradas, por exemplo, em e-mails de contas em atraso, atualizações cadastrais, vantagens financeiras, produtos com preço muito abaixo do mercado, notificações de órgãos públicos, etc. Contudo, para serem mais eficientes, não podem ser utilizadas em ataques sem algum tipo de critério.

Da mesma forma que uma empresa organiza seus métodos de produção para se tornar mais competitiva no mercado e assim gerar mais lucro, um golpista também precisa se organizar. DAKWALA, LAVINGIA e SHAH (2016), dividem um ataque de *phishing* em três fases específicas: *lure* (atrair), *hook* (gancho, anzol) e *catch* (capturar).

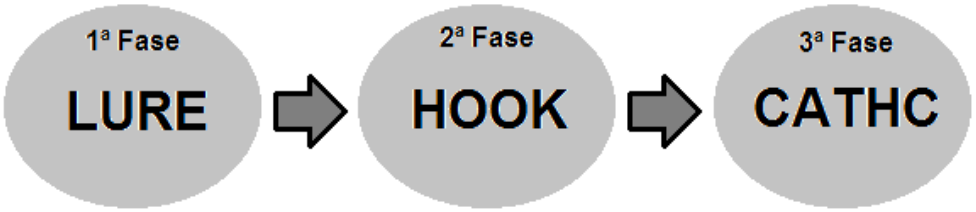


Figura 3.2: Fases de um ataque de *phishing*.
Fonte: Elaborado pelo autor.

A primeira fase de elaboração de um ataque de *phishing* engloba o e-mail de *phishing*. O site de Internet para o qual a vítima é redirecionada após clicar em um *link* de e-mail de *phishing* se enquadra na segunda fase. A terceira fase, por fim, se caracteriza quando a vítima informa dados sensíveis no site falso.

PEREIRA (2012), por sua vez, explica que um ataque pode ser dividido em seis fases: fase de planejamento, fase de preparação, fase de ataque, fase de coleta, fase de fraude e a fase do pós-ataque.

Tanto a forma de organização defendida por DAKWALA, LAVINGIA e SHAH (2016) quanto a defendida por PEREIRA (2012) podem ser mais bem exploradas pelos golpistas quando o ataque de *phishing* possuir características específicas.

3.3 Tipos de Ataques de *Phishing*

O material de referência pesquisado mostra algumas modalidades de ataque de *phishing* cuja elaboração apresenta características específicas que permite subdividi-lo em tipos. Nesse sentido, PEREIRA (2012), lista os mais comuns: *pharming*, *spear-phishing*, *iphishing*, *vishing scam*, mensageiro instantâneo e sites de relacionamento. No entanto, serão descritos apenas os três primeiros por não se distanciarem tanto do contexto de golpes de *phishing* na Internet, foco deste trabalho.

***Pharming* (Envenamento de DNS)**

Pharming é o tipo de ataque que ocorre quando o usuário tenta acessar o endereço legítimo de um site, mas é redirecionado para um site fraudulento. O redirecionamento pode

ocorrer por meio do comprometimento do DNS (*Domain Name System* – Sistema de Nomes de Domínios) que o usuário utiliza; pela ação de códigos maliciosos, que, algumas vezes são instalados por meio de ataques de *phishing* e são escritos para alterar o comportamento do serviço de DNS do computador do usuário; e pela ação direta de um invasor, que venha a ter acesso às configurações do serviço de DNS do computador ou modem de banda larga do usuário (CERT, 2012).

***Spear-Phishing* (Pesca com Arpão)**

Spear-Phishing é o tipo de golpe que ocorre quando um alvo é escolhido para receber um e-mail de *phishing* específico, como por exemplo, funcionários de uma determinada empresa. É um ataque direcionado, mas com características semelhantes ao *phishing*. E-mails de *spear-phishing* são enviados em lotes para um grupo muito restrito de pessoas, não para todos de uma vez, e algumas vezes podem até ser enviados individualmente.

Ataques de *spear-phishing* são, na grande maioria, ineficazes, mas os atacantes mudam suas táticas rapidamente. Nos últimos cinco anos foi observado um aumento no número de ataques cujo alvo são empresas com menos de 250 empregados, com 43% de todos os ataques direcionados a pequenas empresas em 2015 (SYMANTEC, 2016).

Iphishing

Iphishing é o tipo de ataque em que o golpista explora vulnerabilidades de produtos e serviços recém lançados. A velocidade de desenvolvimento de novas técnicas e tecnologias, quando não acompanhadas pelo desenvolvimento de novas técnicas de segurança, produz novas vítimas de *phishing*.

MARTINS (2008) apud PEREIRA (2012), explica que o *iphishing* é a vertente que visa explorar vulnerabilidades consequentes do avanço excessivamente rápido da tecnologia, que acaba por deixar aspectos de segurança em segundo plano, dando lugar a funcionalidade e ao design.

Como exemplo de *iphishing*, PEREIRA (2012), menciona o ataque que faz uso do método do javascript chamado “scrollto”. O autor explica que no momento que a página se carrega, ela pula para outra área da mesma tela, impossibilitando a visualização da URL.

É importante destacar, ainda, que recentemente o *phishing* está sendo utilizado em aplicações móveis. Essas aplicações maliciosas imitam aplicações legítimas e roubam informações confidenciais dos usuários. MARFORIO et al. (2015) explicam que aplicações de *phishing* não exploram sistemas vulneráveis, elas usam recursos padrão do sistema e se utilizam da incapacidade do usuário distinguir uma aplicação legítima de uma aplicação maliciosa.

Na próxima seção serão apresentados dois métodos utilizados pelos golpistas para a otimização de ataques de phishing, seja para o envio de muitos e-mails fraudulentos, seja pela construção de páginas falsas.

3.4 Ferramentas para Realizar Ataques de *Phishing*

Conhecer as ferramentas utilizadas pelos atacantes na elaboração de seus ataques pode ser útil para o usuário da Internet se precaver contra ataques de *phishing*. Para obter algum sucesso o golpista precisa lançar muitos ataques a alvos distintos.

O lançamento de muitos e-mails de *phishing* é chamado de “campanha de *phishing*”.

> Antes de lançar uma campanha, os atacantes precisam ter a capacidade de enviar e-mails em massa. Isso é tipicamente feito via os seguintes métodos: instalando em servidores web programas de envio de e-mails baseados em PHP; e usando robôs de spam; ou usando serviços de spam do “submundo da Internet” como o SafeSend (PHISHLABS, 2013).

Existem, ainda, alguns passos que são seguidos pelos golpistas na elaboração de uma campanha de *phishing*: encontrar ou criar um kit de *phishing*; encontrar onde “hospedar a isca”; hackear e estabelecer o acesso; estabelecer métodos para o envio de e-mails com iscas atrativas; iniciar o envio dos e-mails (muitos deles); coletar as informações roubadas; e usar ou vender essas informações (PHISHLABS, 2013).

Abaixo segue a descrição de uma ferramenta que otimiza o “trabalho” dos atacantes em campanhas de phishing.

Gophish

Gophish é uma ferramenta que otimiza a construção e o envio em massa de e-mail de *phishing*. Pode ser baixada gratuitamente e ser utilizada para criar campanhas visando à captura de informações sigilosas. No Gophish é possível utilizar listas de e-mails que podem ser obtidas, dentre outras formas, pela compra na Internet; por programas maliciosos que coletam dados de computadores infectados ou até mesmo de forma legal utilizando apenas os recursos dos serviços de *webmail*, onde uma mensagem, ao ser encaminhada para vários destinatários, expõe os respectivos endereços de e-mail. A Figura 3.3 mostra parte da configuração inicial de um ataque de *phishing* desta ferramenta.

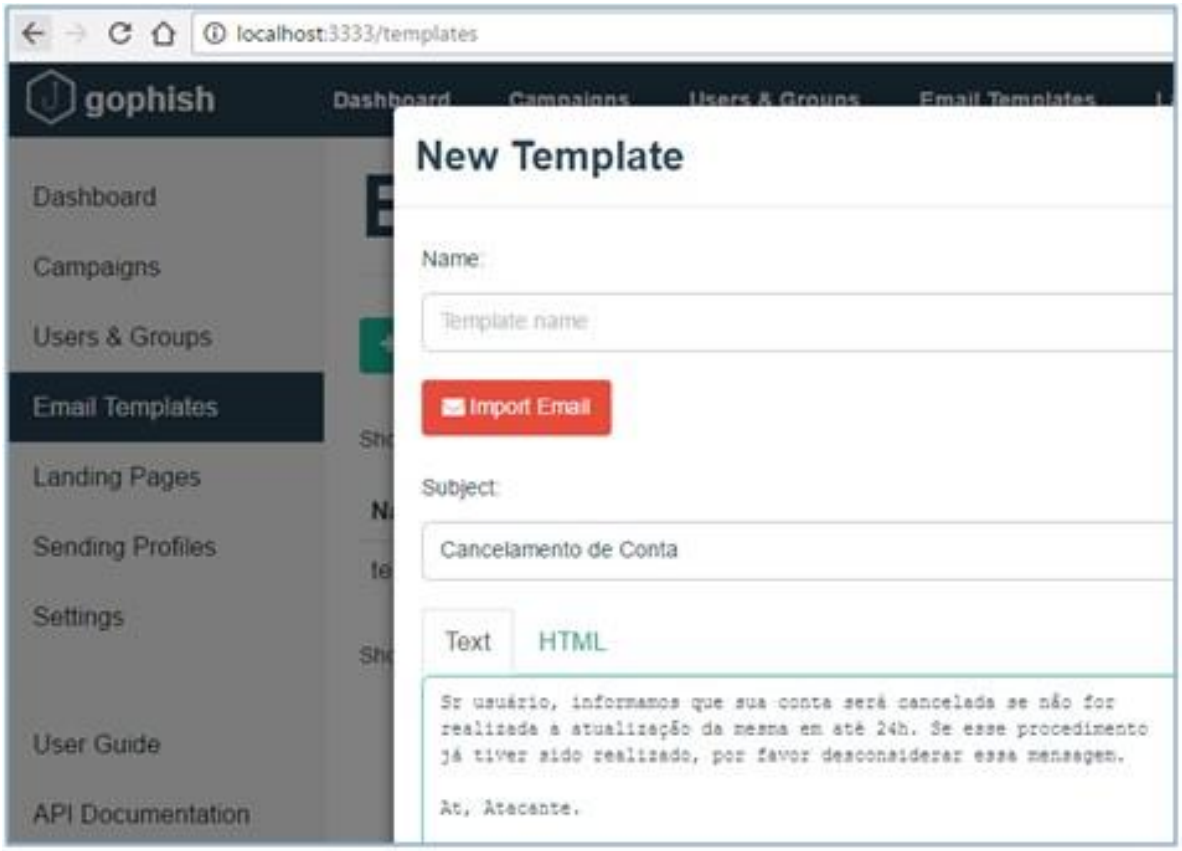


Figura 3.3: Parte da configuração de um ataque de *phishing* no GoPhish.
Fonte: Elaborado pelo autor.

Existem, ainda, sites como o Emkei* e o Anonymizer** onde é possível configurar o envio de e-mails falsos como se fossem de uma empresa legítima, por exemplo.

Os atacantes podem ter em suas mãos, também, ferramentas que constroem automaticamente páginas falsas que simulam as páginas de sites legítimos. Com essa fraude é possível capturar informações sensíveis como *login* e senha dos internautas. Abaixo segue a descrição de um programa que pode auxiliar os atacantes na elaboração de fraudes *online*.

SEToolkit (*Social Enginner Toolkit*)

SEToolkit é um programa que reúne um conjunto de ferramentas que auxiliam o atacante a clonar páginas Web para capturar as credencias das vítimas, principalmente de páginas de sites de redes sociais, entre outras funcionalidades. O ataque com o SEToolkit se dá quando o golpista envia por e-mail uma mensagem solicitando, por exemplo, algum tipo de atualização oferecendo à vítima um *link* para "facilitar o acesso". Este *link*, então, redireciona a vítima para uma página de *login* clonada. Caso a vítima envie suas informações, o atacante as terá em um servidor que pode ser configurado no próprio SEToolkit.

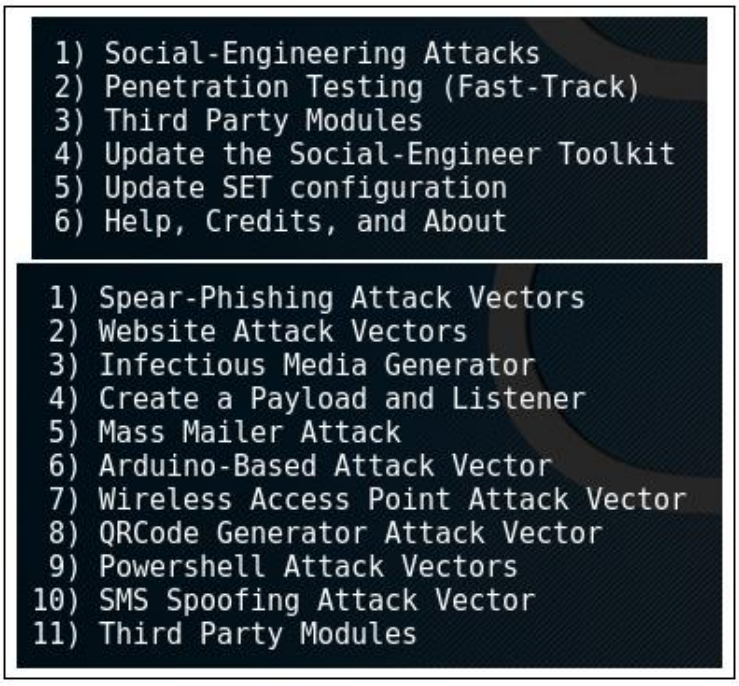


Figura 3.4: Menu e sub-menu da interface do SEToolkit.
Fonte: Elaborado pelo autor.

* Disponível em: https://emkei.cz/.
** Disponível em: http://anonymizer.in/fake-mailer/.

É importante ressaltar que o SEToolkit é uma ferramenta para teste de penetração, mas que também é utilizada por cibercriminosos.

As ferramentas de ataque em massa ou de clonagem de páginas da Internet são alguns dos recursos utilizados pelos golpistas. O internauta que sabe da existência desses recursos entende a necessidade de ser mais cuidadoso com o seu endereço de e-mail e, assim, utilizá-lo apenas em sites confiáveis.

Além do cuidado com o endereço de e-mail, existem outras formas de se proteger contra ataques de *phishing*. Estas formas serão mostradas na seção seguinte.

3.5 Medidas de Proteção Contra Ataques de *Phishing*

Nas seções anteriores foram mostrados os principais tipos de ataques de *phishing* e duas técnicas de otimização de ataques utilizadas pelos golpistas. Esta seção mostra que para se defender de ataques de *phishing* o usuário vai precisar adotar uma postura preventiva quando navegar pela Web, informar-se sobre os tipos de fraudes mais atuais e utilizar ferramentas de auxílio no processo de contenção dessas ameaças. Segue abaixo algumas medidas de proteção que os internautas podem adotar.

Informação

Conhecimento na área de segurança computacional e experiência em Internet diminuem a probabilidade de que um usuário se torne vítima de um ataque de *phishing*. HARRISON (2016), afirma que fatores individuais como conhecimento e experiência em e-mails acrescentam resiliência para ataques de *phishing*.

Neste contexto, uma das principais medidas de proteção contra ataques de *phishing* se dá por meio da educação do internauta. A cartilha de segurança para Internet do CERT (2012), é uma boa fonte de informação para a prevenção de vários tipos de golpes cibernéticos, inclusive o *phishing*.

Pelos prejuízos que causa, o ataque de *phishing* deveria ser amplamente divulgado nos principais meios de comunicação, principalmente os da Internet. No entanto, o que se vê algumas vezes são apenas os relatos das vítimas. Pouquíssima atenção tem sido dada ao compartilhamento de informações sobre *phishing* em mídias sociais (VALECHA et al., 2015). Esse recurso pode ser bastante útil, mas deve ser usado com cuidado, pois os atacantes também podem utilizá-lo para disseminar informações falsas.

Treinamento de funcionários

A capacitação e a conscientização contínua dos funcionários podem servir como fator de elevação do grau de segurança da informação de uma corporação, fortalecendo o que hoje representa o elo mais fraco da segurança da informação numa corporação (ALENCAR et al., 2013).

Recursos didáticos podem ser utilizados no treinamento de funcionários para ajudar a combater ataques de *phishing*. É possível fazer uso, por exemplo, de aplicativos para *smartphones* que ensinam o internauta a reconhecer os principais truques utilizados pelos golpistas. Um desses aplicativos é o NoPhish, que foi desenvolvido por alunos da Universidade Técnica de Darmstadt – Alemanha.

NoPhish é um jogo que treina usuários da Internet a acessarem, analisarem e checarem URLs por meio de exercícios com até oito níveis de dificuldade, habilitando o usuário a distinguir websites confiáveis de não confiáveis. Em alguns níveis dos exercícios propostos, a aplicação pergunta se a URL mostrada é legítima ou é uma URL de *phishing*. Esta aplicação ajuda os seus usuários a tomar as melhores decisões com relação à legitimidade de URLs imediatamente depois de jogar NoPhish, bem como depois de algum tempo passado (CANOVA et al., 2014).

Na Figura 3.5, a seguir, é possível visualizar a tela de introdução e de exercício deste aplicativo.

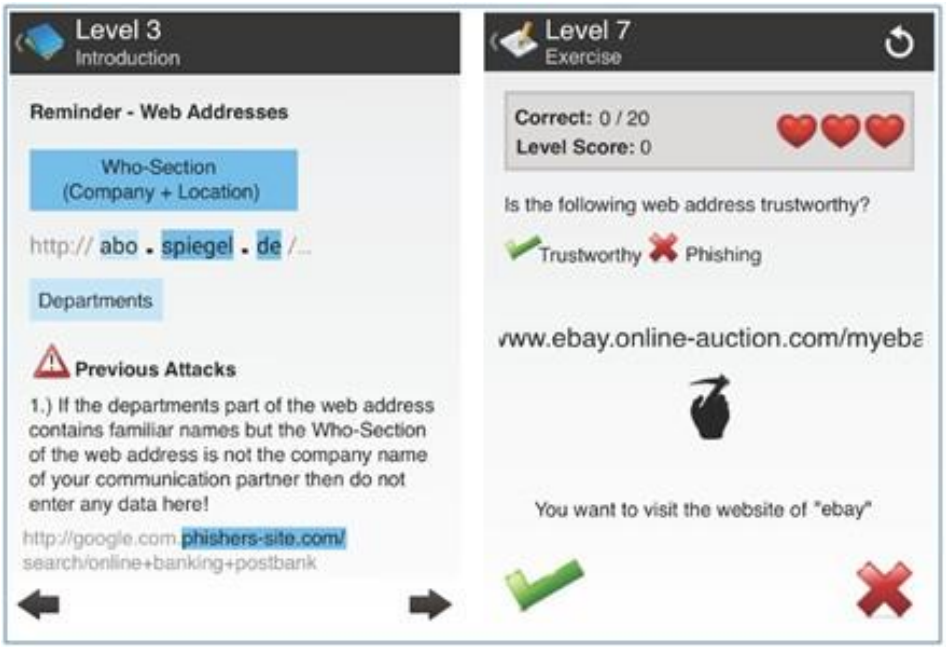


Figura 3.5: Duas telas do aplicativo NoPhish - Introdução e Exercício.
Fonte: CANOVA et al., 2014.

Questionamento

Outra medida preventiva que o internauta deveria adotar seria sempre se questionar porque a ele, dentre tantos, está sendo oferecida determinada vantagem (CERT, 2012). Se este questionamento não puder ser respondido, pode ser mais um sinal de tentativa de golpe.

Ficar atento a e-mails cujo conteúdo informe sobre prêmios, principalmente se for de loterias internacionais, crédito fácil, doação de animais, oferta de emprego e noiva russa*, por exemplo, também podem evitar muitos prejuízos.

Erros gramaticais

Sites e e-mails fraudulentos que geralmente são elaborados por pessoas que não estão familiarizadas com a língua oficial do alvo, geralmente contêm erros de ortografia, concordância, acentuação, entre outros. Estes erros são indicativos de golpe, como o que pode ser visto em várias frases contidas no e-mail da Figura 3.6.

* Golpe em que o golpista faz insinuações sobre um possível relacionamento amoroso, mas solicita ajuda financeira para viajar ao país da vítima.

Fwd: UFPA -WEB- administrador do servidor de atualização.

-------- Mensagem original --------
Assunto: UFPA -WEB- administrador do servidor de atualização.
Data: 2016-08-28 17:51
De: "Marcos Rodrigo Momo" <momo@furb.br>
Para:

Caro titular E -mail

Esta é para informá-lo que nós começamos nosso programa de Fim de e -mail actualização 2016 ano, para a proteção de seus usuários de e-mail . temos vindo a registar congestionamento no nosso servidor , e por isso provedor de e -mail UFPA. será curto-circuito para baixo alguns conta de e -mail não utilizado e seu e-mail pode ser entre a lista se você ainda está usando seu e-mail , você precisa verificar a sua conta de e-mail imediatamente.

Se isso não for concluída até 24 horas. você perderá conta indefinitely.Click e- mail aqui para verificar as suas contas.
https://activeforms.com/correoelectronicouser/atualizao-emailuser

Se o link acima não funcionar, copie e cole o seguinte url no seu browser.
https://activeforms.com/correoelectronicouser/atualizao-emailuser

Serviços de Segurança UFPA.BR
Pedimos desculpas por qualquer inconveniente.

Copyright 2016 Universidade Federal do Pará - Rua Augusto Corrêa, 01 - Guamá CEP 66075-110. Caixa postal 479. PABX +55 91 3201-7000. Belém -Para - Brasil 2016

Figura 3.6: E-mail de *phishing* contendo erros gramaticais.
Fonte: Elaborado pelo autor.

.

Cuidado com senhas

Quando se é vítima de *phishing*, dados sigilosos como *login* e senha de uma conta de e-mail podem ser furtados e alguns problemas consequentemente irão surgir, mas não saber que isso aconteceu é ainda pior, pois o *scammer* pode se passar pela vítima e acessar muitas outras informações por um longo tempo.

O internauta pode estar sendo vítima de golpistas quando começa a ter problemas com órgãos de proteção ao crédito ou recebe o retorno de e-mails que não foram enviados por ele mesmo (CERT, 2012). Neste caso é preciso mudar a senha e todos os mecanismos de recuperação de acesso do serviço comprometido para bloquear o atacante. O mais correto, no entanto, é que o usuário já tenha o hábito de mudar suas senhas frequentemente, antes mesmo de desconfiar que esteja sendo enganado.

Elaborar senhas fortes, ou seja, senhas exclusivas para cada uma das suas contas importantes com combinação de letras, números e símbolos sem informações pessoais ou palavras comuns (GOOGLE, 2016), não repeti-las em outros serviços e ter cuidado no momento de usá-las deve ser o comportamento natural de um usuário da Internet.

Autenticação por duplo fator

A escolha dos serviços online também pode ser de grande ajuda no processo de contenção contra golpes de *phishing*. Uma boa solução de segurança utilizada pelos desenvolvedores é a "autenticação por duplo fator", onde o usuário final além de informar *login* e senha em uma página da Internet, ainda precisa confirmar que está acessando o serviço por meio de um código que é enviado a um dispositivo móvel previamente cadastrado.

Caso o internauta se torne vítima de um ataque de *phishing*, inserindo suas credencias em um site fraudulento, por exemplo, ainda assim estará protegido, mas somente se o atacante não estiver de posse do dispositivo (desbloqueado) cadastrado para a confirmação de acesso ao serviço legítimo.

Digitar ou inspecionar o endereço do site

Para diminuir a possibilidade de acessar sites de *phishing*, o internauta pode digitar o endereço completo do site (URL) que pretende visitar no seu navegador de preferência ao invés de utilizar motores de busca como o do Google. Páginas Web fraudulentas são colocadas na Internet por algumas horas com URLs semelhantes à de grandes instituições visando ludibriar o internauta. Sites como o PhishTank* e o VirusTotal** podem ajudar o internauta a identificar URLs maliciosas.

Alguns ataques de *phishing* utilizam o símbolo "@" para redirecionar o usuário para outro website. O atacante pode criar uma página de Internet com o endereço: http://www.myhomepage.co@yahoo.com?login.com, fazendo o internauta pensar que está sendo direcionado para o website Yahoo.com (GUPTA, 2016). É preciso, então, que o

* Disponível em: https://www.phishtank.com/.
** Disponível em: https://www.virustotal.com/.

internauta sempre cheque a URL do site que está sendo acessado antes de fornecer qualquer tipo de informação, e inspecionar *links* e imagens do site suspeito para evitar ser vítima de *malwares* ou de furto de dados.

O código identificador do país, presente no endereço do site, também indica tentativa de *phishing*. Sites fraudulentos são criados por golpistas em um país e o lançam como isca em outros países. De acordo o PHISHLABS (2016), em 2015, o pico de sites de *phishing* com o código identificador de país *.cn* foi diretamente atribuído a uma campanha de *phishing* cujo alvo foi o principal banco chinês. Em agosto eram aproximadamente 50 domínios, já em novembro, esse número saltou para um pouco mais de 120.

No entanto, como pode ser visto na Figura 3.7, sites hospedados com *.com* ainda respondem por grande parte dos sites de *phishing*.

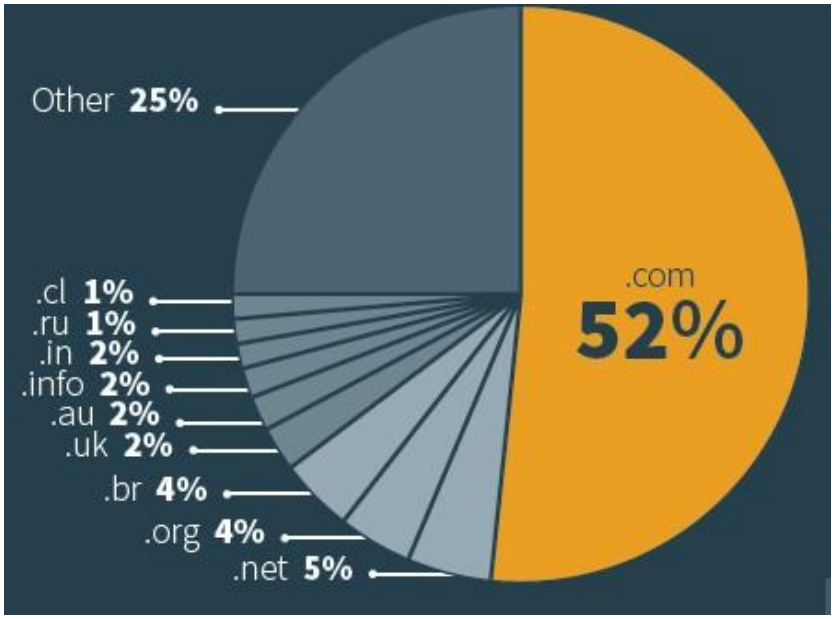


Figura 3.7: Principais domínios associados com websites que hospedam conteúdo de *phishing*.

Fonte: PHISHLABS, 2016.

Utilização de *softwares anti-phishing*

Todas as medidas de proteção citadas acima podem não ser suficientes para ajudar o internauta no combate ao *phishing*. Recentes abordagens, especialmente em universidades,

estão focando seus esforços em comportamento dinâmico como filtragem de websites baseado em reputação ou o uso de algoritmos de heurística para detectar ataques de *phishing* (WOLFF, 2009). Atualmente esses recursos vêm sendo empregados em *softwares*, ou melhor, em ferramentas que ajudam a combater ataques de *phishing*.

No que concerne à heurística, ainda são muitos os falsos positivos gerados por ferramentas *anti-phishing* que se utilizam desses algoritmos, inviabilizando seu uso para detecção de sites fraudulentos (WOLFF, 2009). Já as ferramentas *anti-phishing* que se utilizam do conceito de listas negras, apesar de serem apenas reativas, reforçam o combate a ataques de *phishing*.

Como a quantidade de detalhes com que um usuário da Internet tem de se preocupar é muito grande, a utilização de ferramentas *anti-phishing* pode ser bastante útil no processo de contenção contra ataques de *phishing*.

São exemplos de ferramentas que podem ajudar contra ataques de *phishing*: os navegadores de Internet, programas antivírus com extensões ou recursos *anti-phishing* e extensões *anti-phishing* para navegadores Web. Contudo, essas ferramentas devem possuir um nível de eficácia razoável, caso contrário, o usuário que optar por usá-las pode ficar mais vulnerável ao confiar mais na ferramenta e menos no seu poder de observação.

3.6 Conclusão

Este capítulo apresentou existência de duas formas distintas de ser vítima de um ataque de *phishing*: a forma ativa e a forma passiva. Na forma ativa o atacante dispara e-mails fraudulentos contra seus alvos e aguarda o envio de informações. Já na forma passiva, um usuário da Internet acessa uma página falsa e fornece dados sigilosos sem que tenha sido ludibriado previamente.

Foi visto, também, que os golpistas podem realizar ataques de *phishing* mais elaborados, focando mais no medo ou mais na cobiça, organizando-os em fases predeterminadas fazendo uso de ferramentas que otimizam os ataques. Esses ataques, por sua vez, podem ter características distintas como o *pharming* e o *spear phishing*.

Foram expostas algumas medidas de proteção que o usuário da Internet pode utilizar para se precaver contra ataques de *phishing*. Contudo, merece destaque a escassez na divulgação de informações sobre os golpes. A Internet, por meio das redes sociais, poderia ser mais bem aproveitada com o compartilhamento frequente dos ataques de *phishing*.

Por fim, pode concluir que os atacantes, a cada dia, se tornam mais efetivos e seus ataques mais sofisticados. Nesse sentido, ferramentas como navegadores Web, programas antivírus e extensões *anti-phishing* para navegadores de Internet podem auxiliar o internauta no processo de contenção contra ataques de *phishing*, sendo que a última merece destaque por ser uma das ferramentas mais recentes no combate a sites maliciosos. Algumas dessas ferramentas serão apresentas no próximo capítulo.

Capítulo 4

Uma Avaliação sobre Ferramentas Anti-Phishing

Usuários da grande rede mundial de computadores estão expostos aos mais variados golpes. A atenção redobrada ou o conhecimento de fraudes podem não garantir uma navegação totalmente segura contra ataques de *phishing*. Falhas humanas podem ocorrer em quaisquer situações, e na Internet isso não é diferente.

> As falhas humanas estão se tornando uma causa cada vez mais comum de violações de segurança no Brasil. Um estudo divulgado no último ano pela CompTIA* mostrou que 58% das violações no Brasil foram causadas por erro humano, como descuido geral, falha ao seguir políticas de segurança e falta de expertise (MILITELLI, 2017).

As falhas às quais os internautas estão sujeitos, muitas vezes, também se devem a expertise dos atacantes. Os atacantes frequentemente modificam seus métodos de abordagem assim que deixam de obter sucesso em suas investidas. Novas técnicas, então, são criadas dificultando o combate apenas por meios informativos. Nesse contexto, surgem as ferramentas *anti-phishing*, que são projetadas para proporcionarem mais uma camada de proteção contra golpes na Internet.

Contudo, é preciso observar qual a relevância que estas ferramentas têm no que concerne a proteção do internauta durante sua navegação na Internet. Neste contexto, este capítulo trata da avaliação de ferramentas *anti-phishing*, sendo organizado da seguinte forma: na seção 4.1 são apresentadas algumas ferramentas *anti-phishing*. Na seção 4.2 são discutidos os testes das ferramentas *anti-phishing* apresentadas neste trabalho. E Na seção 4.3 é mostrada a conclusão deste capítulo.

* Associação de comércio sem fins lucrativos que promove os interesses globais dos profissionais e das empresas de TI. Disponível em: HTTPS://www.comptia.org/international/brazil/home.

4.1 Ferramentas *Anti-Phishing*

Ferramentas *anti-phishing* têm como princípio de funcionamento a coleta de informações de outros usuários sobre suas experiências com sites e e-mails fraudulentos. Os desenvolvedores dessas ferramentas possuem comunidades que alimentam uma base de dados, gerando listas negras que podem ser acessadas com a finalidade de bloquear novos ataques, minimizando possíveis danos ao internauta.

As ferramentas avaliadas neste trabalho que auxiliam no processo de contenção a ataques de *phishing* são: navegadores de Internet, programas antivírus com extensão *anti-phishing* e extensões *anti-phishing* para navegadores de Internet. Essas ferramentas são apresentadas a seguir.

4.1.1 Navegadores de Internet

No cenário atual de crescimento dos ataques de *phishing*, um navegador de Internet precisa ser capaz de alertar ao internauta se o site que pretende acessar é ou não malicioso, evitando, assim, a instalação de programas maliciosos, a perda de dados ou até mesmo prejuízos financeiros.

Os navegadores de Internet escolhidos para a avaliação são o Google Chrome e o Mozilla Firefox. Estes navegadores são uns dos mais utilizados no Brasil (STATCOUNTER, 2016 apud GRASEL, 2017), e possuem mecanismos que bloqueiam páginas maliciosas.

Google Chrome

O navegador Google Chrome é um dos mais utilizados da Internet. Até julho de 2016, era usado por aproximadamente 80% dos internautas brasileiros (STATCOUNTER, 2016 apud GRASEL, 2017). Possui um modo de navegação privada que apaga automaticamente histórico de navegação, *cookies* e, principalmente, senhas.

No que concerne a ameaças da Internet, este navegador avisa quando o site que o usuário está tentando acessar é suspeito de *phishing* ou *malware*. A Google mantém uma lista

de sites que podem colocar o internauta em risco, também analisa o conteúdo do site e avisa se ele parece perigoso (GOOGLE, 2016).

Quando a detecção de *phishing* e *malware* está ativada, ao identificar uma página maliciosa, este navegador apresenta as seguintes mensagens: "O site a seguir contém *malware*!", conforme a Figura 4.1; "Perigo: *malware* adiante!"; "Site enganoso à frente", ou seja, o site que o usuário está tentando acessar é suspeito de ser um site de *phishing*; e "O site a seguir contém programas prejudiciais" (GOOGLE, 2016).

Figura 4.1: Alerta do Chrome durante a tentativa de acesso ao site 38zu.cn.
Fonte: Elaborado pelo autor.

A Figura 4.1 apresenta a tela de alerta do navegador de Internet Chrome durante a tentativa de acesso a um site potencialmente malicioso. Se ainda assim o internauta quiser acessar o site, basta clicar em "DETALHES" e aceitar os riscos.

Mozilla Firefox

O Mozilla Firefox é o segundo navegador de Internet mais utilizado por internautas brasileiros (STATCOUNTER, 2016 apud GRASEL, 2017). Disponibiliza vários canais de suporte aos seus usuários, além de uma vasta lista de complementos que auxiliam em uma navegação mais segura.

O navegador Firefox informa sobre os sites que o usuário acessa para aumentar a sua segurança *online*. Assim como outros navegadores de Internet, o Firefox tem sido aperfeiçoado com filtros que bloqueiam sites que constam em listas negras de diversos serviços. Essa abordagem, contudo, requer constante atualização, pois novas ameaças surgem a todo o momento, e essas listas são comumente realimentadas manualmente. Em alguns casos estas listas são atualizadas por processos semi-automáticos (WOLFF, 2009).

O Firefox abrange três níveis de segurança: conexões seguras, ou seja, o usuário tem a possibilidade de usar o Website ID* para garantir que o site é quem diz ser e conferir se sua conexão é segura; proteção de nível mundial, isto é, recursos *anti-phishing* e *anti-malware* protegem o usuário de *trojans* e *spywares*, avisando sobre qualquer suspeita de fraude, por meio de verificações de listas que são atualizadas a cada 30 minutos quando os recursos contra *phishing* e *malware* estão habilitados; e atualizações de segurança automáticas, onde o navegador atualiza-se automaticamente garantindo que o usuário estará sempre protegido (MOZILLA, 2016).

A Figura 4.2, a seguir, exibe um alerta de ataque do Firefox ao internauta. Depois de clicar em "Ignorar este alerta", *link* posicionado no canto inferior direito da figura em questão, o usuário pode acessar o site normalmente. Fechado o site, se o usuário tentar acessá-lo novamente, o bloqueio no navegador não é mais acionado. O bloqueio retorna somente se for feita uma nova tentativa de acesso ao site depois de o navegador ter sido fechado.

* Sistema codificado por cores que avisa ao internauta quais sites pode desconfiar. O verde indica que o site é seguro, enquanto que o cinza indica maior atenção.

Figura 4.2: Alerta do Firefox durante tentativa de acesso ao site 38zu.cn.
Fonte: Elaborado pelo autor.

4.1.2 Programas Antivírus com Extensão *Anti-Phishing*

Foi mostrado que os navegadores de Internet possuem recursos capazes de impedir o acesso a sites maliciosos. No entanto, existem ferramentas que proporcionam uma proteção mais abrangente. Estas ferramentas são os programas *antivírus*.

Alguns programas *antivírus* geram alerta para os resultados dos principais motores de busca da Internet. Eles são uma barreira inicial contra o acesso a sites fraudulentos e também instalam extensões *anti-phishing* nos navegadores Web. A seguir são apresentadas as principais funcionalidades de três programas *antivírus* disponíveis no mercado: Avast, AVG e Avira. Estes foram escolhidos por possuírem versões gratuitas com extensões ou recursos *anti-phishing*.

Avast

O Avast é um antivírus capaz de detectar vírus, *malware* e proteger a rede doméstica de Internet; analisa arquivos desconhecidos em tempo real e identifica sites falsos. O Avast disponibiliza ao internauta o *Avast Online Security*, que é uma proteção para o navegador Chrome, um *plugin* de reputação de sites mantido por uma comunidade de mais de 220

milhões de usuários. Recolhe informações de sites de *phishing* e adverte o usuário caso este acesse algum site de má reputação (AVAST, 2016).

Ao acionar o ícone da extensão no *browser* é possível que o usuário classifique sua experiência no site em que está como "positiva" ou "negativa", ou seja, a ferramenta dispõe de uma classificação para sites da qual o usuário também pode participar. A extensão exibe, ainda, uma lista com sistemas de rastreamento utilizados no site, além de redes sociais, propagandas, sites de análise, entre outros.

AVG

O programa antivírus AVG evita roubo de dados e fraude *online*; bloqueia *links* e arquivos perigosos; verifica *links* na Web, Twitter e Facebook; avisa sobre a presença de anexos mal-intencionados e possui recursos de privacidade para manter os dados do usuário em privacidade (AVG, 2016).

Segundo GARRET (2016), o AVG

> Conta com um sistema de leitura de *links* e páginas da Internet para surpresas desagradáveis. Com esse recurso habilitado, o software lê *links* dispostos em páginas da web para encontrar ameaças, alertando o usuário para que não clique em potenciais focos de distribuição de vírus.

O programa disponibiliza, também, um componente de proteção contra riscos presentes em mensagens de e-mail. Esse componente identifica ameaças em mensagens armazenadas nas caixas de entrada, saída, e até no filtro de *spam* do usuário (GARRET, 2016).

Avira

A ferramenta *anti-phishing* do programa antivírus Avira monitora as páginas que o internauta está acessando, sempre em busca de páginas suspeitas que possam tentar roubar informações pessoais do usuário, como senha de banco ou número de cartão de crédito. A

extensão para navegador de Internet *Avira Browser Safety* protege a privacidade do internauta *online* e bloqueia sites mal-intencionados antes de carregarem (AVIRA, 2016).

4.1.3 Extensões *Anti-Phishing* para Navegadores Web

Contra ataques de *phishing*, é possível, ainda, utilizar um terceiro nível de proteção. O internauta pode fazer uso de extensões *anti-phishing* para navegadores de Internet, pois

> A função dessas ferramentas é determinar se um site visitado é ou não fraudulento com base em informações extraídas durante a navegação. Após a classificação, o resultado normalmente é apresentado ao usuário através de um ícone na janela do navegador, uma janela de alerta ou bloqueio da navegação (OLIVO, 2010).

Algumas dessas ferramentas, além de oferecerem proteção contra sites maliciosos, também auxiliam no processo de contenção contra ataques de *phishing* por e-mail, e por isso, terão este recurso avaliado. A seguir são apresentadas as principais ferramentas que acrescentam mais uma camada de proteção contra ataques de *phishing*.

Netcraft

O Netcraft é uma extensão para os navegadores de Internet Chrome, Firefox e Opera. Funciona coletando informações dos usuários sobre sites e e-mails falsos. Essas informações são comparadas toda vez que uma nova página é acessada. Se o site estiver na lista negra da extensão, são disparados alertas para o usuário como pode ser observado na Figura 4.3.

Com esta extensão, é possível, também, reportar URLs suspeitas de serem maliciosas. Mais de 24,7 milhões de sites de *phishing* foram detectados e bloqueados pela comunidade Netcraft até agosto de 2016 (NETCRAFT, 2016).

Figura 4.3: Alerta do Netcraft no navegador Chrome após o carregamento da página 38zu.cn.
Fonte: Elaborado pelo autor.

McAfee Secure Safe Browsing

A extensão *anti-phishing* para navegador de Internet McAfee Secure Safe Browsing verifica se o site visitado pelo usuário possui algum tipo de atividade maliciosa como *malware*, *phishing*, entre outras. Em caso positivo, a extensão gera alertas ao internauta conforme o apresentado na Figura 4.4.

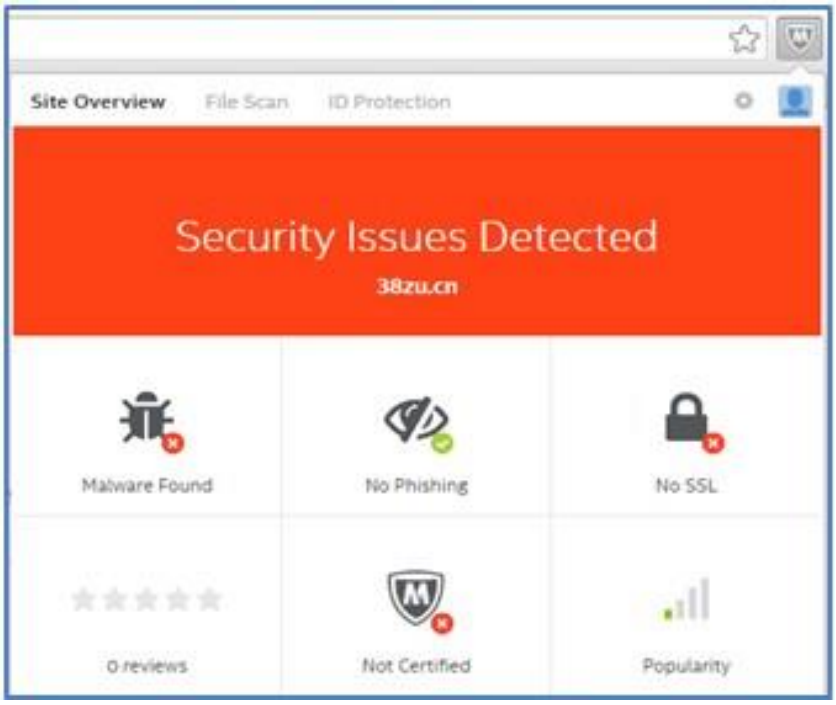


Figura 4.4: Alerta do McAfee no navegador Chrome após o carregamento da página 38zu.cn.
Fonte: Elaborado pelo autor.

Com a extensão McAfee é possível, também, escanear *links* e arquivos. Ela possui um recurso para análise de *links* suspeitos que não será testado por ser da versão completa (paga). A extensão avisa, ainda, se um formulário que o usuário vai preencher não está mantendo as informações seguras; indica se os resultados de pesquisa do Google são seguros; fornece um painel de instrumentos (*dashboard*) e classificação de segurança por meio de cores (verde, amarelo, vermelho). A extensão faz, por fim, seis tipos de análise no site: *malware*, *phishing*, SSL, *reviews*, certificado e popularidade (MCAFEE, 2016).

WOT – Web Of Trust

A extensão *anti-phishing* para navegador de Internet WOT mostra em que sites o usuário pode confiar com base nas experiências de milhões de usuários no mundo inteiro (WOT, 2016). O WOT, assim como o Netcraft, também gera alertas automaticamente quando *links* maliciosos do corpo do e-mail são acionados, conforme a Figura 4.5. Ela apresenta também, alerta de vírus e *malware*, como mostrado na Figura 4.6. A extensão WOT oferece, ainda, recurso chamado de *Scorecard* para julgar se um *link* é malicioso.

Figura 4.5: Alerta do WOT no navegador Chrome durante acionamento de *link*.
Fonte: Elaborado pelo autor.

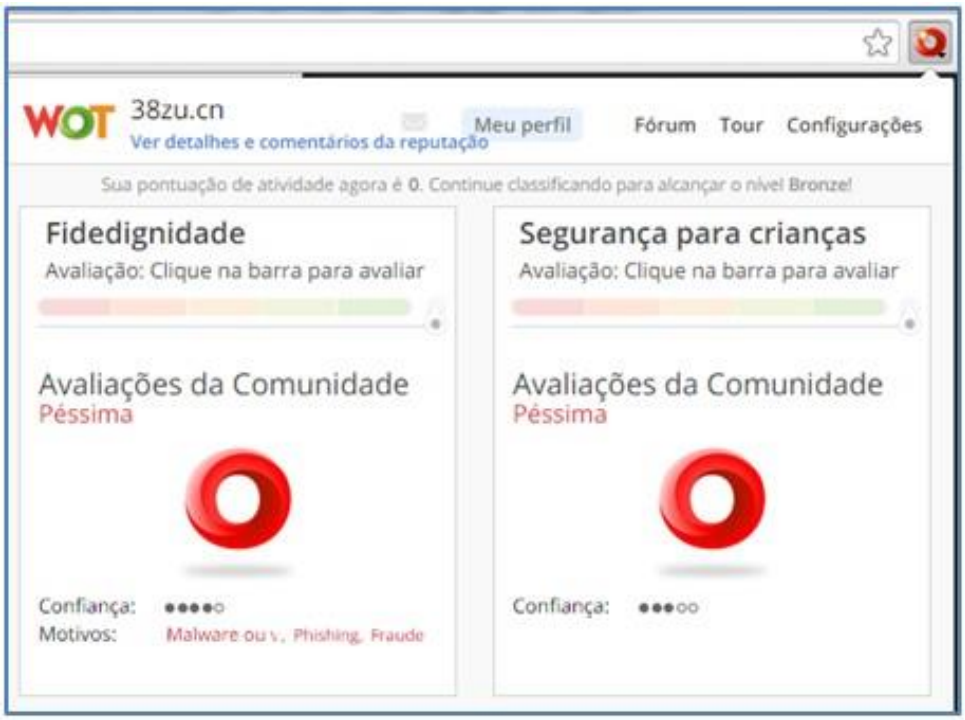


Figura 4.6: Alerta do WOT no navegador Chrome após o carregamento da página 38zu.cn.
Fonte: Elaborado pelo autor.

Urlcheck

A extensão *anti-phishing* para navegador de Internet Urlcheck é uma ferramenta de reputação *online* que ajuda o internauta a analisar sites e endereços IPs em busca de várias ameaças como ataques de *phishing*, lojas *online* falsas e distribuição de *malware*. Esta extensão testa as URLs ou os endereços IPs das ameaças citadas usando bancos de dados, listas negras e ferramentas de diferentes fornecedores, combinando-os em uma única plataforma (URLCHECK, 2016).

Para ocorrer a análise, o ícone do navegador precisa ser acionado, com isso uma nova aba é aberta e, assim, o endereço é checado no site do Urlcheck. Como exemplo, a Figura 4.7 mostra o resultado de uma análise realizada na URL 38zu.cn. A extensão também possui recurso de análise de *link*.

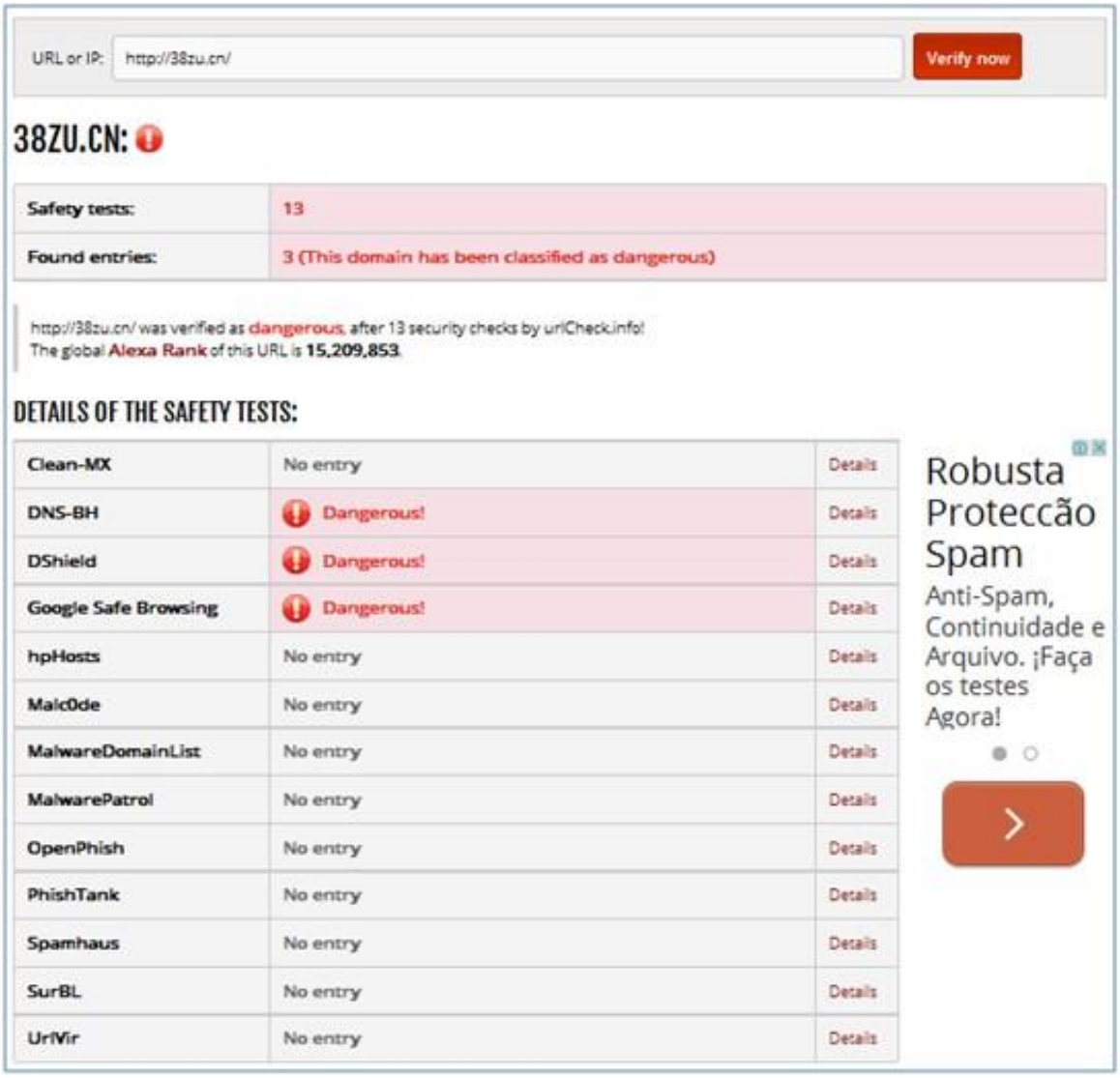


Figura 4.7: Alerta da extensão Urlcheck durante acesso ao site 38zu.cn.
Fonte: Elaborado pelo autor.

4.2 Testes de Ferramentas *Anti-Phishing*

A seção anterior apresentou ferramentas que possibilitam a detecção e o alerta de ataques de *phishing*. Esta seção trata dos testes realizados nas ferramentas citadas, para saber como elas se comportam em relação a possíveis ameaças de *phishing*.

De forma a realizar os testes nas ferramentas *anti-phishing* para posterior avaliação, primeiramente foi estabelecido o ambiente de testes, em seguida o objetivo e a metodologia para a realização dos testes, culminando com a apresentação dos resultados obtidos.

4.2.1 Ambiente de Testes

Para realizar os testes nas ferramentas *anti-phishing*, foi necessário estabelecer o seu ambiente. Este ambiente simula o computador de um usuário que é utilizado para instalação das ferramentas *anti-phishing* e o acesso aos sites e e-mails fraudulentos.

O ambiente de testes foi estabelecido através de um computador com a seguinte configuração:

i) Processador: Intel Core (TM) I3-2120 CPU @ 3.30 GHz;

ii) Memória instalada (RAM): 4,00 GB (utilizável: 2.85 GB);

iii) Sistema Operacional de 32 bits.

As ferramentas testadas com as respectivas versões são:

i) Navegador de Internet Google Chrome. Versão: 53.0.2785.116 m;

ii) Navegador de Internet Mozilla Firefox. Versão: 47.0.1;

iii) Programa antivírus Avast. Versão: 12.1.2272;

iv) Programa antivírus AVG. Versão: 16.111.7797;

v) Programa antivírus Avira. Versão: 15.0.20.59;

vi) Extensão *anti-phishing* Netcraft. Versão: 1.6.3 (Chrome), 1.10.3 (Firefox);

vii) Extensão *anti-phishing* McAfee Secure Safe Browsing. Versão: 2.11;

viii) Extensão *anti-phishing* WOT (Web Of Trust). Versão: 3.0.6 (Chrome), 20151208 (Firefox);

ix) Extensão *anti-phishing* Urlcheck. Versão: 0.1.1-signed.1-signed.

Todos os testes foram realizados com a configuração padrão dos navegadores de Internet, dos programas antivírus e das extensões *anti-phishing* no Sistema Operacional Windows 7 Professional, no período de 04/09/2016 a 26/09/2016.

4.2.2 Objetivo dos testes

O objetivo dos testes era verificar se as ferramentas testadas obtinham sucesso em identificar ataques de *phishing* em sites maliciosos e em e-mails fraudulentos.

4.2.3 Metodologia para Realização dos Testes

A metodologia utilizada para a realização dos testes se deu por meio do registro das respostas que as ferramentas *anti-phishing* exibiam durante o acesso a sites e e-mails de *phishing*.

Os sites escolhidos pertencem a uma lista de dez sites considerados maliciosos pela Google (CERTISIGN, 2015) e (NARUNA, 2015). Já os e-mails testados possuem características de phishing, como arquivos e links maliciosos e palavras que visam ludibriar o internauta como “restituição”, “promoção”, “prêmio”, entre outras. Os testes ocorreram em duas etapas, a primeira para sites, a segunda para emails.

Na primeira etapa, iniciava-se o teste digitando, um por vez, o endereço completo dos seguintes sites no navegador: 38zu.cn, lousecn.cn, fqwerz.cn, ww2.goooogleadsence.biz, gumblar.cn, d99q.cn, orgsite.info e martuz.cn. Logo em seguida, dava-se início a pesquisa pelo endereço informado. Caso a ferramenta testada gerasse algum tipo de alerta de ameaça ao internauta, ou até mesmo bloqueando seu acesso ao site fraudulento, registrava-se como resultado positivo, caso contrário, registrava-se como resultado negativo. A Figura 4.8 mostra o fluxo do teste realizado nesta etapa.

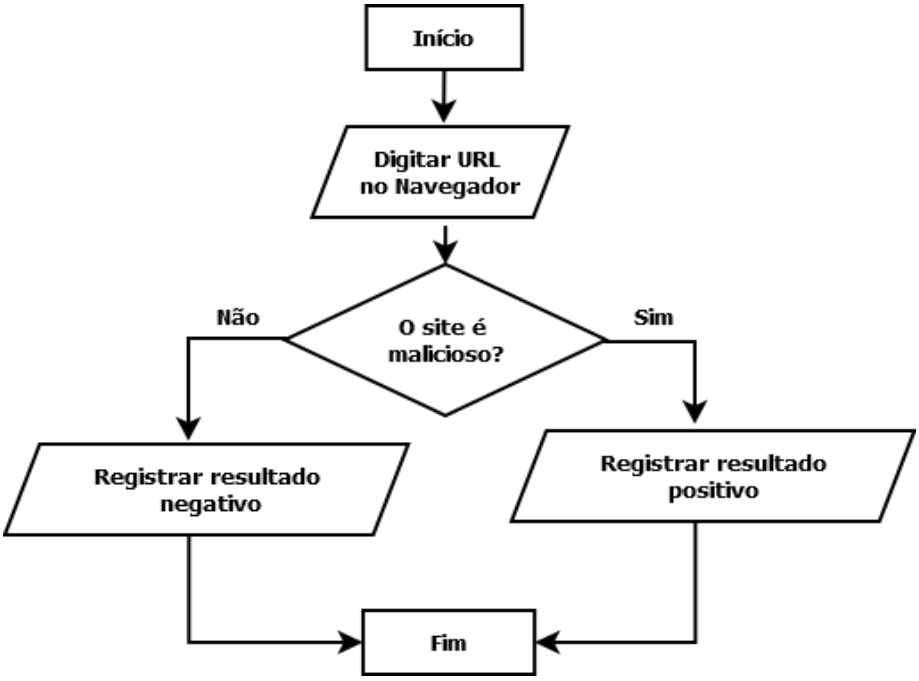


Figura 4.8: Fluxo do teste nas ferramentas *anti-phishing* da etapa 1.
Fonte: Elaborado pelo autor.

A segunda etapa se deu por meio da abertura de e-mails de *phishing* (em anexo) na caixa de entrada de um serviço de webmail. Estes e-mails foram renomeados para E1, E2, ..., En, onde n indica a ordem do e-mail em anexo. Nesta etapa, foi verificado se, ao abrir o e-mail, era gerado algum tipo de alerta de ameaça. Em caso positivo, registrava-se resultado positivo, caso contrário, registrava-se resultado negativo.

Com o e-mail aberto, foi verificada, ainda, a presença de *links* ou arquivos. Se pelo menos um existisse, era realizada uma nova checagem. Caso a ferramenta testada indicasse o *link* ou o arquivo como sendo malicioso, registrava-se resultado positivo, caso contrário, registrava-se negativo. Abaixo é exibido primeiramente o quadro resumo da etapa 2, em seguida o fluxo do teste realizado na etapa em questão, exibido na Figura 4.9.

Quandro 4.1: Resumo dos testes realizados da etapa 2.

Abrir e-mail
Verificar alerta de ameaça
Se houve alerta, registrar positivo
Se não houve alerta, registrar negativo
Verificar presença de *links* e/ou arquivos no e-mail aberto
Testar *links* e/ou arquivos no e-mail aberto
Se houve alerta, registrar positivo
Se não houve alerta, registrar negativo

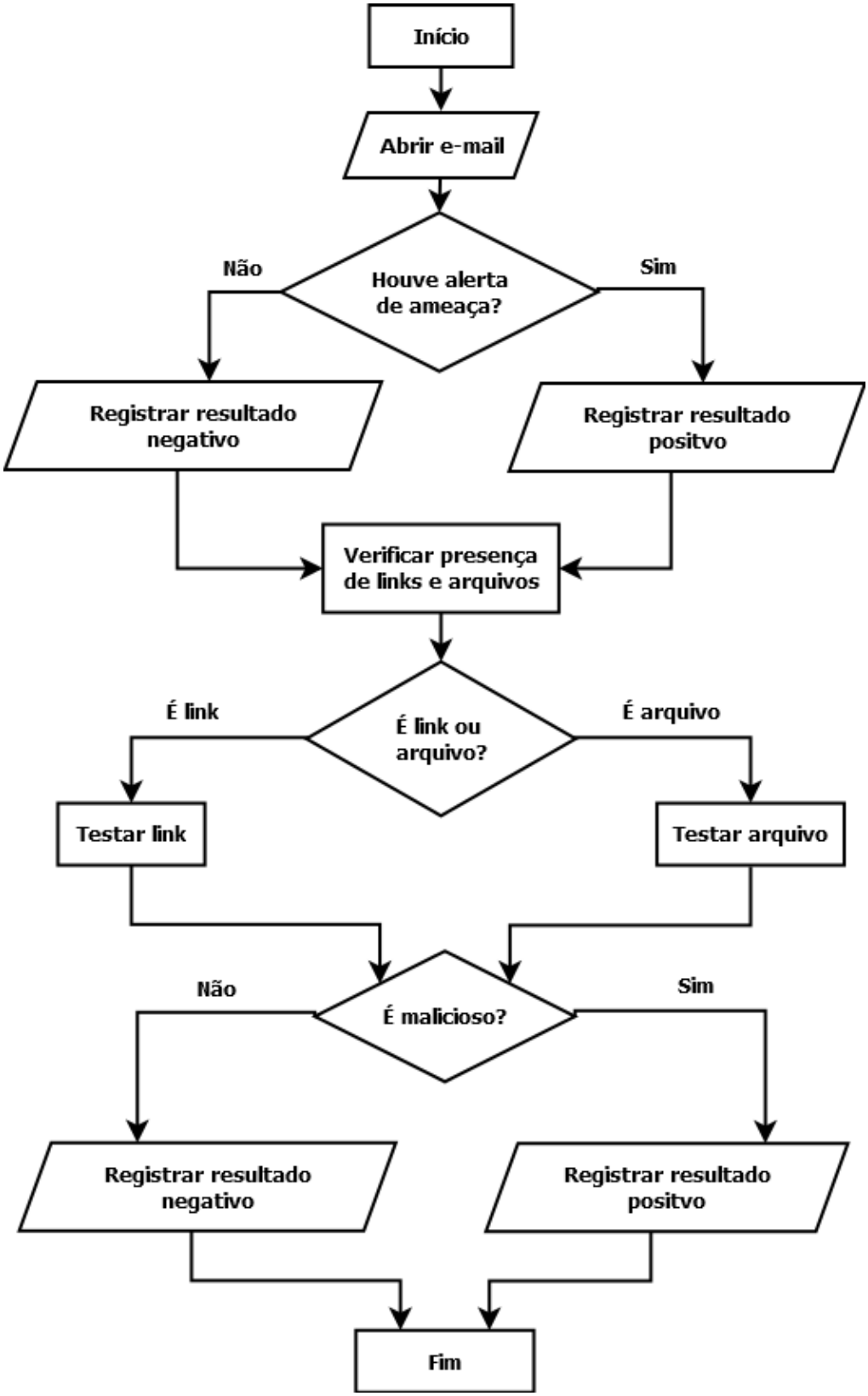


Figura 4.9: Fluxo do teste nas ferramentas *anti-phishing* da etapa 2.
Fonte: Elaborado pelo autor.

A segunda etapa objetivou verificar se a ferramenta alertava sobre o acesso ou bloqueava a abertura de e-mails com características de *phishing* e/ou impedia a abertura de *links* suspeitos de serem maliciosos.

O teste no navegador se deu com o programa antivírus inativo e todas as extensões *anti-phishing* desabilitadas. Os programas antivírus, por sua vez, foram testados com a proteção *anti-phishing* dos navegadores desabilitadas, assim como as extensões *anti-phishing*. Por fim, as extensões *anti-phishing* foram testadas uma por vez, sempre desabilitando as demais. Os navegadores Web tinham seus recursos *anti-phishing* desativados, e os programas antivírus também eram desabilitados.

Como cada ferramenta possuía métodos próprios para identificação de ameaça (cor, pontuação), foi levada em consideração apenas a mudança de estado da ferramenta, ou seja, se a cor padrão para sites bem avaliados é verde, tem-se resultado negativo para *phishing*. Cores como alaranjado ou vermelho foram consideradas como sucesso na identificação de sites maliciosos, implicando em resultado positivo para *phishing*.

A mesma lógica, então, foi utilizada no caso de ferramentas que utilizavam critérios de pontuação. Zero (0) para sites bem avaliados, implicava resultado negativo para *phishing*. Qualquer outro valor para sites suspeitos de serem fraudulentos, indicava resultado positivo para *phishing*.

Para a apresentação do resultado dos testes foram utilizadas tabelas. Para a construção das tabelas com o resultado de acesso aos sites maliciosos foi utilizado sinal positivo (+) para sucesso em detectar tentativa de *phishing* e sinal negativo (–) para falha na identificação. Na tabela com o resultado de abertura de e-mails, também foram utilizados os sinais positivo e negativo. O sinal positivo indica que a ferramenta ou bloqueou a abertura do e-mail, ou gerou algum tipo de alerta depois da abertura do e-mail, ou impediu o acionamento dos *links* suspeitos, ou identificou risco nos *links* suspeitos. Sinal negativo indica completa falta de ação da ferramenta na identificação de ameaça de *phishing*.

4.2.4 Resultado dos Testes

Baseado no objetivo e na metodologia apresentada para a realização dos testes nas ferramentas *anti-phishing*, segue abaixo o resultado dos testes de acesso a sites fraudulentos e abertura de e-mails de *phishing*.

Etapa 1: Acesso a sites maliciosos.

Teste de navegador Web e as respectivas extensões *anti-phishing*.

Navegador: Google Chrome.

Extensões: Netcraft, McAfee e WOT.

Utilizando o navegador de Internet Chrome para acessar os sites maliciosos, quase todos foram bloqueados, apenas orgsite.info deu resultado negativo; a extensão *anti-phishing* Netcraft não acusou resultado positivo apenas para dois sites: gumblar.cn e orgsite.info; a extensão *anti-phishing* McAfee não gerou nenhum tipo de alerta para os sites lousecn.cn, gumblar.cn e orgsite.info; já a extensão *anti-phishing* WOT mostrou alerta para todos os sites. A Tabela 4.1 ilustra os resultados obtidos para este teste.

Tabela 4.1: Capacidade de identificação de *phishing* do navegador Chrome e suas extensões *anti-phishing*.

Site	Chrome	Netcraft	McAfee	WOT
38zu.cn	+	+	+	+
lousecn.cn	+	+	-	+
fqwerz.cn	+	+	+	+
ww2.goooogleadsence.biz	+	+	+	+
gumblar.cn	+	-	-	+
d99q.cn	+	+	+	+
orgsite.info	-	-	-	+
martuz.cn	+	+	+	+

Fonte: Elaborado pelo autor.

Etapa 1: Acesso a sites maliciosos.

Teste de navegador Web e as respectivas extensões *anti-phishing*.

Navegador: Mozilla Firefox.

Extensões: Netcraft, Urlcheck e WOT.

O navegador Firefox obteve resultado idêntico ao navegador Chrome assim como as extensões *anti-phishing* Netcraft e WOT. A extensão Urlcheck obteve o pior resultado dentre todas as extensões, gerando alerta positivo para apenas três sites: 38zu.cn, ww2.googleadsence.biz e gumblar.cn. A Tabela 4.2 ilustra os resultados obtidos para este teste.

Tabela 4.2: Capacidade de identificação de *phishing* do navegador Firefox e suas extensões *anti-phishing*.

Site	Firefox	Netcraft	Urlcheck	WOT
38zu.cn	+	+	+	+
lousecn.cn	+	+	-	+
fqwerz.cn	+	+	-	+
ww2.goooogleadsence.biz	+	+	+	+
gumblar.cn	+	-	+	+
d99q.cn	+	+	-	+
orgsite.info	-	-	-	+
martuz.cn	+	+	-	+

Fonte: Elaborado pelo autor.

Etapa 1: Acesso a sites maliciosos.

Teste de programas antivírus.

Ferramentas: Avast, AVG e Avira.

O programa antivírus Avast e sua extensão para navegador de Internet, instalada nos navegadores Chrome e Firefox, só não identificaram perigo no site orgsite.info. Os programas antivírus AVG e Avira não identificaram atividade maliciosa em nenhum dos sites testados como mostrado na Tabela 4.3.

Tabela 4.3: Capacidade de identificação de *phishing* dos programas antivírus Avast, AVG e Avira.

Site	Avast	AVG	Avira
38zu.cn	+	-	-
lousecn.cn	+	-	-
fqwerz.cn	+	-	-
ww2.goooogleadsence.biz	+	-	-
gumblar.cn	+	-	-
d99q.cn	+	-	-
orgsite.info	-	-	-
martuz.cn	+	-	-

Fonte: Elaborado pelo autor.

Etapa 2: Abertura de e-mails de *phishing*.

Navegadores: Google Chrome e Mozilla Firefox.
Programas antivírus: Avast, AVG e Avira.
Extensões *anti-phishing*: Netcraft, McAfee, Urlcheck, WOT.

Nesta etapa, nenhum tipo de alerta de ameaça foi gerado pelos dois navegadores Web, nem pelos programas antivírus durante a abertura dos e-mails testados. Tampouco houve alerta durante a ativação dos *links* ou abertura dos arquivos maliciosos.

As extensões *anti-phishing* para navegadores de Internet não bloquearam o acesso a nenhum e-mail suspeito de golpe, nem exibiram alertas ao usuário. Algum tipo de ação só foi percebido durante o acionamento dos *links* ou durante a análise com recursos extras das extensões (disponíveis com o botão direito do mouse acionado sobre o *link*).

Com a extensão WOT, por exemplo, antes do acionamento do *link* do e-mail E2, foi possível analisá-lo com o recurso extra, essa análise mostrou que a URL presente no *hiperlink* constava na lista negra do site PhishTank em 18/08/2016. Ao clicar no *link*, houve bloqueio de acesso ao site. Já a análise com o recurso extra no e-mail E3 indicou risco (página

fraudulenta), mas a extensão WOT não bloqueou o acesso, indicou apenas como avaliação insatisfatória.

A extensão Urlcheck foi a que mais identificou ameaças nos e-mails testados. As extensões NetCraft e WOT identificaram apenas duas ameaças cada. Entretanto, vale ressaltar que apenas essas duas ferramentas apresentaram algum tipo de recurso que impedia o acesso a um site considerado malicioso via e-mail. A extensão McAfee detectou apenas uma ameaça. Os programas antivírus e os navegadores não bloquearam nem geraram alertas durante a abertura dos e-mails, tão pouco para o acionamento dos respectivos *links*. A Tabela 4.4 exibe o resultado completo dos testes durante a abertura dos e-mails de *phishing*.

Tabela 4.4: Capacidade de identificação de ameaça de *phishing* em e-mails das ferramentas testadas.

E-mail	Netcraft	McAfee	Urlcheck	WOT	Avast	AVG	Avira	Chrome	Firefox
E1	-	-	-	-	-	-	-	-	-
E2	+	+	+	+	-	-	-	-	-
E3	+	-	+	-	-	-	-	-	-
E4	-	-	-	-	-	-	-	-	-
E5	-	-	-	-	-	-	-	-	-
E6	-	-	-	+	-	-	-	-	-
E7	-	-	+	-	-	-	-	-	-
E8	-	-	-	-	-	-	-	-	-

Fonte: Elaborado pelo autor.

4.3 Conclusão

Neste capítulo foram apresentadas as principais ferramentas que auxiliam o internauta no combate contra ataques de *phishing*. Testes para avaliar se estas ferramentas impediam o acesso a sites fraudulentos ou alertavam o usuário da Internet a não acessá-los foram realizados. As ferramentas também foram testadas por meio da abertura de e-mails de phishing.

Foi possível constatar que as ferramentas em questão fazem comparações do endereço que se quer acessar com os registros de listas negras próprias ou de terceiros, alimentadas por grandes comunidades de usuários da Internet.

Sobre o resultado dos testes foi observado que nenhuma das ferramentas *anti-phishing* testadas foi capaz de evitar completamente o acesso tanto a sites fraudulentos quanto a e-mails de *phishing*. No entanto, as extensões *anti-phishing* se destacaram das demais ferramentas no que concerne a e-mails de *phishing*. Nesse sentido, as ferramentas realmente auxiliam o internauta no processo de contenção contra o *phishing*. Portanto a utilização dessas ferramentas deve ser feita com cautela pelos usuários da Internet.

Capítulo 5

Considerações Finais e Trabalhos Futuros

Com o aumento do número de usuários acessando a Internet, aumentou também o número de vítimas de ataques cibernéticos. Estes ataques, algumas vezes de *phishing*, causam grandes prejuízos financeiros para muitos internautas, por meio da exploração de algumas vulnerabilidades humanas.

Neste trabalho foi mostrado que as vulnerabilidades humanas são exploradas, no contexto da Internet, por golpistas que utilizam técnicas de Engenharia Social combinadas com programas maliciosos objetivando maiores taxas de sucesso. Esta combinação pode ser usada tanto de forma ativa quanto de forma passiva pelo atacante.

O material de referência pesquisado sugere que para diminuir as chances de se tornar uma vítima de *phishing* é necessário que a pessoa, usuária ou não da Internet, dentre outros cuidados, desconfie de pessoas que nunca viu, mas que solicitam informações pessoais ou do local de trabalho; que diminua a quantidade de informações sensíveis disponibilizadas em redes sociais; que seja muito cautelosa ao abrir e-mails de remetentes desconhecidos ou ao clicar em *links*; e, principalmente, caso seja extremamente necessário enviar ou receber informações sensíveis por algum serviço de Internet, que cheque, por meio de outras vias, o receptor ou emissor dessas informações.

Foi mostrado, também, que a conscientização dos internautas, experientes ou não com as armadilhas da Internet, faz-se necessário bem como o uso de ferramentas que possam ajudar a minimizar os danos causados pelos golpistas, já que estes estão sempre se aprimorando. Golpistas mais experientes, por exemplo, elaboram melhor os seus ataques, os organizam em fases e podem, ainda, fazer uso de ferramentas de otimização para atingir um número maior de alvos.

O processo de contenção de ataques de *phishing* não é uma tarefa fácil. O usuário de Internet precisa tomar cuidado com os sites que vai acessar, resultantes ou não das pesquisas que realiza em motores de busca, com os e-mails que abre e, principalmente, com o

reconhecimento de URLs de sites fraudulentos. Para a realização dessas tarefas, ter boas ferramentas *anti-phishing* é essencial.

Como foi recomendada a utilização de ferramentas *anti-phishing* ao internauta, uma avaliação em três grupos destas ferramentas precisou ser realizada. As ferramentas avaliadas foram: navegadores Web, programas antivírus com extensões *anti-phishing* e extensões *anti-phishing* para navegadores Web. Essas ferramentas foram avaliadas por meio de acesso a sites fraudulentos e abertura de e-mails de *phishing*. Os resultados permitiram concluir que as ferramentas *anti-phishing* testadas, mesmo não sendo totalmente eficazes, ajudam o internauta a se precaver contra alguns ataques de *phishing* na Internet.

Como proposta para trabalhos futuros, por fim, testes mais abrangentes envolvendo extensões *anti-phishing* para navegadores Web. Estes testes podem relacionar o tamanho da comunidade de usuários da extensão que alimentam suas respectivas bases de dados com a eficácia em alertar novos tipos de ataques. Testes que meçam a capacidade dos serviços de webmail em identificar ataques de *phishing*, também ficam como sugestão.

Referências

ALENCAR, G. D.; LIMA, M. F.; FIRMO, A. C. O efeito da conscientização de usuários no meio corporativo no combate à engenharia social e *phishing*. IX Simpósio Brasileiro de Sistemas de Informação (SBSI'13), pp. 254-259, 2013.

APWG. *ANTI-PHISHING* WORK GROUP. *Phishing* Activity Trends Report, 1st, 2nd quarter, 2016.

AVAST. *Anti*vírus. Disponível em: https://www.avast.com/. Acesso em: 26/03/2016.

AVG. *Anti*vírus. Disponível em: http://www.avg.com/. Acesso em: 15/09/2016.

AVIRA. *Anti*vírus. Disponível em: http://www.avira.com.br/melhor-*anti*virus/. Acesso em: 15/09/2016.

BRADESCO. Banco Bradesco – E-mails falsos. Disponível em: https://www.bradescoseguranca.com.br/html/seguranca_corporativa/pf/emails-e-telas-falsas/emais-fasos.shtm. Acesso em: 07/11/2016.

CANOVA, G. et al. NoPhish: an *anti-phishing* education app. 2014. In: International Workshop on Security and Trust management. Springer International Publishing. p. 188-192.

CARMONA, Lisandro. Avast. Blog. Cuidado com e-mails (*phishing*) bancários neste final de ano. 2013. Disponível em: https://blog.avast.com/pt-br/2013/12/23/cuidado-com-emails-*phishing*-bancarios-neste-final-de-ano/. Acesso em: 15/05/2016.

CERT. CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Estatísticas dos Incidentes Reportados ao CERT.br. 2015. Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 15/05/2016.

CERT. CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Cartilha de segurança para a Internet, versão 4.0/cert.br. São Paulo: Comitê gestor de Internet no Brasil. 2012.

CERON, Joao et al. O processo de tratamento de incidentes de segurança da UFRGS. In: Workshop de Tecnologia da Informação das IFES (3.: 2009: Belém).[Anais..]. Belém: UFPA, 2009. 2009.

CERTISIGN. Os 10 sites mais perigosos da Internet. 2015. Disponível em: http://www.certisignexplica.com.br/os-10-sites-mais-perigosos-da-internet/. Acesso em: 04/09/2016.

CETIC. CENTRO DE ESTUDOS SOBRE AS TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO. Ticdomicícilos: publicações. 2015. Disponível em: http://cetic.br/pesquisa/domicilios/indicadores. Acesso em: 15/05/2016.

DA SILVA, M. A. R.; XAVIER, F. C. Deep web e a rede TOR: qual a sua relação? Revista Científica Phronesis, (2). 2015.

DAKWALA, Anuj; LAVINGIA, Kruti; SHAH, Rushabh. A novel approach to improve the efficiency of fake websites detection techniques: Survey. 2016.

EL PESCADOR. *Phishing* & Engenharia Social: Entenda porque essas técnicas estão interligadas. 2015. Disponível em: https://www.elpescador.com.br/blog/index.php/*phishing*-engenharia-social-entenda-porque-essas-tecnicas-estao-interligadas/. Acesso em: 04/03/2017.

FRAGA, Bruno. Técnicas de Invasão. 2016. Autor: Bruno Fraga. Disponível em: https://www.youtube.com/watch?v=ZgwlxgXg0zo.
Acesso em: 30/03/2017.

GARRET, Felipe. AVG: baixe e proteja seu PC contra todas as ameaças. 2016. Disponível em: http://www.techtudo.com.br/tudo-sobre/avg.html. Acesso em 23/03/2017.

GOOGLE. Gerenciar alertas de *phishing* e malware. Disponível em: https://support.google.com/chrome/answer/99020?hl=pt-BR&ref_topic=3421433. Acesso em: 15/09/2016.

GRASEL, Grasiel Felipe. Qual o melhor navegador? Edge, Chrome, Opera ou Firefox. Disponível em: https://www.ofinadanet.com.br/post/12336-qual-o-melhor-navegador-ie-chrome-opera-safari-ou-firefox. Acesso em 04/02/2017.

GUPTA, Rejendra; SHUKLA, Piyush Kumar. Experimental analysis of browser based novel *anti-phishing* system tool at educational level. I. J. Information Technology and Computer Science, 2016, 2, 78-84.

HADNAGY, Christopher. Social Engineering: The Art of Human Hacking. Wiley Publishing. 2011.

HARRISON, Brynne; SVETIEVA, Elena; VISHWANATH, Arun. Individual processing of *phishing* emails: How attention and elaboration can protect against individual *phishing* victimization. Online Information Review, 2016, 40(2): 265-281.

KEYWORTH, Marie; WALL, Matthew. The ‘bogus boss’ email scam costing firms millions. BBC. Disponível em: http://www.bbc.com/news/business-35250678. Acesso em 01/11/2016.

LAS-CASAS, Pedro Henrique et al. Uma metodologia para identificação adaptativa e caracterização de *phishing*. XXXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. 2016.

LASZKA, Aron; VOROBEYCHIK, Yevgeniy; KOUTSOUKOS, Xenofon D. Optimal Personalized Filtering Against Spear-*Phishing* Attacks. In: AAAI. 2015, p. 958-964.

MARFORIO, Claudio et al. Personalized security indicators to detect application *phishing* attacks in mobile platforms. 2015.

MCAFEE. McAfee Secure Safe Browsing. Disponível em: https://www.mcafeesecure.com/safe-browsing/. Acesso em: 15/09/2016.

MELLO, Laerte Peotta de et al. Análise de malware: Investigação de Códigos Maliciosos Através de uma Abordagem Prática. XI Simpósio Brasileiro em Segurança da Informação e Sistemas Computacionais. Brasília, DF. 2011.

MILHOR, Carlos Eduardo. Sistema de desenvolvimento para controle eletrônico dos motores de combustão interna ciclo Otto. 2002. Tese de Doutorado. Universidade de São Paulo.

MILITELLI, Leonardo. Como lidar com as falhas dos programas *anti-phishing*. Disponível em: http://www.itforum365.com.br/seguranca/ameacas/como-lidar-com-as-falhas-dos-programas-*anti-phishing*. Acesso em: 04/02/2017.

MOREIRA, Robson Antonio. Principais formas de ataque e prevenção à informação no ambiente da Internet. 2016. Revista FATEC Sebrae em debate: gestão, tecnologias e negócios. Vol. 3, Nº 5, ISSN: 2358-9817.

MOZILLA. Como funciona a proteção contra *phishing* e software malicioso. Disponível em: https://support.mozilla.org/pt-BR/kb/como-funciona-protecao-*phishing*-e-software-malicioso. Acesso em: 08/10/2016.

NARUNA, Romana. Os 10 sites mais perigosos da Internet. 2015. Disponível em: http://www.e-konomista.com.br/d/sites-mais-perigosos/. Acesso em 04/09/2016.

NETCRAFT. Internet Security and Data Mining. Disponível em: https://www.netcraft.com/. Acesso em 15/09/2016.

OLIVO, Cleber Kiel. Avaliação de características para detecção de *phishing* de email. 2010. Dissertação (Mestrado em Informática) – Pontifícia Universidade Católica do Paraná, Curitiba.

OWASP. About the open web application security project – Cross-Site Request Forgery (CSRF). Disponível em: https://www.owasp.org/index.php/Cross-Site_Request_Forgery. Acesso em: 08/10/2016.

PEREIRA, Cleber Guedes. *Phishing*: conceitos e ações preventivas aplicadas à empresa. 2012. Dissertação (Pós-Graduação) – Centro Universitário de Brasília.

PHISHLABS. How to fight back against *phishing*: a guide to mitigating and deterring attacks targeting your customers. 2013.

PHISHLABS. *Phishing* Trends & Intelligence Report – Hacking the Human. 2016.

PINHEIRO, Cleiton. *Phishing* através de técnicas Black-Hat. 2017. Disponível em: http://0x27null.blogspot.com.br/2017/01/*phishing*-atraves-de-tecnicas-bl4ck-h4t.html?m=1. Acesso em: 04/02/2017.

REINALDO FILHO, Demócrito. A responsabilidade dos bancos pelos prejuízos resultantes do *phishing*. Juiz de Direito (32ª Vara Cível do Recife), 2006.

ROSS, J. Anderson. Security Engineering: A guide to building dependable distributed systems. Second Edition. Indianapolis, US. Ed Wiley. 2008.

SMITH. Hackers Segredos de Confissões. Disponível em: http://followscience.com/content/206153/ebook-hackers-secrets-and-confessions/. Acesso em: 22/11/2016.

SYMANTEC. Internet Security Threat Report, Volume 21. 2016.

URLCHECK. What is urlcheck.info? Disponível em: http://urlcheck.info/en/. Acesso em: 15/09/2016.

US-CERT. UNITED STATES COMPUTER EMERGENCY READINESS TEAM. Avoiding Social Engineering and *Phishing* Attacks. 2009. Disponível em: https://www.us-cert.gov/ncas/tips/ST04-014. Acesso em: 29/10/2016.

VALECHA, Rohit et al. An exploration of *phishing* information sharing: A heuristic-systematic approach, WISP 2015 Proceedings. Paper 2. 2015.

WIKIPEDIA. Cross-Site Request Forgery. Disponível em: https://en.wikipedia.org/wiki/Cross-site_request_forgery. Acesso em 08/10/2016.

WOLFF, Marcus. Detection Framework for *Phishing* Websites. 2009. Thesis (Master of Science) – Florida State University.

WOT. Web Of Trust. Disponível em: https://www.mywot.com/. Acesso em 15/09/2016.

Anexos

Os e-mails enumerados abaixo contêm algumas características de ataque de *phishing* e, por isso, foram utilizados para a realização de testes que verificavam se ao serem abertos ou terem seus *links* acionados, tanto os programas antivírus, quanto as extensões para navegadores Web identificavam estes e-mails como tentativa de ataque de *phishing*.

E1: E-mail do DETRAN com características de *phishing*. Contém *link* malicioso.

De: bobtrama <bobtrama@hotmail.com>
Enviado: quarta-feira, 31 de agosto de 2016 03:12
Para: antonilsonjack@hotmail.com
Assunto: Comunicado Detran Sobre CNH

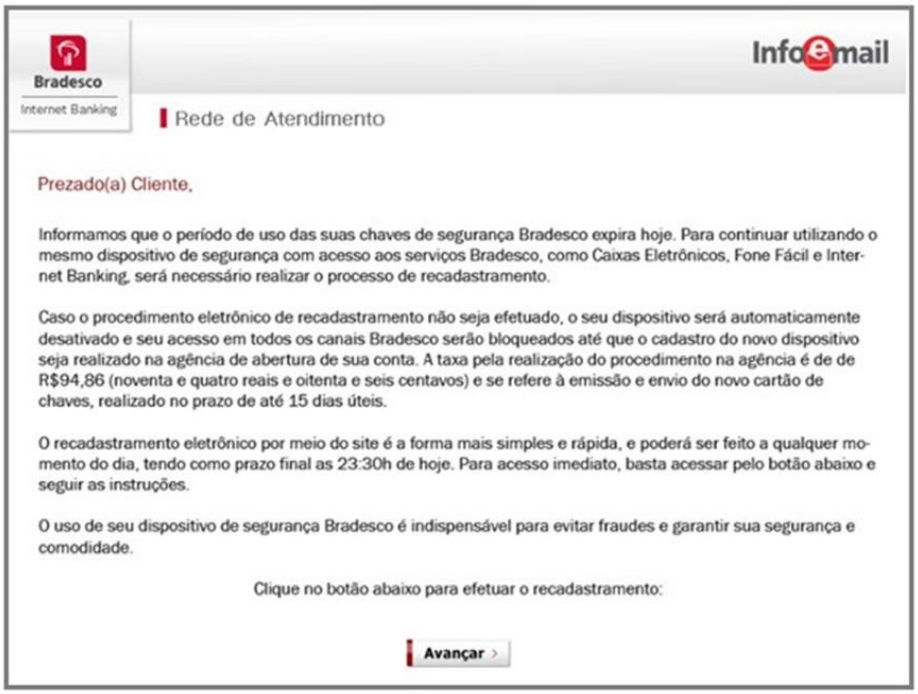
Sua **CNH** Foi Suspensa.

CNH foi suspensa por ter acumulado 87 pontos em um período menor que um ano.

Dúvidas sobre suspensão da Carteira de Habilitação

Entre em contato tire suas dúvidas e evite "dor de cabeça"
visualizar documento detalhado.pdf (2 KB)

E2: E-mail de *phishing* do Banco Bradesco solicitando clique para recadastramento. Contém botão malicioso.



Bradesco
Internet Banking

Infoemail

Rede de Atendimento

Prezado(a) Cliente,

Informamos que o período de uso das suas chaves de segurança Bradesco expira hoje. Para continuar utilizando o mesmo dispositivo de segurança com acesso aos serviços Bradesco, como Caixas Eletrônicos, Fone Fácil e Internet Banking, será necessário realizar o processo de recadastramento.

Caso o procedimento eletrônico de recadastramento não seja efetuado, o seu dispositivo será automaticamente desativado e seu acesso em todos os canais Bradesco serão bloqueados até que o cadastro do novo dispositivo seja realizado na agência de abertura de sua conta. A taxa pela realização do procedimento na agência é de de R$94,86 (noventa e quatro reais e oitenta e seis centavos) e se refere à emissão e envio do novo cartão de chaves, realizado no prazo de até 15 dias úteis.

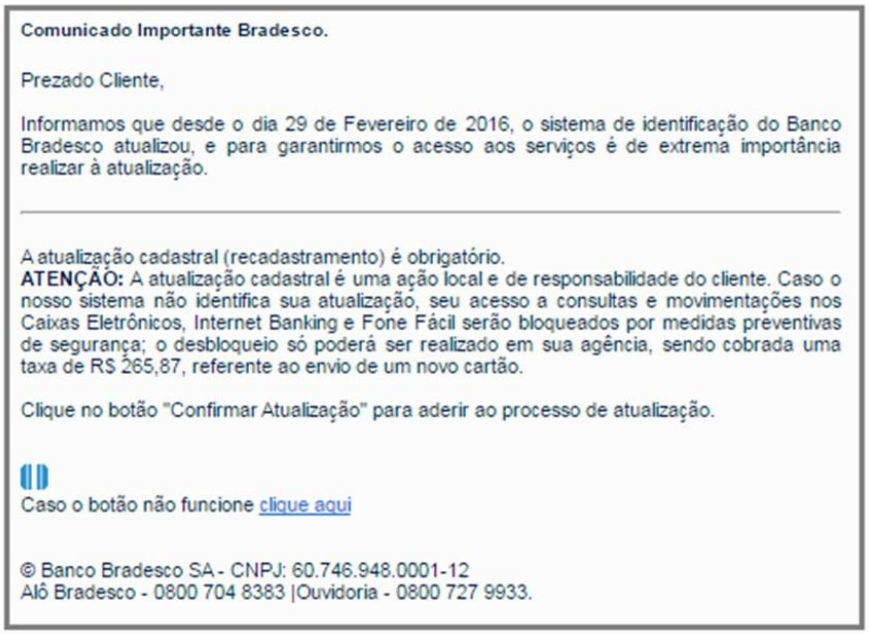
O recadastramento eletrônico por meio do site é a forma mais simples e rápida, e poderá ser feito a qualquer momento do dia, tendo como prazo final as 23:30h de hoje. Para acesso imediato, basta acessar pelo botão abaixo e seguir as instruções.

O uso de seu dispositivo de segurança Bradesco é indispensável para evitar fraudes e garantir sua segurança e comodidade.

Clique no botão abaixo para efetuar o recadastramento:

Avançar >

E3: E-mail de *phishing* do Banco Bradesco informado sobre suposta atualização. Contém botão e *link* maliciosos.



Comunicado Importante Bradesco.

Prezado Cliente,

Informamos que desde o dia 29 de Fevereiro de 2016, o sistema de identificação do Banco Bradesco atualizou, e para garantirmos o acesso aos serviços é de extrema importância realizar à atualização.

A atualização cadastral (recadastramento) é obrigatório.
ATENÇÃO: A atualização cadastral é uma ação local e de responsabilidade do cliente. Caso o nosso sistema não identifica sua atualização, seu acesso a consultas e movimentações nos Caixas Eletrônicos, Internet Banking e Fone Fácil serão bloqueados por medidas preventivas de segurança; o desbloqueio só poderá ser realizado em sua agência, sendo cobrada uma taxa de R$ 265,87, referente ao envio de um novo cartão.

Clique no botão "Confirmar Atualização" para aderir ao processo de atualização.

Caso o botão não funcione clique aqui

© Banco Bradesco SA - CNPJ: 60.746.948.0001-12
Alô Bradesco - 0800 704 8383 |Ouvidoria - 0800 727 9933.

E4: E-mail de *phishing* do Banco do Brasil solicitando atualização. Contém botão e *links* maliciosos.

Enc: Ainda não detectamos sua atualização (2)

De: Banco do Brasil S/A <module@sebemge.com.br>
Enviado: quinta-feira, 2 de junho de 2016 16:15
Para: rsamarone@hotmail.com
Assunto: Ainda não detectamos sua atualização

Banco do Brasil

Prezado Cliente,

Nosso sistema ainda não possui registros da atualização obrigatória em sua conta.
É necessário realizar essa atualização para garantir sua segurança e continuar usando nossos serviços.
Para iniciar, siga os passos a seguir.

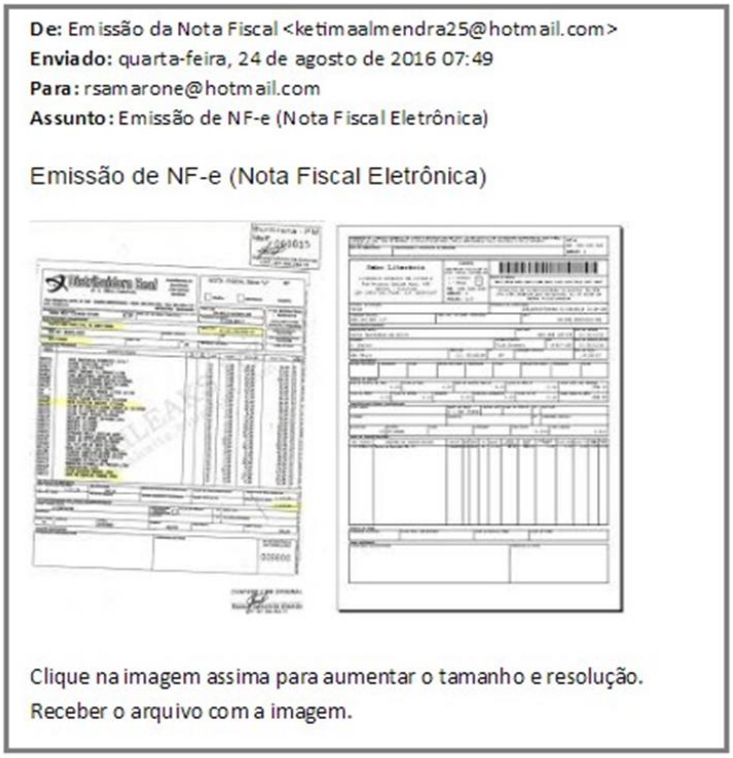
Iniciar Atualização

Qualquer dúvida estamos a disposição.

Atenciosamente,
Luiz Henrique de Freitas, Diretor de Tecnologia
Banco do Brasil

Copyright. All rights reserved.
Você pode cancelar a assinatura.

E5: E-mail de *phishing* contendo *links* maliciosos camuflados em imagens solicitando clique para aumento de resolução.

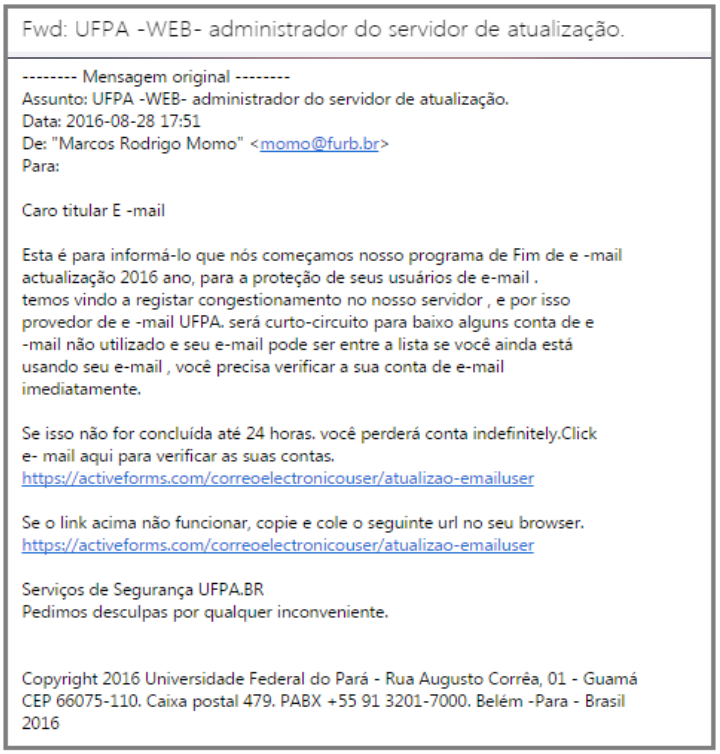


De: Emissão da Nota Fiscal <ketimaalmendra25@hotmail.com>
Enviado: quarta-feira, 24 de agosto de 2016 07:49
Para: rsamarone@hotmail.com
Assunto: Emissão de NF-e (Nota Fiscal Eletrônica)

Emissão de NF-e (Nota Fiscal Eletrônica)

Clique na imagem assima para aumentar o tamanho e resolução.
Receber o arquivo com a imagem.

E6: E-mail de *phishing* com tom de ameaça contendo muitos erros gramaticais e *links* maliciosos.



Fwd: UFPA -WEB- administrador do servidor de atualização.

-------- Mensagem original --------
Assunto: UFPA -WEB- administrador do servidor de atualização.
Data: 2016-08-28 17:51
De: "Marcos Rodrigo Momo" <momo@furb.br>
Para:

Caro titular E -mail

Esta é para informá-lo que nós começamos nosso programa de Fim de e -mail actualização 2016 ano, para a proteção de seus usuários de e-mail . temos vindo a registar congestionamento no nosso servidor , e por isso provedor de e -mail UFPA. será curto-circuito para baixo alguns conta de e -mail não utilizado e seu e-mail pode ser entre a lista se você ainda está usando seu e-mail , você precisa verificar a sua conta de e-mail imediatamente.

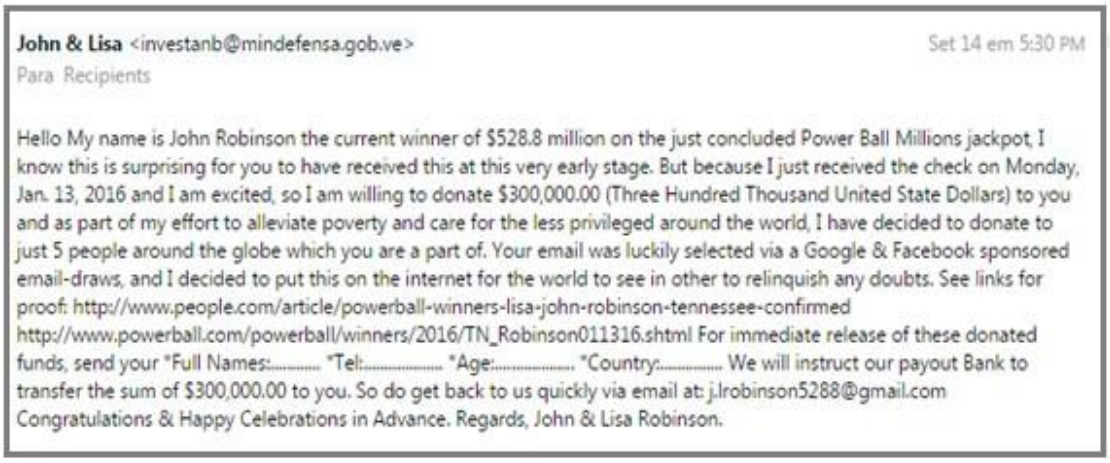
Se isso não for concluída até 24 horas. você perderá conta indefinitely.Click e- mail aqui para verificar as suas contas.
https://activeforms.com/correoelectronicouser/atualizao-emailuser

Se o link acima não funcionar, copie e cole o seguinte url no seu browser.
https://activeforms.com/correoelectronicouser/atualizao-emailuser

Serviços de Segurança UFPA.BR
Pedimos desculpas por qualquer inconveniente.

Copyright 2016 Universidade Federal do Pará - Rua Augusto Corrêa, 01 - Guamá CEP 66075-110. Caixa postal 479. PABX +55 91 3201-7000. Belém -Para - Brasil 2016

E7: E-mail de *phishing* que não contém *links*, apenas URLs que redirecionam o alvo para sites maliciosos.



John & Lisa <investanb@mindefensa.gob.ve> Set 14 em 5:30 PM
Para Recipients

Hello My name is John Robinson the current winner of $528.8 million on the just concluded Power Ball Millions jackpot, I know this is surprising for you to have received this at this very early stage. But because I just received the check on Monday, Jan. 13, 2016 and I am excited, so I am willing to donate $300,000.00 (Three Hundred Thousand United State Dollars) to you and as part of my effort to alleviate poverty and care for the less privileged around the world, I have decided to donate to just 5 people around the globe which you are a part of. Your email was luckily selected via a Google & Facebook sponsored email-draws, and I decided to put this on the internet for the world to see in other to relinquish any doubts. See links for proof: http://www.people.com/article/powerball-winners-lisa-john-robinson-tennessee-confirmed http://www.powerball.com/powerball/winners/2016/TN_Robinson011316.shtml For immediate release of these donated funds, send your *Full Names:..... *Tel:..... *Age:..... *Country:..... We will instruct our payout Bank to transfer the sum of $300,000.00 to you. So do get back to us quickly via email at: j.lrobinson5288@gmail.com Congratulations & Happy Celebrations in Advance. Regards, John & Lisa Robinson.

E8: E-mail de *phishing* dos Correios contendo *links* maliciosos.

De: bobtrama <bobtrama@hotmail.com>
Enviado: quinta-feira, 25 de agosto de 2016 13:09
Para: antonilsonjack@hotmail.com
Assunto: NOTIFICAÇÃO SEDEX

Correios

NOTIFICAÇÃO SEDEX

Atenção, foram realizadas tentativas de entrega no seu endereço e por motivo de ausência de destinatário sua encomenda retornou na data 12/08/2016 para nosso centro de distribuição de encomendas e cartas.
Para localizar sua encomenda solicitar o reenvio clicando Aqui.
ID OBJETO: SR586324157 7BR
INFORMAÇÕES:
Serão realizadas 3 (três) tentativas de entrega nos seguintes dias e horários: A segunda e a terceira tentativa são realizadas nos dias úteis imediatamente subseqüentes. Caso as 3 tentativas de entrega domiciliar sejam frustradas, o objeto ficará disponível para reenvio pelo prazo de 7 dias corridos.

VISA Rio2016