CENTRO PAULA SOUZA

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Segurança da Informação

TÉCNICAS UTILIZADAS PELA ENGENHARIA SOCIAL: ESTUDO DE CASO COM ALUNOS DO CURSO DE SEGURANÇA DA INFORMAÇÃO DA FATEC-AM

MAYARA DE LOURDES ALVES

Americana, SP
2015

CENTRO PAULA SOUZA

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Segurança da Informação

TÉCNICAS UTILIZADAS PELA ENGENHARIA SOCIAL: ESTUDO DE CASO COM ALUNOS DO CURSO DE SEGURANÇA DA INFORMAÇÃO DA FATEC-AM

MAYARA DE LOURDES ALVES

may.dmc3@gmail.com

Trabalho Monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec-Americana, sob a orientação da Prof. Dra. Acácia Ventura.

Área: Engenharia Social e Fator Humano

Americana, SP
2015

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

Alves, Mayara de Lourdes

A48t Técnicas utilizadas pela engenharia social: estudo de caso com alunos do curso de segurança da informação da Fatec-AM. / Mayara de Lourdes Alves. – Americana: 2015.

64f.

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

Orientador: Prof. Dr. Acácia de Fátima Ventura

1. Segurança em sistemas de informação I. Ventura, Acácia de Fátima II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Mayara de Lourdes Alves

TÉCNICAS UTILIZADAS PELA ENGENHARIA SOCIAL: UM ESTUDO DE CASO COM ALUNOS DO CURSO DE SEGURANÇA DA INFORMAÇÃO DA FATEC AM

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: Engenharia Social e Fator Humano.

Americana, 08 de Dezembro de 2015.

Banca Examinadora:

Acácia de Fátima Ventura (Presidente)
Doutora
Fatec Americana

Maria Cristina Luz Fraga Moreira Aranha (Membro)
Doutora
Unisal

Humberto Celeste Innarelli (Membro)
Doutor
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer a Deus, por não desistir de mim, e me dar forças para chegar até aqui, em segundo lugar, gostaria de agradecer a minha orientadora Doutora Acácia Ventura que me ajudou e me apoiou acreditando em mim, aconselhando e ensinando a cada dia a melhorar, se dedicando para o desenvolvimento junto a mim, da minha pesquisa.

Agradeço também aos professores que tive ao longo dos semestres e que foram excelentes me apoiando e me ensinando para o meu aprendizado, e que também me apoiaram, também a Professora Maria Cristina Luz Aranha.

Aos meus pais, e meu namorado que foram muito pacientes comigo nesse período, me apoiando, também aos familiares, amigos e colegas de sala, que me ajudaram, sempre para que eu pudesse chegar até aqui, agradeço também a um amigo de quatro patas que não está mais entre nós, infelizmente nos deixou no dia 14 de agosto desse ano, mas que mesmo sem dizer uma palavra sempre ficou ao meu lado durante 11 anos quando precisei, e dedico esse trabalho em especial a ele.

DEDICATÓRIA

Aos meus pais, meu namorado, a minha família e amigos,
e também a um grande amigo que era parte da família.

RESUMO

Atualmente cada vez mais tem sido necessária a implementação de segurança nas empresas para proteção dos ativos e das informações que essas organizações guardam, pois, cada vez mais a tecnologia está presente nas empresas e vidas pessoais do ser humano, e o armazenamento desses dados são feitos no meio computacional. Um profissional de segurança da informação tem como objetivo minimizar as vulnerabilidades que as organizações estão sujeitas, e uma das principais ameaças, é a engenharia social, onde o engenheiro utiliza-se a arte de manipular e persuadir as pessoas, para conseguir as informações necessárias. Os engenheiros sociais utilizam várias técnicas para obter sucesso naquilo que desejam, e consideram o fator humano o mais frágil para quebra da segurança da informação. Com isso um profissional da área e funcionários sem esse conhecimento, e que não estão preparados, poderão comprometer toda uma organização, ao sofrer um possível ataque. O objetivo geral desta monografia constitui estudar o conhecimento dos alunos de Segurança da Informação do primeiro ao sexto semestre e o quão preparados estão, ao sofrer um possível ataque de engenharia social, a metodologia utilizada será a dialético e a pesquisa básica, sendo que para a abordagem as pesquisas foram quantitativa, qualitativa, exploratória e descritiva, concluindo que os resultados obtidos no questionário mostraram que até mesmo alunos do curso pesquisado estão sujeitos a cair nas técnicas de engenharia social, mesmo não havendo uma grande evolução no decorrer dos semestres.

Palavras Chave: Segurança; Técnicas; Informação.

ABSTRACT

Currently it has increasingly been required to implement safety in undertakings to protect the assets and information that these organizations keep, therefore, increasingly technology is present in businesses and personal lives of human beings, and the storage of such data is made in computational environment. A professional information security area, aims at minimizing the vulnerabilities organizations are subject and one of the main threats is social engineering, where the engineer used art to manipulate and persuade people to get the necessary information, using various techniques to succeed in what they want, and considers the human factor weakest, breach of information security. With this professional area and employees without this knowledge, and who are not prepared may compromise an entire organization, to suffer an attack. The overall aim of the thesis is to study the knowledge of Information Security students from the first to the sixth semester and how prepared they are, after suffering a possible social engineering attack. The methodology will be dialectic and basic research, and for the approach the research was quantitative, qualitative, exploratory and descriptive. Conclusion based on the questionnaire shows that even students in the program are subject to falling into the social engineering techniques, even without a major evolution over the semesters.

Keywords: Security; Techniques; Information.

LISTA DE FIGURAS, QUADRO, TABELAS E GRÁFICOS

SUMÁRIO

INTRODUÇÃO

Cada vez mais o termo Segurança da Informação tem sido um assunto conhecido e necessário nas organizações. Com a utilização do meio digital as empresas necessitam desse ambiente computacional para o andamento do negócio, e também mantém as informações armazenadas e processadas nesse ambiente, e para que essa organização de TI ou não, possa proteger esse bem de valor, o aspecto de Segurança da Informação torna-se um elemento chave para isso, pois irá minimizar ao máximo que esses ativos das empresas, fiquem em risco (FONTES, 2006, Introdução).

A Segurança da Informação é um conjunto de normas e tem como principal objetivo a proteção da informação, minimizando os riscos do negócio e protegendo assim os ativos da empresa. Para que isso ocorra baseia-se em três atributos principais e indispensáveis, que são: a disponibilidade, integridade e confidencialidade de uma informação, garantindo que ela esteja sempre disponível quando necessário, e que seja somente para a pessoa autorizada sendo, também, essencial que esses dados estejam íntegros livres de qualquer alteração ou modificação não autorizada (FONTES, 2006).

Esses atributos podem ser quebrados, interferindo assim no sigilo da informação, e comprometendo toda existência de uma organização, e muitas vezes isso ocorre por ações humanas. Mitnick e Simon (2003, p.3), dizem esse ser “o elo mais fraco da segurança da informação”.

Diante disso, no escopo desse trabalho será feito um estudo com os alunos do Curso de Segurança de em Tecnologia da Informação na FATEC Americana, para identificar a contribuição do curso para a formação profissional dos alunos com relação a esse ponto, em que o fator humano se torna a principal falha em uma organização, utilizando-se algumas técnicas de engenharia e persuasão na engenharia social para a pesquisa.

Para tanto o estudo **justifica-se** em função de: Segundo Peixoto (2006, p.36), “A engenharia social está inserida como um dos desafios (se não o maior deles)

mais complexos no âmbito das vulnerabilidades encontradas na gestão da segurança da informação”.

Com isso, considera-se o quão importante a engenharia social é para a área de Tecnologia da Informação. Pode afetar os três principais tributos de segurança da informação (Confidencialidade, Integridade e Disponibilidade) como descritos, ameaçando assim o sigilo da informação. É importante que um profissional da área tenha o conhecimento necessário sobre o termo engenharia social, pois esse pode afetar toda uma empresa. Um profissional poderá treinar e aconselhar aqueles com menor conhecimento no assunto para melhor sigilo da informação nas organizações. A pesquisa aplicada nos alunos será do primeiro ao sexto semestre, para identificar a contribuição do curso para esse fator importante que ameaça a vulnerabilidade da área, podendo assim comprometer toda uma empresa. (PEIXOTO, 2006).

Já o **Problema** foi: Segundo Mitnick e Simon (2006), muitos profissionais da área de Segurança em Tecnologia da Informação, acreditam que estão imunes a ataques e vários tipos de vulnerabilidades, pois utilizam produtos de segurança padrão, como *firewall*, dispositivos de autenticação, antivírus, e não é bem assim, eles chamam isso de Ilusão da segurança, pois a principal falha para segurança da informação é o fator humano, e quando percebem que não estão realmente seguros já é tarde demais. Foi realizada uma pesquisa para estudar se o curso de formação em segurança da informação está contribuindo para essa percepção em um ataque de persuasão da engenharia social, utilizada pelos engenheiros sociais.

Como **Pergunta** que se buscou responder foi: O curso de Segurança da Informação contribui para o aumento a percepção dos alunos no tocante a Engenharia Social?

As **Hipóteses** foram: a) O curso está contribuindo para o melhoramento nesse tocante e ter assim um resultado evolutivo ao decorrer dos semestres na comparação dos grupos; b) O curso não está contribuindo podendo assim gerar um resultado não conclusivo ao decorrer dos semestres, c) Poderão ocorrer variações entre os semestres sendo mais conclusivos em algumas perguntas do que em

outras, e d) Os Resultados da comparação dos semestres podem ser similares, com uma diferença mínima, sendo assim não conclusivos.

O **objetivo geral** consistiu em estudar e pesquisar o conhecimento que os alunos do Curso Superior de Tecnologia em Segurança da Informação da Fatec – Americana do primeiro ao sexto semestre têm sobre “enganar e invadir” e as técnicas utilizadas por engenheiros sociais, buscando compreender a contribuição que a formação acadêmica proporcionou aos mesmos.

Os **objetivos específicos** foram: a) Fazer um levantamento bibliográfico sobre Segurança da Informação e Engenharia Social, objetivando identificar as técnicas utilizadas pelos engenheiros sociais; b) Fazer uma pesquisa de campo com os alunos do Curso Superior de Tecnologia em Segurança da Informação da Fatec – Americana do primeiro ao sexto semestre, visando conhecer o grau de conhecimento que eles adquiriram durante o curso sobre as técnicas de engenharia social utilizada pelos engenheiros sociais e, c) Discutir o conteúdo teórico estudado atrelado aos dados obtidos no estudo de caso, buscando identificar se o curso contribui ou não na percepção dos alunos sobre as técnicas de engenharia social.

Como **método** utilizado para o desenvolvimento deste trabalho foi o Dialético, que:

> [...] 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 estudá-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).

De acordo com Gil (2008, p.14, apud PRODANOV e FREITAS, 2013, p. 36):

> [...] a dialética fornece as bases para uma interpretação dinâmica e totalizante da realidade, uma vez que estabelece que os fatos sociais não possam ser entendidos quando considerados isoladamente, abstraídos de suas influências políticas, econômicas, culturais etc.

A **pesquisa** foi classificada do ponto de vista da sua natureza como Pesquisa Básica, que: “objetiva gerar conhecimentos novos úteis para o avanço da ciência sem aplicação prática prevista. Envolve verdades e interesses universais”. (KAUARK, MANHÃES, MEDEIROS, 2010, p. 26).

Para a abordagem do problema foram utilizadas as pesquisas: Quantitativa e a Qualitativa, onde quantitativa, pois baseada “em hipóteses claramente indicadas e variáveis que são objeto de definição operacional", e qualitativa, porque “costuma ser direcionada, ao longo do seu desenvolvimento; além disso, não busca enumerar ou medir eventos e, geralmente, não empregam instrumental estatístico para análise dos dados; seu foco de interesse é amplo e parte de uma perspectiva diferenciada da adotada pelos métodos quantitativos”. (NEVES, 1996, p. 1).

Para que os objetivos fossem atingidos utilizaram-se as pesquisas: Exploratória e Descritiva. Para Marconi e Lakatos (2003, p. 188) as pesquisas exploratórias são:

> [...] investigações de pesquisa empírica cujo objetivo é a formulação de questões ou de um problema, com tripla finalidade: desenvolver hipóteses, aumentar a familiaridade do pesquisador com um ambiente, fato ou fenômeno, para a realização de uma pesquisa futura mais precisa ou modificar e clarificar conceitos. Empregam-se geralmente procedimentos sistemáticos ou para a obtenção de observações empíricas ou para as análises de dados (ou ambas, simultaneamente).

Já a pesquisa descritiva "visa descrever as características de determinada população ou fenômeno, ou o estabelecimento de relações entre variáveis. Envolve o uso de técnicas padronizadas de coleta de dados: questionário e observação sistemática. Assume, em geral, a forma de Levantamento". (KAUARK, MANHÃES e MEDEIROS, 2010, p. 29).

Já para os procedimentos técnicos foram utilizadas: a pesquisa Bibliográfica e o Estudo de Caso. Bibliográfica para "quando elaborada a partir de material já publicado, constituído principalmente de livros, artigos de periódicos e, atualmente, material disponibilizado na Internet”. (KAUARK, MANHÃES e MEDEIROS, 2010, p. 28).

E para o Estudo de caso os autores (p. 29) dizem: "quando envolve o estudo profundo e exaustivo de um ou poucos objetos de maneira que se permita o seu amplo e detalhado conhecimento”.

O trabalho foi estruturado em três capítulos, sendo que o **primeiro** apresenta o estudo bibliográfico sobre segurança da informação, descrevendo sobre os três pilares básicos e políticas de segurança da informação. Ainda nesse mesmo capítulo também foi feito um estudo bibliográfico sobre a engenharia social, o elo mais fraco de segurança da informação, as ferramentas utilizadas pelos engenheiros sociais e as técnicas utilizadas por esses mestres na persuasão, o **segundo** discute fatores do estudo de caso, sendo a análise dos dados da pesquisa aplicada ao curso de segurança da informação, comparando em gráficos os resultados obtidos.

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

1 SEGURANÇA DA INFORMAÇÃO E A ENGENHARIA SOCIAL

Com a revolução industrial e tecnológica as informações deixaram de serem manipuladas no meio físico, passando assim a serem manipuladas e armazenadas no meio digital, obviamente a informação é o ativo mais importante dentro de uma organização, portanto foi necessário desenvolver meios para que a mesma não sofresse impactos severos que impedissem a continuidade do negócio, surgindo assim o conceito de segurança da informação, que visa proteger a informação através da análise da empresa e estabelecimento de políticas.

1.1 SEGURANÇA E INFORMAÇÃO

Para se entender o conceito de Segurança da Informação é necessário em um primeiro momento o esclarecimento dos elementos nos quais o mesmo é composto.

Sêmola (2003) afirma que, com o passar do tempo as organizações foram influenciadas por novidades e mudanças o tempo todo conforme o mercado. Desde as Revoluções Industrial e Elétrica, com a expansão do mercado, aumentou-se a competitividade passando por momentos como, por exemplo, a terceirização e o mais recente deles, a Tecnologia da Informação com aplicação ao negócio.

A informação sempre esteve presente em cada um desses passos, como um importante fator para gestão do negócio. Acrescenta ainda que independentes do ramo no mercado de cada empresa ainda assim ao longo de seu trajeto usufruíram da informação, objetivando o melhor resultado para os negócios.

Peixoto define a informação como: “Ato ou efeito de informar-se; Conjunto de conhecimentos sobre alguém ou alguma coisa;” O autor ainda acrescenta que: “A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para continuidade operacional da empresa.” (PEIXOTO, 2006, p. 37).

Com relação à definição sobre segurança Sêmola (2003), explica que é um fator importante que não pode faltar em uma empresa seja qual for o seu porte, pois visa proteger o mais importante ativo dentro de uma organização, que é a informação.

Fontes (2006) assim como Sêmola, diz que informação é um ativo importante dentro de uma organização, e por esse motivo tudo aquilo que envolve seu processamento, transmissão e armazenamento devem ser protegidos. O autor ainda diz a informação ser de valor para empresa e que sem ela, a organização não faz o seu negócio.

Ativo: “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).

1.2 SEGURANÇA DA INFORMAÇÃO

> Segurança da informação é um conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada (FONTES, 32006, p. 11).

Para Peixoto (2006, p. 37-38), Segurança da informação é uma área de conhecimento que guarda e protege os ativos da informação, contra acessos indevidos e não autorizados.

Afirma ainda, serem muitas as vulnerabilidades existentes em uma organização, essa sendo da área de TI ou não. Também afirma que muitas dessas vulnerabilidades passam despercebidas nas empresas. O mesmo diz também que a informação é a alma do negócio, pois mesmo que não seja palpável sabe-se o quão importante ela é em uma organização.

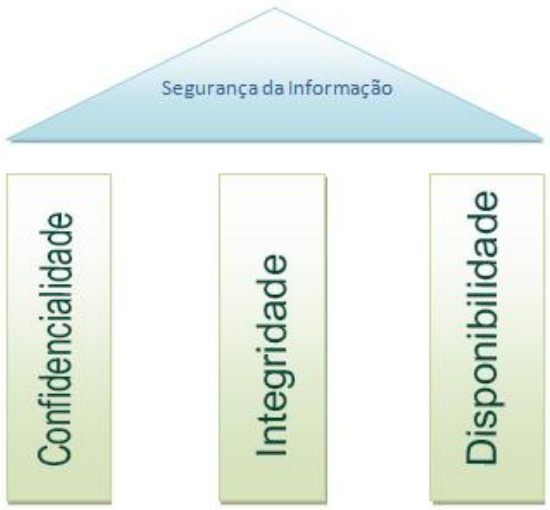
Em concordância com Peixoto, Sêmola (2003) afirma também ser uma área de conhecimento com o foco na proteção dos ativos da informação, para evitar ao máximo acesso não autorizados e indisponibilidade desses ativos.

Sendo assim, existe um conceito unânime entre os autores especialistas da área no que se refere à segurança da informação, afirmando em sua maioria que o intuito principal é proteger a informação contra acesso indevido e indisponibilidade, garantindo assim a continuidade do negócio (SÊMOLA, 2003).

1.2.1 Pilares da segurança da informação

Goodrich e Tamassia (2013) explicam que com o avanço da tecnologia e o crescimento do uso de redes de computadores dentro das organizações, percebe-se o quanto esse sistema é frágil e passível de invasão. Sendo assim especialistas da área de tecnologia da informação desenvolveram um conceito no qual a segurança da informação se baseia. Dentre os conceitos de segurança da informação há os três pilares básicos que garantem a proteção e o sigilo da informação, sendo eles: Confidencialidade, integridade e disponibilidade.

Figura 1: Pilares da Segurança da Informação



Fonte: Goodrich e Tamassia (2013, p. 3), adaptada pela autora.

> **Confidencialidade:** Evitar a revelação não autorizada de informação. Isto é, confidencialidade envolve a proteção de dados, propiciando acesso àqueles que são autorizados a vê-los e não permitindo que os outros saibam algo a respeito de seu conteúdo. (GOODRICH e TAMASSIA, 2013, p.4).

Afirmam ainda que manter o sigilo dessa informação é fundamento da segurança da informação, principalmente hoje, com todas essas ameaças que podem afetar cada vez mais a confidencialidade da informação.

Para Fontes (2006), a confidencialidade está ligada ao fato de que o acesso e utilização da informação devem ser feito unicamente pelos que precisam dela para prática de suas ações profissionais na empresa.

Para Peixoto (2006), as informações precisam ser protegidas conforme o grau de sigilo de cada um, limitando o uso somente a pessoas destinadas.

> **Integridade:** Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais (SÊMOLA, 2003, p. 45).

Para explicar o que é integridade, Goodrich e Tamassia (2013) utilizam uma brincadeira de criança praticada nas escolas, o telefone sem fio. Esse é um bom exemplo para compreensão, onde as crianças fazem um circulo e a criança escolhida cria uma mensagem, essa é passada para outra criança por um sussurro, e depois para outra e assim por diante até retornar à mesma criança que criou à mensagem, quando retorna, quase sempre a mensagem chega distorcida, pois sofreu alterações ao longo do caminho.

Peixoto (2006), explica que mesmo após o envio e o recebimento da informação corretamente, essa ainda sim precisa chegar íntegra ao seu destino, não tendo sofrido nenhum tipo de alteração ou mudança que irá comprometer informação original.

> **Disponibilidade:** Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade. (SÊMOLA, 2003, p.45).

Peixoto (2006) faz uma observação interessante para destacar sobre a importância de esse último pilar importante para segurança da informação. O mesmo afirma que de nada adianta se ter confidencialidade e integridade, se essa informação não estiver disponível para o acesso quando necessário. Explica que esse é um dos maiores desafios, ou seja, manter essa informação de maneira confiável e íntegra.

Na visão de Fontes (2006) também a informação precisa estar acessível para realização dos objetivos e missão, Goodrich e Tamassia (2003), concluem que a modificação e acessibilidade dessa informação serão somente para os que estiverem autorizados.

Outros atributos citados na visão de Fontes (2006), que também garantem a proteção da informação:

Legalidade: Na qual o uso das informações precisa estar conforme a lei.

Auditabilidade: O acesso e o uso da informação precisam ser registrados, para uma possível identificação futura.

Não repúdio de auditoria: O autor da modificação ou alteração da informação não poderá negar o fato, pois possuem maneiras de garantir essa autoridade.

1.2.1.1 Riscos, Ameaças e Vulnerabilidades

Riscos: É a probabilidade em que essas ameaças poderão ser exploradas através das vulnerabilidades, ocasionando-se assim a perda dos três pilares e o impacto dos negócios Sêmola (2003).

Ameaças: Eventos ou agentes que provocam ocorrências que comprometem as informações e também os ativos, explorando as vulnerabilidades, comprometendo perca de confidencialidade, integridade e disponibilidade, podendo gerar também o impacto aos negócios da empresa (SÊMOLA 2003).

Vulnerabilidade: Ainda na visão de Sêmola (2003), o autor explica que é a fragilidade ou fraqueza vinculada aos ativos que manipulam a informação, e que quando explorada por uma ameaça, possibilita um evento de um incidente de segurança, atingindo negativamente qualquer um e até mesmo todos os princípios de segurança da informação. Alguns exemplos de vulnerabilidades citados pelo autor são: Físicas, Naturais, *Hardware*, *Software*, Mídias e Comunicação Sêmola (2003). São apresentados, também, três grupos classificados pela intencionalidade, podendo ser:

Natural: Originadas por fenômenos da natureza, como por exemplo, enchentes, tempestades, incêndios, terremotos dentre outros.

Involuntárias: Ameaças inconsistentes, na maioria das vezes causadas pelo desconhecimento, podendo ser causadas por erros imprevistos, falta de energia.

Voluntárias: Causadas pelo ser humano e de maneira proposital, como espiões, *hacker,* invasores, ladrões, *vírus* de computadores.

Goodrich e Tamassia (2013) dizem que a vulnerabilidade é um aspecto importante na área de segurança da informação. Através da vulnerabilidade o atacante pode explorar as fraquezas e ter acesso a informações privadas, permitindo inúmeras maneiras de ataques.

Para tentar diminuir esses riscos, é necessário definir propriedades de segurança, para uma análise dos tipos de ataques que poderão vir a ocorrer, e assim poder estar preparados, com o desenvolvimento de defesas específicas.

1.2.2 Políticas de Segurança da Informação

> A Política de Segurança da Informação define o conjunto de normas, métodos e procedimentos utilizados para manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação (FERREIRA e ARAÚJO, 2008, p.9).

Medidas de Segurança: São os procedimentos, práticas utilizadas para proteger a informação e seus ativos, podendo impedir que essas ameaças usem as vulnerabilidades.

Fontes (2006) explica que a política de segurança deve estar sempre alinhada ou vinculada aos objetivos do negócio da empresa. A organização tem que utilizar os recursos necessários para que seja possível o desenvolvimento de suas formas de negócio, não prejudicando assim a segurança da informação ou essa vulnerabilidade dos negócios.

Para Sêmola (2003), essas medidas podem ser de três maneiras, Preventivas: com o objetivo de evitar, tanto quanto possível, que incidentes aconteçam, Detectivas: para a detecção de ou do indivíduo causador da ameaça, evitando assim que essas explorem venerabilidades, e Corretivas: que seriam ações com o foco na correção, como exemplo restauração de *backup*, planos de recuperação de desastres, entre outras medidas.

Barreiras de Segurança: Na visão do autor, confirma-se que o correto é estudar e analisar o desafio de como proteger a informação utilizando camadas, outra denominação para as seis barreiras de Segurança da Informação. Essas barreiras têm como objetivo, reduzir os riscos. São: Desencorajar, Dificultar, Discriminar, Detectar, Deter e Diagnosticar.

Define-se a “política de segurança da informação como um conjunto de regras bem definidas”, e afirma-se também que esse pode ser atendido em *framework,* na qual um dos componentes desse é possibilitar que projetistas possam definir uma assim uma política de segurança da informação (GOODRICH e TAMASSIA, 2013, p. 438).

Goodrich e Tamassia (2013) descrevem algumas ferramentas que pesquisadores de segurança em computadores desenvolveram para minimizarem-se as vulnerabilidades dos pilares, dentre elas estão:

Controle de acesso: São Regras e Políticas que delimitam a permissão a informação confidencial somente para pessoas ou sistemas com autorização.

Segurança Física: A formação de barreiras físicas como portas e câmeras para limitar o acesso a bens computacionais protegidos.

Sêmola (2003) define que a sessão das informações espera que a segurança ocorra antes que as ameaças cheguem e se dissipem para outros meios ou brechas onde não deveriam cruzar. Afirma, assim como Goodrich e Tamassia, que a Criptografia e autenticação, dentre outros recursos, são válidas para o sigilo da informação.

Assim como para Confidencialidade, os autores também citam algumas ferramentas de apoio à integridade da informação, dentre elas estão:

Cópia de Segurança: Ou *backup*, utilizado para o armazenamento redundante dos dados na qual possam ser restaurados, se houver algum problema com o original.

O mesmo diz que a qualidade de uma informação está ligada diretamente a sua disponibilidade e cita algumas ferramentas para providenciar a disponibilidade:

Redundâncias Computacionais: A disposição de computadores e dispositivos reservas para quando houver falhas (daí o uso da palavra redundância).

Sendo assim o mesmo conclui que a política de segurança da informação, define restrições sobre ações do sujeito, com relação ao sistema, afirma também essas políticas serem úteis e imprescindíveis.

> 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. Algumas autoridades recomendam que 40% do orçamento geral para segurança da empresa seja aplicado no treinamento da conscientização. (MITNICK e SIMON 2003, p.195).

1.3 ENGENHARIA SOCIAL

Engenharia: "Arte de aplicar conhecimentos científicos e empíricos e certas habilidades específicas à criação de estruturas, dispositivos e processos que se utilizam para converter recursos naturais em formas adequadas ao atendimento das necessidades humanas” (PEIXOTO, 2006, p.4).

Social: "Da sociedade, ou relativo a ela. Sociável. Que interessa à sociedade" (PEIXOTO, 2006, p.4).

> **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). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos (KONSULTEX, 2004 apud PEIXOTO, 2006, p. 4).

Na visão de Mitnick e Simon (2003), é um método diferente para definição do uso da persuasão para influenciar, e fazer com que as pessoas concordem com uma ação ou pedido. Dizem que é através da engenharia social que o atacante irá enganar influenciar, manipular e convencer a vítima de que ele é alguém que na verdade não é aproveitando assim para conseguir as informações almejadas. Mann (2011), em concordância com Mitnick e Simon também indicam ser a arte para manipular e enganar as pessoas para que assim elas forneçam ou realizem uma ação.

Peixoto (2006) usa um exemplo interessante da Bíblia sobre como Eva se deixou influenciar pela serpente, para explicar que desde a antiguidade o ser humano tem sido vítima da Engenharia Social. Assim como Revista Gestão de Riscos (2011) dos autores Lennert e Oliveira, em concordância com Mitnick e Simon (2003), afirmam ser o elo mais fraco na Segurança da Informação. A engenharia tem como especialidade enganar, influenciar, manipular e persuadir as pessoas, e através dessas estratégias de manipulação, fazer com que os engenheiros sociais alcancem seus objetivos.

> O termo Engenharia Social passou a ser amplamente disseminado na área de Segurança nos últimos anos. Apontado como um dos maiores riscos atuais, os ataques de Engenharia Social ainda são muito eficazes, já que se apoiam em falhas de interpretação do próprio cérebro humano (LENNERT E OLIVEIRA, 2011, p.24).

E esse tem sido bastante discutido em setores das indústrias já que a chance de perdas de informação ocasionada por ataques bem sucedidos de Engenharia Social podem custar caro e afetar os setores críticos de sucesso de uma organização. (LENNERT E OLIVEIRA, 2011).

Cita também que segundo o ex *hacker* e atual consultor de Segurança da Informação Kevin Mitnick, é bem mais fácil manipular, enganar e persuadir uma pessoa para conseguir as informações desejadas, do que desperdiçar esforço, tempo e investimentos tentando invadir algum sistema ou computador.

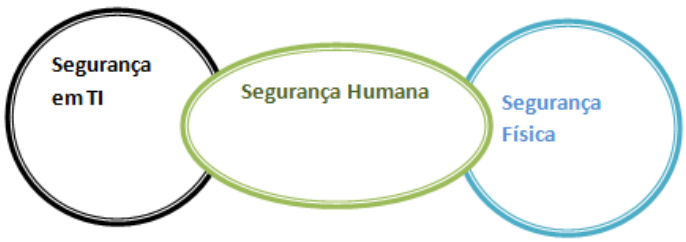
Seguindo essa linha de raciocínio o fator humano torna-se uma marionete, um verdadeiro fantoche, quando manipulado por um engenheiro social. Eles possuem várias técnicas para praticar um ataque de engenharia, mas todas essas irão depender de um atributo próprio da decisão humana, chamado de propensão cognitiva.

> Propensão Cognitiva: Um padrão de desvio no julgamento que ocorre em determinadas situações. Essas distorções na mente humana são difíceis de eliminar e podem acarretar em erros de percepção, interpretação não lógica ou julgamento errado (REVISTA DE GESTÃO DE RISCOS, 2011, p.25).

Como afirmado por Mitnick e Simon (2003), ninguém está cem por cento seguro, e aqueles que acham que estão vivem uma "ilusão de segurança", com a proposta de diminuir as vulnerabilidades e os riscos ocasionados pela engenharia social e outras ameaças, o autor propõe a adoção de uma política de segurança da informação. Esse conjunto de regras bem definidas irá possibilitar, boas práticas em de uma empresa, para que os funcionários saibam como mitigar essa situação, protegendo a informação, o ativo mais importante dentro de uma empresa.

1.3.1 O elo mais fraco da segurança

Figura 2: Segurança humana - O elo perdido



Fonte: MANN (2011, p. 19), adaptado pela autora.

"Segurança tem início e termina com as pessoas" (FRISCH apud PEIXOTO, 2006, p.3).

Mitnick e Simon (2003) dizem que por mais reforçada que seja a segurança aplicada, seja ela física ou de TI, ainda sim as pessoas estão vulneráveis, pois o elo mais fraco é o fator humano. Reforçar a segurança uma simples ilusão, pois ninguém está 100% seguro e que se torna pior quando a ingenuidade e toda essa credulidade e ignorância entram em campo.

E prosseguem dizendo que o atacante irá encontrar uma maneira de manipular, enganar e influenciar algum funcionário de segurança da empresa, até que esse revele as informações que o mesmo realmente deseja saber.

Mann (2011) também concorda com o ponto de vista abordado por Kevin e Simon e diz que as pessoas desde a infância aprendem a seguir as instruções. Alguns aspectos considerados como vulnerabilidades humanas a serem exploradas são: Ignorância, Credulidade, Desejo de Ser Amado e Ser Prestativo.

1.3.2 Perfil do engenheiro social

"Quando você combina uma inclinação para enganar as pessoas com os talentos da influência e persuasão, você chega ao perfil de um engenheiro social" (MITNICK e SIMON 2003, p. 13).

Peixoto (2006) diz o perfil de um engenheiro social: ser uma pessoa de personalidade educada, criativa, simpática, agradável, flexível, carismática. Acrescenta também ser dinâmico com assuntos interessantes e envolventes, Kevin e Simon (2003) acrescentam que os engenheiros sociais costumam ser charmosos educados e agradam facilmente.

Peixoto afirma, ainda, que o engenheiro social prevê a presunção e a resistência, e esse sempre estará preparado para converter a desconfiança em confiança. Um engenheiro social eficaz estuda o seu ataque assim como é feito em um jogo de xadrez, e antecipa as perguntas que sua vítima poderá fazer, estando preparado para repondê-las corretamente.

Uma observação interessante apresentada por Mitnick e Simon (2003), é que na maioria dos exemplos abordados os engenheiros sociais é referenciada como "eles", pois a maior quantidade dos praticantes dessa área é do sexo masculino, mas afirmam também que embora não existam muitas engenheiras sociais, o número vem crescendo, e acrescenta que elas possuem uma vantagem distinta sobre os homens, pois podem utilizar a sensualidade para conseguir a cooperação.

Uma afirmação feita pelo autor Lennert e Oliveira (2011) é que nem todo mundo que pratica a engenharia social necessariamente é um *hacker*, e para um melhor entendimento dessas técnicas que eles utilizam para os ataques o mesmo descreve alguns exemplos de pessoas que podem praticar essas ações e o que as levam a isso.

QUADRO 1: Tipos de Intrusos

INTRUSOS	OBJETIVOS
Estudantes	Bisbilhotar mensagens de correio eletrônico de outras pessoas por diversão;
Hackers/Crackers	Testar sistemas de segurança ou roubar informações;
Representantes Comerciais	Descobrir planilhas de preços e cadastro de clientes;
Executivos	Descobrir plano estratégico dos concorrentes;
Ex-funcionários	Sabotagem por vingança;
Contadores	Desfalques financeiros;
Corretores de valores	Distorcer informações para lucrar com o valor das ações;
Vigaristas	Roubar informações, como senhas e números de cartões de créditos;
Espiões	Descobrir planos militares;
Terroristas	Espalhar pânico pela rede e roubar informações estratégicas;

Fonte: Adaptada de Lennert e Oliveira (2011, p.25).

1.3.2.1 Ferramentas Utilizadas

Peixoto (2006) exemplifica que para a prática da maioria das ações de ataque os engenheiros sociais utilizam algumas ferramentas, dentre elas estão:

Telefone: Fingir ser alguém que não é. Esse é um dos ataques mais comuns de engenharia social, como por exemplo, um analista de suporte.

Pessoalmente: A persuasão e a maneira de conversar são os principais triunfos de um engenheiro social para esse tipo de ataque. O mesmo assume o papel de alguém que não é. Manipula a vítima para convencer a mesma que o que diz é verdade, e se o engenheiro conhece o ambiente esse ataque pode ter mais sucesso ainda. Algumas das armas utilizadas por eles são, a intimidação, sedução, dramaticidade e credibilidade.

Chats (bate papo): Para essa técnica Peixoto (2006) informa que se passar por alguém que realmente não é, fica mais fácil com a utilização desta ferramenta. Também informa que, com a utilização de fotos, fica mais fácil a vítima acreditar e ser seduzida. Cita como exemplo o aplicativo Messenger.

Fax: Primeiro passo, segundo Peixoto (2006), os engenheiros obtém o número de fax da vítima, e depois o usam para o envio de formulários de preenchimentos, requisições, para futuramente receberem um retorno do que desejam.

Internet (Coleta de Informações): Um bom exemplo são sites clonados, como de sites bancários.

E-mail: E-mails falsos, *phishing scam;* entre outros.

Cartas/Correspondência: Apesar da pouca modernidade, ainda assim pode ser considerado um meio poderoso, pois irá direcionar como vítimas alvos, as pessoas mais velhas ou aqueles que resistem à tecnologia, pois essa técnica é usada para enviar cartas às vítimas como documentos falsos usando logomarcas parecidas com as originais.

Spyware: "Software "espião" usado para monitorar de modo oculto as atividades do computador de um alvo" (PEIXOTO, 2006, p.6).

Mergulho no lixo: O lixo pode ser um recurso valioso, quando nas mãos de um engenheiro social, pois muitas empresas e pessoas descartam informações essenciais no lixo.

Surfar sobre os ombros: Cuidado quando estiver digitando no teclado em lugares públicos ou com muita gente alguma informação importante, como senhas, pois sempre pode ter alguém com certo interesse para descobrir o que se está digitando.

1.4 TÉCNICAS DE ENGENHARIA SOCIAL

Peixoto (2006) diz que mesmo com as constantes mudanças e inovações que os engenheiros buscam a cada segmento de um novo ataque nessa arte de enganar, ainda sim usufruem de alguns aspectos clássicos.

1.4.1 Persuasão e seus Princípios

Dentre as técnicas utilizadas pelos engenheiros a persuasão está presente na maioria, pois assim como afirmado pelos autores citados, a engenharia é um método diferente para definição do uso da persuasão para influenciar e manipular as pessoas. Cialdini (2006) demonstra seis princípios importantes para técnica de persuasão.

Princípio de Contraste: Dentre os princípios da persuasão encontra-se o Princípio de Contraste, que irá afetar segundo Cialdini (2006) o modo como se olha a dessemelhança entre duas coisas que são expostas uma depois da outra. Isso indica que se o segundo objeto demonstrado for razoavelmente desigual do primeiro, consequentemente será visto com uma diferença maior do a que realmente existe.

Um dos exemplos mostrado pelo autor indica que se levantar um objeto leve antes para depois erguer um que seja pesado, o segundo objeto irá parecer mais pesado do que se esse tivesse sido levantado sem erguer o mais leve antes. Esse princípio se aplica a todas as categorias de percepção, não somente ao peso. Em um segundo exemplo o autor explica que se falar com uma mulher bonita e depois com outra que seja não tão atraente como a primeira, a segunda parecerá menos bonita do que de fato é.

Apresentando um cenário real utilizado pelos lojistas, esse princípio é bem comum. Na maioria das vezes quando se entra em uma loja para comprar roupas, eles oferecem primeiro um produto mais caro, e depois o produto mais barato, caso a compra do mais caro não seja feita, o produto mais barato irá parecer ser mais barato ainda. Se o produto mais barato fosse apresentado antes do produto mais caro, o feitiço iria virar contra o feiticeiro, pois apresentando o produto mais caro depois em comparação ao primeiro, ele apresentaria ser mais caro do realmente é.

Esse princípio possui muita influência e essa é bastante explorada. Diz também que uma das vantagens desse princípio é que esse é praticamente indetectável e para os que o usam podem deixar o cenário a seu favor.

Princípio de Reciprocidade: Esse princípio é o clássico “dar e receber” Cialdini (2006) cita como exemplo um cenário onde é feito envio de cartões de natal para pessoas estranhas e mesmo não conhecendo nenhuma delas, o remetente recebe vários cartões em troca, enviados por essas pessoas. Essa retribuição demonstra um dos mais poderosos artifícios de influência ao nosso redor a lei da reciprocidade. Para essa regra a intenção é tentar retribuir da mesma maneira o que recebeu.

Sendo assim por padrão essa sensação de dívida ao receber algo, faz com que o ser humano sinta-se na obrigação da retribuição futura. Segundo sociólogos essa sensação é tão difundida que não possui sociedade humana que não siga essa regra.

Outro exemplo apresentado pelo autor é que esse princípio possui uma força inusitada onde na solicitação de um pedido dá a chance de uma resposta positiva será bem maior do que se não houvesse esse favor anteriormente.

Princípio de compromisso e coerência: Esse princípio é citado por Cialdini (2006) como um motivador central para comportamento humano. É uma tendência que irá levar o ser humano a ser coerente e levá-lo a tomar decisões que normalmente não tomaria. O autor considera este princípio uma arma de influência social, para tomada de decisões não planejadas, é um reconforto para decisões já tomadas, a sensação de realizar-se a escolha certa.

> Devido ao fato de a coerência ser geralmente de nosso interesse, criamos facilmente o hábito de ser automaticamente coerentes, mesmo em situações em que isso não é sensato. Quando isso ocorre impensadamente, a coerência pode ser desastrosa (CIALDINI, 2006, p. 59).

Em um dos exemplos apresentados pelo autor, em um cenário no qual alguns apostadores em corridas de cavalo de cavalo passaram, a se sentir mais confiantes após a confirmação da compra do bilhete de aposta. Assume-se a coerência para a decisão tomada.

Princípio de Prova Social: Afirma-se nesse princípio o modo como o ser humano determina ou julga o que é correto, baseando-se no que as demais pessoas julgam ser correto. Considerar-se mais apropriado um comportamento conforme a frequência em que a sociedade o faz.

A propensão para se julgar uma ação a mais adequada, quando outras pessoas a realizam bem, funciona e muito, a probabilidade de erros será menor, agindo conforme a sociedade e não o oposto deles. Considera-se essa característica a força, mas também a fraqueza desse princípio, pois esse proporcionará um atalho ao ser humano sobre qual decisão tomar e agir, mas também tornará a utilização desse atalho, uma vulnerabilidade para ataques de golpistas e aproveitadores.

Um exemplo citado por Cialdini (2006) são os *barmen***,** que deixam algumas notas no pote de gorjeta utilizado por cliente, para que assim fique a impressão que outros clientes anteriores já depositaram a gorjeta ou em outro exemplo visando o lado bom desse princípio.

Em geral, o ser humano sente-se inseguro em relação a si próprio, quando a situação é pouco clara ou ambígua, quando a incerteza reina, tem-se maior probabilidade de ver e aceitar as ações dos outros como corretas. (CIALDINI, 2006, p. 126)

Princípio de Simpatia: Cialdini (2006), afirma que o ser humano atende mais facilmente pedido de pessoas próximas, de quem mais gostam ou conhecem, mas contradiz que por mais incrível que pareça, essa regra da simpatia é mais utilizada por pessoas estranhas que tenham a intenção da aceitação de um pedido.

Existem alguns fatores desse princípio, dentre eles estão: Atração Física, Semelhança, elogio, contato de cooperação e o condicionamento e associação.

Atração física, o autor relata que pessoas mais atraentes tendem a conseguir com mais frequência essa interação social, aceitação e concordância de um pedido do que pessoas menos atraentes perante a sociedade. Outro fator que gera simpatia é a semelhança, e esse é válido quando possuem espaços como opiniões, estilo de vida, origem ou traços de personalidade.

Mitnick e Simon (2003) exemplificam dizendo que em um ataque de engenharia social, quando o engenheiro ira tentar imitar a vítima, o comportamento dela e interesses para gerar essa aparência de semelhança.

Dentre os fatores o elogio também é citado, e na visão do autor, as pessoas gostam de serem elogiadas, mesmo que esse não seja verdadeiro, assim também como o fator de contato e cooperação na qual o mesmo exemplifica informando que quase sempre as pessoas gostam mais de coisas que parecem familiares a elas. Por último o autor cita o condicionamento e associação, pessoas tende-se a associarem-se a aquilo que melhora a imagem delas.

Princípio de Autoridade: Cialdini (2006) explica que esse princípio irá usufruir da subordinação e autoria sobre as pessoas, pois por padrão, as pessoas acreditam e aceitam ordens de pessoas que para elas são de autoridade.

Essa obediência e aceitação mecânica, até mesmo de uma autoridade não real, mas a sociedade está predestinada a seguir. Outro detalhe importante é que esse princípio também tem influência da maneira de como as supostas autoridades estão vestindo.

Na afirmação de Lennert e Oliveira (2011) e também de Mitnick e Simon (2003), um engenheiro social que visa atacar uma empresa, por exemplo, poderá se passar por um funcionário de autoridade dentro da empresa, como gerente, supervisor, diretores.

Mitnick e Simon (2003) afirmam, em concordância com Cialdini (2006) que as pessoas possuem essa propensão para atender uma solicitação de autoridades, pessoas com esse cargo e que possuem esse poder de para fazer algo ou alguma coisa.

Princípio de Escassez: Baseia-se nas características de que a partir do momento em que algo ou alguma coisa se torna raro ou com sua disponibilidade limitada, esse parece ser de mais valor, essas oportunidades chegam a ser valiosas.

Esse princípio consiste nessa regra onde em um dos exemplos citados por Cialdini (2006) é que se uma pessoa está no meio de uma conversa com outra e o telefone de uma delas toca, por mais interessante que a conversa esteja, a atratividade de atender ao telefone será maior, pois esse será um momento oportuno, podendo perder a informação que seria passada no telefone, sendo assim a conversa se tornaria menos recuperável que a conversa pessoal no momento, de devido a isso mais rara.

Outro exemplo interessante na visão de Cialdini (2006) que também vive esse princípio de escassez são os colecionadores de figurinhas ou de antiguidades, que

quanto mais difícil é de se encontrar uma figurinha, por exemplo, mais rara ela irá se tornar.

Um exemplo citado por Mitnick e Simon (2003) em um ataque de engenharia social para esse princípio seria pela ferramenta de envio de *e-mails*, por esse poderia distribuir *e-mails* informando que os 500 primeiros que cadastrarem em um site, ganhará ingressos para estreia de um filme.

1.4.2 Informações Inofensivas X Valiosas

Muitas pessoas acreditam que passar apenas uma informação não terá problema algum. Depende; é ai que se enganam. Para um engenheiro as informações são como um jogo de quebra-cabeça, onde a cada informação adquirida é uma nova peça no jogo, e ao final, após adquirir todas as informações necessárias para o seu objetivo o jogo estará completo. Necessário à atenção a qualquer informação dita para alguém.

> Vale a seguinte regra: Não dê nenhuma informação pessoal ou interna da empresa, nem identificadores para ninguém, a menos que a sua voz seja conhecida e o solicitante tenha necessidade de saber a informação (PEIXOTO, 2006, p.8).

Um bom exemplo é citado por Mitnick e Simon (2003), no qual segundo o ditado diz que até os paranoicos têm inimigos, assim como eles as organizações também têm, e ficam de olho na infraestrutura da rede, para futuramente, comprometer o que essa guarda.

Mitnick e Simon (2003) descrevem como a arte para conseguir o acesso às informações que as pessoas ou empregados de uma organização consideram como inofensivas, mas que na verdade elas não são. Em um dos exemplos citados pelo autor, o atacante chamado Didi, se faz passar por um funcionário da empresa, e consegue o número de telefone de três departamentos, aparentemente informações inofensivas. Um desses números o levou ao departamento de centro de custos, onde conseguiu uma cópia da lista de telefones dos empregados da empresa. Além das habilidades de persuasão e manipulação, ele usufruiu de alguns jargões corporativos e de gentileza para alcançar o objetivo.

"Nunca é demais prevenir, educar e estar cada vez mais atendo, pois aquelas informações que você acha que são inofensivas podem ser as chaves para os segredos mais valiosos que a empresa guarda” (PEIXOTO, 2006, p.8).

1.4.3 Criando a Confiança

Peixoto afirma que por mais estranho que possa parecer, qualquer um em qualquer lugar e a qualquer instante, está sujeito a ser enganado. Destaca que: "Confiança não é transitiva: Eu confio em Maria, e Maria confia em João - isso não significa que eu confio em João” (PEIXOTO, 2006, p.8).

Para explicar a frase acima, o autor, demonstra um cenário onde alguém confiando em Maria deixa-a ter acesso aos seus dados secretos. Maria confiando em João copia seus dados para ela e permite que João tenha acesso a eles também. Maria traiu a confiança da pessoa que a deixou ter acesso aos seus dados, pois houve um vazamento de suas informações a João. O engenheiro adquire essa confiança, e depois cria esse vínculo de amizade. Quando a vítima não demonstra suspeita, fica mais fácil adquirir essa confiança para um engenheiro social.

Segundo o autor um conselho bem conhecido ensaiado pelos pais na infância deve ser adotado, "Não confie em estranhos!".

Entre os conselhos deixados por Mitnick e Simon (2003) para não cair nessa técnica, seria a vítima parar para pensar se o indivíduo, com quem está falando, realmente é quem ele diz ser, se realmente o conhece, pois em alguns eventos raros, o indivíduo pode não ser quem diz ser, e com isso as pessoas precisam aprender a reparar, pensar e indagar a autoridade.

1.4.4 Pretexto ou você pode me ajudar?

Um método poderoso na qual o engenheiro finge necessitar de ajuda, para aplicar o golpe. Semelhante ao "Simplesmente Pedindo", o atacante também irá solicitar o pedido de informação, mas a diferença é que o mesmo irá usufruir da dramaticidade e humildade para realizar esse pedido. A boa vontade e disposição de

ajudar ao próximo é um prato cheio para o engenheiro alcançar seu objetivo (PEIXOTO, 2006).

Lennert e Oliveira (2011) também confirmam que para essa técnica o atacante inventa um cenário, toda uma história para atacar a vítima, direcionando de uma forma para que tenha mais chances de fazer com que ela divulgue o que o autor precisa saber.

Goodrich e Tamassia (2013) explicam que nessa técnica de engenharia social, o atacante inventa um pretexto ou uma história para conseguir o que precisa. No exemplo, o autor utiliza uma garota chamada Eve que liga para um suporte técnico e diz que não se lembra de sua senha, porém, a mesma está questionando sobre a senha de um segundo indivíduo, na qual o autor cita como Alice.

Sendo assim o analista do suporte de ajuda, questiona algumas informações pessoais sobre Alice, que Eve irá conseguir responder facilmente (pois estudou a vítima), e dessa maneira o analista acabará ajudando Eve, trocando a senha de Alice e informando uma nova. Para esse exemplo, Eve, pode ter levado algumas horas para descobrir essas informações pessoais de Alice, como exemplo nome do cachorro, nome dos pais, data de nascimento, nome completo dentre outros, mas esse tipo de ataque será mais rápido e eficaz do que um de força bruta. O autor afirma que não será necessário hardware ou software especializado e nem muito investimento.

No exemplo citado por Mitnick e Simon (2003), o atacante liga para um administrador de sistemas de uma empresa (no escritório de vendas) fingindo ser Joseph Jones do departamento de desenvolvimento de negócios, o mesmo informa que irá ficar em um hotel e pede ao funcionário para configurar a conta dele temporariamente para que ele possa acessar o correio eletrônico, sem a necessidade de ligações interurbanas, o atacante confirma algumas informações e o funcionário faz a checagem no banco de dados, o indivíduo responde corretamente o questionário feito a ele e após isso administrador altera a senha inicial para o mesmo.

1.4.5 Isca (*Baiting*)

Essa técnica, segundo Goodrich e Tamassia (2013), o atacante usa um "presente" como isca, para conseguir com que a vítima instale algum software malicioso em sua máquina. Citam como exemplo, onde o atacante deixa um *pen drive* ou outras unidades USB em áreas como um estacionamento de alguma empresa que tenha um sistema apontado como "seguro", e nesse dispositivo deixa indicações de *softwares* famosos ou nomes de jogos. A ideia, nesta técnica, é que o funcionário que encontrar na pausa de almoço ou chegada entre com ele na empresa e conecte no computador, para que o software malicioso se instale.

Outro bom exemplo de se explicar essa técnica em concordância com o autor Lennert e Oliveira (2011), é a utilização de "Cavalos de Tróia" em mídias, ou unidades USB, deixando inocentemente em algum local público como no exemplo de Goodrich e Tamassia, um estacionamento de uma empresa, e no aguardo que a vítima ache e coloque em um computador alvo seja esse empresarial ou pessoal.

1.4.6 *Quid pro quo* (uma coisa pela outra) ou posso ajudar?

"Ficamos agradecidos quando lemos um problema e alguém com conhecimento, habilidade e disposição nos oferecem ajuda" (MITNICK, SIMON 2003, p. 44).

Abusando do poder da persuasão, o engenheiro cria um problema para vítima, e como uma luz no fim do túnel, o mesmo será a solução perfeita para o seu eventual problema, porém, esse será o real problema da vítima, após a solução para o suposto problema, o engenheiro irá usar dessa sua gratidão para conseguir o que precisa (PEIXOTO, 2006).

Para que essa técnica ocorra com sucesso Goodrich e Tamassia (2013) explicam que o atacante irá lhe oferecer ajuda para que a vítima se sinta grata a ele pelo favor, e queria retribuir de alguma maneira. No exemplo dos autores, Bob liga para Alice fingindo ser do serviço de ajuda a empresa dela, informa que algum colega de trabalho a indicou, e nisso se oferece para ajudá-la com algum problema que está tendo com o computador se estiver tendo algum, ou para ajudar na criação

de uma senha mais forte, oferecendo qualquer ajuda, após prestar os serviços à vítima sem pedir algo em troca, o mesmo poderia sugerir a vítima para fornecer sua senha para possíveis consertos futuros, e na gratidão e como cita a mesma “pressão social", ela poderá ceder para retribuir o favor confiando em Bob.

Em concordância com Goodrich e Tamassia 2013, os autores Lennert e Oliveira (2011) afirmam que nessa técnica o engenheiro eventualmente irá se passar por alguém do suporte técnico que presta serviços a uma empresa, e alguém tendo um problema realmente ele será prestativo para ajudar, na resolução do problema, poderá pedir algumas ações ao usuário, ou até mesmo a sua senha, para ter acesso à máquina da vítima, e assim poder realizar a instalação de algum software malicioso, sem que a vítima perceba.

1.4.7 *Phishing* (Pescador)

> Phishing, phishing-scam ou phishing/scam, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p. 9).

Utiliza-se de algumas páginas falsas para atrair a atenção da vítima, como: Páginas falsas de comércio eletrônico ou Internet Banking, páginas falsas de redes sociais ou de companhias aéreas, mensagens contendo formulários, mensagens contendo *links* para códigos maliciosos ou até mesmo solicitações de recadastramentos (CARTILHA DE SEGURANÇA PARA INTERNET. 2012).

Lennert e Oliveira (2011) explicam que para que essa técnica ocorra, o atacante utilizasse da ação de envio de *e-mail*, na qual o *e-mail* é enviado à vítima se passando por algo na qual realmente existe, como bancos ou companhias de cartões de crédito, e com isso pede para realizar a confirmação, com chantagens falsas, se caso não o fizer. Junto ao *e-mail* normalmente consta um *link* que direciona para uma página falsa, porém muito próxima a original, às vezes com mínimos detalhes de diferenças, e nela é onde serão solicitadas as informações, seja de banco, pessoais ou de cartões.

1.4.8 Engenharia social inversa ou Golpe Inverso

Para que esse ataque ocorra com sucesso, a engenharia reversa necessita de um pouco mais de planejamento do engenheiro social, o plano precisa ser bem executado também, pois nesse o atacante irá se passar por uma autoridade de poder, e com isso poderá adquirir as informações daqueles que irão lhe pedir ajuda ou alguma informação (LENNERT e OLIVEIRA 2011).

No exemplo demonstrado por Mitnick e Simon (2003), Eric consegue fazer com que um delegado de um escritório de teletipo, informa-se o número privado do Departamento de Trânsito para uma pessoal totalmente estranha, confiando que esse era um delegado, sem fazer nenhuma verificação.

1.4.9 Lixo

Para essa técnica usada pelos engenheiros, o autor ressalta como um conselho a todas as empresas que não sabem como descartar corretamente o lixo, os engenheiros podem usar isso a favor deles para adquirirem as informações privadas de uma organização, como listas telefônicas velhas, anotações de senhas, relatórios, organogramas (LENNERT e OLIVEIRA 2011).

Rafael (acessado em: 26/10/2015), afirma não serem muitas as empresas, que são cuidadosas no descarte correto do lixo, sendo essa uma rica fonte de informação para os engenheiros sociais. Algumas informações citadas pelo autor que podem ser úteis nas mãos dos engenheiros são: senhas, nome de funcionários, contados de clientes, transações efetuadas, telefones dentre outros.

Um exemplo dessa técnica está disponível no documentário: Hackers anjos e Criminosos (2009) disponibilizado pela Discovery Channel, na qual o atacante Ian Murphy, conhecido como capitão Zap, tinha o foco em atingir o sistema de cobranças computadorizados da empresa americana AT&T, pois afirmou no documentário, ser muito alto as cobranças feitas por eles. Utilizando a técnica do lixo, capitão Zap, encontrou manuais que foram descartados dos equipamentos da empresa, senhas padrões que ainda estavam configuradas e com isso, foi possível realizar a invasão no sistema da organização e mudar os horários dos relógios para

baixar as cobranças das ligações de todos. Capitão Zap se autonomeou como *Robin Hood* moderno. Ele só foi descoberto 18 meses depois.

1.4.10 Simplesmente pedindo

A mais simples das técnicas, nessa o engenheiro simplesmente pede a vítima a informação que deseja saber. Com um pouco de conhecimento e jargões usados no ambiente, e a estrutura coorporativa da empresa são alguns dos truques do mesmo. Após isso, será mais fácil adquirir a confiança da vítima que irá fornecer as informações (PEIXOTO, 2006).

De acordo com os autores a engenharia social é um termo importante e também um método utilizado para conseguir as informações desejadas com mais facilidade e menos gastos. Devido ao ser humano ser o elo mais fraco da segurança da informação e assim, o principal alvo dos atacantes de engenharia social, desenvolveu-se uma pesquisa para análise sobre esse conhecimento ao tema dos alunos do curso de segurança da informação.

Mitnick e Simon (2003, p.26) afirmam que vários ataques de engenharia social são complexos e necessitam de muitas etapas de planejamento, sem contar o conhecimento da tecnologia e manipulação para um ataque bem sucedido, não é o caso desse ataque “Simplesmente Pedindo”, os autores afirmam esse ser direto, basta somente pedir. Explicam também que “é da natureza humana confiar em colegas, particularmente quando a solicitação passa no teste como sendo razoável”.

2 ESTUDO DE CASO

Com o estudo de caso será possível realizar a análise dos dados, e verificar o conhecimento dos alunos do curso de segurança da informação, observando assim a variação das respostas em comparação de ambos os grupos.

2.1 DESCRIÇÃO DA POPULAÇÃO PESQUISADA E PROCEDIMENTO UTILIZADO

2.1.1 Descrição da população pesquisada

Para análise da pesquisa foi desenvolvido um questionário com 10 perguntas utilizando técnicas de persuasão e de engenharia social para aplicação do primeiro ao sexto semestre, sendo as questões 1,3 e 4 baseadas no livro de Cialdini (2006) e conforme a adaptação de Pierini (2013), e as demais de autoria própria baseadas nos exemplos de técnicas de engenharia social demonstradas pelos autores citados no decorrer deste trabalho.

2.1.2 Procedimento utilizado

Foram aplicados 149 questionários, entregues pessoalmente aos alunos do Curso de Segurança da Informação, da Fatec – Americana, do primeiro ao sexto semestres, nos turnos matutino e noturno.

Para a tabulação, os questionários foram agrupados em dois grupos, os chamados de iniciantes: alunos respondentes regularmente matriculados do primeiro ao terceiro semestres e de veteranos: os alunos respondentes regularmente matriculados do quarto ao sexto semestres.

Os questionários foram tabulados, foram elaborados tabelas e gráficos para facilitar a análise dos resultados obtidos por ambos os grupos, conforme segue abaixo.

Importante destacar que as questões, serão classificadas não pelo enunciado, mas sim pela técnica utilizada pela engenharia social que consta de cada “historinha” contada nas questões e também que para o questionário não possui resposta correta, mas sim, melhores respostas para as tomadas de decisões.

OBS.: O questionário consta como apêndice.

2.2 APRESENTAÇÃO DOS DADOS

Inicia-se apresentando o número total de alunos matriculados, por semestres e o número de respondentes. Destaca-se que a Fonte de todos os gráficos e tabelas foi elaborada pela autora.

Tabela 1: Alunos matriculados e alunos respondentes

SEMETRES	ALUNOS MATRICULADOS	ALUNOS RESPONDENTES	%
Primeiro	97	30	7,56
Segundo	70	24	6,05
Terceiro	75	21	5,29
Quarto	65	28	7,05
Quinto	45	18	4,53
Sexto	45	28	7,05
Total	397	149	37,53

Observa-se que a pesquisa teve uma abrangência de 37,53% da população matriculada no curso de segurança da informação.

2.2.1 Apresentação dados dos respondentes

Os respondentes iniciantes totalizaram 75, o que representa 50,34% da população total. Quanto às idades tem-se:

Tabela 2: Idade dos respondentes iniciantes

IDADES	RESPONDENTES
18 a 20 anos	26
21 a 23 anos	17
24 a 26 anos	6
27 a 29 anos	4
Acima de 30 anos	22
Total	75

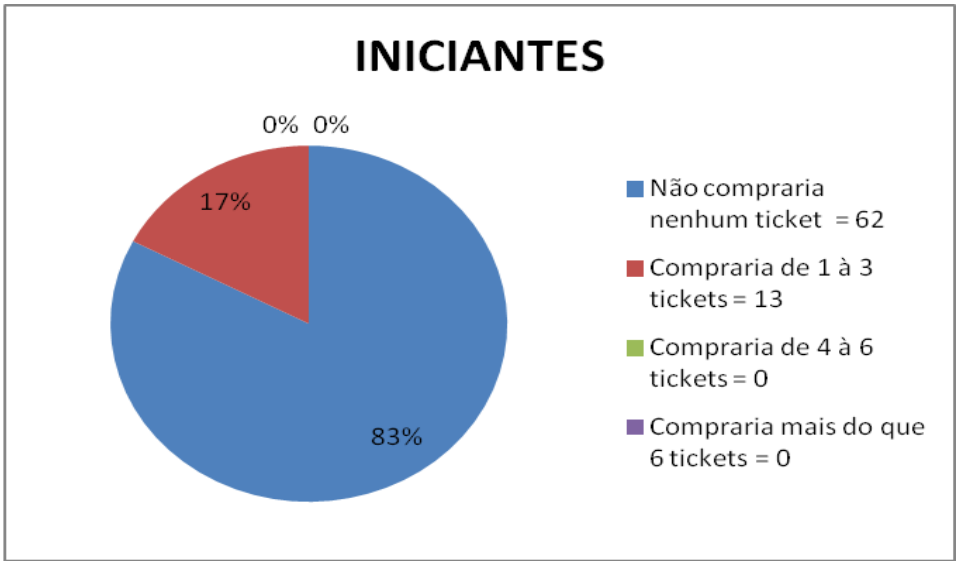
Os respondentes veteranos totalizaram 74, o que representa 49,66% da população total. Quanto às idades ficaram assim distribuídos:

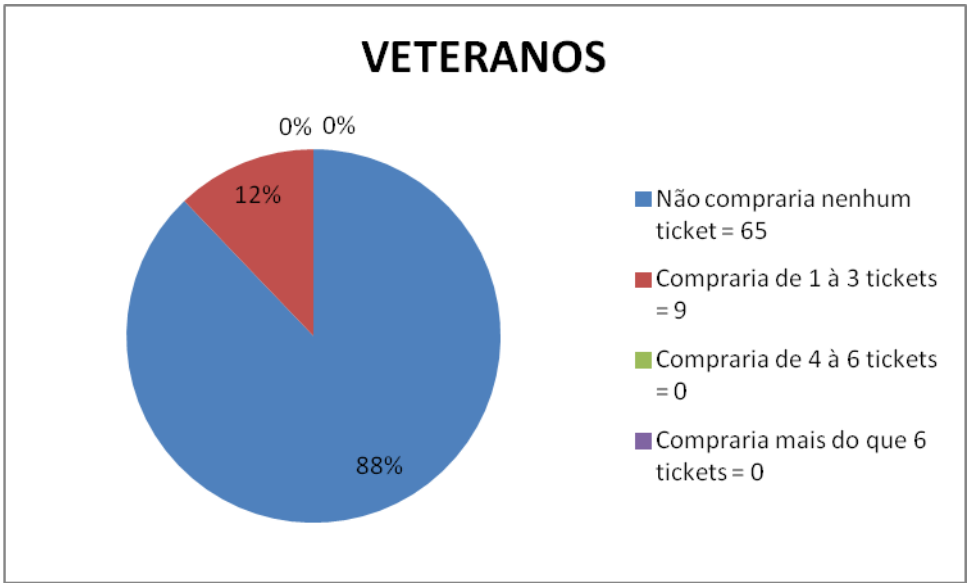
Tabela 3: Idade dos respondentes veteranos

IDADES	RESPONDENTES
18 a 20 anos	14
21 a 23 anos	25
24 a 26 anos	10
27 a 29 anos	11
Acima de 30 anos	14
Total	74

Percebe-se que a maioria dos respondentes estão no que a teoria chama de geração Y, que tem uma característica a ser destacada aqui: vivem com sobrecarga de informações, dificultando a correlação de conteúdos, o que pode auxiliar na compreensão das respostas que vem a seguir, porém não as justificam.

Gráficos 1: Princípios de Reciprocidade: Iniciantes e Veteranos





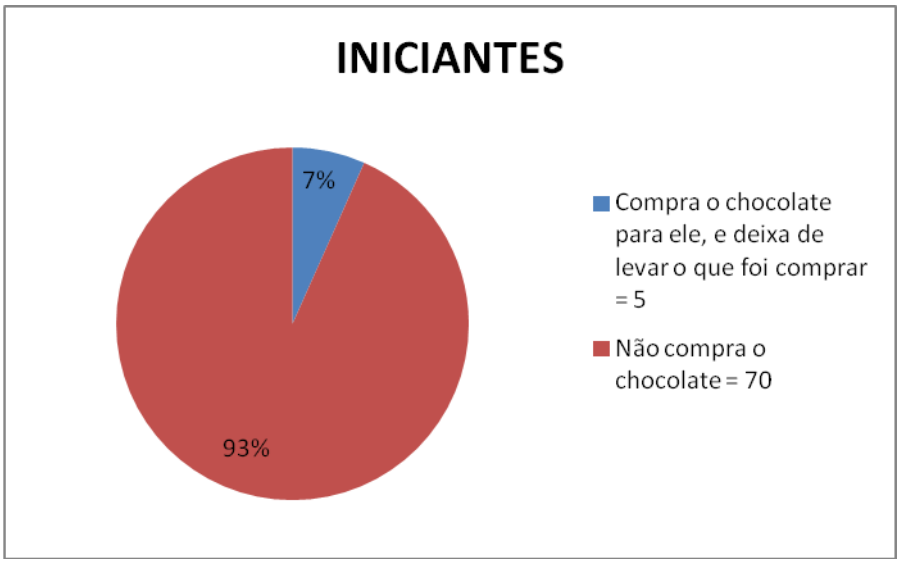
A questão pode ser analisada de duas maneiras, na visão da psicologia social que compreende a reciprocidade como valorizada socialmente, pois as relações mútuas contribuem para a conservação de normas sociais. É apresentada como uma norma imprescindível para uma convivência saudável. Na visão das teorias dos princípios de persuasão relacionadas com a engenharia social ela está relacionada com o “dar e receber”, compreendida como uma regra de retribuir da mesma maneira que recebeu. O que faz com que o indivíduo sinta-se na “obrigação” de retribuir. O que a psicologia chama de manipulação.

Na questão um, a o atacante, após pagar uma bebida para vítima, oferece para a outra pessoa que compre os *tickets*, pois não poderá participar. As técnicas do atacante se enquadram de início dentro do princípio de simpatia, pois conforme a afirmação de Cialdini (2006) e esse quando utilizado por estranhos mal intencionados, será com o propósito de que a vítima aceite o pedido proposto.

Começa a conversar com a vítima e em seguida adota o princípio da reciprocidade, quando o atacante paga a vítima uma bebida, essa gentileza tem como propósito, que a mesma, ao longo da conversa, se sinta agradecida e em dívida com sujeito, aceitando comprar alguns *tickets* no momento em que forem oferecidos.

Nota-se que os resultados obtidos entre Iniciantes de Veteranos foram similares, em ambos os grupos houve uma frequência maior de alunos com 83% Iniciantes e 88% Veteranos que não comprariam nenhum *ticket*, não sendo influenciados por esse princípio da persuasão e apenas 17% e 12% comprariam entre 1 a 3 *tickets* para ajudar o sujeito a boas intenções, sendo assim, a diferença foi mínima de 5%.

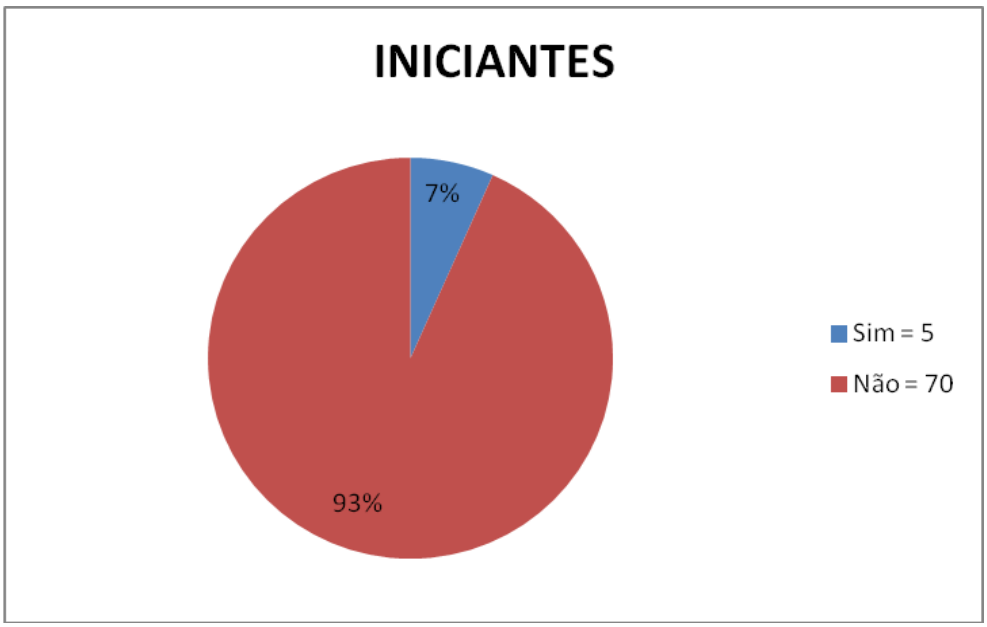
Gráficos 2: Princípios da Manipulação: Iniciantes e Veteranos

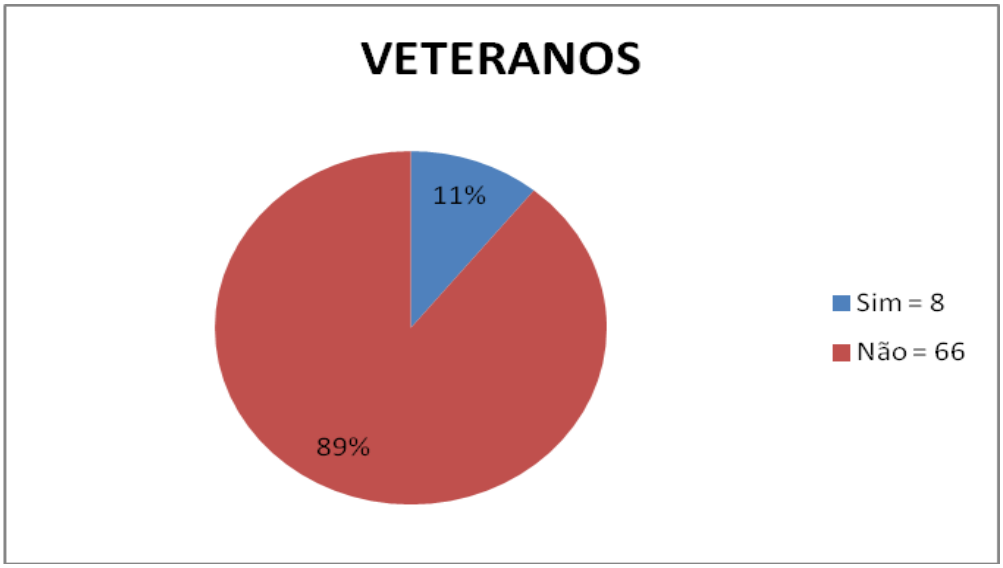


Importante destacar que a manipulação, estratégia utilizada por crianças e adultos, diz respeito a um comportamento arbitrário por parte de quem utiliza tal artifício. A maioria dos autores que estudam o assunto acredita que a manipulação seja um conjunto de ações desonestas e altamente agressivas, em função de ser utilizada para que alguém mude seu comportamento e/ou opinião para beneficiar o manipulador.

Kevin e Simon (2006 p.206), dizem que os próprios filhos são manipuladores, e possuem habilidades similares às utilizadas pelos engenheiros sociais, e que essas somente são deixadas quando eles amadurecem e se socializam. Afirma também que "Todo pai já foi alvo do ataque de um filho. Quando um jovem quer muito alguma coisa, pode ser incansável, chegando ao ponto de incomodar demais".

Gráficos 3: Princípios da Prova Social: Iniciantes e Veteranos





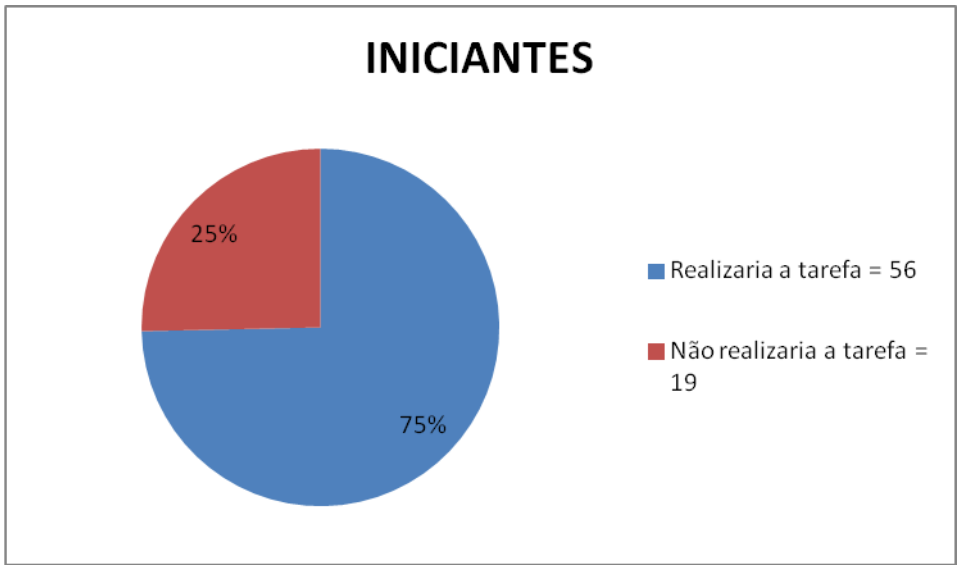
Como informado esse princípio irá se basear no julgamento feito pelo ser humano sobre as ações ou decisões mais adequadas conforme o que as demais pessoas julgam correto.

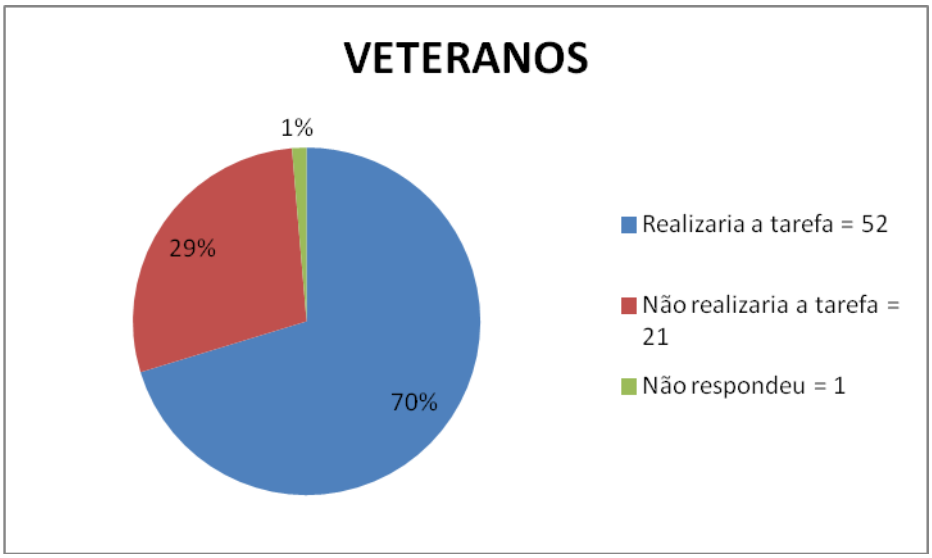
Na questão, o modelo de celular aprovado por familiares e amigos, demonstra esse princípio em ação, sobre a influência do entrevistado, se aceitaria ou não comprar outro celular somente porque os demais o têm, mesmo contendo basicamente as mesmas funcionalidades que o mesmo já possui.

Para não ceder a esse princípio a não compra do aparelho de telefone celular, se enquadraria como sendo a mais adequada, e nota-se que a maior parte dos entrevistados tanto do grupo de iniciantes quanto do grupo de veteranos também teve um resultado semelhante, com um aumento de apenas 4% dos entrevistados que comprariam o celular.

Nota-se que dos Iniciantes 7% comprariam o aparelho enquanto para os veteranos, esse valor subiu para 11% dos alunos. Que não comprariam o aparelho não deixando ser influenciados pelo princípio de persuasão foram 93% dos iniciantes e 89% dos veteranos.

Gráficos 4: Princípios da Autoridade: Iniciantes e Veteranos





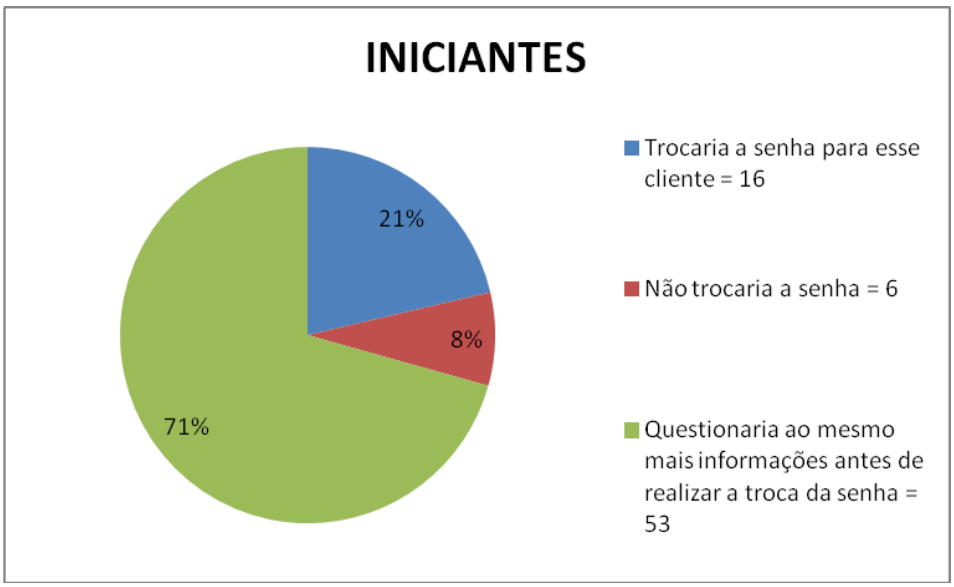
É surpreendente como o ser humano segue as ordens de alguém com um poder maior de autoridade, como gerentes, supervisores, diretores, presidentes, pais, policiais dentre outros.

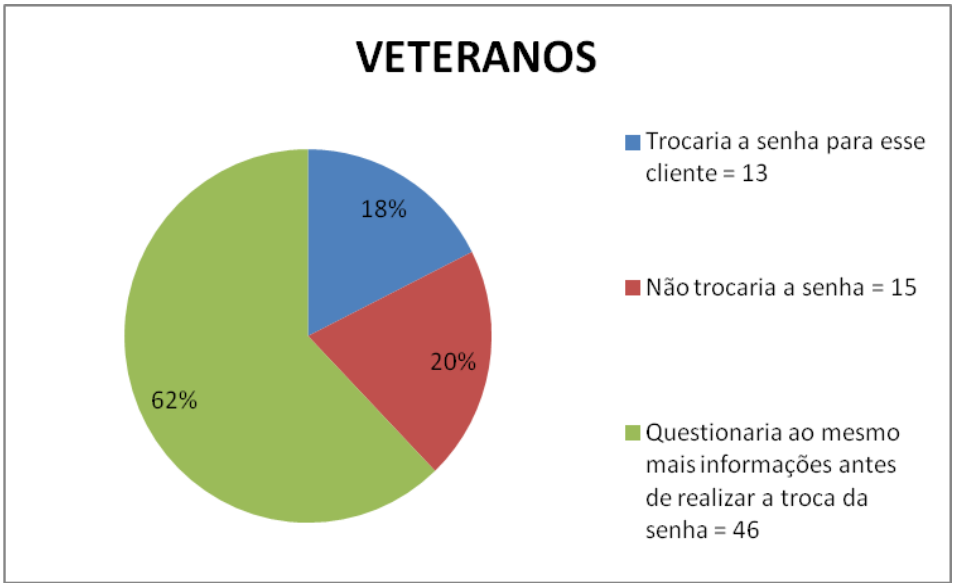
Esse princípio gera a aceitação e obediência quando feito por alguém com autoridade, Cialdini (2006) afirma que as vestes da pessoa também irão influenciar nesse poder.

No questionário essa questão teve uma grande influência nos grupos demonstrados, um pouco mais para os iniciantes do que para os veteranos, 75% dos iniciantes realizariam a tarefa passada pelo chefe, mesmo que isso prejudicasse outra pessoa, enquanto 70% dos veteranos realizariam.

Para os iniciantes 25% dos entrevistados não iriam realizar a tarefa comparado a 29% dos veteranos que não realizariam e 1% que não respondeu o questionário, para não deixar ser influenciada por esse princípio, a tarefa não poderia ser realizada. Notar também que de acordo com a técnica de engenharia social inversa citada acima, na visão de Lennert e Oliveira (2011), o engenheiro poderia se passar por uma autoridade de poder e conseguir essas informações do funcionário, por exemplo, com apenas uma ligação.

Gráficos 5: Técnica pretexto ou você pode me ajudar? : Iniciantes e Veteranos

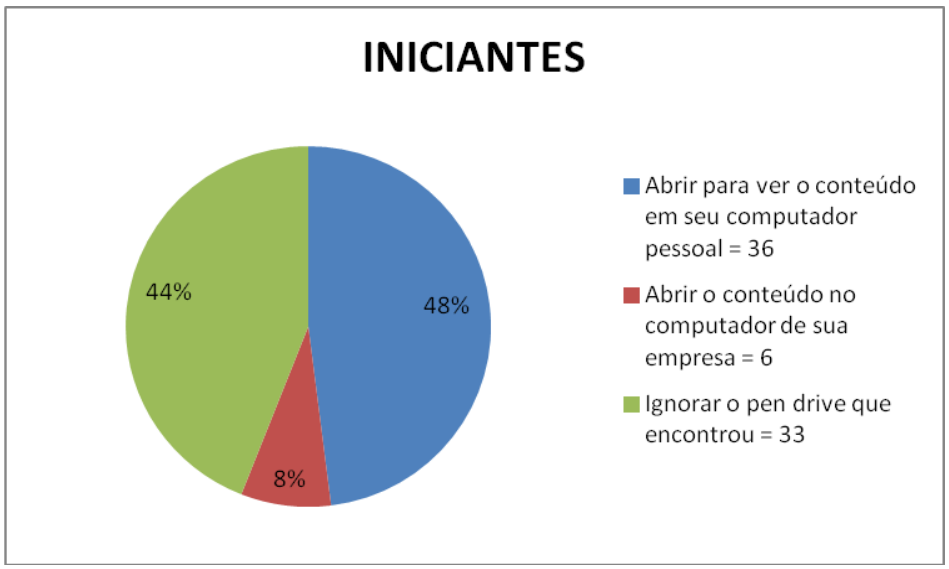


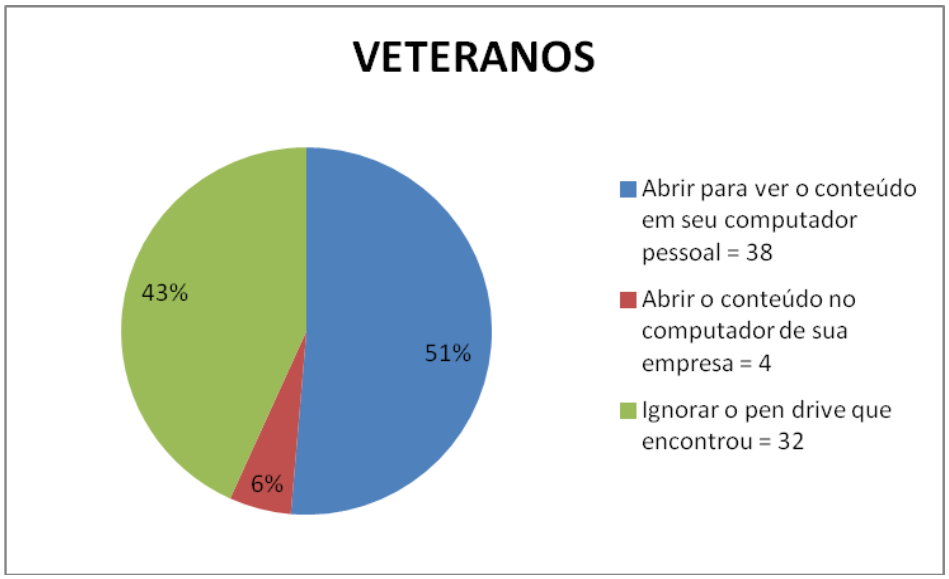


Para essa técnica o engenheiro não irá ficar tão exposto, como em algumas outras técnicas, como afirmado por Lennert e Oliveira (2011) e Goodrich e Tamassia (2013), o atacante irá criar um cenário ou um pretexto para conseguir as informações que precisa da vítima, no exemplo, do questionário atacante se passa pelo suposto cliente, que precisa de ajuda, pois esqueceu a sua própria senha, para esse ataque, o mesmo já possui todo um cenário criado, pois estudou a vítima para o ataque e atuação.

Na análise dos dados obtidos para essa questão, houve uma diferença um pouco maior entre os resultados, para as pessoas que trocariam a senha para esse suposto cliente, constou 21% dos alunos do grupo de iniciantes e 18% do grupo dos veteranos, entre alunos que não trocariam a senha para o cliente ficou com 8% para os iniciantes e uma porcentagem um pouco maior para os veteranos de 20%, e dos que questionariam mais informações antes de realizar a troca, dependendo de como se aplicam as políticas de segurança da informação da empresa, por exemplo, de poder ou não trocar a senha para o cliente, após definidas pela organização, nos resultados ficou com 71% dos iniciantes e 62% dos veteranos. Para essa questão as opções mais apropriadas seriam não trocar a senha e questionar mais informações antes de realizar a troca dependendo da política de segurança da organização.

Gráficos 6: Técnica Isca (*Baiting*) : Iniciantes e Veteranos





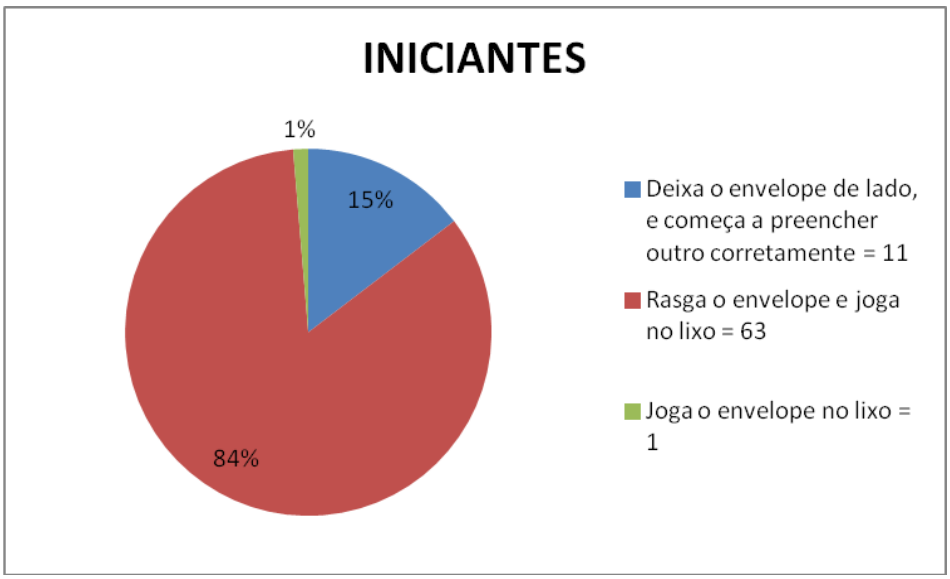
Essa técnica utilizada pelo engenheiro irá tentar atingir a característica da curiosidade da vítima, assim como a afirmação “o peixe morre pela boca”, deixando uma isca na água para fisgar no momento certo, o atacante irá deixar uma mídia USB, ou algum outro tipo em um local de interesse para que alguém o pegue e de padrão abra ou no computador pessoal ou da empresa.

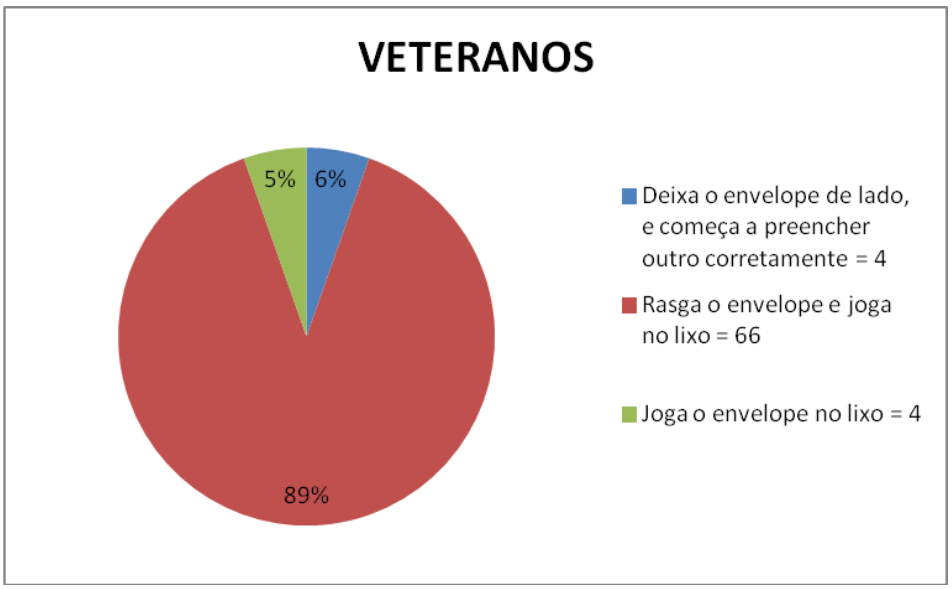
Na questão apresentada constaram três alternativas, onde o entrevistado poderia escolher entre abrir o *pen drive* no computador pessoal, no da empresa ou ignorá-lo.

A diferença dos alunos de ambos os grupos que ignoraria o *pen drive* foi mínima de 1%, 44% dos iniciantes ignorariam e 43% dos veteranos. Dentre as alternativas para abrir o conteúdo, sendo na empresa 8% dos iniciantes comparado a 6% dos veteranos, uma diferença mínima também de 2%.

A alternativa respondida foi para abrir o *pen drive* no computador pessoal, alguns descreveram essa possibilidade de abri-lo em uma Máquina Virtual. Segundo os autores Goodrich e Tamassia (2013) não abrir o pen drive nessas situações seria a melhor maneira de garantir a segurança.

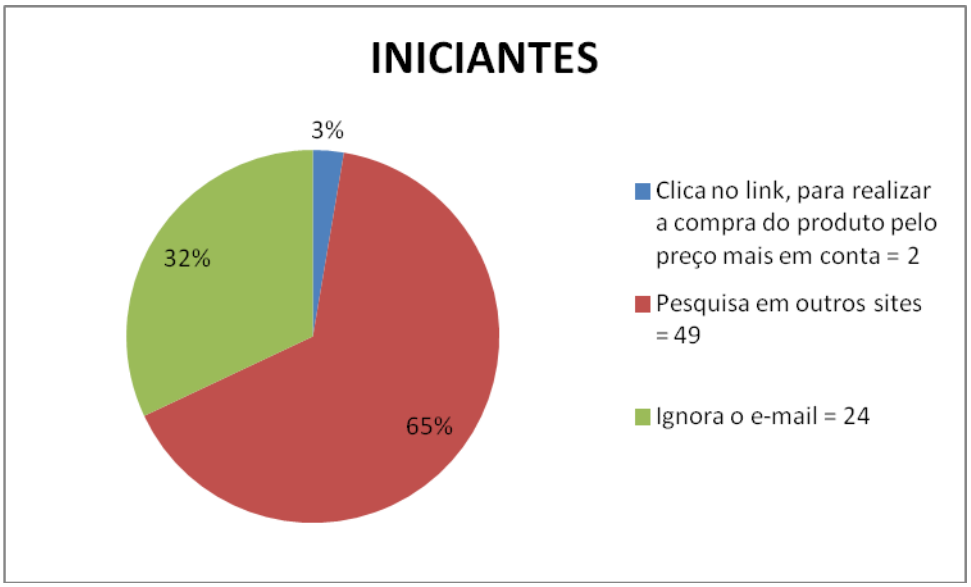
Gráficos 7: Técnica do Lixo: Iniciantes e Veteranos

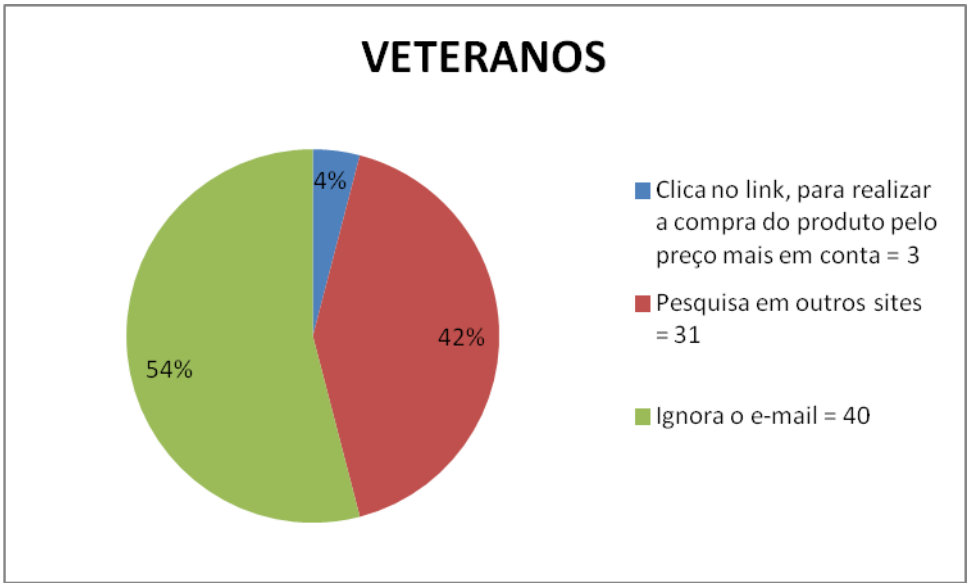




No exemplo descrito por Peixoto (2006), fica como um conselho para empresas que descartam o lixo de maneira incorreta, pois o que pode não servir para elas, poderá ser usado como um triunfo para aqueles que buscam alguma vulnerabilidade na organização. No questionário apresentado, aborda como a pessoa irá descartar seu próprio lixo. O entrevistado vai ao banco para realizar um depósito e esse preenche algumas informações incorretas, devido não poder utilizar rasura, esse envelope teria que ser descartado. Para os alunos dentre as alternativas apresentadas 1% do grupo de iniciantes jogaria o envelope no lixo, comprado a 5% dos veteranos. Para alternativa de deixar o envelope de lado, 15% dos iniciantes, com uma queda de 9% para o grupo de veteranos 6%. A alternativa com mais respostas seria a mais aconselhada na maneira de descarte do lixo, pois essa consiste em rasgar o envelope e depois descartá-lo no lixo, dificultando assim caso algum engenheiro, por exemplo, fosse vasculhar. Essa alternativa teve 84% dos iniciantes e 89% dos veteranos.

Gráficos 8: Técnica *Pishing* (Pescador): Iniciantes e Veteranos

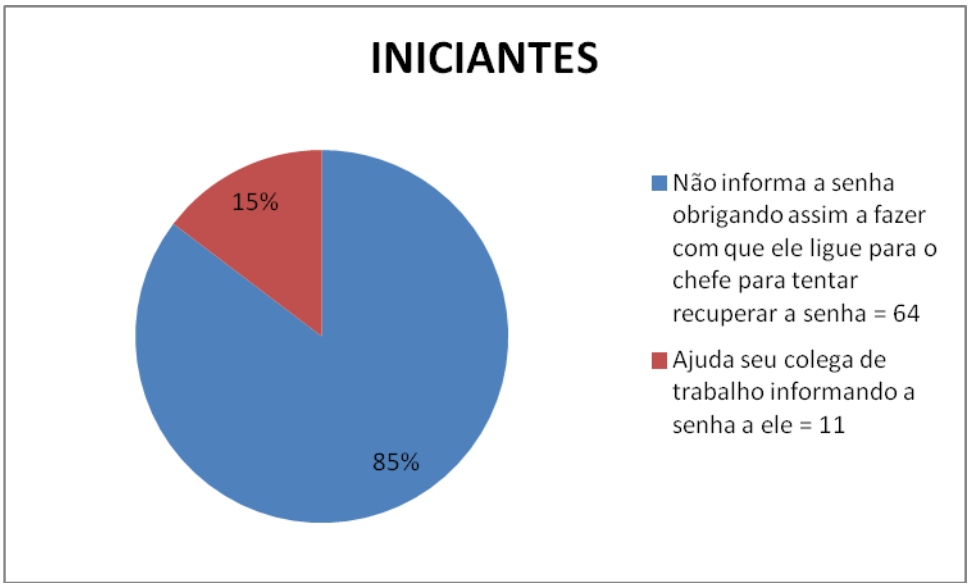


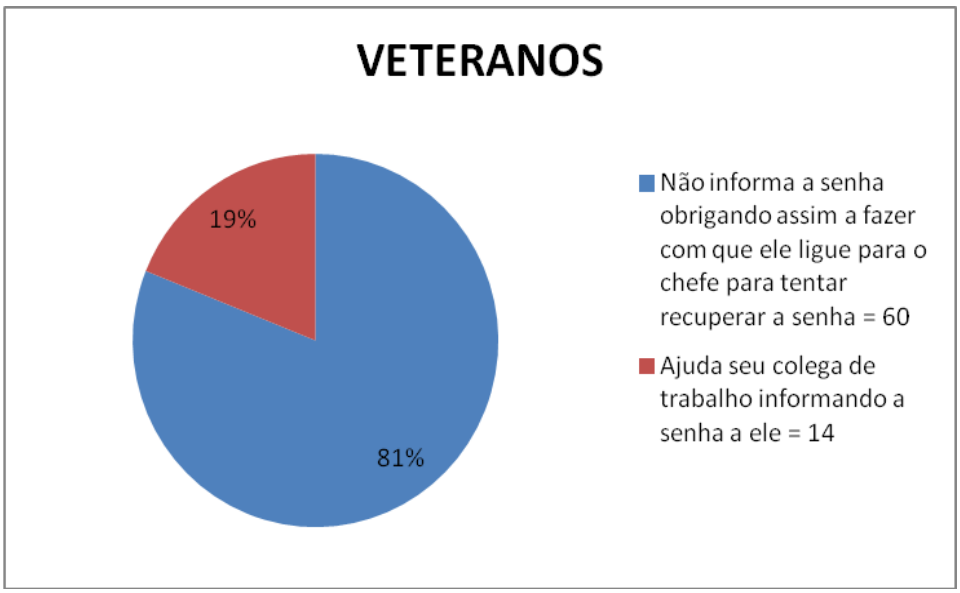


Essa técnica é muito utilizada para fraudes bancárias, utilizando páginas falsas de bancos, companhias aéreas, geralmente essa é feita pelo envio de *e-mail* a vítima, na qual terá o propósito de essa, clique no *link* e preencha as informações na página direcionada, com essa intenção, utilizando um site da compra de um produto de pesquisas anteriores pela vítima.

A questão também mostra três possibilidades de resposta, 32% dos entrevistados iniciantes ignorariam o *e-mail*, enquanto um aumento significativo de 22%, sendo esse 54% dos veteranos também ignoraria esse *e-mail*, sendo essa uma das opções aconselhadas. A pesquisa em outros sites para comparação foi de 65% dos iniciantes e 42% dos veteranos. Já para a alternativa para clicar no link e verificar o conteúdo, apenas 3% dos iniciantes e 4% dos veteranos escolheriam a alternativa não recomendada.

Gráficos 9: Técnica Simplesmente pedindo: Iniciantes e Veteranos



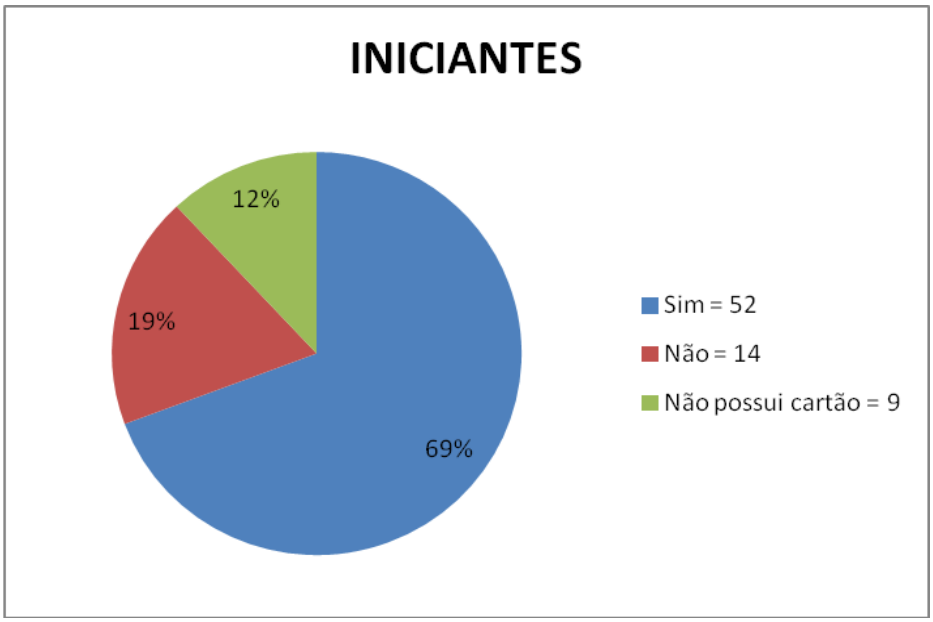


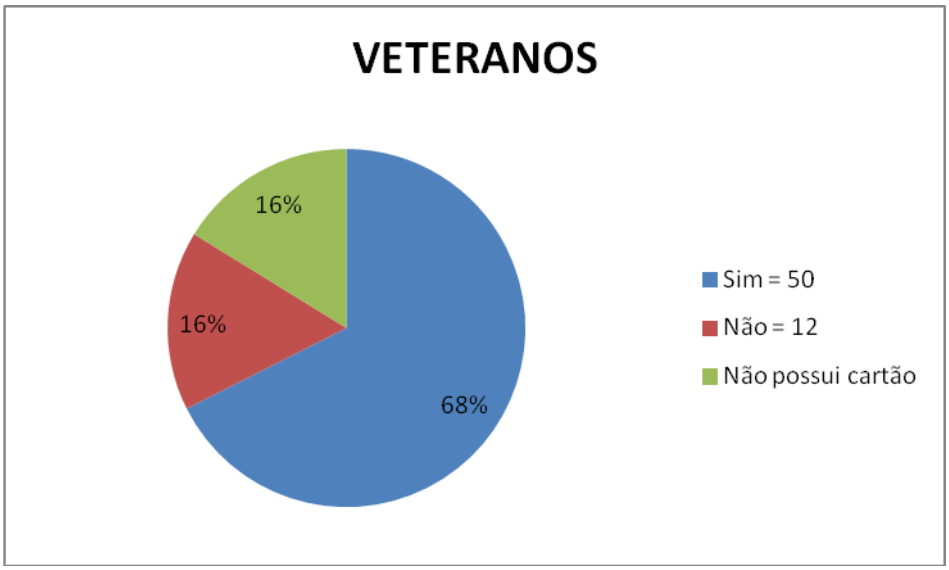
Para essa técnica, não precisa de muita manipulação ou persuasão, a simpatia e um pouco de conhecimento sobre o ambiente e jargão podem facilitar para o atacante.

Na questão apresentada, um suposto colega de trabalho que precisou ficar até mais tarde com o entrevistado, e de última hora ele infelizmente irá precisar ficar até mais tarde, e por não mais se lembrar da senha pessoal, pede a senha para poder fechar a empresa. Dentre as alternativas, apenas 15% dos entrevistados iniciantes ajudariam o colega, e 19% dos veteranos ajudariam. A alternativa correta seria não passar a senha, conforme a política de segurança da informação algumas

empresas essa prática pode não ser autorizada, 85% dos iniciantes não informaria a senha, e 81% dos veteranos também não.

Gráficos 10: Percepção do perigo (Vulnerabilidade): Iniciantes e Veteranos





A questão foi acionada como um alerta aos usuários de cartões de créditos, pois em caso de perda e/ou furto, o indivíduo poderá ser lesado, pois o código no verso do cartão é um “passaporte” para as compras *online.*

CONSIDERAÇÕES FINAIS

A partir da apresentação dos dados e sua análise, observa-se que, no decorrer do Curso de Segurança da Informação não houve diferença significativa no tocante a uma estratégia que deveria estar absorvida, principalmente, pelos alunos veteranos.

Nota-se que as mesmas escolhas foram feitas em ambos os grupos, fazendo com que os resultados dos iniciantes e veteranos fossem parecidos também nas alternativas escolhidas, o que deve ser preocupante para o curso e deixa uma série de questões para o grupo de docentes possa se debruçar, tais como: a matriz curricular deveria ser revista? O que está faltando para que os alunos absorvam um conteúdo tão importante para a sua futura vida profissional? Dentre inúmeras outras questões que poderiam ser feitas.

Outra questão importante diz respeito ao número de alunos, tanto do primeiro ao terceiro semestre, quanto do quarto ao sexto que responderam as questões quatro e seis, relacionadas ao princípio de autoridade e das técnicas de engenharia social Isca (*Baiting*), nota-se que ambos os grupos responderam alternativas que não seriam mais aconselhadas de acordo com a visão dos autores estudados, pois, de acordo com a questão quatro, realizando a tarefa dita pelo chefe, estaria sendo influenciada pelo princípio de autoridade, e já a questão seis o mais adequado seria não abrir o *pen drive* no computador pessoal e também não abrir no da empresa. Sendo assim a alternativa de número três, ignorar o pen drive que encontrou seria a melhor alternativa.

Atrelada às questões acima citadas, pode-se hipotetizar que se na matriz curricular do curso tivesse um número significativo de disciplinas que enfatizassem questões da engenharia social, os resultados poderiam ter sido mais significativos, gerando assim uma diferença entre os semestres iniciantes e os veteranos. Esse fator também pode não ter sido conclusivo devido à personalidade e caráter de cada um.

Por outro lado nota-se que essas técnicas realmente funcionam contra o ser humano, principalmente quando a ignorância, a credulidade, o desejo de ser amado e de ser prestativo “entram em jogo”, conforme a afirmação dos autores no estudo bibliográfico.

Infelizmente, ao serem analisadas as questões não houve uma diferença que pudesse considerar o resultado como conclusivo, mas, por outro lado, oito das dez questões foram respondidas corretamente por ambos os semestres.

Quanto à população estudada, observa-se exatamente o que ocorre em tantos outros locais de trabalho, isto é, a utilização da engenharia social e que os princípios de persuasão podem influenciar o ser humano e com isso comprometer a confidencialidade, integridade e disponibilidade da informação.

Foi possível, através do estudo e da análise dos dados notar que não houve uma grande contribuição da formação acadêmica nas respostas obtidas pelo questionário, considerando a diferença mínima entre as resposta dos iniciantes e veteranos.

Para o estudo a hipótese (d) foi à correta, onde se afirmou que o resultado da comparação dos semestres poderia ser similar entre os grupos, com uma diferença mínima, sendo assim não conclusivas.

Conclui-se, como a afirmação de Peixoto (2006) que, que a engenharia social está entre um dos maiores desafios da segurança da informação atingindo diretamente o fator humano, sendo esse o elo mais fraco, e que somente a formação acadêmica não irá determinar as decisões de um possível ataque de engenharia social.

Como sugestão para trabalhos futuros, poderia se aplicado esse mesmo questionário em profissionais da área formados, ou em funcionários de empresas para estudar a importância de treinamentos nas organizações. Outra sugestão diz respeito ao estudo da Engenharia Social atrelada à Geração Y, considerando que são extremamente informais, agitados, ansiosos e impacientes e imediatistas e

acompanham a velocidade da Internet, nesse caso o mesmo instrumento poderia ser utilizado. E finalmente, estudar a influência dos contos infantis na formação dos indivíduos, visto que nas histórias infantis o vilão manipula e utiliza a arte da persuasão para atingir seus objetivos, sugestão pensada a partir da questão de número 2.

REFERÊNCIAS BIBLIOGRÁFICAS

CARTILHA DE SEGURANÇA PARA INTERNET. (2012). **Golpes na Internet.** Disponível em: http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 04 out. 2015. p. 9-10 e 28.

CIALDINI, Robert B. **O poder da persuasão:** você pode ser mais influente do que imagina. Tradução Marcello Lino. Rio de Janeiro: Elsevier e São Paulo: HSM. 2006. p. 11-13; 17-19; 56-59; 66; 114-117; 164; 167-173; 184-190; 206-208.

DISCOVERY CHANNEL. **Hackers Anjos e Criminosos.** (2009). Disponível em: https://www.youtube.com/watch?v=vLulG30EM9c. Acesso em: 06 novembro 2015.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio Tadeu de. **Política de Segurança da Informação:** Guia prático para elaboração e implementação. Riachuelo/RJ: Ciência Moderna. 2008. p. 9 e 36.

FONTES, Edison. **Segurança da Informação:** O usuário faz a diferença. São Paulo: Saraiva. 2006. Introdução; p. 1 e 10-12.

GOODRICH, Michael T. & TAMASSIA, Roberto. **Introdução à Segurança de Computadores.** Tradução Maria Lúcia Blanck Lisbôa. Porto Alegre/RS: Bookman. 2013. p. 2; 4-6; 41-43 e 438.

KAUARK, Fabiana da Silva; MANHÃES, Fernanda Castro e MEDEIROS, Carlos Henrique. **Metodologia da pesquisa:** um guia prático. Itabuna/BA: Via Litterarum. 2010, p. 26, 28 e 29.

LENNERT, Luiz Sérgio e OLIVEIRA, Marcos Altemari de. **Engenharia social:** uma ameaça fraudulenta crescente. Revista Gestão de Riscos. 64ª ed. São Paulo: BM Design. 2011, p. 23-27.

MANN, Ian. **Engenharia Social.** São Paulo: Edgard Blucher. 2011. p. 19; 46-49.

MARCONI, Marina de Andrade e LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5º ed. São Paulo: Atlas S.A. 2003, p. 188.

MITNICK, Kevin D. e SIMON, Willian L. **A arte de enganar.** Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. Tradução Kátia Aparecida Roque. 4º reimpr. São Paulo: Pearson. 2003. p. . xiii; 3-6; 17-24; 32; 42-44; 63-65; 77; 85; 114-116; 195-198; 205-210.

MITNICK _____. **A arte de invadir:** As verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos. Tradução Maria Lúcia G.. São Paulo: Pearson. 2003. p. . 206.

NEVES, José Luis. **Pesquisa Qualitativa** – Características, Usos e Possibilidades. Caderno de Pesquisa em Administração. São Paulo. 1996. v.1, nº3. p. 1.

PEIXOTO, Mário César Pintaudi. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport. 2006, p. 3-12; 36-30; 45.

PIERINI, Rodrigo Alexandre de Andrade. **Persuasão em engenharia social.** Monografia (Graduação de Tecnologia em Segurança da Informação) Americana: Biblioteca - FATEC Americana 2013.

PRODANOV, Cleber Cristiano e FREITAS, Ernani Cesar de. **Metodologia do trabalho científico:** Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. 2º ed. Novo Hamburgo/RS: Universidade Feevale. 2013, p. 34-36.

RAFAEL, Gustavo de Castro. **Engenharia Social**: As técnicas de Ataque mais Utilizadas. Disponível em: http://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/. Acesso em: 26 out. 2015. 23h15.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** Uma Visão Executiva. Rio de Janeiro: Elsevier. 2003, p. 1; 7; 43-52.

QUESTIONÁRIO DE SEGURANÇA DA INFORMAÇÃO

Eu Mayara de Lourdes Alves, aluna regularmente matriculado no 6º Semestre do Curso Superior de Tecnologia em Segurança da Informação, estou desenvolvendo meu Trabalho Monográfico que tem por objetivo: “estudar e pesquisar o conhecimento que os alunos do Curso Superior de Tecnologia em Segurança da Informação da Fatec – Americana do primeiro ao sexto semestre tem sobre “enganar e invadir” utilizadas por engenheiros sociais, buscando compreender a contribuição que a formação acadêmica proporcionou aos mesmos”. Para tanto solicito sua colaboração respondendo as questões abaixo. Suas respostas serão utilizadas para fins estritamente científicos.

SEMESTRE QUE VOCÊ ESTÁ MATRICULADO: _____

IDADE: _____

1) Uma pessoa que você acabou de conhecer em uma lanchonete lhe paga uma bebida e começa conversar com você. Após algum tempo conversando, a pessoa diz que está com uma cartela com 6 tickets, de um sorteio de um carro que ocorrerá no centro da cidade e que não poderá participar, mas pede que você compre o ticket que custa 5 reais cada. Você:

( ) Não compraria nenhum ticket ( ) Compraria de 1 à 3 tickets

( ) Compraria de 4 à 6 tickets ( ) Compraria mais do que 6 tickets

2) Você vai ao supermercado com seu filho e o mesmo vê um chocolate na prateleira, você informa a ele que não pode pegar no momento pois levou o dinheiro contado para o que foi comprar, porém o mesmo não entende e começa a falar mais alto, e depois um escândalo até chamar a atenção, você então:

( ) Compra o chocolate para ele, e deixa de levar o que foi comprar.

( ) Não compra o chocolate.

3) Suponha que várias pessoas do seu circulo social (família, colega de trabalho, amigos, etc.) compraram um novo modelo de celular com um preço relativamente igual e com basicamente as mesmas funcionalidades que o seu celular atual, sem quaisquer diferenças notáveis. Com o passar do tempo, você percebe que o celular começa a se tornar o assunto das conversas corriqueiras dessas pessoas. Caso você tivesse a chance de trocar o seu celular por um celular do mesmo modelo, você trocaria o aparelho?

( ) Sim ( ) Não

4) Seu chefe lhe atribui uma tarefa. Você percebe que essa tarefa pode não dar certo ou possa prejudicar algum outro colega de trabalho de alguma maneira. Então você conversa com seu chefe sobre as possíveis falhas e as consequências daquela tarefa, mas ele, invariavelmente, diz que aquela tarefa precisa ser realizada e da maneira especificada. Você:

( ) Realizaria a tarefa ( ) Não realizaria a tarefa

5) Supondo que você trabalha no suporte técnico de uma empresa, e recebe uma ligação de um cliente, para qual vocês oferecem suporte, o mesmo informa não se lembrar mais de sua senha, você questiona ao mesmo algumas informações pessoais como: nome dos pais, idade, data de nascimento, nome completo e número de telefone e o mesmo confirma todas corretamente, então após isso você:

( ) Trocaria a senha para esse cliente. ( ) Não trocaria a senha.

( ) Questionaria ao mesmo mais informações antes de realizar a troca da senha.

6) Em um dia indo para o trabalho você se depara com um pen drive de 32GB no estacionamento com a descrição de um software em lançamento que você tanto estava esperando e não pode comprar, devido ao preço você irá:

( ) Abrir para ver o conteúdo em seu computador pessoal.

( ) Abrir o conteúdo no computador de sua empresa.

( ) Ignorar o pen drive que encontrou.

7) Você vai ao banco para depositar o dinheiro na compra de um Nintendo 3DS, ao preencher quase todas as informações como, número da conta, nome completo, você percebe que errou nas informações do nome da pessoa que irá receber o envelope, e esse não pode ser rasurado, então você:

( ) Deixa o envelope de lado, e começa a preencher outro corretamente

( ) Rasga o envelope e joga no lixo ( ) Joga o envelope no lixo.

8) Ao abrir o seu e-mail você nota que recebeu um e-mail com a oferta de um produto que estava pesquisando para comprar já faz algum tempo, e no anúncio está por um preço bem mais em conta, junto a ele consta o link para o site da compra, então você:

( ) Clica no link, para realizar a compra do produto pelo preço mais em conta.

( ) Pesquisa em outros sites. ( ) Ignora o e-mail.

9) Você e um colega de trabalho são os últimos a sair da empresa, pois tiveram que ficar até mais tarde para a atualização de um software em um cliente, na saída seu colega informa que esqueceu a senha dele e pede se você pode informar a sua para ele fechar a empresa, pois surgiu um imprevisto e ele ficará até mais tarde, você:

( ) Não informa a senha obrigando assim a fazer com que ele ligue para o chefe para tentar recuperar a senha.

( ) Ajuda seu colega de trabalho informando a senha a ele.

10) Se você tem cartão de credito, responda a pergunta: Seu cartão tem código de segurança no verso?

( ) sim ( ) não