Faculdade de Tecnologia de Americana

Curso de Segurança da Informação

ENGENHARIA SOCIAL

LÍGIA TEIXEIRA

Americana, SP

2011

Faculdade de Tecnologia de Americana

Curso de Segurança da Informação

ENGENHARIA SOCIAL

LÍGIA TEIXEIRA

furlanetto.ligia@gmail.com

Trabalho de conclusão de curso para
obtenção de
grau de
Tecnólogo em segurança da Informação

Professor Orientador:
Humberto Celeste Innarelli

Americana, SP

2011

FICHA CATALOGRÁFICA elaborada pela
BIBLIOTECA – FATEC Americana – CEETPS

Teixeira, Lígia
T266e Engenharia social. / Lígia Teixeira. – Americana: 2011.
69f.

Monografia (Graduação em Análise de Sistemas e Tecnologia da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Ms. Humberto Celeste Innarelli

1. Segurança em sistemas de informação I. Innarelli, Humberto Celeste II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Bibliotecária responsável Ana Valquiria Niaradi – CRB-8 região 6203

Banca Examinadora

Orientador: Humberto Celeste Innarelli

Convidado: Irineu Ambrozano Filho

Presidente: Benedito Aparecido Cruz

"O preço da liberdade é a eterna vigilância".

Thomas Jefferson

Agradecimentos

Agradeço ao Professor Humberto Celeste Innarelli pelo auxilio e apoio na construção deste documento.

Agradeço também ao Professor Irineu Ambrozano Filho pelo auxilio durantes as aulas de Projeto Articulador de Segurança da Informação.

Agradeço ao meu amigo Jose Luis Schifferli Lopes, pela ajuda, apoio e dicas que me ajudaram na construção deste documento.

Agradeço aos meus amigos da faculdade: Leonys, Mariana e Natália, pela participação na minha vida acadêmica e pela amizade que se traçou durante este período.

Porém, agradeço principalmente ao meu noivo Rogério Nunes de Freitas, por estar ao meu lado nos momentos difíceis, me apoiar e me ajudar durante toda a minha caminhada acadêmica.

Dedicatória

Prefiro não dedicar esta monografia a ninguém em especial e sim aos profissionais e alunos que venham a utilizar este presente documento. Espero que as informações aqui contidas possam auxiliar e esclarecer dúvidas sobre o assunto.

Resumo

Nenhuma política de segurança está completa sem abordar o tema engenharia social, que consiste em uma técnica de roubo de informações com uso de ferramentas como persuasão e pesquisa. Apesar de sua importância a engenharia social ainda é pouco abordada, principalmente por profissionais da área administrativa. A principal visão do mercado atual em relação à engenharia social é acreditar que ela seja responsabilidade exclusiva dos profissionais de Tecnologia da Informação, deixando assim todos os outros departamentos da empresa vulneráveis a ataques, afinal é o elo fraco da corrente que provavelmente quebrará a política de segurança e colocará a empresa em perigo. Muitos casos reais apontam que a falta de preparação dos profissionais é a causa de incidentes com engenharia social. Muitos dos golpes hoje aplicados para fraudes e roubos de informação existem e são usados há muito tempo e ainda assim continuam fazendo vítimas.

Palavras Chave: Engenharia Social, Manipulação e persuasão.

Abstract

No security policy is complete without approaching the social engineering theme, that consists in an information theft technique with tools like persuasion and research. Despite its importance, the social engineering is still very little used, specially by the professionals in the administrative area. The main view of the current market about social engineering is to belive that it is a responsibility exclusivelly of the thechnology information professionals, leaving all other departments vulnerable to attacks. Actually it is the weak link of the chain that probably break the security policy and put the company in danger. Many real cases indicate that the lack of professional training is the main cause for incidents with social engineering. Many of the coups applied today in frauds and information robbery have existed and been used for a long time and they still continue to make victims.

Keywords: Social Engineering, manipulation and persuasion.

Lista de Figuras e Tabelas

Sumário

1. Introdução

“Segurança tem início e termina nas pessoas.”
Ellen Frisch

A dramaturgia sempre utilizou a manipulação para criar mais efeito a cenas e personagens. Quem nunca chorou assistindo “A vida é bela” ou se emocionou em “Náufrago”? , Além de manipulações emocionais muitos filmes também utilizam de técnicas mais avançadas de manipulação na criação de cenas. Muitos personagens fictícios já apresentaram ao público seu poder de persuasão, manipulando situações e até mesmo outros personagens. Todos que assistiram “O auto da compadecida”, por exemplo, puderam perceber como João Grilo (personagem de Matheus Nastchergaele) manipulava outros personagens e situações, chegou a desafiar personagens perigosos como o Satanás (personagem de Luís Melo) e o Cangaceiro Severino de Aracaju (personagem de Marco Nanini). Comentários como: "ele tem lábia", "ele sabe argumentar", "ele consegue persuadir os outros personagens", são constantes quando personagens como João Grilo usam suas artimanhas em outros personagens.

Outros filmes onde manipulação e roubo de informações são o tema foram realizados, muitos destes com o tema principal voltado a tecnologia como: menina-má.com, a senha: Sworfish, Matrix e Johnny Mnemonic. Porém, nem toda a ficção destes filmes deixa de ser realidade, na verdade alguns destes filmes mostram ataques reais onde uma técnica de manipulação chamada Engenharia Social possibilitou ataques a empresas que perderam milhões. Filmes como “prenda-me se for capaz” 3.3, “Piratas no Vale do Silício” e “Caçada Virtual”, retratam esse cenário.

O tema que será abordado nesta monografia relata sobre a engenharia social, técnica usada para manipular pessoas e situações com objetivo de roubar informações e/ou fraude. Tal técnica, apesar de parecer apenas objeto dramaturgo, também faz parte da vida real e com freqüência, geralmente usado por estelionatários, ladrões, hackers e outros, para aplicar golpes, entretanto, o seu uso não se limita apenas a estes casos. Como será apresentada nos capítulos seguintes, a engenharia social também é utilizada em vários momentos da vida de uma pessoa e em várias profissões, um detetive, por exemplo, precisa de

ferramentas apresentadas pela engenharia social para obter informações de interesse de seus clientes. A maior parte da abordagem desta monografia será dada aos casos onde a engenharia social é utilizada para roubo de informações e derivados, ou seja, os casos onde a técnica auxilia em atos ilegais.

O objetivo principal desta monografia é apresentar as negligências decorrentes do envolvimento do fator humano e da engenharia social no aspecto de segurança da informação, assim como a necessidade de que todas as áreas da empresa saibam lidar com tais acontecimentos, pois, com os incidentes cada vez maiores na área computacional, mais especificamente, na parte de segurança da informação, torna-se cada vez mais necessário que se invista em métodos que auxilie na proteção de informações importantes. Tanta precaução acaba se tornando incompleta quando não se pensa no fator humano envolvido.

A necessidade de cuidados não envolve apenas os funcionários de TI da empresa, todas as áreas devem estar conscientes dos perigos e preparados para lidar com tentativas de ataques por engenharia social.

O projeto desta monografia fora executado em três fases. O primeiro passo foi à pesquisa sobre o tema, em segundo a montagem teórica que engloba toda a contextualização e definição do tema, e exemplos reais, apresentados nos tópicos:

- Engenharia Social 2
- Definindo Engenharia Social 2.1
- Motivação 2.2
- Técnicas e Vulnerabilidades 2.3
- Casos reais de Engenharia Social 3
- Golpe do bilhete premiado 3.1
- Mitnick: 3.2
- Frank Abagnale: Prenda me se for capaz 3.3
- Tragédia em realengo 3.4
- O caso de Robin Sage 3.5
- Simone Neves e os empregos na Copa 3.6

A terceira e última parte tratou de uma pesquisa realizada com alunos e professores de cursos nas áreas tecnológicas e administrativas. O resultado da

pesquisa e estáticas, assim como a conclusão da pesquisa, será apresentada a partir do capítulo 4. E para finalizar, a conclusão que se obteve ao final da construção deste documento 5.

2. Engenharia Social

“O engenheiro social emprega as mesmas técnicas persuasivas que usamos no dia-a-dia. Assumimos papéis tentamos obter credibilidade. Cobramos obrigações recíprocas. Mas o engenheiro social aplica essas técnicas de uma maneira manipuladora, enganosa, altamente antiética, freqüentemente com efeito devastador.“

Psicólogo social Dr. Brad Sagarin

“Apesar do nome, a Engenharia Social nada tem a ver com ciências exatas ou sociologia. Na verdade, trata-se de uma das mais antigas técnicas de roubo de informações importantes de pessoas descuidadas, através de uma boa conversa.” (Virinfo,2002).

Pode se considerar a existência da engenharia social tão antiga quanto à criação do homem. Na Bíblia, é possível encontrar menções ao ato. Em Gênesis três [16], por exemplo, um dos primeiros capítulos da bíblia, o qual relata a criação da terra e do ser humano, é apresentada uma conversa entre Eva e a serpente, na qual a serpente, considerada na bíblia como a mais astuta de todas as alimárias do campo criadas por Deus, convenceu Eva de que o fruto que havia sido proibido pelo criador por ser “venenoso”, na verdade abria seus olhos para o mundo e tornaria a quem comece do fruto como Deuses. A serpente realizou assim o primeiro ato de engenharia social que o homem possui conhecimento e registro. Utilizando apenas da persuasão (2.3) a serpente conseguiu manipular Eva. Claro, a serpente não sabia que esse ato poderia ser considerado “engenharia social”, seu objetivo era apenas o ato de manipular.

A engenharia social está presente na vida do ser humano praticamente desde sua infância. “Que criança nunca ouviu as histórias de chapeuzinho vermelho, branca de neve ou de João e Maria?”, pois, contos como estes apresentam técnicas e usos de engenharia social. Como em Branca de Neve onde a Bruxa se torna uma vendedora e convence Branca de neve a comer a maça envenenada. Ou em João e Maria, onde a Bruxa ilude as pobres crianças com guloseimas e doces. Em ambas as histórias, o vilão se torna aquilo que a vitima mais precisa no momento, estudando o contexto em que a vitima se encontra e procurando a melhor maneira para manipular-la. Não foi uma infeliz coincidência a casa da Bruxa em João e Maria

ser feita de doces, a Bruxa sabia que as crianças estavam com fome e sozinhas, apenas realizou o sonho de qualquer criança, doces à vontade. Nas duas histórias o final é feliz, já que apesar das vítimas serem manipuladas o golpe acabou sem êxito. Mas na vida real os prejuízos podem ser grandes e até irreversíveis. A partir de tais histórias pode-se concluir que o objetivo da engenharia social é a manipulação. Todas as técnicas que serão abordadas posteriormente são utilizadas diariamente, muitas vezes sem a intenção de fraude ou similar, mas sim, como uma atitude rotineira. Como a criança que utiliza de todos os seus artifícios em busca de convencer a mãe de que precisa de um brinquedo novo.

No contexto social, pode-se observar a existência da engenharia social em vários momentos da vida, as próprias histórias infantis ensinam as crianças o uso de tal técnica. Muitas vezes a engenharia social é utilizada sem que o executor tenha consciência de que o ato possui um nome e ferramentas que podem ser usadas para fins maiores.

Deixando os contos e histórias e passando ao contexto empresarial, e o foco em da segurança da informação, encontramos um cenário onde “informação” é um dos mais importantes patrimônios coorporativos, ou seja, cuidar da segurança informação da empresa passou a ser uma missão. Lembrando que ao falar de segurança da informação é importante englobar toda a estrutura da empresa, física e lógica. Muitas são as técnicas e ferramentas que podem ser utilizadas pelos analistas de TI para que a proteção física da empresa seja garantida, mas e o fator humano? Como garantir que as informações não sejam expostas por funcionários e colaboradores? Ou seja, onde se encaixa a engenharia social no ambiente coorporativo?

Vários especialistas alertam, sobre a importância e a necessidade de uma proteção mais ampla quando se trata de engenharia social:

“Com o crescente número de invasões sofridas pelas empresas em suas bases de dados, estas estão voltando suas atenções para a modernização de seus parques tecnológicos, com atualizações de firewalls, formas de criptografia, e muitos outros mecanismos de segurança, deixando o fator humano em segundo plano.” Popper, Marcos A. e Brignoli, Juliano T.[11].

Kevin Mitnick (capítulo 3.2), um dos hackers mais famosos do mundo admitiu ter utilizado de Engenharia Social para diversas de suas invasões, inclusive a rede da Sprint, quando se passou por um engenheiro da Nortel Networks e utilizou de

persuasão para conseguir logins e senhas de usuários. Segundo Mitnick a ameaça da engenharia social é substancial: “As pessoas deveriam saber que você pode comprar a melhor tecnologia do mundo, mas isto não protegerá sua empresa contra estas técnicas.”, também de acordo com ele a maioria das pessoas não acredita que possa sofrer um ataque de engenharia social “A maioria das pessoas acha que, por não se considerarem ingênuas, não podem ser manipuladas. Mas nada está mais longe da verdade do que isto”. [20]

“A engenharia social, propriamente dita, está inserida como um dos desafios (se não o maior deles) mais complexos no âmbito das vulnerabilidades encontradas na gestão da segurança da informação”. (Peixoto, 2006).

A partir dos próximos capítulos será possível entender a engenharia social mais a fundo e perceber que engenharia social é um tema que engloba não apenas a área computacional da empresa, todos os departamentos da empresa devem estar preparados para se proteger de possíveis golpes, ou como disse Kevin Mitnick: “a segurança não é um problema para a tecnologia — ela é um problema para as pessoas e a direção." [20]

2.1. Definindo Engenharia Social

"A segurança não é um produto, ela é um processo".
Bruce Schneier

O conceito de engenharia social é mais amplo que a breve descrição dada no capítulo anterior. Neste capítulo o tema será mais bem descrito e definido. A seguir serão apresentadas algumas definições técnicas dadas por especialistas da área de segurança sobre o tema:

"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." [8].

“O conceito de Engenharia Social resume-se em a arte de trapacear, construir métodos e estratégias de enganar em cima de informações cedidas por pessoas ou ganhar a confiança para obter informações. São ações antigas, oriundas dos tempos mais remotos que ganharam um novo termo: ENGENHARIA SOCIAL. Podemos dizer que a Engenharia Social é um tipo de ataque utilizado por crackers, onde a principal ‘arma’ utilizada é a habilidade de lhe dar com pessoas, induzindo-as a fornecer informações, executar programas e muitas vezes, fornecer senhas de acesso.” [10].

“Engenharia social é a ‘arte’ de utilizar o comportamento humano para quebrar a segurança sem que vítima sequer perceba que foi manipulada.” (SANS Intitute, [5]).

“Tentativas, com sucesso ou não, de influenciar pessoas em revelar informações ou agir de uma determinada maneira que resulte em acesso não autorizado a, ou uso não autorizado de, ou liberação não autorizada de um sistema, rede ou dados” (CISSP Official Guide).

Ou segundo Kevin Mitnick: “É um termo diferente para definir o uso de persuasão para influenciar as pessoas a concordar com um pedido.” [8]

Concluindo todas as definições apresentadas, engenharia social é quando se utiliza de técnicas para manipular o fator mais fraco da cadeia de segurança “o homem”. O fator humano sem dúvidas apresenta as mais diversas possibilidades a um engenheiro social, é mais fácil conseguir informações pedindo a um funcionário que a partir de um software. Kevin Mitnick deixou essa idéia explicita em seu depoimento ao congresso. Segundo ele a segurança é uma ilusão, investir milhões em segurança física é criar uma falsa idéia de segurança, quanto mais os especialistas dificultam as invasões que utilizam vulnerabilidades técnicas, mais os invasores exploram o elemento humano. “Quebrar um "firewall humano" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo.” ([3]).

2.2. Motivação

"Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza se isso é verdadeiro sobre o primeiro".
Albert Einstein

Falar sobre qual a motivação de um engenheiro social é uma tarefa difícil, diversos fatores podem influenciar uma invasão ou uma tentativa de manipulação. Dentre ele destacam-se:

- Curiosidade;
- Ego;
- Obter vantagem;
- Obter conhecimento;
- Obter informações valiosas;
- Vingança;
- Testar conhecimento;
- Testar o sistema;
- Desfalques financeiros;
- Destruir informações.

A história de que as invasões são realizadas apenas por dinheiro ou informações valiosas não é verídica. Frank Abagnale(3.3) deixa claro essa afirmação quando em seu livro “Prenda-me se for capaz”, expõe em um de seus casos que utilizou engenharia social para obter dinheiro de forma ilegal de um banco, entretanto não estava interessado no dinheiro envolvido e sim em “castigar” o dono do banco por ser arrogante, “Os modos de Cashman tinham me irritado, e eu simplesmente queria dar uma ferrada nele. [25]”

No tópico seguinte serão abordadas as principais técnicas que os engenheiros sociais utilizam em seus golpes, e as principais vulnerabilidades que podem ocorrer e enfraquecer uma estrutura de segurança facilitando golpes.

2.3. Técnicas e Vulnerabilidades

"Nomes, lista de ramais, endereços eletrônicos, organogramas e outros dados da empresa, comumente ficam expostos em lugares onde transitam pessoas estranhas. Um hacker pode simplesmente entrar na empresa como se fosse um técnico em manutenção ou consultor que tem livre acesso às dependências da empresa e, enquanto caminha pelos corredores, podem ir captando todas estas informações que porventura estejam expostas".

(Maia, 2002).

O fator humano pode ser considero o "elo fraco" da segurança da informação, ou seja, qualquer deslize ou erro pode provocar uma falha de toda a política de segurança, a Figura 1 representa tal afirmação. O ser humano apresenta certas características que podem ser consideradas propicias ao engenheiro social, por representarem ou possibilitarem brechas, dentre tais características, destacam-se (Junior, 2006):

- Vontade de ser útil: O ser humano procura ser Cortez ou ajudar os outros quando necessário;
- Buscar amizades: os humanos costumam se sentir bem quando elogiados, de maneira que muitas vezes ficam abertos para fornecer informações;
- Prorrogar responsabilidades: muitas vezes o ser humano considera não ser o único responsável pelo conjunto de responsabilidades ou atividades;
- Persuasão: é caracterizada pela capacidade de convencer, buscando assim a respostas desejadas para alcançar um objetivo. Isso acontece porque o ser humano possui características que o tornam vulneráveis a manipulação.

Figura 1- Elo mais fraco (Peixoto, 2006)

Além das características apresentas, outros fatores podem influenciar o ser humano e provocar fragilidades e vulnerabilidades, como o funcionário desmotivado ou descontente com a empresa em que trabalha ou simplesmente pelo funcionário não se importar com a empresa que trabalha.

“Algo que pode ser facilmente percebido é que usuários não ligam para a empresa na qual trabalha. Eles só se preocupam mesmo com o pagamento, sua avaliação e aumento de salário”. (SCHWARTAU, 2010).

“Outra grande vulnerabilidade dentro da empresa é o próprio funcionário insatisfeito, desmotivado e desvalorizado. Todo o investimento em tecnologia, treinamentos e conscientização, pode ser jogado fora se a companhia não cuidar e valorizar seus funcionários.” (PRESCOTT, 2007).

“Eu não sou criptoanalista, nem matemático. Apenas sei como as pessoas cometem erros e elas cometem sempre os mesmos erros.” (MITNICK; SIMON, 2005, traduzido por Cássio Bastos Alves [28]).

“Os seres humanos são seres imperfeitos e multifacetados. Além disso, situações de risco modificam seus comportamentos, e, decisões serão fortemente baseadas em confiança e grau de criticidade da situação.” (VARGAS, 2002).

Outros especialistas consideram os erros de segurança advindos da engenharia social frutos do excesso de ego e autoconfiança do ser humano. “A falta de consciência das pessoas a respeito das técnicas de Engenharia Social e o seu excesso de autoconfiança (pois a maioria das pessoas não se considerara ingênuas

e acham que não podem ser ludibriadas) são os principais aspectos que favorecem o sucesso da Engenharia Social.”[28].

“Mesmo aqueles que descobrem que foram atacados, dificilmente admitem o fato, com receio de prejudicarem sua reputação. Na Inglaterra, por exemplo, as empresas já podem ostentar um certificado de que exercitam boas práticas de mercado no que diz respeito à segurança da informação, que rapidamente está se tornando um diferencial competitivo para as empresas que souberem administrá-lo.” (SALDANHA, 2002).

“Geralmente o engenheiro social é um tipo de pessoa agradável. Ou seja, uma pessoa educada, simpática, carismática. Mas, sobretudo criativa, flexível e dinâmica. Possuindo uma conversa bastante envolvente.” (ARAUJO, 2005).

Todos esses fatores cruzados ao perfil do engenheiro social é uma arma perigosa. Em conjunto com as ferramentas descritas a seguir, possibilita o golpe, a manipulação e por fim o roubo das informações.

“Enganar, convencer, ludibriar, persuadir. Na aula de hackerismo, a técnica de fazer pessoas executarem tarefas que facilitem a missão do hacker, é matéria básica e obrigatória. Em algum momento o invasor esbarra em uma barreira intransponível tecnicamente, mas que pode se tornar uma tarefa simples se existe uma pessoa tomando conta. A forma de falar, o tipo de informação necessária, a paciência para esperar o momento oportuno e a sagacidade de tentar de formas diferentes, fazem da engenharia social uma arte para poucos.” [18]

Algumas formas de ataque que o engenheiro social pode utilizar são:

- Ataque por telefone: o engenheiro pode utilizar o telefone como uma ferramenta de ataque, se passando por um cliente, suporte técnico, ou até outro funcionário da empresa. Solicitando informações que podem ser consideradas insignificantes para a vítima, mas pode possuir valor para o atacante.

"O funcionário nem vai questionar se a pessoa que ligou disser que quer algo a pedido do CEO da empresa" [20]

- Bisbilhotar o lixo: muitas informações podem ser descartadas de maneira incorreta. Os lixos coorporativos podem possuir organogramas da empresa, usuário e senhas de funcionários, numero de contas de bancarias, telefones etc.

"As listas telefônicas podem fornecer os nomes e números das pessoas-alvo, o organograma mostra quem são as pessoas que estão no comando, às apólices mostram o quanto à empresa é segura ou insegura, os manuais dos sistemas ensinam como acessar as informações e assim todo e qualquer lixo poderá ser de grande valia para uma pessoa mal intencionada." (Granger, 2001)

- Descobrir senhas: o fator mais favorável para o engenheiro social é a facilidade em descobrir senhas. Normalmente os funcionários anotam suas senhas em papeis ou compartilham com outros funcionários. É comum também, as senhas serem frágeis, ex: contendo dia do aniversário, nome dos filhos etc.
- Engenharia social inversa: é a técnica mais avançada de engenharia social. Caso executado com eficiência apresentará informações valiosas.

"Os três métodos de ataques de engenharia social inversa são sabotagem, propaganda e ajuda. Na sabotagem, o hacker causa problemas na rede, então divulga que possui a solução para este, e se propõe a solucioná-lo. Na expectativa de ver a falha corrigida, os funcionários passam para o hacker todas as informações por ele solicitadas. Após atingir o seu objetivo, o hacker elimina a falha e a rede volta funcionar normalmente. Resolvido o problema os funcionários sentem-se satisfeitos e jamais desconfiarão que fossem alvos de um hacker". (Granger, 2001).

- Footprint: utiliza de softwares específicos para obter informações.
- Ataque online: o engenheiro social ataca via chat, redes sociais etc. com base em senhas de usuários, que normalmente seguem o padrão "facilidade". A partir do momento que o atacante possuir a senha da vitima de alguma rede social, ele pode utilizá-la dentro dos sistemas da empresa, pois, muitas vezes por comodismo o usuário acaba utilizando à mesma senha em varias contas.

"Talvez a maneira mais fácil de conseguir um acesso é através da Internet. A displicência dos usuários que criam senhas fáceis de serem descobertas, que ficam longos períodos sem alterá-las, e ainda utilizam a mesma senha para acesso a várias contas, torna o ataque mais simples. Basta enviar um cadastro oferecendo um brinde ou a participação em um sorteio que solicite o nome e senha do usuário e pronto. O hacker terá a sua disposição tudo o que é necessário para um ataque, sem grande esforço." (Granger, 2001).

Dentre todas as ferramentas duas merecem destaque: a persuasão e a pesquisa. Ambas podem ser consideradas as “chaves” para qualquer ataque de engenharia, elas são a base para qualquer ataque, são elas que possibilitam o uso das demais ferramentas. Ao iniciar qualquer ataque o engenheiro social precisa, primeiramente, pesquisar sobre a vítima saber tudo que puder a seu respeito para assim montar seu ataque. E no momento do ataque a principal arma do engenheiro é a persuasão, ele utilizará a persuasão em conjunto com qualquer ferramenta ou em qualquer ataque. Pode-se concluir que a pesquisa e a persuasão são essenciais para um engenheiro social e que qualquer ataque depende destas para que ocorra. No requisito vulnerabilidades a “inocência humana” é o principal fator. “É de a natureza humana achar que é improvável que você seja enganado em determinada transação, pelo menos até que tenha algum motivo para acreditar no contrário. Nós ponderamos o risco e, em seguida, na maior parte das vezes, damos às pessoas o benefício da dúvida. Esse é o comportamento natural das pessoas civilizadas, pelo menos as pessoas civilizadas que nunca foram enganadas, manipuladas ou trapaceadas em uma soma grande em dinheiro. Quando éramos crianças, nossos pais nos ensinavam a não confiar em estranhos. Talvez todos devessem adotar esse antigo princípio no ambiente de trabalho de hoje.” [3]. É preciso sempre duvidar, os funcionários devem ser conscientizados para que sempre duvidem de pessoas pedindo informações, para que estejam preparados para identificar um ataque. O ideal é que o funcionário aprenda a questionar as necessidades de tais informações e sempre procurar se informar a respeito da pessoa que esta realizando o pedido.

No capítulo 3 serão apresentados casos reais de engenharia social, sendo possível assim, observar melhor como funciona um ataque de engenharia social e o uso das ferramentas para manipular e obter informações.

3. Casos reais de engenharia social

"O computador mais seguro do mundo teria de estar guardado num cofre, desligado, no fundo do oceano. Guardado por tubarões, exércitos e porta-aviões. E mesmo assim seria possível convencer alguém que o estivesse guardando a ligá-lo"
Kevin Mitnick

Neste capítulo serão apresentados casos reais onde o uso de engenharia social provocou prejuízos a empresas e a sociedade. Os subtítulos Mitinick: 3.2 e Frank Abagnale: Prenda-me se for capaz 3.3, trataram de histórias reais que inspiraram livros e filmes. A partir deste capítulo será possível afirmar a idéia de que a engenharia social não esta presente apenas em ataques a empresas e na área tecnológica. Os casos apresentados abaixo apresentam histórias de hackers, fraudadores e assassinos que obtiveram auxilio da engenharia social, mesmo não sabendo ao certo que este era a nomenclatura correta para o ato que executavam isso porque, a engenharia social está tão presente no dia-dia da sociedade e ela quase não se dá conta da importância que existe no tema.

O primeiro tópico é um breve relato sobre um golpe bastante utilizado e apesar de desgastado continua criando vítimas, demonstrando assim o tamanho da inocência e fragilidade humana.

3.1. Golpe do bilhete premiado

"Comete fraude todo àquele que se aproveita da ignorância do outro para prejudicá-lo."
Cód. Penal

O foco que vem ganhando maior proporção é a fraude, atualmente vários casos estão usando engenharia social a fim de obter vantagens sobre outra pessoa. Dificilmente alguém nunca ouviu falar sobre um caso destes, talvez apenas não consiga identificar a engenharia social no ato, mas ela esta ali. Casos como os famosos e antigos golpes dos bilhetes premiados que apesar de ocorrerem com

freqüência ainda funcionam. De acordo com o jornal da rede globo, ([34], 2009), o golpe é aplicado desde os anos 40 e ainda faz vítimas. De acordo com o delegado Wilson Negrão, são vários fatores que influenciam as vítimas:

"É um golpe antigo que remonta a década de 1940. Mas são vários fatores que influenciam no golpe: a lábia do criminoso, a ingenuidade das pessoas e a perspectiva de ganho fácil de ambos os lados" [34]

Como se pode observar o caso se assemelha bastante a engenharia social, as vítimas são abordadas graças a sua "ingenuidade" e para que ocorra tal manipulação o bandido usa de suas técnicas de persuasão.

"A vítima está sempre sozinha. Um homem mais velho com aparência simples pede ajuda. Diz que ganhou na loteria, mas que é analfabeto e que está sem documentos. Em troca de ajuda para sacar o dinheiro, oferece 10% do valor do prêmio." [34]

Figura 2- Bilhete Falsificado [34]

3.2. Mitnick: O Pirata e o Samurai

"Qual é a maior ameaça à segurança dos bens da sua empresa? Isso é fácil: o engenheiro social, um mágico inescrupuloso que faz você olhar a sua mão esquerda enquanto com a mão direita rouba seus segredos. Esse personagem quase sempre é tão amistoso, desembaraçado e prestativo que você se sente feliz por tê-lo encontrado."

Kevin Mitnick

"Tive acesso não autorizado aos sistemas de computadores de algumas das maiores corporações do planeta, e consegui entrar com sucesso em alguns dos sistemas de computadores mais protegidos que já foram desenvolvidos. Usei meios técnicos e não técnicos para obter o código-fonte de diversos sistemas operacionais e dispositivos de telecomunicações para estudar suas vulnerabilidades e seu funcionamento interno."

"Toda essa atividade visava satisfazer minha própria curiosidade, ver o que eu poderia fazer e descobrir informações secretas sobre os sistemas operacionais, telefones celulares e tudo o que chamasse minha atenção."

Figura 3- Kevin Mitniki [12]

Considerado o maior hacker do mundo, Kevin Mitnick iniciou sua história cedo, ainda na adolescência invadiu os computadores da escola onde estudava em

Los Angeles para alterar suas notas, com apenas 17 anos efetuou invasões a sistemas mais avançados como as instalações da Pacific Bell, onde se interessou por manuais técnicos.

Kevin chegou a invadir o sistema aéreo dos EUA, considerado um dos sistemas de computadores mais seguros, utilizando engenharia social como sua principal ferramenta. Outras invasões de Kevin prejudicaram a NSA, centro de espionagem dos EUA, provedores de internet, operadores de telefonia etc.

Sua vida inspirou livros, dentre eles, dois livros escritos pelo próprio Kevin Mitnick em conjunto com outros hackers e especialistas em segurança: "A arte de invadir pessoas: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos" [4] e "A arte de Enganar." [3]. E um livro escrito por Jeff Goodell, O Pirata eletrônico e o Samurai. Ambos os livros escritos por Kevin abordam o uso de engenharia social para trapaças e roubos de informações. No livro A arte de invadir pessoas Kevin descreve as técnicas de engenharia social, explica e apresenta exemplos de casos de invasões com uso de engenharia social. Já no livro A arte de enganar, são apresentados casos reais de golpes cometidos, como:

- Invadindo os cassinos por um milhão de pratas: A história de Alex Mayfield e três amigos em suas “aventuras” em roubos de cassino;
- A invasão na prisão do Texas: A história de Willian e Danny, dois presidiários com a mesma paixão, computadores.
- Um engenheiro em ação: a história de Whurley e suas táticas de engenharia social;
- Etc.

No livro “O pirata eletrônico e o samurai”, Jeff Goodell descreve Kevin como obsessivo, rebelde e solitário. O foco do livro é apresentar a prisão de Kevin realizada em 1995. Quando sua obsessão o levou longe demais. Ao invadir o computador de Tsutomu Shimomura, especialista em segurança, Kevin assinou sua sentença, foi esse deslize que o colocou definitivamente na prisão. Este livro também inspirou um filme “caçada virtual (takedown)”.

Kevin permaneceu cinco anos presos e foi liberado após pagar uma fiança de U$4000 e prometer manter distância de computadores, telefones celulares e portáteis por três anos, também foi proibido de ganhar dinheiro, explorando suas aventuras em livros e artigos até 2007.

Hoje 11 anos após sua saída da prisão, Kevin mudou seu foco em 180º, é analista de segurança e tem sua própria empresa a Mitnick Security Consulting [21], uma mudança significativa em sua vida, passou de vilão a mocinho. "A grande diferença é que hoje eu ainda sou um hacker, mas sou pago para fornecer serviços de segurança".

Durante sua visita ao Campus Party em 2010, Kevin apresentou algumas de suas experiências, dentre elas o site Tecnocracia [18] destacou um caso interessante ocorrido no Reino Unido, onde era oferecido a determinados usuários chocolate em troca de suas senhas. O resultado foi positivo para os atacantes e extremamente negativo para a equipe de segurança, pois 90% dos usuários aceitaram a troca.

Em entrevista a revista veja Kevin declarou sua opinião sobre a segurança da informação nos dias atuais, “Hackers, na minha época, eram apenas indivíduos interessados em roubar o fruto proibido. Hoje é tudo sobre dinheiro. Existe um mercado de venda de exploits e vulnerabilidades, o crime organizado está envolvido. Se antes era diversão, agora é pela grana mesmo” [12].

3.3. Frank Abagnale: Prenda me se for capaz

“Quem é você? - Perguntou uma morena maravilhosa quando me deitei ao seu lado nas areias de Miami Beach.
Qualquer um que eu queira ser-respondi. E, de fato era.”
Frank Abagnale Jr.

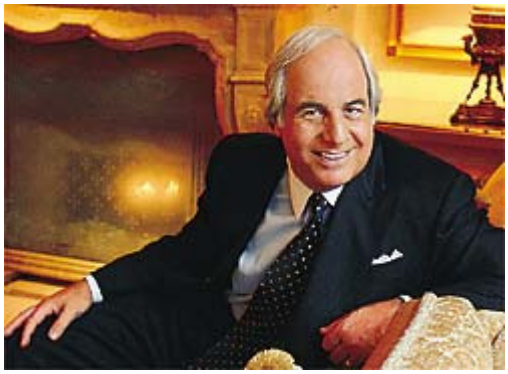


Figura 4- Frank Abagnale Jr. [13]

Frank Abagnale Jr. é a prova de que engenharia social não é utilizada apenas em golpes a empresa através de tecnologia da informação ou em busca de informações armazenadas na empresa. Frank utilizou a engenharia social em golpes "diferentes". Ele iniciou seus golpes em 1963 e em cerca de 4 anos, Frank já tinha falsificado chegues por todos os estados americanos e em 26 países. Estes não foram os únicos golpes de Frank, ele também se tornou piloto de avião, médico, advogado e professor, sem nunca ter se formado em uma faculdade e possuindo com apenas 16 anos, quando iniciou seus golpes.

Assim como Mitnick, Frank teve seus "dons" utilizados pela policia e passou para o outro lado do golpe "a defesa". Hoje Frank possui sua empresa, a Abagnale & Associates [29].

Abaixo um trecho do livro de Frank Abagnale, "prenda-me se for capaz" [25] que inspirou o filme, também chamado "prenda-me se for capaz" [27]:

> “(...) Estava sentado no restaurante do aeroporto almoçando, quando uma conversa na mesa ao lado chamou minha atenção. Era um dialogo entre um velho de rosto severo, e um acompanhante muito jovem e servir, aparentemente um

empregado. Pela conversa, julguei que o mais velho era um banqueiro a caminho de uma convenção em San Francisco, e pelos comentários que ele fez para o jovem, ficou claro para mim que ele esperava que o banco fizesse dinheiro em sua ausência. Ele era frio, arrogante e claramente orgulho de sua posição. Quando o chamaram pelo sistema de alto-falantes do aeroporto internacional, eu descobri o seu nome: Jasper P. Cashman.

Naquela tarde empreendi uma **pesquisa discreta** sobre os antecedentes de Jasper P. Cashman, utilizando a biblioteca de um jornal local, J.P. Cashman era um proeminente em sua comunidade, um magnata que enriquecera por seus próprios méritos. Começara como atendente em seu banco, quando a casa financeira tinha menos de cinco milhões em ativos. Ele agora era o presidente e os ativos do banco excediam cem milhões.

No dia seguinte **examinei o banco**. Era um prédio novo, ainda ostentando seu lema de expansão na enorme vitrine frontal. O interior era espaçoso e agradável. Atendentes ao lado, executivos juniores espalhados ao longo da parede de oposta. Executivos seniores em elegantes escritórios com paredes de vidro. O escritório de Cashman ficava no terceiro andar. J.P. Cashman não em contato pessoal com seus subalternos.

Aluguei um carro, dirigi até uma cidade modesta a duzentos e oitenta quilômetros de distancia e, com um chegue administrativo falso, abri uma conta no banco no valor de dez mil dólares. Em seguida retornei para a cidade de Cashman e, no dia seguinte, telefonei para seu banco. Não estava realmente interessado no dinheiro envolvido no golpe. Os modos de Cashman tinham me irritado, e eu simplesmente queria dar uma ferrada nele.

Eu era a imagem do homem de negócios rico quando entrei no seu banco. Terno cinza de três peças. Sapatos de couro de jacaré muitíssimo bem lustrados. Gravata Countess Mara. Uma pasta de couro fina e elegante.

O jovem que estive com Cashman no aeroporto era um dos executivos juniores. Sua mesa era limpa e bem arrumada, e a placa com seu nome reluziam de nova. Ele obviamente fora promovido recentemente. Aboletei-me na poltrona diante de sua mesa.

-Senhor, posso ajudá-lo em alguma coisa? – perguntou aparentemente impressionado por meu vestuário e comportamento.

- Sim, na verdade o senhor pode. Sou Robert Leeman, de Junction, e preciso descontar um chegue, um chegue bem alto. Tenho todas as identificações necessárias e você pode telefonar para meu banco e verificar, mas não acho necessário. J.P. Cashman me conhece e ele irá atestar meu cheque. Você pode ligar para ele. Ou melhor, eu farei isso, porque preciso mesmo falar com ele.

Antes que o rapaz pudesse reagir, estiquei o braço, peguei o telefone em sua mesa e disquei o ramal correto de Cashman.

-Sim, senhor Cashman, por favor! Ele não está? Há, sim, acho que ele mencionou isso na semana passada, mas acabei esquecendo. Bem, quando Cashman voltar diga a ele que Bob Leeman esteve aqui. Diga que eu e Jean estamos ansiosos para receber ele e Mildred em Junction para aquela cassada. Ele vai entender! Sim, obrigado.

Coloquei o telefone no gancho e levantei uma expressão irritada no rosto.

-Hoje não é meu dia- queixei-me. - precisava deste dinheiro. Não vou conseguir ir até Junction e voltar a tempo de fechar esse acordo. Bem, tenha um bom dia, senhor.

Comecei a me virar, mas o jovem executivo me deteve.

-Há... o chegue que o senhor quer é mito alto, senhor Leeman?

-Bastante. Preciso de $7500,00. Acha que pode cuidar disso? Posso lhe dar o numero da minha conta em Junction.

Sem esperar uma resposta, sentei-me novamente na poltrona preenchi rapidamente um chegue de $7500,00 e o dei a ele. Conforme previra, ele não telefonou ao banco em Junction.

-Senhor, pedirei ao senhor James, o vice-presidente, que de o seu aval nisto. Tenho certeza de que não haverá qualquer problema. Volto em um momento.

Então ele se levantou e se dirigiu a um dos escritórios com paredes de vidro.

Entrou no escritório de James e disse (conforme soube mais tarde) exatamente o que eu havia condicionado a dizer.

-Senhor, um senhor Leeman de Junction esta aqui. Ele precisa descontar um chegue vultoso. É uma amigo pessoal do senhor Cashman e queria vê-lo, mas, como o senhor sabe o senhor Cashman esta em São Francisco.

-Um amigo pessoal do velho?

-Sim, senhor. Comercial e social, pelo que entendi.

-Troque o chegue. Com toda a certeza não queremos irritar um dos associados do velho.

Um minuto depois o jovem executivo entregava um chegue falso a um atendente.

-Troque esse chegue para este cavaleiro, por favor. Senhor Leeman, estou feliz em poder ajudá-lo.

Não fiquei muito satisfeito com o golpe do cão de Pavlov. “Na verdade não gostei nem um pouco de aplicá-lo.”

Como é demonstrado no texto, Frank utilizou de engenharia social em seu golpe. Nos trechos destacados do texto, podemos observar que antes de executar o golpe ele pesquisou sobre a vítima e o banco, e após planejar o golpe ele se arrumou, criando uma imagem falsa que ajudasse na fraude e durante o golpe ele esbanjou seu domínio pela técnica de persuasão. Outro ponto a se destacar no texto foi à motivação de Frank, como mencionado nos capítulos anteriores, a motivação de um engenheiro social é subjetiva, não engloba apenas informações ou dinheiro, como neste caso, por exemplo, Frank apenas estava irritado com as maneiras do dono do banco.

3.4. Tragédia em realengo

“Você não pode deixar ninguém invadir o seu jardim para não correr o risco de ter a casa arrombada.”

Vladimir Maiakovski

No dia 07 de Abril de 2011, ocorreu na cidade do Rio de Janeiro um ataque a alunos e professores de uma escola na zona oeste do Rio. A Escola Municipal Tasso da Silveira situada no bairro de realengo, foi invadida pelo atirador Wellington Menezes de Oliveira, deixando 12 mortos e 18 feridos.

O objetivo não é apresentar informações sobre essa terrível tragédia e sim, demonstrar o uso de engenharia social que ocorreu neste atentado, e como a falha de segurança humana pode vir a provocar outros acontecimentos semelhantes.

Outro ponto a ser apresentado é que a solução que o governo entende por certa e uma perspectiva diferente dessa solução.

Em alguns momentos durante o planejamento e a execução do crime, o assassino utilizou de técnicas de engenharia social para obter o que desejava. Segundo fatos apresentados no jornal da globo, a escola possuía requisitos de segurança como: câmeras distribuídas por todo o prédio, muro alto, grade e um porteiro responsável pela entrada e saída de pessoas do prédio. E mesmo assim, a maneira como o assassino obteve acesso ao prédio foi simples e sem violência, podermos considerar que ele utilizou da tão comentada técnica de engenharia social "a persuasão", ele "argumentou" com o porteiro e obteve acesso ao prédio. Mas para tal acontecimento, ele utilizou de outra técnica de engenharia social, a pesquisa. Uma semana antes do atentado, o assassino foi à escola onde havia estudado, e, portanto já possuía certo conhecimento do local, com a desculpa de obter uma segunda copia do histórico escolar, nesta visita ele procurou também por uma antiga professora sua e com base na conversa que teve com tal professora conseguiu informações sobre ex-alunos darem palestras na instituição, essa foi à desculpa utilizada pelo assassino para convencer o porteiro a deixá-lo entrar no prédio na semana seguinte, a mesma desculpa foi apresentada a professora da sala onde ele iniciou seu ataque.

Abaixo as afirmações dadas pelo diretor sobre tal acontecimento:

"Ele veio na semana passada aqui na escola e pediu na secretaria a segunda via do histórico escolar. Naquele dia, ele perguntou se a professora Dorotéia ainda estava na sala de leitura. Os funcionários confirmaram. Ontem, quando ele chegou aqui, pegou o documento e perguntou se podia ir à sala de leitura falar com a Doróteia. Foi tudo planejado, premeditado, e **ele usou as informações que obteve** para se aproveitar para colocar a sua maluquice em prática", disse Marduk. [33]

"A Doróteia contou que ele chegou e falou normalmente com ela, não parecia drogado, nem alcoolizado. Ela perguntou se ele iria fazer uma palestra para os alunos, pois temos uma semana em que ex-alunos que tiveram sucesso vêm aqui contar suas experiências de vida, denominada na escola de "prata da casa". Ele respondeu para ela que não, **mas ficou com a informação**", disse o diretor. [31]

O relato do diretor deixa claro o uso dessas duas técnicas de engenharia social, a pesquisa e a persuasão.

Vários estados brasileiros estão preocupados em como manter a segurança nas escolas, levantando necessidades como implantação de detectores de metal. Olhando todo o contexto, como já mencionado neste documento, o investimento em segurança física se torna incompleta e ineficiente se o fator humano envolvido não estiver preparado para identificar e contornar tais situações. Torna-se cada dia mais primordial saber preparar o fator humano contra as técnicas de engenharia social. Preparar desde o porteiro ao gerente ou nesse caso diretor, para que a segurança inicie na entrada, no momento da identificação e não termine em momento algum, é necessário que exista todo um acompanhamento sobre quem possui acesso e quais informações são repassadas a essa pessoa.

3.5. O caso de Robin Sage

“Fique calado e em segurança; o silêncio nunca o trairá.”
O’Reilly

Robin Sabe foi uma criação de Thomas Ryan, especialista em segurança, com intuito de tentar invadir redes de especialistas em segurança usando um perfil falso. Em cerca de um mês de experiência, o perfil de Robin Sabe, no twitter, facebook e linkedin conseguiu mais de 300 amigos. A suposta analista em ameaças virtuais da Marinha norte-americana chegou a receber ofertas de emprego e obteve informações valiosas e sigilosas enganando membros do departamento de defesa, militares, funcionário e fabricantes de armas, empresas grandes como o Google e a NSA (Agência Nacional de Segurança Americana).

Entre algumas informações que o Ryan obteve a partir de sua experiência, destacam-se:

- Descobriu senhas de acesso a email e banco com informações obtidas no perfil de suas vítimas;
- Contatos com fornecedores do exército norte americano;
- Contatos com pessoas da agência nacional de segurança (NSA)
- Horário de partida de helicópteros militares;

- Ofertas de emprego;
- Convites para palestrar em conferências de segurança;
- Etc.

A Figura 5-Robin Sage [30], apresenta a foto utilizada no falso perfil, o intuito de se utilizar uma foto feminina é facilitar a manipulação de homens e apresentar uma imagem “delicada” o que também auxilia na hora de manipular as vítimas.

O objetivo de Thomas Ryan foi alcançado, ele provou que falta "malícia" nas redes social. Um caso como esse nunca deveria ocorrer, todas as "vítimas" eram envolvidas com segurança, portanto deveriam ser os mais preparados para lidar com essas situações, mas o experimento provou que não existe esse preparo.

Figura 5-Robin Sage [30]

3.6. Simone Neves e os empregos na Copa

“É mais trabalhoso conduzir os homens pela persuasão que pela força.”
Paul Claudel

Simone Neves acusada de vender falsas vagas de empregos para a Copa e para as Olimpíadas que aconteceram no Brasil foi presa no dia 18 de Abril de 2011 em frente ao prédio da Petrobrás onde supostamente trabalhava. Suas principais vítimas eram pessoas próximas, aos quais ela manipulava com um ótimo currículo distribuído na Internet e e-mails falsos que teriam sido enviados por funcionários do Comitê Olímpico Brasileiro (COB).

Relatos de vítimas:

“Me fez uma proposta financeira realmente interessante. Juntando CLT com pessoa jurídica, isso era especificado através de e-mails, quase R$ 30 mil". [26]

“Ela me cobrou R$ 2 mil para o agenciamento. Ela foi bem categórica. Não tem como receber a sua documentação sem o valor do agenciamento". [22]

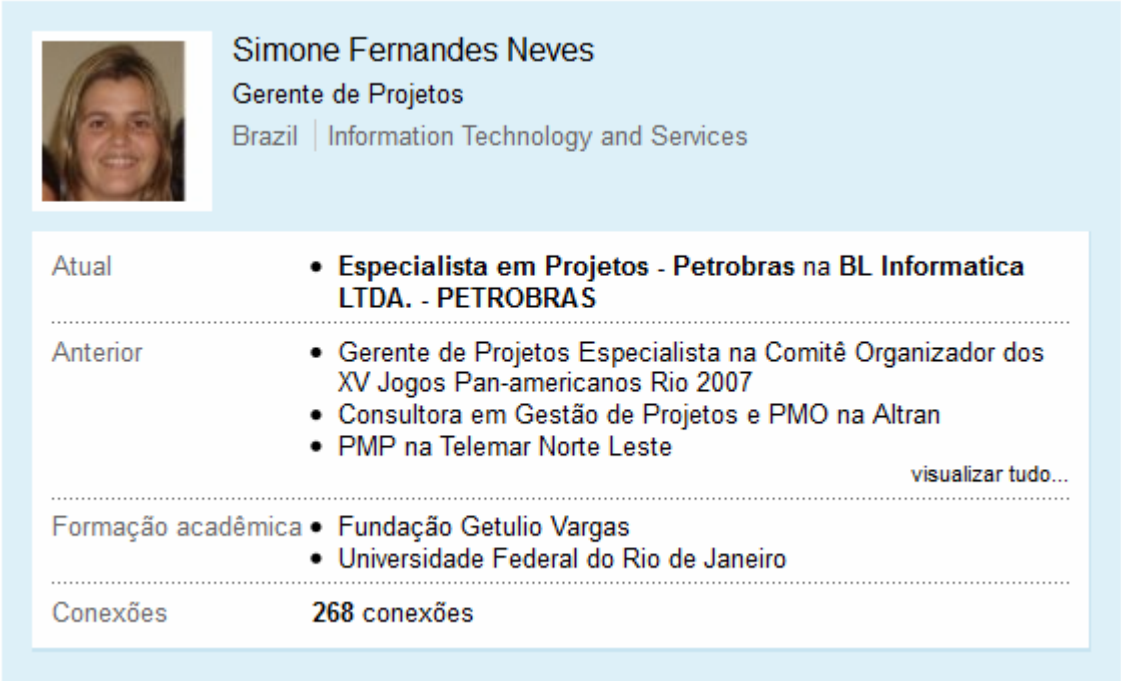
“Eu trabalhava no Recife, tinha minha vida toda estabilizada. Mudei para o Rio de Janeiro para poder assumir este cargo, esta função. Ela disse que eu iria assumir um cargo de coordenação e que o salário seria em torno de R$ 12 mil”. [26]

Este golpe retrata o uso de engenharia social em cada detalhe. Simone Neves utilizou de técnicas de engenharia social para criar todo o contexto que possibilitou seu golpe. Em seu perfil no Linkedin, Simone exibia uma carreira profissional impecável, que era utilizada para convencer suas vítimas.

Além dos conhecimentos apresentados, Simone relatava experiência em empresas como Petrobras e Rede globo. A assessória da Petrobras informou ao jornal da globo que Simone não consta em seu quadro de funcionários, o mesmo ocorreu com a COB que garante que Simone não possui qualquer vínculo com a instituição. [26]

Cobertura completa e vídeos disponível no site da globo [22] e do Bom Dia Brasil [26]. Perfil fictício da golpista disponível no linkedin [24].

As ilustrações a seguir apresentam trechos do perfil de Fernanda disponível no linkedin.



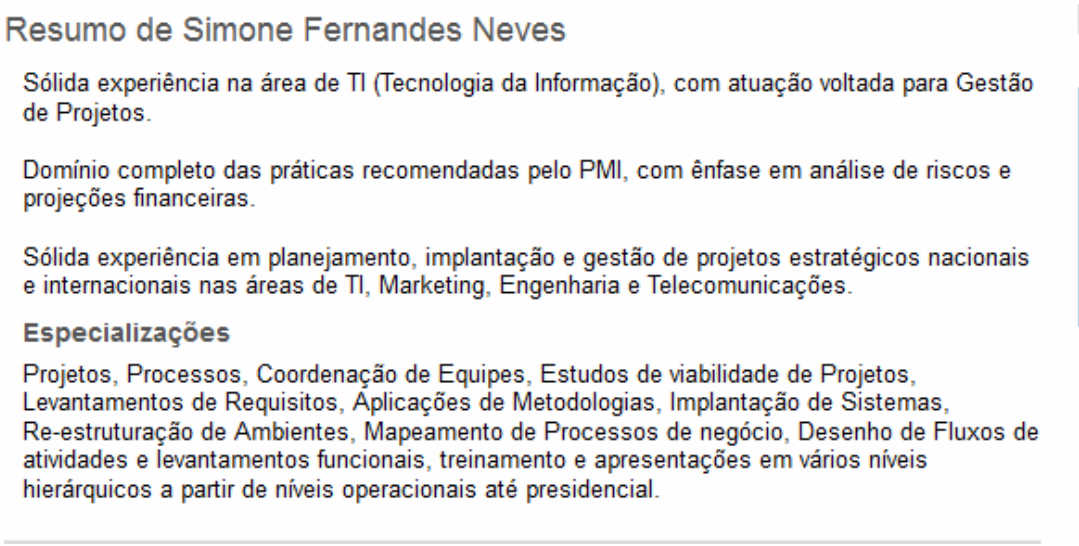
Simone Fernandes Neves

Gerente de Projetos

Brazil | Information Technology and Services

Atual	• **Especialista em Projetos** - **Petrobras** na **BL Informatica LTDA.** - **PETROBRAS**
Anterior	• Gerente de Projetos Especialista na Comitê Organizador dos XV Jogos Pan-americanos Rio 2007 • Consultora em Gestão de Projetos e PMO na Altran • PMP na Telemar Norte Leste visualizar tudo...
Formação acadêmica	• Fundação Getulio Vargas • Universidade Federal do Rio de Janeiro
Conexões	**268** conexões

Figura 6- Perfil de Simone Neves [24]



Resumo de Simone Fernandes Neves

Sólida experiência na área de TI (Tecnologia da Informação), com atuação voltada para Gestão de Projetos.

Domínio completo das práticas recomendadas pelo PMI, com ênfase em análise de riscos e projeções financeiras.

Sólida experiência em planejamento, implantação e gestão de projetos estratégicos nacionais e internacionais nas áreas de TI, Marketing, Engenharia e Telecomunicações.

Especializações

Projetos, Processos, Coordenação de Equipes, Estudos de viabilidade de Projetos, Levantamentos de Requisitos, Aplicações de Metodologias, Implantação de Sistemas, Re-estruturação de Ambientes, Mapeamento de Processos de negócio, Desenho de Fluxos de atividades e levantamentos funcionais, treinamento e apresentações em vários níveis hierárquicos a partir de níveis operacionais até presidencial.

Figura 7- Perfil de Simone Neves (conhecimentos) [24]

4. Estudo de caso

"Num discurso, mentiras, verdades e dissimulação é apenas um detalhe. O objetivo é a persuasão."

Jajazito

Como se observou nos casos apresentados no capítulo anterior (3), o mal preparo dos profissionais esta diretamente ligado aos crescente golpes de engenharia social.

Durante este capítulo serão abordados os dados obtidos a partir de uma pesquisa realizada sobre engenharia social em faculdades e universidades no período de 1º de abril a 12 de abril, no ano de 2011.

4.1. Objetivos da pesquisa

O objetivo principal da pesquisa é apresentar as informações obtidas a partir da pesquisa. Espera-se também, a partir desta pesquisa, comprovar a relevância das afirmações e informações apresentadas nos capítulos anteriores assim como a hipótese apresentada no tópico seguinte.

4.1.1. Hipótese

A grande proporção de ataques de engenharia social se dá pelos motivos:

- As diferentes áreas da empresa acreditam que a necessidade de se cuidar da segurança da informação dentro da empresa deve vir unicamente do departamento de TI;
- Falta preparação dos funcionários sobre o tema;
- A falta de capacitação dos profissionais ainda na faculdade.

A pesquisa pretende:

- Identificar a capacitação de professores e alunos sobre o assunto, assim como a opinião destes sobre o assunto;
- Identificar a capacitação que os cursos oferecem sobre o tema;

- Identificar diferenças entre a preparação dos cursos de TI e a capacitação dos cursos administrativos;
- Apresentar a opinião de profissionais das áreas administrativas e tecnológicas;
- Apresentar a opinião de alunos das áreas administrativas e tecnológicas.

4.2. Coleta de dados

A coleta de dados ocorreu via questionário, enviado as instituições aos coordenadores que deveriam repassar tais questões aos professores e alunos que se enquadrasse no perfil da pesquisa, todo o contato foi realizado por e-mail. Os questionários deveriam ser preenchidos e retornados por e-mail.

4.3. Universo potencial

Para realização da presente pesquisa cerca de 15 faculdades foram contatadas, porém, dentre as faculdades escolhidas para participar da aplicação da pesquisa apenas 8 faculdades optaram por participar, e dentre estas apenas 2 apresentaram uma participação efetiva na pesquisa, com um número razoável de participantes. Em algumas faculdades ocorreu retorno de poucos alunos e professores que se interessaram pelo assunto, em outras a pesquisa foi barrada por ser considerado um assunto não interessante ao foco dos cursos.

Na faculdade Asmec de Ouro Fino, o coordenador do curso de análise de sistemas não retornou o email e o coordenador do curso de administração após saber mais sobre o assunto relatou que “o tema não é importante para a área administrativa, é um foco para a área de TI”, esse pensamento é perigoso quando se trata de engenharia social, como foi abordado nos capítulos anteriores a maioria das falhas de segurança ocorrem graças à falta de informações sobre o assunto.

Nos gráficos apresentados a seguir é possível observar a distribuição do público entrevistado. Na Figura 8 pode-se observar a quantidade de participantes efetivos da pesquisa (4 questionários foram desconsiderados por não estarem com todas as questões obrigatórias respondidas), são 42 professores e 87 alunos dando

em um total de 129 participantes. Os 87 alunos estão divididos de acordo com a área de graduação, 23% dos alunos participantes são da área administrativa enquanto 77% são alunos de cursos tecnológicos, a Figura 9 representa essa porcentagem.

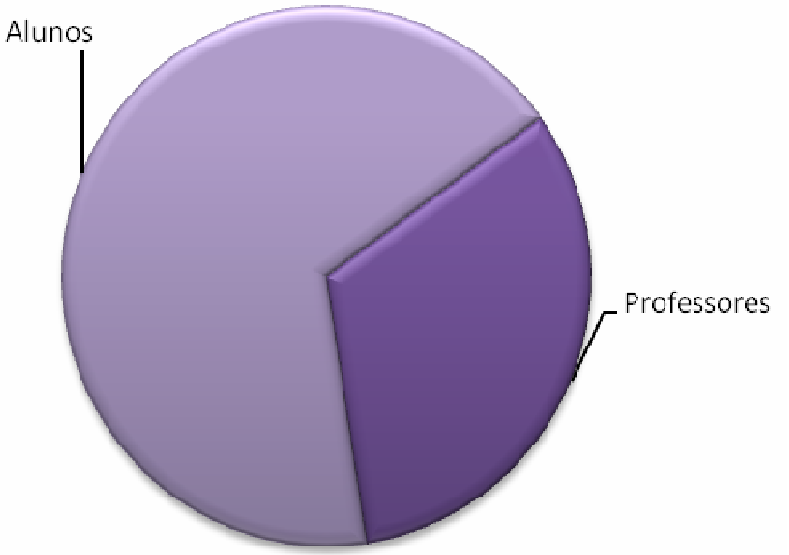


Figura 8- Participantes da pesquisa

Fonte: Autor

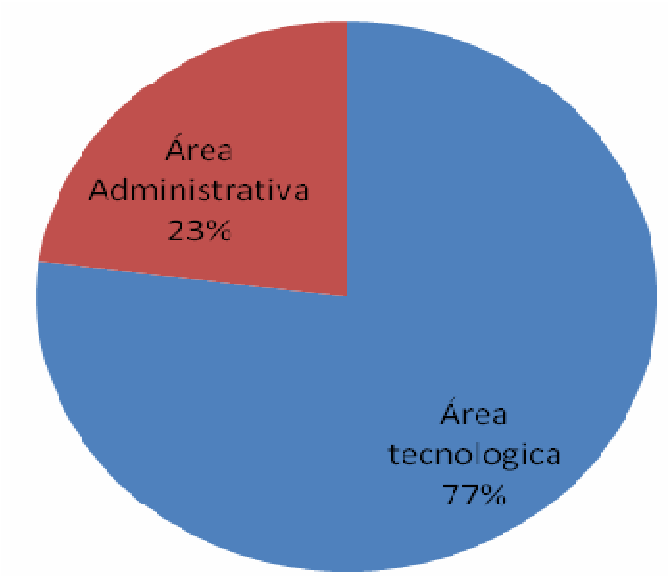


Figura 9- Porcentagem de alunos por curso

Fonte: Autor

Dentre as faculdades participantes da pesquisa, o destaque de maior participação foi a da Fatec de Itapetininga com 54 participantes e em segundo a Fatec Americana com 48 participantes. Os cursos abordados nestas faculdades foram:

- Fatec Itapetininga: Informática para Gestão de Negócios;
- Fatec Americana: Gestão Empresarial e Análise de Sistemas;

A Figura 10 apresenta a distribuição de todos os participantes nas 8 faculdades entrevistadas.

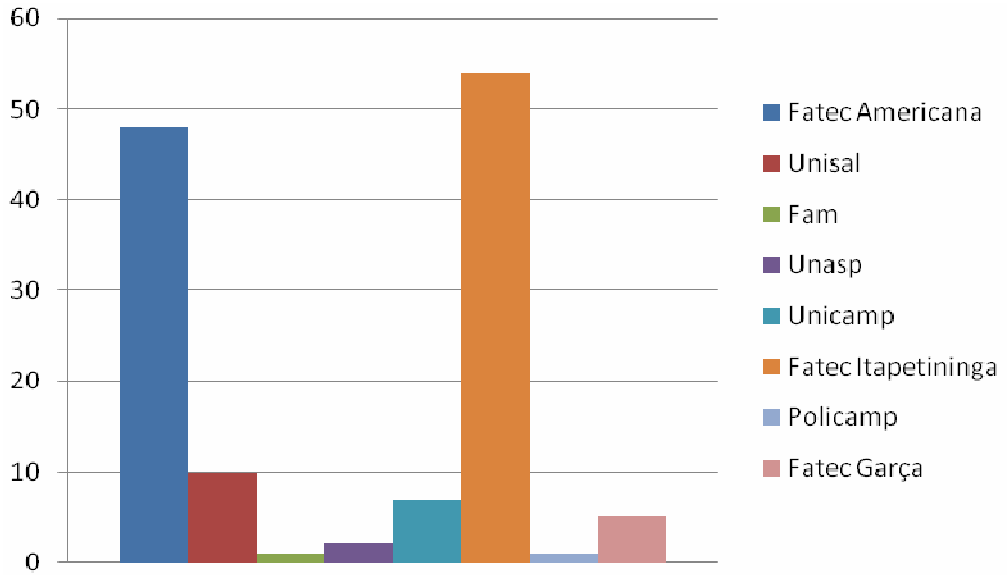


Figura 10- Participantes por faculdade

Fonte: Autor

No próximo capítulo será apresentada a carta de apresentação sobre o assunto que foi anexado ao questionário.

O [Anexo 01] apresenta o questionário enviado aos professores e o [Anexo 02] apresenta o questionário dos alunos.

4.3.1. Carta de apresentação

O objetivo da carta de apresentação foi possibilitar aos alunos e professores participantes da pesquisa informações sobre o tema e sobre procedimentos para a realização do questionário. Uma breve apresentação do assunto é apresentada na

carta de apresentação com o intuito de possibilitar que o entrevistado entender sobre a pesquisa e a definir o conceito de engenharia social.

"O intuito do presente questionário é realizar um levantamento sobre o conhecimento que professores e alunos possuem sobre Engenharia Social. Todas as informações apresentadas serão utilizadas apenas para fins acadêmicos, mais especificamente no trabalho de graduação da aluna Lígia Teixeira, do curso de Segurança da Informação, Fatec Americana.

A resposta do questionário deve ser enviado até dia 12/04/2011 para o email furlanetto.ligia@gmail.com. O email também fica disponível caso exista dúvidas e/ou interesse no assunto. Abaixo uma breve apresentação sobre o assunto:

Com os incidentes cada vez maiores na área computacional, mais especificamente, na parte de segurança da informação, torna-se cada vez mais necessário que se invista em métodos que auxilie na proteção de informações importantes. Tanta precaução acaba se tornando incompleta quando não se pensa no fator humano envolvido. Os homens são alvos fáceis para os chamados engenheiros sociais, pessoas que utilizam métodos de manipulação para persuadir funcionários a entregarem informações valiosas.

"O engenheiro social emprega as mesmas técnicas persuasivas que usamos no dia-a-dia. Assumimos papéis tentamos obter credibilidade. Cobramos obrigações recíprocas. Mas o engenheiro social aplica essas técnicas de uma maneira manipuladora, enganosa, altamente antiética, freqüentemente, com efeito, devastador".Psicólogo social Dr. Brad Sagarin

De maneira resumida, Engenharia Social é uma forma de manipular pessoas para obter informações. Apesar de parecer, engenharia social, não é um problema apenas para a área de TI. Toda a empresa deve estar preparada para ataques advindos da técnica, principalmente porque os alvos principais do engenheiro social são os profissionais desavisados, mal preparados e sem conhecimento do assunto.

Novamente, coloco-me a disposição caso exista interesse e dúvidas sobre o assunto e aguardo as respostas dos questionários.

Lígia Teixeira

Email: furlanetto.ligia@gmail.com"

4.4. Análise de dados da pesquisa

Neste capítulo serão abordadas as informações recolhidas com a pesquisa.A apresentação da pesquisa ocorrerá na seguinte divisão:

- Conhecimento sobre tema: abordagem do conhecimento que os entrevistados possuem sobre engenharia social;
- Vítimas: entrevistados que foram vítimas, empresas que já sofreram ataques de engenharia social;
- Abordagem dos cursos: como o assunto é abordado em sala de aula, como os professores repassam informações de segurança;
- Conhecimentos em segurança: o que os alunos sabem sobre requisitos de segurança, e quais desses requisitos estão certos.

4.4.1. Conhecimento sobre o Tema

"Ninguém vai dar segurança para você! É um problema seu."
Luiz Gasparetto

O primeiro ponto que a pesquisa aborda é o conhecimento sobre o assunto que alunos e professores possuem. A pergunta abordando esse assunto atribuía três opções:

A: Sim, conheço bem o tema.
B: Não, nunca sequer ouvi falar.
C: Já ouvi falar, mas não sei a fundo do que se trata.

Em uma primeira análise, a pesquisa retrata que 51% dos entrevistados já ouviram falar sobre o tema, porém, não tem um conhecimento tão amplo sobre o assunto. A Figura 11- Conhecimento sobre o tema apresenta essa retratação. Porém, realizando uma divisão entre as diferentes categorias dos participantes podemos observar que essa realidade não se exprime em todas as categorias.

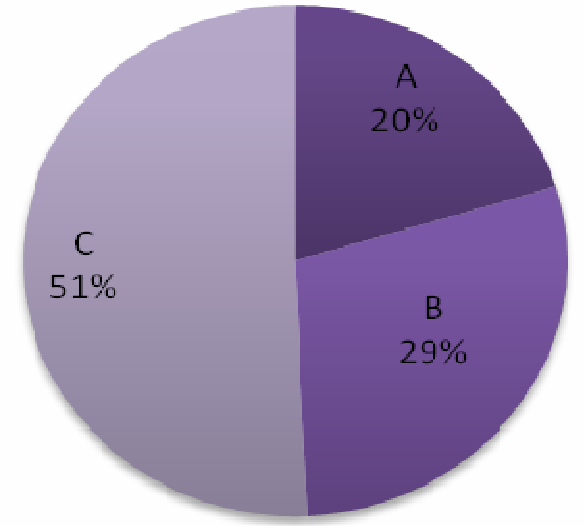


Figura 11- Conhecimento sobre o tema

Fonte: Autor

A Tabela 1 apresenta um resumo sobre os conhecimentos apresentados por alunos e professores sobre o assunto. Pode-se observar que tanto na categoria professor quanto na tecnológica o tema engenharia social é conhecido, entretanto de maneira superficial, enquanto na categoria administrativa o não conhecimento do assunto é predominante.

Tabela 1

	Professores	Administrativo	Tecnológicos
A	21%	10%	22%
B	26%	70%	18%
C	52%	20%	58%

Fonte: Autor

É extremamente importante que exista uma definição correta sobre o assunto. A pesquisa demonstra que existe uma confusão sobre a definição do tema, Cristiano Almeida, aluno da Fatec Itapetininga, relatou que possui conhecimento sobre o conceito abordado pela engenharia social, porém, não sabia dessa nomeação ao conceito:

"Em questão do assunto "Engenharia social" eu nunca ouvi falar com este termo, provavelmente nas nossas aulas ou na empresa onde trabalho haja outro nome ou qualificação diferente, mas com o mesmo sentido."

Outro aluno com comentário semelhante é o Renato, da Fatec Itapetininga:

“Sobre o Termo Engenharia Social, nunca ouvi falar, mas com a definição dada pela carta de introdução reconheço o assunto, talvez ainda não tenha escutado este termo na faculdade devido ao fato de não ter estudado sobre a matéria de segurança da informação, mas em outras matérias como redes e sistemas operacionais, já foi comentado sobre a importância da segurança da informação e meios de proteger dados, assunto que se relaciona com o tema do questionário.”

Outro problema presente é a troca de conceitos que o jogo de palavras “engenharia” e “social” dá sentido e sua real definição. Às vezes ao tentar decifrar o conceito a partir do sentido das palavras, pode ocorrer certa confusão sobre conceitos, como apresentou Cesariano Ferreira, professor da Fatec Itapetininga:

“Acredito que o tema é conhecido e muito provavelmente a grande maioria dos professores sabem como agir. Porém esse título “engenharia social” me é estranho (nunca ouvi falar sobre o assunto). E não me passa significado negativo (afinal, sou engenheiro), pois quando transmito valores éticos aos meus alunos, por exemplo, posso me considerar um engenheiro social (ajudo na construção da cidadania), ou não?”.

O conceito de engenharia é “construir”, entretanto engenharia social nada tem a ver com contrução de conhecimento para a sociedade, ao contrário, o foco da engenharia social é manipulação.

O fato da área administrativa apresentar o maior indice de desconhecimento sobre o tema, reforça como dito nos capítulos anteriores, a importância da preparação de todas os departamentos da empresa, pois, o tema é uma preocupação de toda a empresa, não apenas da área de TI. Essa afirmação ficou retratada nos casos reais (3), onde foram abordadas o uso de engenharia social muitas vezes em casos que não se usava TI, como no caso Frank Abagnale Jr. 3.3. Limitar a preocupação com o tema, atribuindo a responsabilidade para a área de TI é abrir brechas para o engenheiro social, afinal, ele sempre procura pelo “elo mais fraco”, pois este apresentará mais fragilidade e tende a ser um ponto mais fácil para se abordar.

4.4.2. Vítimas de engenharia social

"Nossa segurança está em risco quando a parede de nosso vizinho está em chamas."

Horácio

O questionário também buscou saber se os entrevistados foram vítimas de engenharia social e se as empresas em que trabalham ou trabalhavam já sofreram algum ataque de engenharia social.

A primeira questão a abordar esse ponto foi à questão número 3 em ambos os questionários:

"Você já foi vitima de um engenheiro social?"

As possíveis respostas eram:

A. Não sei, não posso identificar, pois não conheço o tema.
B. Não que tenha percebido.
C. Sim, já fui vitima uma vez.
D. Sim, já fui vitima mais de uma vez.
E. Sim, porém identifiquei o golpe e consegui contornar a situação.

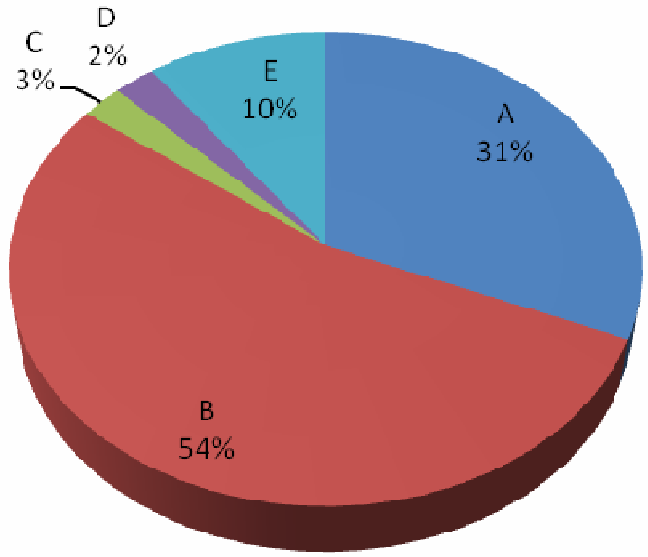


Figura 12-Vítimas

Fonte: Autor

A Figura 12-Vítimas apresenta os resultados obtidos na abordagem desta questão. Apenas 15% dos entrevistados garantem já ter sido vítimas de um engenheiro social, entre estes 10% afirmam ter conseguido identificar o golpe e contornar a situação. A maior parte dos entrevistados (54%) garantem não ter sido vítimas ou pelo menos não terem percebido que foram vítimas e 31% indica não conhecer o tema a ponto de saber identificar um ataque. Muitas vítimas acabam não percebendo que foram manipuladas, muitas vezes o engenheiro social utiliza as informações que conseguem dessas vítimas que podemos considerar “secundárias” apenas para conseguir informaçõs sobre suas reais vítimas (primárias).

A segunda questão sobre vítimas, é voltada as empresas. O objetivo é saber se os funcionarios possuem conhecimento sobre fatos ocorridos nas empresas que trabalham. O esperado para esta questão era que os entrevistados, em sua maioria, respondessem que não possuem conhecimento sobre o fato, essa atitude pode ocorrer graças a três fatores:

1- Apresentar falhas de segurança das empresas é demonstrar suas fragilidades, as empresas preferem não correr esse risco, deixando consciente sobre tais fatos, apenas os especialistas responsáveis, essa atitude é correta e deve ser seguida. Ou seja, neste caso, muitos funcionários não saberiam sobre tais fatos, mesmo que tenham ocorrido;
2- Muitos funcionários possuem a consciência de que repassar informações sobre a fragilidade da empresa que trabalha é perigoso, e preferem dizer que não possuem conhecimento sobre o fato. Essa atitude é a mais correta, informações intenas não devem ser passadas a pessoas externas a empresa;
3- O entrevistado realmente não sabe sobre o fato.

As possíveis respostas para essa questão eram:

A. Não tenho conhecimento sobre o fato.
B. Não, graças a uma política de conscientização de funcionários e treinamentos sobre o assunto.

C. Sim, mesmo a empresa/faculdade possuindo uma política de conscientização de funcionários e treinamento, foi vitima de um engenheiro social.
D. Sim, a empresa/faculdade não possuía treinamento e/ou não conscientizava seus funcionários.

A Figura 13- Empresas vítimas, apresenta o resultado obtido na questão 4.

Como já era esperado, a maioria dos entrevistados (86%) respondeu que não possui conhecimento sobre o fato. De certa forma, pode-se considerar esse resultado positivo, pois dentre os três fatores apresentados anteriormente para que tal resultado ocorre-se, dois eram positivos a segurança da empresa, e não apresentar fatos sobre erros e fragilidades da empresa é uma atitude correta e incentivada pela segurança da informação. Levantando ainda o tema segurança da informação, temos a politica de segurança, que auxilia na proteção das informações da empresa, o essencial seria que todas as empresas tivessem e praticassem tais politicas. Segundo os entrevistados (7%), afirmam que uma politica de segurança impediu que a empresa se tornasse uma vitima. Apenas 2% dos entrevistados, relataram que a politica de segurança não foi o suficiente para impedir que empresa sofresse um ataque e 5% relatou que a empresa sofreu um ataque e que não possui politicas de segurança.

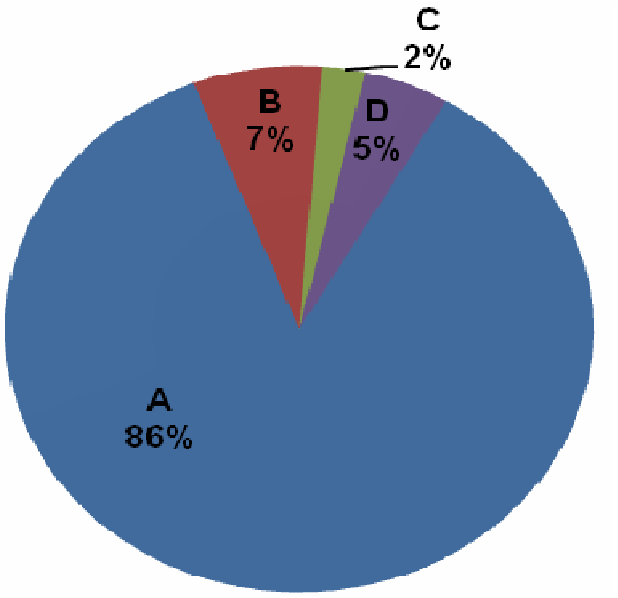


Figura 13- Empresas vítimas

Fonte: Autor

A política de segurança, assim como palestras de conscientização e treinamentos, é importante para manter a segurança de uma empresa, a engenharia social deve ser um tema a ser explorado durante tais palestras e treinamentos. O professor Luiz Antonio Betin Cicolin, da Unicamp, relatou tal fato em sua resposta do questionário:

"Além de professor, trabalho em empresa que tem política rígida de segurança da informação. O tema engenharia social é abordado em treinamentos internos nesta empresa."

Uma aluna da Unicamp, que não será identificada com o intuito de manter a privacidade da empresa intacta, relatou um breve comentário sobre o assunto, com uma historia onde o roubo de informações prejudicou uma empresa:

"Na empresa que trabalhei um grupo de funcionários chave, que tinham acesso as informações estratégicas, criaram empresa concorrente através de patrocínio, com as informações roubadas. Informações técnicas, procedimentos, relação de clientes, fornecedores, especialistas."

4.4.3. Abordagem dada pelos cursos

"A desconfiança é a mãe da segurança."
Madeleine Scudéry

A segunda hipótese levantada nesta monografia e abordada por ambos os questionários, (alunos e professores), é a necessidade de se preparar os alunos durante a faculdade para que ao chegar ao mercado de trabalho o profissional esteja preparado e saiba como se proteger de ataques.

A primeira questão que aborda o assunto é a questão número dois em ambos os questionários. A questão tenta abordar se a faculdade retrata o tema aos alunos e se não, se os professores costumam abordar o tema para encobrir essa falha.

As possíveis respostas à questão são:

A. Sim, porém a matéria não aprofunda no assunto.
B. Sim, o tema é bem abordado.
C. Não, porém procuramos passar aos alunos informações relevantes ao tema. (professore) ou Não, mas o tema já foi comentado por professores. (aluno)

D. Não, o tema nunca foi abordado. (professor). Não, nunca sequer mencionaram o tema nas aulas. (aluno).

De acordo com os resultados obtidos pela pesquisa, o tema não é abordado pelas faculdades, ou não de maneira relevante. De acordo com os resultados, 18% dos entrevistados responderam que existe uma matéria especifica sobre o tema, entretanto, tal matéria não aborda o tema de maneira profunda, a abordagem em nível relevante apenas é apresentada por 2% dos entrevistados. Apesar de uma quantidade significativa (26%), relatar que apesar de não existir nenhuma matéria que estabeleça um contato aos alunos sobre o tema, os professores costumam abordar tais necessidades, a maioria das respostas (54%) indica que o tema nunca foi mencionado durante as aulas.

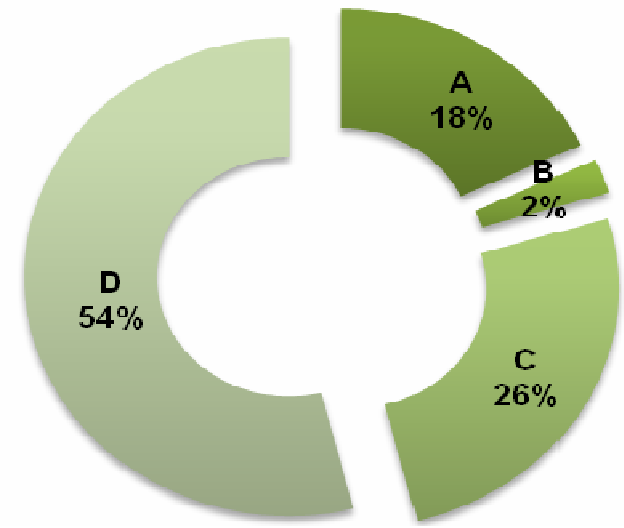


Figura 14- Abordagem do tema

Fonte: Autor

Outra questão apresentada aos professores, também afirma a falta de abordagem dada às faculdades ao assunto. O objetivo da questão é demonstrar se os professores costumam passar aos alunos informações sobre segurança da informação, com o intuito de que eles saibam como proteger as suas informações e as informações das empresas quem venham a trabalhar. As possibilidades de resposta a questão são apenas A- Sim e B- Não.

Assim como abordagem do tema engenharia social, a abordagem sobre regras de segurança são pouco mencionados aos alunos. A Figura 15 apresenta essa informação.

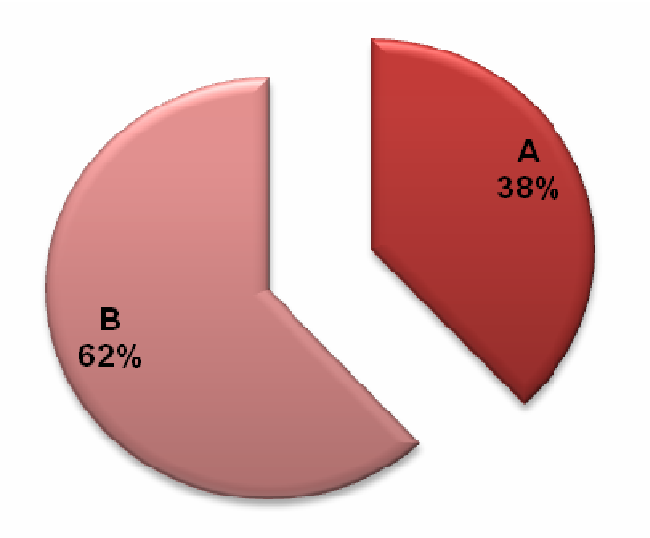


Figura 15- Abordagem sobre segurança da informação
Fonte: Autor

Segundo os dados levantados com a pesquisa, apenas 38% dos professores costumam mencionar regras de segurança, enquanto 62% dos professores não costumam abordar tal tema. Para alguns professores, abordar regras e técnicas de segurança são desnecessarias, o Professor Sandro Tonso, da Unicamp, retrata tal pensamento em seu questionario:

"Eu não trato de "engenharia social" nas minhas aulas, mas construo linhas de reflexão que procuram preparar as pessoas para serem críticas e procurarem compreender as reais intenções que estão por trás de todas as ações que presenciamos. Desta forma, mais que construir procedimentos técnicos de evitar a "engenharia social", preparamos as pessoas para serem boas avaliadoras das propostas que se apresentam a nós diariamente.

"Não sei se compreendo exatamente "engenharia social", mas, pelo que li, trata-se de estratégias que não serão anuladas pela criação de senhas complicadas ou senhas diferentes para cada e-mail, etc. A questão me pareceu muito mais profunda e envolve necessariamente uma dimensão ética, uma postura de respeito à alteridade e de noção de coletivo".

É importante preparar os alunos para terem uma análise crítica e assim saberem como se defender, entretanto, só a análise crítica muitas vezes não é o suficiente, regras e técnicas de segurança são extremamente importantes. Como abordado anteriormente no capítulo 2.3, muitas técnicas usadas pelos engenheiros sociais visam se aproveitar de segurança, e isso inclui senhas frágeis, compartilhamento de senhas, senhas anotadas em papeis etc.

Aos professores que costumam passar informações de segurança aos alunos, foi apresentada outra questão chave quando o assunto é segurança. “Quais requisitos de segurança os alunos devem saber?”. Essa questão poderia ter quantas respostas fossem necessárias, e as opções de respostas eram:

A. Se não conseguir armazenar as senhas, deve anotar, pois as senhas devem ser complexas.
B. Nunca anotar senhas em cadernos ou agendas.
C. Nunca anotar senhas em papeis que fiquem em seu local de trabalho;
D. Nunca anotar as senhas em local algum.
E. Para facilitar memorizar as senhas, criar senhas que lembrem algo, como data de aniversario de algum parente.
F. Nunca criar senhas fáceis, como datas comemorativas ou nomes de animais e personagens, as senhas devem ser complexas.
G. Passar senhas para colegas de trabalho não é problema, afinal, eles trabalham juntos.
H. Passar senhas para amigos é normal, se não se pode desconfiar de todo mundo.
I. As senhas pessoais e principalmente as empresarias nunca devem ser passadas para amigos pessoais, familiares ou colegas de trabalho.
J. Para facilitar a memorização, é normal utilizar a mesma senha para email pessoal e para trabalho.
K. É aconselhável que cada email tenha uma senha diferente, para dificultar caso haja um furto de senha.
L. Nunca pedir ajuda com questões internas para pessoas não identificadas.
M. Não aceitar ajuda de estranhos com questões internas da empresa.
N. Aceitar ajuda de colegas de trabalho quando necessário.

O. Quando receber uma solicitação por telefone de uma pessoa não conhecida não passar informações internas.
P. Sempre responder solicitações, pessoas importantes podem estar solicitando.

Muitas das opções apresentadas não são requisitos de segurança, ao contrário, são opções que não devem ser realizadas. O intuito de apresentar tais opções é levantar se as informações que estão sendo passadas pelos professores aos alunos estão corretas.

Os quesitos “armazenamento de senhas” e “memorização” trazem polêmica ao questionário, alguns profissionais acreditam que esses fatores são irrelevantes e que “forçar” o usuário a memorizar suas senhas não é uma atitude correta, como relata Antonio Cesar Dall´Evedove, professor da Fatec Garça:

“O problema de memorização de senha ou outra coisa qualquer é uma coisa muito individual, eu penso, pois depende muito da capacidade de uma pessoa tem para poder armazenar algo em sua memória.”

A capacidade de memorização das senhas pode ser algo subjetivo, entretanto, quando se trata de segurança da informação, as senhas são os principais pontos fracos. Algumas questões devem ser esclarecidas aos funcionários para que eles entendam a importância de se criar senhas complexas e de não deixá-las expostas. É importante lembrar que o engenheiro social pode utilizar até da menor falha de segurança.

Uma técnica abordada anteriormente no capítulo 2.3 é o famoso “pedindo ajuda”, é importante saber como agir caso encontre algum problema técnico ou preste um serviço.

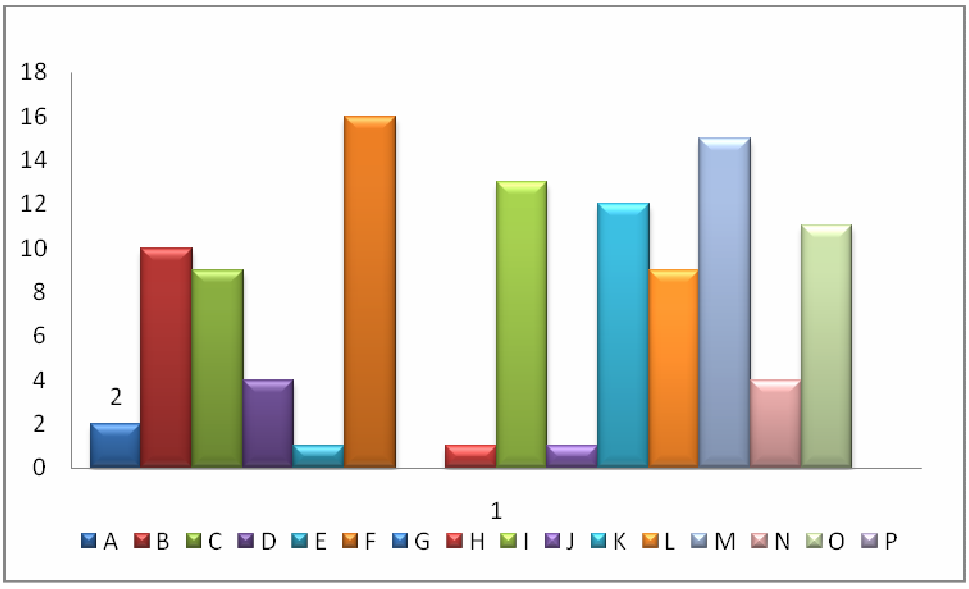


Figura 16-Requisitos de segurança

Fonte: Autor

A Figura 16-Requisitos de segurança, apresenta quais questões de acordo com os professores entrevistados são mais importantes quando se trata de segurança. As questões mais votadas foram:

F- Nunca criar senhas fáceis, como datas comemorativas ou nomes de animais e personagens, as senhas devem ser complexas.

I- As senhas pessoais e principalmente as empresarias nunca devem ser passadas para amigos pessoais, familiares ou colegas de trabalho.

K- É aconselhável que cada email tenha uma senha diferente, para dificultar caso haja um furto de senha.

M- Não aceitar ajuda de estranhos com questões internas da empresa.

O- Quando receber uma solicitação por telefone de uma pessoa não conhecida não passar informações internas.

De maneira geral, as questões escolhidas pelos professores demonstram que as informações que estão sendo passadas aos alunos estão corretas. Questões com falhas relevantes como: E, G, H e P, tiveram pouco ou nenhum voto, o que demonstra maior consciência dos professores sobre as questões de segurança. A única questão importante que foi pouco mencionada é a questão “D- Nunca anotar as senhas em local algum”.

No tópico seguinte serão abordadas as respostas dos alunos sobre questões de segurança e em seguida será estabelecida uma relação entre as questões dadas pelos professores e pelos alunos.

4.4.4. Atitudes de segurança dos alunos

Para os alunos as questões de segurança foram divididas em dois focos:

- Sobre senhas;
- Sobre informações compartilhadas.

Podiam ser escolhidas quantas respostas fossem necessárias. Para o primeiro foco as respostas possíveis eram:

A. Possuo dificuldade em lembrar senhas, costumo anotar em cadernos, celulares ou agendas;
B. Possuo dificuldades em lembrar senhas, costumo criar anotações e lembretes que deixo perto do meu computador;
C. No serviço, meus colegas de trabalho sabem minha senha de acesso, não acho isso um problema;
D. Na minha vida pessoal, meus amigos e colegas sabem minhas senhas de redes sociais;
E. Meus amigos e colegas pessoais sabem minha senha de trabalho;
F. Costumo colocar senhas semelhantes em várias contas para facilitar a memorização;
G. Costumo colocar coisas fáceis na minha senha, tenho dificuldade em memorizar senhas;
H. Sempre crio senhas diferentes para cada email ou rede social;
I. Costumo criar senhas difíceis e/ou complexas;
J. Jamais passo minhas senhas a colegas de serviço;
K. Jamais passo minhas senhas a amigos ou colegas;
L. Já sofri roubo de senhas de e-mail ou redes sociais;
M. Nunca sofri roubo de senhas de email ou redes sociais;

A Figura 17-Requisitos de segurança, senhas (alunos), apresenta um resumo das informações levantadas pelo questionário, lembrando que esse gráfico apresenta uma visão geral, com ambas as áreas abordadas.

As questões mais votadas foram:

J- Jamais passo minhas senhas a amigos ou colegas;
K- Jamais passo minhas senhas a amigos ou colegas;

Dentre os alunos entrevistados, 57 deles relataram nunca ter sofrido roubo de senhas, pode-se considerar uma estatística normal aos resultados obtidos. A maioria dos dados apresentados até esse ponto pelos alunos combina com os dados apresentados pelos professores, entretanto, uma questão é contraditória. Os professores definiriam que é recomendável utilizar senhas diferentes nas contas de email, entretanto, 39 alunos disseram colocar senhas semelhantes em várias contas de email, enquanto 36 alunos disseram colocar senhas diferentes. Pode parecer inofensivo, mas senhas semelhantes é um efeito cascata, se uma senha é descoberta conseqüentemente as contas do usuário que possuem senhas semelhantes também serão burladas. Apenas 1 entrevistado relatou que seus amigos possuem conhecimento sobre suas senhas de redes sociais, o que pode ser uma situação perigosa em conjunto com as opções C e E, entretanto a opção E não possui nenhum relato enquanto a opção C possui 3 votos e é uma situação mais perigosa, pois, a senha de acesso deve ser restrita, não pode ser passada e ninguém mesmo que seja amigo, colega de trabalho etc.

Também sobre senhas, 44 alunos disseram que costumam criar senhas complexas enquanto 8 disseram criar senhas fáceis. A situação de armazenamento não foi bem abordada pelos professores, entretanto, o reflexo desta falha é inferior ao esperado, o que mostra que os alunos possuem consciência dessa falha, apenas 10 alunos relatam ter dificuldades em armazenar senhas e costumam anotar as senhas em cadernos, celulares e agendas, enquanto 1 aluno relatou anotar as senhas e deixar perto do computador.

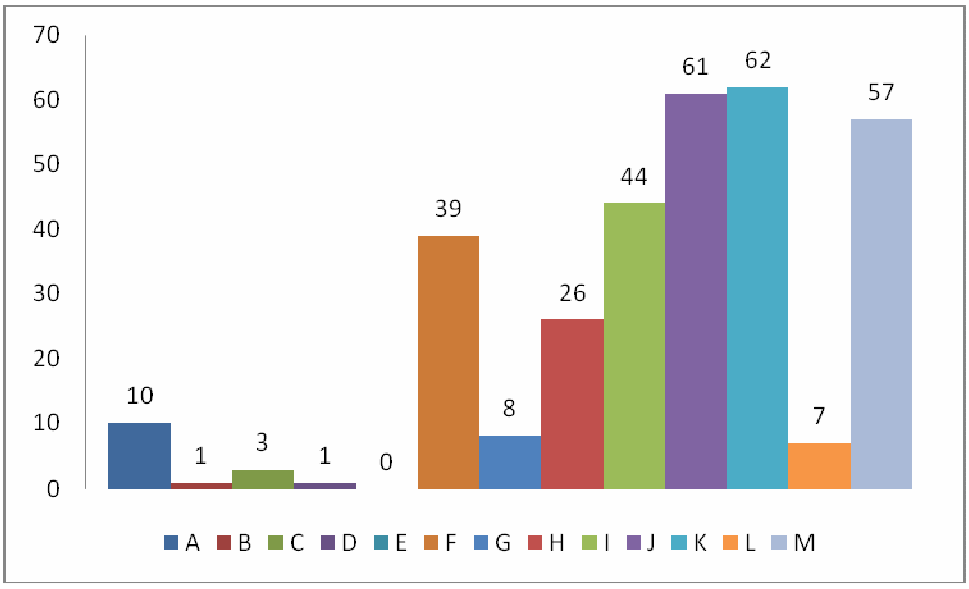


Figura 17-Requisitos de segurança, senhas (alunos)

Fonte: Autor

Sobre compartilhamento de informações, as opções possíveis eram:

A. Costumo ajudar pessoas que não conheço sobre assuntos internos da empresa;
B. Costumo receber pedidos de ajuda por telefone, não vejo problemas em passar informações por telefone;
C. Sempre que recebo um pedido de ajuda, costumo primeiramente procurar identificar a pessoa com que estou falando;
D. Costumo ajudar pessoas ao telefone, entretanto limito a ajuda de acordo com a informação que a pessoa pede e de quem se trata;
E. Prefiro não passar informações sobre a empresa por telefone, sempre desconfio disso;
F. Sempre que encontro uma dificuldade com meu computador de trabalho, peço ajuda a algum colega de trabalho;
G. Sempre que encontro uma dificuldade com meu computador de trabalho, peço auxilio a equipe de TI da minha empresa;
H. Sempre que encontro uma dificuldade com meu computador de trabalho, peço ajuda a pessoas conhecidas;
I. Sempre aceito ajuda de pessoas que não conheço afinal eles que se oferecem para ajudar;
J. Não costumo aceitar ajuda de estranhos, desconfio de atitudes assim.

A Figura 18-Requisitos de segurança, compartilhamento de informações, retrata os resultados obtidos nesta categoria. As opções escolhidas nesta categoria também refletem as opções passadas pelos professores. A maioria dos alunos relata não aceitar ajuda de estranhos, não passar informações a estranhos e identificar com que está conversando antes de liberar informações. 30 alunos também relatam que costumam acionar a equipe de TI da empresa quando encontra algum problema e 17 alunos costumam pedir informações a pessoas conhecidas. Ainda existe a opção de pedir ajuda a colegas de trabalho, e 18 alunos votaram nesta opção. Apesar de estes resultados apresentarem um nível pequeno de escolhas o ideal seria que somente a equipe de TI cedesse auxilio aos funcionários, e ainda existe o fator de desconfiança em ofertas de ajuda que de acordo com as questões 41 alunos costumam desconfiar de ofertas e ajuda e 50 alunos costumam identificar primeiro quando alguém pede algum auxilio. Esse número é maior do que o de alunos que aceitam ajuda sem identificar a pessoa ou pedem ajuda de colegas, mas ainda é baixo, se esse resultado for processado de acordo com o universo potencial, percebesse que apenas 47% dos alunos entrevistados costumam desconfiar e 57% costumam identificar com quem esta conversando. Ou seja, existe uma porcentagem de 53% dos alunos que não relatam desconfiar de ofertas de ajuda de outros.

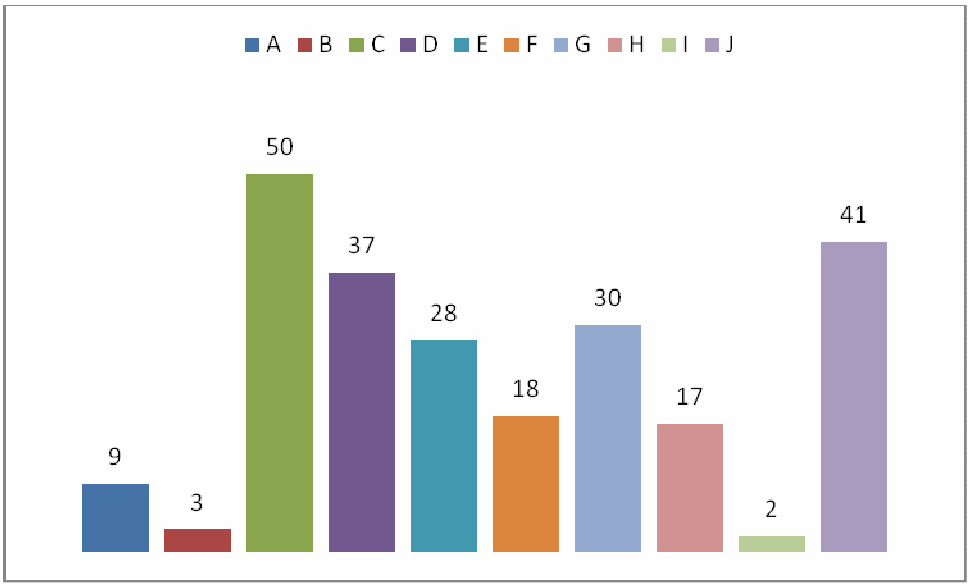


Figura 18-Requisitos de segurança, compartilhamento de informações(alunos)

Fonte: Autor

5. Conclusão

Este documento procurou apresentar informações que venham à melhor das empresas e da sociedade sobre segurança da informação retratando um foco importante para tal acontecimento: o conhecimento e preparação para combater a engenharia social.

A partir da definição do assunto, aqui retratada, é possível estabelecer laços com a realidade atual e identificar com mais eficiência fatores de risco. Torna-se possível perceber que a engenharia social sempre esteve presente na sociedade e que faz vítimas diariamente com golpes algumas vezes modernos e em alguns casos com golpes antigos, como o do bilhete premiado que apesar de antigo e ultrapassado ainda é usado por fraudadores e ainda faz vítimas. Casos como estes mostram o despreparo que existe sobre o assunto.

Outro objetivo deste documento era relatar informações relevantes sobre o cenário atual da segurança da informação e a importância que tratar da engenharia social possui neste cenário.

Com a pesquisa procurou-se apresentar dados que comprovassem a hipótese aqui levantada, e ao final deste trabalho pode-se afirmar tais hipóteses como verdadeiras, provou-se que:

- As diferentes áreas da empresa acreditam que a necessidade de se cuidar da segurança da informação dentro da empresa deve vir unicamente do departamento de TI;
- Falta preparação dos funcionários sobre o tema;
- A falta de capacitação dos profissionais ainda na faculdade.

Espera-se que a partir deste documento profissionais de diferentes áreas possam se conscientizar e assim conscientizar outros profissionais, levando a um processo que a longo prazo possa diminuir de golpes e fraudes, pois apenas a capacitação e a conscientização pode realmente preparar as empresas e a sociedade para lidar com este assunto importante que é a engenharia social.

6. Bibliografia

[1] _____. **Referências**: NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

[2]<http://www.linkedin.com/pub/simone-fernandes-neves/17/377/4b4>. Acesso em: 19 de março de 2011.

[3]A Arte de Enganar. Kevin D. Mitnick e William L. Simon. Tradução: Kátia Aparecida Roque. Revisão técnica: Olavo José Anchieschi
Gomes. Ed. Pearson Education do Brasil Ltda. São Paulo, 2003.

[4] A Arte de Invadir Pessoas: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos. Kevin D. Mitnick e William L. Simon. Tradução Maria Lúcia G. I. Rosa. Revisão técnica: Julio César Pinto e Hoenir Ribeiro da Silva. Ed. Pearson Prentice Hall. São Paulo, 2005.

[5] A segurança da Informação nas Empresas: Ampliando seus horizontes além da tecnologia. Dawel, George. Ed. Ciência Moderna Ltda. Rio de Janeiro, 2005.

[6]A Vulnerabilidade Humana na Segurança da Informação. Eduardo Edson de Araujo. Curso de Sistemas de Informação da Faculdade de Ciências Aplicadas de Minas. Uberlândia, 2005.

[7] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Citação: NBR-10520/ago - 2002. Rio de Janeiro: ABNT, 2002.

[8] Engenharia Social e Segurança da Informação na Gestão Coorporativa. Mário César Pintaudi Peixoto. Ed. Brasport. Rio de Janeiro, 2006.

[9] Engenharia Social: hackeando pessoas. Antonio Marcelo e Marcos Antonio de Azevedo Pereira. Ed. Brasport. Rio de Janeiro, 2005.

[10] Engenharia Social: parte 1. Disponível em: <www.webartigos.com>. Acesso em: 02 de março de 2011.

[11]Engenharia Social: Um perigo eminente. Marcos Antonio Popper e Juliano Tonizetti Brignoli. Instituto Catarinense de Pós-Graduação – ICPG Gestão Empresarial e Estratégias de Informática. Santa Catarina.

[12] Entrevista: Kevin Mitnink- O bandido virou mocinho. Disponível em: <www.veja.abril.com.br>. Acesso em: 15 de março de 2011.

[13] Estelionatário presa por vender falsos empregos para Copa 2014 e Olimpíadas 2016. Disponível em: <http://m.estadao.com.br>. Acesso em: 19 de março de 2011.

[14] Falso perfil na Internet engana especialistas em segurança. Disponível em: <http://noticias.r7.com/rio-de-janeiro>. Acesso em 19 de Abril de 2011.

[15] Filmes Inspiradores. Disponível em: <http://marlinazul.blogsome.com>. Acesso em: 28 de fevereiro de 2011.

[16] Gênesis três. Disponível em: <www.bibliaonline.com.br>. Acesso em: 28 de fevereiro de 2011.

[17] Gestão de Segurança da Informação: o fator humano. Paula Fernando Fonseca. Curso de Pós Graduação em Redes e Segurança de Computadores da Pontifícia Universidade. Curitiba, 2009.

[18] Kevin Mitnick: O elo fraco são as pessoas. Disponível em: <http://tecnocracia.com.br>. Acesso em: 15 de março de 2011.

[19] Mitnick: A ganância tomou o lugar da curiosidade hacker. Disponível em: <http://tecnologia.terra.com.br>. Acesso em: 15 de março de 2011.

[20] Mitnick: Ameaça é a engenharia social. Disponível em: <http://info.abril.com.br>. Acesso em 16 de fevereiro de 2011.

[21] MitnickSecurity. Página de acesso: <http://mitnicksecurity.com>. Acesso em 16 de março de 2011.

[22] Mulher é suspeita de vender empregos falsos para copa e olimpíadas. Disponível em: <www.g1.com.br>. Acesso em: 19 de março de 2011.

[23] O Pirata Eletrônico e o Samurai. Disponível em: <http://www.skoob.com.br>. Acesso em: 16 de março de 2011.

[24] Perfil profissional de Fernanda Neves. Disponível em:

[25] Prenda-me se for capaz. Abagnale, Frank W. Ed. Record. Rio de Janeiro, 2003, 2º Edição.

[26] Presa golpista que vendia vagas para Olimpíadas e Copa de 2014. Disponível em: <www.g1.com.br/bom-dia-brasil>. Acesso em: 19 de março de 2011.

[27] Resista se puder. Disponível em: <www.veja.abril.com.br>. Acesso em: 15 de março de 2011.

[28] Segurança da Informação Vs. Engenharia Social: como se proteger para não ser mais uma vitima. Cássio Bastos Alves. Centro Universitário do Distrito Federal. Brasília, 2010.

[29] Site de Frank Abagnale. Disponível em: <www.abagnale.com>. Acesso em 12 de Abril de 2011.

[30] Sucesso de falsa especialista em segurança supera espiões russos. Disponível em: <www.g1.globo.com>. Acesso em 19 de abril de 2011.

[31] Tragédia em realengo. Disponível em: <www.g1.globo.com>. Acesso em 11 de abril de 2011.

[32] Um pouco de Kevin Mitnick. Disponível em: <www.forum-invaders.com.br>. Acesso em: 16 de março de 2011.

[33] Veja a cobertura completa de ataque em escola do realengo. Disponível em: <http://noticias.r7.com/rio-de-janeiro>. Acesso em 19 de Abril de 2011.

[34] Velho golpe do bilhete premiado ainda faz vítimas no país. Disponível em: <www.g1.globo.com>. Acesso em 02 de maio de 2011.

[Anexo 01] Questões Professores

Questões professores

Informações Gerais

Nome (opcional):

Matérias e cursos que leciona:

Área de formação:

- Formação:

☐ Graduação na área que leciona
☐ Graduação em outra área
☐ Especialização na área que leciona
☐ Especialização em outra área
☐ Mestrado na área que leciona
☐ Mestrado em outra área
☐ Doutorado na área que leciona
☐ Doutorado em outra área
☐ Outros:

Informações Específicas

- Possui conhecimentos sobre Engenharia Social:

☐ Sim, conheço bem o tema.

☐ Não, nunca sequer ouvi falar.
☐ Já ouvi falar, mas não sei a fundo do que se trata.

- A ementa do curso que leciona aborda o tema engenharia social:

☐ Sim, porém a matéria não aprofunda no assunto.
☐ Sim, o tema é bem abordado.
☐ Não, porém procuramos passar aos alunos informações relevantes ao tema.
☐ Não, o tema nunca foi abordado.

- Você já foi vitima de um engenheiro social:

☐ Não sei, não posso identificar, pois não conheço o tema.
☐ Não que tenha percebido.
☐ Sim, já fui vitima uma vez.
☐ Sim, já fui vitima mais de uma vez.
☐ Sim, porém identifiquei o golpe e consegui contornar a situação.

- Durante sua trajetória profissional e acadêmica, alguma empresa ou faculdade em que trabalhou sofreu ataque de engenharia social:

☐ Não tenho conhecimento sobre o fato.
☐ Não, graças a uma política de conscientização de funcionários e treinamentos sobre o assunto.
☐ Sim, mesmo a empresa/faculdade possuindo uma política de conscientização de funcionários e treinamento, foi vitima de um engenheiro social.
☐ Sim, a empresa/faculdade não possuía treinamento e/ou não conscientizava seus funcionários.

- Sobre as aulas, costuma passar aos alunos informações sobre como agir com questões de segurança da informação:

☐ Sim
☐ Não

- Se sim, quais das opções abaixo se encaixam aos requisitos de segurança que eles devem ter (assinalar quantos forem necessários):

☐ Se não conseguir armazenar as senhas, deve anotar, pois as senhas devem ser complexas.
☐ Nunca anotar senhas em cadernos ou agendas.
☐ Nunca anotar senhas em papeis que fiquem em seu local de trabalho;
☐ Nunca anotar as senhas em local algum.
☐ Para facilitar memorizar as senhas, criar senhas que lembrem algo, como data de aniversario de algum parente.
☐ Nunca criar senhas fáceis, como datas comemorativas ou nomes de animais e personagens, as senhas devem ser complexas.
☐ Passar senhas para colegas de trabalho não é problema, afinal, eles trabalham juntos.
☐ Passar senhas para amigos é normal, se não se pode desconfiar de todo mundo.
☐ As senhas pessoais e principalmente as empresarias nunca devem ser passadas para amigos pessoais, familiares ou colegas de trabalho.
☐ Para facilitar a memorização, é normal utilizar a mesma senha para email pessoal e para trabalho.
☐ É aconselhável que cada email tenha uma senha diferente, para dificultar caso haja um furto de senha.
☐ Nunca pedir ajudar com questões internas para pessoas não identificadas.
☐ Não aceitar ajuda de estranhos com questões internas da empresa.
☐ Aceitar ajuda de colegas de trabalho quando necessário.
☐ Quando receber uma solicitação por telefone de uma pessoa não conhecida não passar informações internas.

☐ Sempre responder solicitações, pessoas importantes podem estar solicitando.

- Comentários (opcional):

[Anexo 02] Questões Alunos

Questões alunos

Informações Gerais

Nome (opcional):

Curso:

Faculdade:

Semestre:

Formação Extra:

- ☐ Curso técnico na área de formação
- ☐ Pós-graduação na área de formação
- ☐ Curso técnico em outra área
- ☐ Graduação em outra área
- ☐ Pós-graduação em outra área
- ☐ Outros:

Trabalha na área de formação:

- ☐ Sim
- ☐ Não

Informações Específicas

- Possui conhecimentos sobre Engenharia Social:

☐ Sim, conheço bem o tema.
☐ Não, nunca sequer ouvi falar.
☐ Já ouvi falar, mas não sei a fundo do que se trata.

- No seu curso existe alguma matéria que prepare os alunos sobre o perigo da engenharia social:

☐ Sim, porém a matéria não aprofunda no assunto.
☐ Sim, o tema é bem abordado.
☐ Não, mas o tema já foi comentado por professores.
☐ Não, nunca sequer mencionaram o tema nas aulas.

- Você já foi vitima de um engenheiro social:

☐ Não sei, não posso identificar, pois não conheço o tema.
☐ Não que tenha percebido.
☐ Sim, já fui vitima uma vez.
☐ Sim, já fui vitima mais de uma vez.
☐ Sim, porém identifiquei o golpe e consegui contornar a situação.

- A empresa em que trabalha já foi vitima de engenharia social:

☐ Não tenho conhecimento sobre o fato.
☐ Não, graças a uma política de conscientização de funcionários e treinamentos sobre o assunto.
☐ Sim, mesmo a empresa possuindo uma política de conscientização de funcionários e treinamento, foi vitima de um engenheiro social.
☐ Sim, a empresa não possuía treinamento e/ou não conscientizava seus funcionários.

- Com quais das atitudes abaixo você mais se identifica (assinalar quantas for necessário):

- Sobre senhas:

☐ Possuo dificuldade em lembrar senhas, costumo anotar em cadernos, celulares ou agendas;

☐ Possuo dificuldades em lembrar senhas, costumo criar anotações e lembretes que deixo perto do meu computador;

☐ No serviço, meus colegas de trabalho sabem minha senha de acesso, não acho isso um problema;

☐ Na minha vida pessoal, meus amigos e colegas sabem minhas senhas de redes sociais;

☐ Meus amigos e colegas pessoais sabem minha senha de trabalho;

☐ Costumo colocar senhas semelhantes em várias contas para facilitar a memorização;

☐ Costumo colocar coisas fáceis na minha senha, tenho dificuldade em memorizar senhas;

☐ Sempre crio senhas diferentes para cada email ou rede social;

☐ Costumo criar senhas difíceis e/ou complexas;

☐ Jamais passo minhas senhas a colegas de serviço;

☐ Jamais passo minhas senhas a amigos ou colegas;

☐ Já sofri roubo de senhas de e-mail ou redes sociais;

☐ Nunca sofri roubo de senhas de email ou redes sociais;

- Sobre compartilhamento de informações:

☐ Costumo ajudar pessoas que não conheço sobre assuntos internos da empresa;

☐ Costumo receber pedidos de ajuda por telefone, não vejo problemas em passar informações por telefone;

☐ Sempre que recebo um pedido de ajuda, costumo primeiramente procurar identificar a pessoa com que estou falando;

☐ Costumo ajudar pessoas ao telefone, entretanto limito a ajuda de acordo com a informação que a pessoa pede e de quem se trata;

☐ Prefiro não passar informações sobre a empresa por telefone, sempre

desconfio disso;

☐ Sempre que encontro uma dificuldade com meu computador de trabalho, peço ajuda a algum colega de trabalho;

☐ Sempre que encontro uma dificuldade com meu computador de trabalho, peço auxilio a equipe de TI da minha empresa;

☐ Sempre que encontro uma dificuldade com meu computador de trabalho, peço ajuda a pessoas conhecidas;

☐ Sempre aceito ajuda de pessoas que não conheço, afinal eles que se oferecem para ajudar;

☐ Não costumo aceitar ajuda de estranhos, desconfio de atitudes assim.

- Comentários (opcional):