

RESUMO

O presente artigo tem por objetivo principal abordar a engenharia social no que se refere aos seus métodos, técnicas e meios utilizados pelo engenheiro social para enganar sua vítima e comprometer assim a segurança da informação, de maneira que o leitor possa reconhecer esse tipo de abordagem para assim não ser mais uma vítima dessa prática tão comum nos dias de hoje. O artigo também tem como objetivo despertar o interesse e a conscientização das pessoas e das organizações para esse perigo eminente, pois esse é o melhor caminho para proteger a informação. O artigo não tem como objetivo abordar a parte técnica da segurança da informação, no que se referem aos protocolos, códigos e etc. Partindo do princípio que a maioria dos usuários não compreende isso, pois são leigos nesse assunto. O artigo foi dividido em três grandes momentos. No primeiro momento será abordado o conceito de engenharia social e segurança da informação assim como a importância da informação nos dias de hoje para as pessoas e principalmente para as organizações. Em um segundo momento, serão expostas algumas características inerentes ao ser humano que assim o torna presa fácil, assim como também as características do engenheiro social, para que assim possa ser reconhecido. Também serão tratados os procedimentos que não podem ficar de fora de uma política de segurança da informação, como por exemplo, os planos de treinamento e conscientização dos funcionários. Por último, serão dadas dicas de como se proteger para não ser mais uma vítima da engenharia social. Com isso o leitor terá uma visão mais ampla dos riscos, danos e consequências causadas pela engenharia social, assim como o que precisa ser feito para combatê-la e como se proteger.

Palavras-chave: *Engenharia Social. Segurança da Informação. Conscientização.*

ABSTRACT

This article aims to address the main social engineering regarding to its methods, techniques and methods used by social engineers to fool his victim and thereby compromise the security of information, so that the reader can recognize this kind of approach for not being a victim of this practice so common nowadays. The article also aims to arouse interest and awareness of people and organizations for this imminent danger, because this is the best way to protect information. The article is not intended to address the technical aspects of information security, as they refer to protocols, codes and so on. Assuming that most users do not understand this, because they are laymen in this matter. The article was divided into three great moments. At first we will address the concept of social engineering and information security as well as the importance of information nowadays for people and especially for organizations. In a second stage, it will be exposed some inherent characteristics of the human being that makes it a so easy prey, as well as

the characteristics of the social engineer, so it can be recognized. It also will address the procedures that can not be left out of an information security policy, such as plans for training and awareness of employees. Finally, it will be given tips on how to protect yourself for not being another victim of social engineering. Thus the reader will have a broader view of risks, consequences and damage caused by social engineering, as well as what must be done to combat it and how to protect yourself.

Key words: *Social Engineering. Information Security. Awareness.*

LISTA DE FIGURAS

Figura 1 – O ciclo	16
Figura 2 – Os pilares da Segurança da Informação	19
Figura 3 – Aspectos da segurança da informação	19
Figura 4 – Atual modelo da segurança da informação.	24
Figura 5 – Proposta de novo modelo para Segurança da Informação.	24
Figura 6 – Elo mais fraco	25
Figura 7 – Como é metade de oito para o Engenheiro Social.	29
Figura 8 – Ambiente sem políticas de Segurança.	32

LISTA DE TABELAS

Tabela 1 – Tipos de intrusos e seus objetivos.	27
Tabela 2 – Áreas de Risco, Táticas e Estratégias	54

SUMÁRIO

INTRODUÇÃO	12
1. CONCEITOS DE ENGENHARIA SOCIAL E SEGURANÇA DA INFORMAÇÃO	15
1.1. O QUE É A ENGENHARIA SOCIAL	15
1.2. O QUE É INFORMAÇÃO E QUAL A SUA IMPORTÂNCIA	17
1.3. O QUE É SEGURANÇA DA INFORMAÇÃO.	17
1.4. TIPOS DE VULNERABILIDADES	21
2. O FATOR HUMANO	23
2.1. SUAS VULNERABILIDADES	25
2.2. COMO AGE O ENGENHEIRO SOCIAL	27
3. A IMPORTÂNCIA DA POLÍTICA DE SEGURANÇA, TREINAMENTO E CONSCIENTIZAÇÃO	30

3.1. AMEAÇAS	30
3.2. POLÍTICA DE SEGURANÇA	31
3.2.1. Plano de treinamento e conscientização	34
3.2.2. Plano de resposta a incidentes	39
4. TIPOS DE FRAUDES USANDO A ENGENHARIA SOCIAL, SUAS TÉCNICAS E MEIOS UTILIZADOS	42
4.1. MEIOS MAIS COMUNS PARA ATACAR	42
4.2. TÉCNICAS DE ATAQUE MAIS COMUNS	43
5. DICAS PARA NÃO SER MAIS UMA VÍTIMA DA ENGENHARIA SOCIAL	47
5.1. COMO SE PROTEGER	47
5.1.1. Elaborando senhas fortes	55
CONCLUSÃO	59
REFERÊNCIAS	61

INTRODUÇÃO

Hoje em dia, a informação é o ativo mais valioso das organizações. Ao mesmo tempo passa também a ser o mais visado e desejado por pessoas mal intencionadas com objetivo de vasculhar por curiosidade, furtar para obter informações sigilosas e valiosas, trazer danos seja por diversão, benefício próprio ou vingança, descobrir segredos e etc. Por isso, mais do que nunca, existe uma preocupação enorme com relação à segurança das informações nas organizações e até mesmo nos lares, pois ela representa a inteligência competitiva dos negócios (competitividade) e lucratividade. Por isso está exposta a uma enorme variedade de ameaças e vulnerabilidades.

A questão é que as organizações dão ênfase somente na atualização dos seus parques tecnológicos como, por exemplo, tecnologias de ultima geração, produtos cada vez mais sofisticados, *firewalls*, *anti-malwares*, Sistemas de detecção de intrusão (IDS), dispositivos de autenticação cada vez mais poderosos, *tokens*, *Smart cards*, biometria e etc. Claro que toda essa tecnologia é importante e fundamental para a segurança da informação, mas não é o bastante. De nada adiantará trancar sempre as portas de sua casa, manter cadeados ou sistemas de segurança que monitorem ou dificultem a entrada pelas portas, sendo que alguém de dentro de casa sempre abre as portas para o bandido. Dessa maneira, todo investimento vai por água abaixo.

Infelizmente ainda não é da cultura das empresas investirem no treinamento e na conscientização dos seus funcionários, afinal eles também fazem parte da segurança da informação, mas as empresas acabam deixando de lado outro aspecto tão importante quanto à tecnologia, que é o fator humano, que por sinal é o elo mais fraco da segurança

da informação. Quanto mais a tecnologia e os dispositivos de segurança evoluem dificultando assim a exploração de vulnerabilidades, mais os invasores explorarão o fator humano, pois como diz o próprio ditado: “Não há Patch contra a Burrice Humana.” (MARCELO; PEREIRA, 2005, p. 3). Há somente uma maneira de combater a questão do fator humano e isso deve ser feito através de treinamentos e conscientização dos funcionários. Empregados devem ser treinados e orientados sobre o que a informação precisa para estar protegida e como protegê-la.

“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, p. 36). A falta de consciência das pessoas a respeito das técnicas de Engenharia Social e o seu excesso de autoconfiança são os principais aspectos que favorecem o sucesso da Engenharia Social. Uma empresa que realmente leva a sério a questão da segurança da informação e considera isso como uma prioridade em sua cultura corporativa passa a treinar seus funcionários assim que são admitidos, de maneira que nenhum funcionário possa receber acesso a um microcomputador antes de participar de pelo menos uma aula básica sobre conscientização em segurança da informação.

O objetivo desse artigo é ajudar as pessoas a entenderem como elas são manipuladas e ensinar as barreiras que devem ser construídas por elas para não serem vítimas da engenharia social. Em resumo esse artigo tem como objetivo levantar a conscientização das pessoas com relação à séria ameaça causada pela engenharia social e ajudá-las a terem certeza que suas empresas ou até mesmo seus próprios lares estão menos suscetíveis a serem explorados por essas técnicas.

Esse artigo tem como escopo a parte não técnica da segurança da informação, que envolve métodos utilizados pelos intrusos para roubar informação, comprometerem a integridade da informação que se acredita ser segura, mas na realidade não é, ou destruir o ativo mais importante das empresas que são suas informações, utilizando o método da engenharia social.

Esse artigo não terá como escopo a parte técnica da segurança da informação, partindo do princípio que a maioria esmagadora dos usuários é leiga e que muitas vezes mal consegue operar um microcomputador, quanto mais compreender códigos, protocolos e etc.

Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e

pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis.(MITNICK; SIMON, 2003, p. 3).

1. CONCEITOS DE ENGENHARIA SOCIAL E SEGURANÇA DA INFORMAÇÃO

1.1. O QUE É A ENGENHARIA SOCIAL

O termo engenharia social ficou mais conhecido em 1990, através de um famoso *hacker* chamado Kevin Mitnick. Esse termo designa para práticas utilizadas a fim de se obter informações sigilosas ou importantes de empresas, pessoas e sistemas de informação, explorando a confiança das pessoas para enganá-las. Pode-se também definir engenharia social como a arte de manipular pessoas a fim de contornar dispositivos de segurança ou construir métodos e estratégias para ludibriar pessoas, utilizando informações cedidas por elas de maneira a ganhar a confiança delas para obter informações. (SILVA, E., 2008).

Muitos são os significados e interpretações dadas ao termo “Engenharia Social”. Uma das melhores encontradas é a seguinte:

Engenharia Social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos. (KONSULTEX, 2004 apud PEIXOTO, 2006, p. 4).

O termo “engenharia” foi atribuído a essa prática porque é construída sobre informações e táticas de acesso a informações sigilosas de forma indevida. Já o termo “social” foi atribuído porque utiliza pessoas que vivem e trabalham em grupos organizados. Essas práticas simplesmente ganharam esse novo termo, pois são bem antigas sendo bastante utilizadas por detetives a fim de obterem informações e também por magistrados com o objetivo de comprovar se um declarante fala a verdade. (SANTOS, 2004).

De acordo com Peixoto (2006, p. 36), “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.”

Os ataques de engenharia social podem ser divididos em dois grupos:

Os ataques diretos: Como o próprio nome já diz, são aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas, fax e até mesmo pessoalmente. Este exige do engenheiro social, um planejamento antecipado e bem detalhado, além de um segundo plano para caso o primeiro não dê certo, além de muita criatividade e articulação para que o plano seja bem sucedido.

Os ataques indiretos: Caracterizam-se pela utilização de *softwares* ou ferramentas para invadir como, por exemplo, vírus, *Cavalos de Troia* ou através de sites e *e-mails* falsos para assim obter informações desejadas.

A figura abaixo ilustra o ciclo de ataque da engenharia social que consiste em quatro fases (Reunir Informações, Desenvolver o Relacionamento com a vítima, Exploração e Execução). Cada ataque de engenharia social é único, com a possibilidade de envolver múltiplas fases/ciclos e/ou pode até mesmo agregar o uso de outras técnicas de ataque mais tradicionais para atingir o resultado final desejado (ALLEN, 2006, p. 5, tradução nossa).

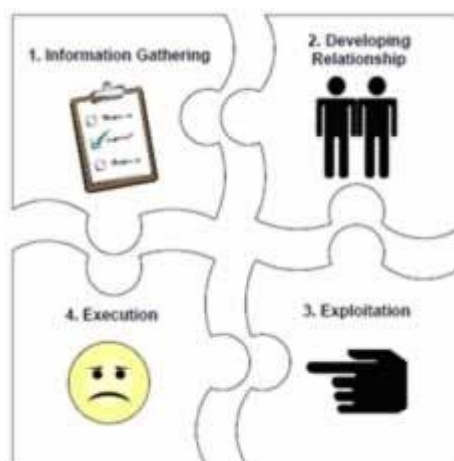


Figura 1 – O ciclo

Fonte: (ALLEN, 2006)

1.2. O QUE É INFORMAÇÃO E QUAL A SUA IMPORTÂNCIA

“A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional da empresa.” (PEIXOTO, 2006, p. 37).

Informação também se define como:

Ato ou efeito de informar ou informar-se; comunicação, indagação ou devassa. Conjunto de conhecimentos sobre alguém ou alguma coisa; conhecimentos obtidos por alguém. Fato ou acontecimento que é levado ao conhecimento de alguém ou de um público através de palavras, sons ou imagens. Elemento de conhecimento suscetível de ser transmitido e conservado graças a um suporte e um código (PEIXOTO, 2006, p. 4).

O Código de prática para a gestão da segurança da informação diz o seguinte:

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS-ABNT, 2005, p.2)

1.3. O QUE É SEGURANÇA DA INFORMAÇÃO.

De acordo com Peixoto (2006, p. 37), “O termo segurança da informação pode ser designado como uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade”.

De acordo com as pesquisas mais recentes, aproximadamente 53% das empresas brasileiras apontam os funcionários insatisfeitos como a maior ameaça à segurança da informação, 40% delas afirmam ter sido vítimas de algum tipo de invasão, 31% não sabem dizer se sofreram ataques e somente 29% alegam nunca ter sofrido ataques, [...]. Em 22% dos casos de ataque, as organizações não conseguiram detectar as causas e em 85% dos casos não souberam quantificar o prejuízo. (BANNWART, 2001 apud PEIXOTO, 2006, p. 36).

A segurança da informação é formada pelos seguintes pilares básicos, que podem ser definidos da seguinte maneira (PEIXOTO, 2006):

- Confidencialidade: É a garantia de que as informações transmitidas chegarão ao seu destino sem que se dissipem para outro lugar onde não deveria passar. Várias tecnologias como, por exemplo, criptografia e autenticações podem ser usadas, desde que mantenham a integridade das informações;
- Integridade: É a garantia de que as informações não sofreram nenhuma modificação durante o trajeto entre a pessoa que enviou e a pessoa que recebeu a informação, garantindo assim a sua real veracidade após chegarem ao destino.
- Disponibilidade: De nada adianta possuir integridade e confidencialidade, se a informação nunca está disponível. Então, o grande desafio é manter essa estrutura de passagem de informações de forma confiável e íntegra sem que haja impossibilidade de captar as informações.

Alguns modelos chegam a incluir mais dois pilares básicos que seriam os seguintes:

- Não repúdio e autenticidade: Conhecido como responsabilidade final, tem como objetivo verificar a identidade e autenticidade de alguém ou até mesmo de um agente exterior a fim de garantir a integridade de origem.

Dessa maneira o modelo seria representado como na imagem abaixo:



Figura 2 – Os pilares da Segurança da Informação

Fonte: (PILARES..., [200-?])

Os pilares acima refletem na organização e também envolvem três aspectos principais:

- Pessoas: Usuários bem orientados, treinados e conscientizados.

- Processos: Regras bem claras para utilização dos recursos tecnológicos fornecidos pela empresa e leis que venham punir de maneira rigorosa os infratores em caso de desvio de informações.
- Tecnologia: Sistemas bem implementados para garantir a proteção das informações da empresa.



Figura 3 - Aspectos da segurança da informação

Fonte: (SKYLAN, 2010)

A informação precisa ser protegida, pois:

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT, 2005, p.2).

A segurança da informação é necessária pelos seguintes motivos:

A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado. [...] a função da segurança da informação é viabilizar os negócios[...] (ABNT, 2005, p.2).

Como o próprio Comitê Gestor da Internet no Brasil diz:

Computadores domésticos são utilizados para realizar inúmeras tarefas, tais como: transações financeiras, sejam elas bancárias ou mesmo compra de produtos e serviços; comunicação, por exemplo, através de e-mails; armazenamento de dados, sejam eles pessoais ou comerciais, etc. (COMITÊ GESTOR DA INTERNET NO BRASIL, 2006, p. 1).

E altamente recomendado que você se preocupe com a segurança do seu microcomputador, pois ninguém gostaria que:

- Suas senhas e cartões de crédito fossem furtados e utilizados por outras pessoas;
- Sua conta do *Internet Banking* fosse utilizada por terceiros;
- Seus dados pessoais fossem alterados, destruídos ou visualizados por terceiros;
- Seu computador fosse danificado e arquivos importantes perdidos;

Segundo (COMITÊ GESTOR DA *INTERNET* NO BRASIL, 2006), pessoas mal intencionadas tentam invadir computadores a fim de:

- Usar computador de terceiros para atividades ilícitas para dificultar sua identificação;
- Lançar ataques contra outros computadores;
- Usar seu disco rígido para armazenar dados.
- Destruir informações;
- Disseminar *Spam*;
- Se passar por outras pessoas em mensagens de *e-mail*;
- Espalhar vírus de computador;
- Furtar número de cartões de crédito ou senhas de banco;
- Furtar dados do seu computador em geral como, por exemplo, informações do seu imposto de renda.

O rápido crescimento do uso do computador e a difusão da Internet têm contribuído para um crescimento fenomenal de crimes de computador e uma diversidade significativa de

criminosos de computador. Embora a maioria dos ataques que causam perda financeira venha de dentro, estudos mostram que a maioria dos ataques vêm de fora da organização. (PIPKIN, 2003, p. 8, tradução nossa).

1.4. TIPOS DE VULNERABILIDADES

Os principais tipos de vulnerabilidades existentes podem ser do tipo: (PEIXOTO, 2006).

- Físicas: Salas de CPD mal planejadas, estrutura de segurança fora dos padrões exigidos;
- Naturais: computadores são propensos a sofrerem danos naturais, como tempestades, incêndio, além, por exemplo, de falta de energia, acúmulo de poeira, aumento da umidade e temperatura.
- Hardware: Desgaste do equipamento, obsolescência ou má utilização;
- Software: Má instalação, erros de configuração, vazamento de informações e, dependendo do caso, perda de dados ou indisponibilidade de recursos;
- Mídias: Disquetes e CDs podem ser perdidos ou danificados, e a radiação eletromagnética pode causar danos às vezes irreparáveis nas mídias;
- Comunicação: Acessos não autorizados ou perda de comunicação;
- Humanas: Tratadas anteriormente, como, por exemplo, as técnicas de engenharia social, as vulnerabilidades referindo-se ao fator humano, como falta de treinamentos, conscientização, o não seguimento das políticas de segurança.

Como afirma Peixoto (2006, p. 39), “Infelizmente ainda não é da cultura de nosso país as empresas adotarem potencial investimento em segurança digital mais especificamente na segurança das informações.”

Pesquisa feita pela Symantec com 200 companhias sedadas no Brasil revela que 80% investem até 10% do orçamento total em segurança e 57% dedicam até 5%. O estudo mostra ainda que os vírus e códigos maliciosos seriam a causa de 54% dos problemas digitais enfrentados. Em seguida estariam as vulnerabilidades de software e hardware com 32% e os ataques causados por funcionários 30%. (MAGALHÃES, 2004 apud PEIXOTO, 2006, p. 39).

2. O FATOR HUMANO

Segundo Kevin Mitnick:

Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis.(MITNICK; SIMON, 2003, p. 3).

Em qualquer organização, por maior que seja a sua segurança, sempre haverá um fator de desequilíbrio chamado "fator humano". O velho ditado que diz que um segredo deixa de ser um segredo quando mais alguém sabe é uma das máximas existentes dentro da segurança da informação. Os maiores engenheiros sociais tiram proveito das fraquezas ou gostos pessoais de seus alvos para assim aproximar e conseguir alcançar seus objetivos. (MARCELO; PEREIRA, 2005).

Um dos maiores problemas hoje em dia na segurança da informação está relacionado ao ser humano e sua ignorância. Práticas que permitem o acesso não autorizado a dados, lugares, objetos e entre outros, fragiliza qualquer esquema de segurança da informação, uma vez que as pessoas acabam tendo acesso a informações indevidas, colocando em risco a segurança da informação. A questão comportamental pode afetar significativamente as demais medidas de segurança, por mais modernas que elas sejam. (SILVA, M.; COSTA, 2009)

Um dos grandes assuntos discutidos atualmente é a questão da inclusão do fator humano como um dos elementos base da segurança da informação. Existem propostas de modelos para inclusão desse fator primordial como um dos pilares fundamentais da segurança da informação, pois o modelo atual considera o fator humano em um nível não base.



Figura 4 – Atual modelo da segurança da informação.

Fonte: (SILVA, M.; COSTA, 2009)



Figura 5 – Proposta de novo modelo para Segurança da Informação.

Fonte: (SILVA, M.; COSTA, 2009)

O fator humano é uma das maiores causas de invasões e ataques, devido a vários motivos que serão abordados de maneira mais profunda posteriormente, como por exemplo, a escolha de senhas fracas ou pelo esquecimento de algum cuidado básico de segurança.

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).

2.1. SUAS VULNERABILIDADES

Podemos destacar as seguintes características do ser humano que o torna vulnerável e suscetível a ataques de engenharia social: (JUNIOR, 2006).

- Vontade de se tornar útil: O ser humano procura ser Cortez ou ajudar os outros quando necessário.
- Buscar amizades: Os humanos costumam se sentir bem ao serem 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 o objetivo. Isso acontece porque o ser humano possui características que o tornam vulneráveis a manipulação.

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).



Figura 6 - Elo mais fraco

Fonte: (PEIXOTO, 2006)

Eu não sou criptoanalista, nem matemático. Apenas sei como as pessoas cometem erros e elas cometem sempre os mesmos erros. (MITNICK; SIMON, 2005, p. 247, tradução nossa).

“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 citado por POPPER; BRIGNOLI, 2003, p. 7).

Em razão de todos esses fatores, sempre haverá brechas de segurança devido ao comportamento humano e sua falta de consciência com relação à segurança da informação, onde a engenharia social poderá produzir bons resultados.

“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 citado por POPPER; BRIGNOLI, 2003, p. 2).

Após uma meticulosa análise, pode-se concluir que dificilmente haverá alguém ou alguma companhia que nunca tenha sofrido pelo menos uma tentativa de ataque utilizando a engenharia social.

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.

A maioria dos funcionários acha que o problema da segurança da informação é tratado somente pela tecnologia em si como, por exemplo, firewalls, antivírus e outras tecnologias, por isso é de fundamental importância criar programas de treinamento e conscientização sobre a segurança da informação, pois o fator humano é a linha de frente para proteção geral da empresa. Esse assunto será abordado de maneira mais detalhada no capítulo subsequente.

Com o aumento crescente de ataques e invasões sofridos pelas empresas, estas estão procurando modernizar seus parques tecnológicos, adquirir novos produtos como firewalls, formas de criptografia, Sistemas de Detecção de Intrusão (IDS), dispositivos de autenticação cada vez mais poderosos e muitos outros mecanismos de segurança, e acabam muitas vezes deixando em segundo plano outro aspecto tão importante quanto à tecnologia, e esse aspecto é o fator humano.

“Não há Patch contra a Burrice Humana.” (MARCELO; PEREIRA, 2005, p. 3).

2.2. COMO AGE O ENGENHEIRO SOCIAL

“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, p. 27).

A tabela abaixo exhibe os tipos de intrusos e seus respectivos objetivos ao utilizar a engenharia social. (POPPER; BRIGNOLI, 2003).

Tabela 1 – Tipos de intrusos e seus objetivos.

Intrusos	Objetivos
Estudantes	Vasculhar mensagens de <i>e-mail</i> alheias por diversão ou curiosidade.
<i>Crackers</i>	Quebrar sistemas de segurança e roubar informações.
Representantes Comerciais	Encontrar planilhas referentes a preços ou cadastro de clientes.
Executivos	Descobrir plano estratégico dos seus concorrentes.
Espiões	Descobrir planos militares.

Tabela 1 – Tipos de intrusos e seus objetivos.

Intrusos	Objetivos
Terroristas	Causar pânico pela rede e roubar informações estratégicas.
Contadores	Desfalques financeiros.
Corretores de valores	Adulterar informações para obter lucro com o valor das ações.
Ex-funcionários	Causar prejuízos apenas por vingança.
Vigaristas	Roubar informações, como senhas e números de cartões de crédito.

Fonte: (POPPER; BRIGNOLI, 2003).

Os ataques de engenharia social são normalmente praticados por *Crackers*, que são *hackers* mal intencionados, pois ainda existe uma confusão enorme com relação a esses dois termos, pois o termo “*Hacker*” está mais relacionado ao indivíduo que possui um elevadíssimo grau de conhecimento em assuntos relacionados à computação como, por exemplo, linguagens de programação, redes de computadores e entre outros conhecimentos e muitas vezes esses eruditos utilizam todo o seu conhecimento para melhorar *softwares* de forma legal ao contrário dos *Crackers* que têm como objetivo trazer danos, roubar informações, dinheiro e etc.

A ideia de *hackear* pode invocar imagens estilizadas de vandalismo eletrônico, espionagem, cabelo tingido e *piercing*. A maioria das pessoas associa *hackear* com violação da lei, portanto insinuam que todos aqueles que se dedicam a atividades *hackers* são criminosos. É verdade que existem pessoas lá fora, que utilizam

técnicas *hackers* para quebrar a lei, mas *hackear* não está muito relacionado a isso. Na verdade, *hackear* está mais relacionado a seguir a lei do que quebrá-la. (ERICKSON, 2009, p. 1, tradução nossa).

O profissional da arte de enganar pessoas utiliza-se de técnicas de persuasão e exploração da ingenuidade dos usuários, criando um ambiente psicológico perfeito para seu ataque, como por exemplo, utilizando identificações falsas, carisma e o apelo sentimental a fim de conquistar a confiança da vítima. Normalmente o engenheiro social procura deixar sua vítima bem tranquila, passando-se por alguém do mesmo nível hierárquico ou superior dentro da organização ou até mesmo por clientes e fornecedores de maneira a induzi-los a fornecer informações, executar programas ou até mesmo fornecer senhas de acesso. Esses profissionais da arte de enganar podem utilizar como pretexto situações de emergência ou de segurança da empresa e geralmente, não pedem muita informação de uma só vez para a mesma pessoa e sim aos poucos e para pessoas diferentes, para que ninguém desconfie dele. Muitas vezes eles usam disfarces dos mais variados tipos como, por exemplo: faxineiros, consultores, gerentes e etc.

O chamado engenheiro social é dotado de um enorme poder de criatividade. Essa criatividade é tão grande que na maioria das vezes, a vítima nem imagina que foi usada e muito menos que acabou de abrir o caminho para um invasor. Para que um ataque de engenharia social seja bem sucedido, é necessária bastante paciência e persistência e essa é uma das grandes características dos engenheiros sociais.

Uma das primeiras e mais obvias maneiras de atravessar um firewall é a trapaça. (RUSSELL, 2003, p. 283, tradução nossa).

Se alguém perguntar a uma pessoa normal quanto é a metade de oito, normalmente essa pessoa irá responder quatro, mas o Engenheiro Social vê a resposta como na imagem abaixo:

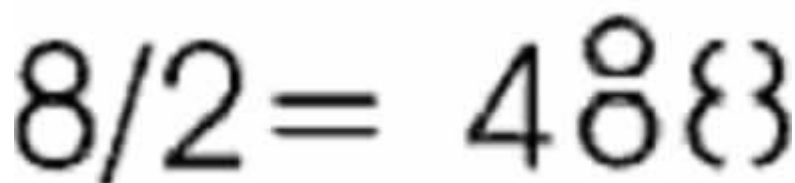

$$8/2 = 4888$$

Figura 7 - Como é metade de oito para o Engenheiro Social.

Fonte: (MARCELO; PEREIRA, 2005)

Difícilmente um ser humano teria essa visão. Quase todo mundo tem somente a visão matemática, ou seja, o mais óbvio, mas o engenheiro social nem sempre se guia pelo mais

lógico. Muitas vezes o ilógico pode ser a melhor resposta para o problema em questão. (MARCELO; PEREIRA, 2005).

3. A IMPORTÂNCIA DA POLÍTICA DE SEGURANÇA, TREINAMENTO E CONSCIENTIZAÇÃO

Mitnick afirma o seguinte:

Como diz o ditado; até mesmo os verdadeiros paranóicos [sic] provavelmente têm inimigos. Devemos assumir que cada empresa também tem os seus — os atacantes que visam a infra-estrutura [sic] da rede para comprometer os segredos da empresa. Não acabe sendo uma estatística nos crimes de computadores; está mais do que na hora de armazenar as defesas necessárias implementando controles adequados por meio de políticas de segurança e procedimentos bem planejados. (MITNICK; SIMON, 2003, p. 23).

3.1. AMEAÇAS

Concordando com o que diz Peixoto (2006), muitas vezes nos sentimos ameaçados em determinadas situações, mas isso não quer dizer necessariamente que você se sente vulnerável. Já na situação oposta, quando alguém se considera vulnerável, certamente essa pessoa se vê ameaçada. Não é uma regra, mas é válida se comparada com o que diz respeito às informações.

Na ótica de Peixoto (2006), As ameaças são o resultado das vulnerabilidades existentes, o que prova a perda dos elementos básicos para existir segurança da informação que são eles a confidencialidade, integridade e disponibilidade. Essas ameaças podem ser divididas em:

- Naturais: Fenômenos da natureza. Como por exemplo, raios que danificam equipamentos, chuvas, umidade, terremotos e etc.
- Involuntárias: Aquelas que ocorrem por causa do desconhecimento, erros ou acidentes e entre outros.
- Voluntárias: São aquelas propositais, resultantes de ações como, por exemplo, ações de *Crackers*, espiões, disseminadores de vírus de computador.

3.2. POLÍTICA DE SEGURANÇA

Para evitar ou diminuir o risco de informações confidenciais serem acessadas indevidamente, perdidas ou até mesmo adulteradas dentro das organizações, é necessário que haja uma série de procedimentos claramente estabelecidos aonde quer que estas informações venham transitar.

“Nós não tocamos em redes, nós tocamos nas pessoas. Porque, no fim, o elo mais fraco em todas essas coisas é a pessoa que está à frente da tela.” (SCHWARTAU, 2010 p. 1).

Política de segurança da informação pode ser definida como uma série de instruções bem claras a fim de fornecer orientação para preservar as informações. Esse é um elemento essencial para o controle efetivo da segurança da informação de maneira a combater e prevenir possíveis ameaças ou ataques que venham a comprometer a segurança da informação nas empresas ou organizações. Essas políticas estão entre as mais significativas no que diz respeito a evitar e detectar os ataques da engenharia social. (FONSECA, 2009).



Figura 8 - Ambiente sem políticas de Segurança.

Fonte: (PEIXOTO, 2006)

Concordando com o que diz Fonseca (2009), o controle efetivo da segurança é posto em prática através do treinamento dos funcionários, bem como através de políticas e procedimentos que devem ser muito bem documentados. É importante salientar que uma política de segurança não elimina a possibilidade de ataques de engenharia social, mesmo que a política seja seguida corretamente por todos os funcionários. Sendo assim, o objetivo é tornar mínimo o risco, a um nível que seja aceitável.

As políticas de segurança que serão apresentadas neste artigo incluem questões que talvez não estejam diretamente direcionadas a engenharia social, mas de maneira indireta fazem parte das técnicas normalmente utilizadas nos ataques de engenharia social. Um

bom exemplo são as políticas relacionadas à abertura de anexos em *e-mails*, que podem ocasionar a instalação de vírus, *Cavalos de Troia* e etc., fazendo com que o invasor tenha controle da máquina da vítima. Esse tipo de ato é bastante utilizado por engenheiros sociais.

Concordando com o que diz Fonseca (2009), um bom programa de segurança da informação deve começar com uma avaliação dos riscos visando determinar as seguintes questões:

- Quais informações, ou que tipo de informação precisará estar protegida e qual o seu nível de proteção.
- Quais ameaças ou que tipo de ameaça pode atingir a empresa.
- Quais prejuízos a empresa teria se um desses sinistros viesse a acontecer.

Concordando com o que diz Fonseca (2009), o objetivo da avaliação dos riscos é levantar as informações que precisam de proteção imediata para que assim possam ser priorizadas. Também deverá haver uma análise de custo/benefício a fim de saber o custo da informação que será protegida, lembrando de um ponto importantíssimo nessa política de segurança é o apoio firme da alta gerência, demonstrando claramente seu interesse e comprometimento por considerar isso fundamental para o bom funcionamento da empresa ou organização, de maneira que os próprios funcionários venham perceber esse interesse da alta gerência.

Ao desenvolver uma política de segurança, deve-se levar em consideração que existem funcionários que não têm conhecimento da linguagem técnica. Portanto, os jargões técnicos não devem ser usados para que o documento possa ser facilmente entendido por qualquer funcionário. O documento também deve deixar bem claro a importância da política de segurança para que dessa maneira os funcionários não encarem isso como perda de tempo. Devem ser criados dois documentos separadamente, onde um deles apresentará as políticas e o outro abordará os procedimentos. Isso deve acontecer porque os procedimentos usados para implementar as políticas, podem mudar com maior frequência do que a própria política em si. Além disso, ao redigir as políticas, deve-se também analisar se a tecnologia que será utilizada para implantar determinada política poderá realmente ser usada pela empresa, levando em consideração o custo/benefício. Então, os redatores da política de segurança de uma organização devem manter o foco em políticas adequadas de acordo com o ambiente e objetivo do negócio da empresa, pois cada empresa possui uma cultura organizacional particular, assim como requisitos de segurança da informação baseados de acordo com suas necessidades. (FONSECA, 2009).

É importante ressaltar também que a política de segurança nunca deve ser imutável ou inflexível, pois as novas técnicas de ataques usando a engenharia social estão surgindo a cada dia assim como as próprias tecnologias e ou procedimentos para combatê-las. Para que a política de segurança esteja sempre atualizada, devem-se estabelecer procedimentos regulares com o objetivo de identificar as novas ameaças e assim combatê-las através das tecnologias e ou procedimentos adequados. Lembrando que esse documento atualizado deve sempre estar disponível em um lugar bem acessível a todos os funcionários. Isso facilitará bastante a consulta dos funcionários ao surgir alguma dúvida relacionada às políticas e procedimento de segurança. Quanto mais rápido o funcionário conseguir acessar esse documento, melhor será. (MITNICK; SIMON, 2003).

3.2.1. Plano de treinamento e conscientização

Talvez haja pouquíssimos assuntos de extrema importância e ao mesmo tempo tão entediantes para a maioria dos funcionários, pelo qual deverão ainda passar por treinamentos como a questão da segurança da informação. Por isso é vital que haja artifícios para prender suas atenções e inclusive entusiasamá-los. (FONSECA, 2009).

Concordando com o que diz Fonseca (2009), um programa de conscientização sobre segurança da informação em uma empresa, tem como objetivo principal, influenciar os funcionários a mudarem seus hábitos e motivá-los a participarem do treinamento, para assim conscientizá-los que eles são parte da segurança da informação na empresa e que ela poderá sofrer um ataque a qualquer momento. Com essa consciência e bem motivados, eles buscarão cumprir sua parte para proteger o ativo mais importante da empresa que são suas informações. Esses funcionários ainda precisam ser treinados e educados de maneira que possam ter consciência das informações que precisam ser protegidas e como protegê-las para que assim possam identificar facilmente um ataque de engenharia social. Esses programas de treinamento e conscientização devem ser realizados constantemente, pois com o passar do tempo o preparo das pessoas diminui além de novas ameaças e técnicas usadas pelos engenheiros sociais surgirem constantemente, o que faz com que seja necessário reforçar e atualizar os princípios da segurança da informação na mente dos colaboradores.

Uma empresa que realmente leva a questão da segurança da informação a sério e como uma prioridade em sua cultura corporativa, passa a treinar seus funcionários assim que são admitidos, de maneira que nenhum funcionário possa receber acesso a um microcomputador antes de participar de pelo menos uma aula básica sobre conscientização em segurança da informação.

Um ótimo aspecto a ser abordado que pode funcionar como um grande agente motivador para os funcionários é esclarecê-los de que a segurança da informação não é um assunto de interesse somente da empresa, mas também dos próprios funcionários, pois a própria empresa possui informações particulares a respeito dos seus funcionários. Inclusive algumas analogias podem ser feitas para criar entusiasmo nos empregados, como por exemplo, informá-los de que não cuidar da segurança das informações no ambiente de trabalho é o mesmo que não cuidar do cartão do banco ou do número do cartão de crédito de alguém. Ou seja, os funcionários perceberão que ao colaborarem estarão protegendo não somente informações da empresa, mas também suas informações pessoais. Outro bom artifício seria a demonstração das técnicas de engenharia social através da dramatização, reportagens ou através de vídeos educativos sobre o assunto, que exibam casos reais de maneira que seja ao mesmo tempo algo educativo e divertido. (FONSECA, 2009).

Concordando com o que diz Fonseca (2009), é interessante deixar bem claro que nem sempre um programa desse tipo deve ser encarado como algo genérico para todas as áreas da empresa. Muito pelo contrário, muitas vezes o treinamento deve ser adaptado de acordo com os requisitos específicos de cada grupo dentro da organização, pois apesar de muitas vezes as políticas serem aplicadas a todos os funcionários, há situações em que será necessária a existência de políticas específicas para determinados cargos ou grupos distintos dentro das organizações, como por exemplo, os gestores, o pessoal da tecnologia, os usuários de microcomputadores, o pessoal das áreas não técnicas, os assistentes administrativos, recepcionistas e o pessoal da segurança física da empresa. Uma observação interessante a ser feita com relação aos funcionários da segurança física é que normalmente esse tipo de funcionário não tem acesso aos microcomputadores e às vezes nem mesmo possuem proficiência para operá-los, mas nem por isso devem ser excluídos do treinamento, pois os engenheiros sociais costumam utilizá-los como peças importantes para conseguirem acesso privilegiado a locais restritos como, por exemplo, algumas salas ou escritórios que venham posteriormente permitir a invasão de algum computador. Por isso em alguns casos, o treinamento precisa sofrer adaptações. Como no exemplo supracitado, os guardas da segurança não precisariam passar pelo treinamento completo que os usuários de microcomputadores deveriam passar. Já aqueles funcionários que não puderem participar dos treinamentos em classe, deverão ser incluídos no treinamento através de outras formas de instrução como, por exemplo, vídeos, treinamentos baseado em computadores, cursos on-line ou por material escrito. Também é muito importante ressaltar a questão dos empregados que mudarem de cargo, função e etc. Esses funcionários deverão passar por um novo processo de treinamento ajustado às suas novas atribuições.

É fundamental em um programa de conscientização deixar bem claro a importância de seguir as políticas de segurança corretamente e os danos que a empresa poderá vir a sofrer se estas não forem seguidas perfeitamente. Os funcionários também devem ser advertidos a respeito das consequências que sofrerão se não cumprirem as normas e procedimentos estabelecidos, pois muitas vezes, os próprios funcionários ignoram ou até mesmo negligenciam os procedimentos que acham desnecessários, ou aqueles considerados tediosos segundo entendimento próprio. Elaborar um resumo dessas consequências e divulgá-los amplamente é um ótimo procedimento a ser realizado. Algo muito interessante que também pode ser colocado em prática é a recompensa para os funcionários que seguem as boas práticas de segurança da empresa de maneira correta. Pois sabemos que o incentivo é sempre algo muito motivador. Também é interessante divulgar amplamente por toda empresa através de circulares internas, boletins periódicos on-line ou pela própria *Intranet*, os casos frustrados de quebra de segurança onde um funcionário atuou de maneira correta evitando algum sinistro. (MITNICK; SIMON, 2003).

Como o próprio ditado diz: A melhor maneira de resolver um problema é evitá-lo. No entanto a questão da prevenção nas empresas é uma tarefa nada fácil, pois a maioria das empresas não dá a devida atenção para essa questão. Elas concentram seus recursos financeiros somente na manutenção de sistemas e em novas tecnologias, ao invés de destinar parte desses recursos para treinamento e conscientização dos funcionários para combater a engenharia social. Recursos como *Intranet* ou correio eletrônico podem ser tão úteis para a divulgação, por exemplo, de lembretes de segurança como mudança de senhas, pois o grande risco é quando os funcionários relaxam na questão da segurança. Por isso é de extrema importância insistir, já que esse tipo de ameaça é tão real nos dias de hoje, quanto às falhas técnicas de segurança.

Concordando com o que diz Fonseca (2009), um bom e objetivo processo de conscientização sobre segurança da informação não pode deixar de lado os seguintes tópicos:

- Descrever a forma com que engenheiros sociais utilizam suas aptidões para manipular e ludibriar.
- Táticas empregadas pelos engenheiros sociais para cumprirem suas metas.
- Como identificar a ação de um engenheiro social.
- Como agir ao desconfiar de alguma solicitação suspeita.
- A quem reportar as tentativas de ataque fracassadas ou que tiveram êxito.

- Questionar solicitações, independentemente do cargo ou importância que o solicitante julga ter.
- Não confiar em pessoas que fazem solicitações de informações, sem antes examinar perfeitamente sua real identidade.
- Como proceder para proteger informações sigilosas.
- Como encontrar as políticas e procedimentos de segurança da informação e sua importância na proteção das informações.
- Sintetizar e explicar o sentido de cada política de segurança como, por exemplo, a questão da criação de senhas difíceis de serem descobertas.
- A obrigação do cumprimento das políticas de segurança e as consequências para o empregado e para a organização caso haja algum descumprimento.
- Como divulgar material ou informação restrita.
- Melhores práticas de uso do correio eletrônico de maneira a não se tornar vítima da engenharia social, vírus e armadilhas em geral.
- Questões físicas da segurança como, por exemplo, a utilização de crachás e o questionamento para com aqueles que estão nas dependências da organização sem utilizá-lo.
- Eliminação de documentos que contenham informações confidenciais independentemente se sua natureza é física ou eletrônica.
- Deixar bem claro que testes serão feitos periodicamente dentro da organização para verificar quais funcionários estão procedendo corretamente e quais não estão.
- Fornecer material informativo como, por exemplo, lembretes através do meio de comunicação que julgar conveniente.
- Parabenizar publicamente o(s) funcionário(s) destaque(s) na segurança da informação.

Testes de intrusão e vulnerabilidades usando a engenharia social podem ser feitos periodicamente com o objetivo de encontrar falhas ou descobrir o descumprimento das políticas de segurança e até mesmo pontos fracos no próprio treinamento dos

funcionários. É interessante avisar os funcionários que testes desse tipo serão realizados periodicamente. (MITNICK; SIMON, 2003).

Tudo isso se resume em uma reeducação na organização de maneira a inserir uma nova cultura que abrange cem por cento da empresa, pois qualquer falha poderá ser fatal.

Pode-se considerar que o programa de treinamento teve um bom aproveitamento se todos que participaram do programa estiverem convencidos e motivados com a consciência de que a segurança da informação faz parte do seu trabalho diário. (FONSECA, 2009).

3.2.2. Plano de resposta a incidentes

Não existe infraestrutura de segurança da informação que venha garantir cem por cento de proteção, pois as falhas sempre existirão, por mais remotas que sejam. Portanto as empresas devem estar preparadas para reconhecer, analisar e responder aos incidentes de segurança o mais rápido possível, pois isso é fator fundamental para amenizar os estragos ou diminuir custos com reparos. É importante que as experiências anteriores com outros incidentes sejam usadas para prevenir ocorrências semelhantes no futuro ou até mesmo para aprimorar a segurança atual. O documento que define as diretrizes para tratar incidentes de segurança chama-se Plano de Resposta a Incidentes. Ele possui os procedimentos e medidas a serem tomadas para remediar, corrigir ou contornar os incidentes. O tratamento de cada incidente dependerá de alguns fatores como, por exemplo, a sua magnitude e o risco que trará para a empresa. (POPPER; BRIGNOLI, 2003).

Como já foi abordado anteriormente, cada empresa possui suas particularidades e culturas organizacionais, portanto, os procedimentos de respostas para os incidentes são também muito particulares, pois variam de organização para organização. O mais importante é que independente do porte da empresa ou do seu ramo de atividades, ela deverá possuir o seu próprio Plano de Respostas a Incidentes.

As seguintes medidas não podem ser deixadas de lado em um Plano de Resposta a Incidentes: (POPPER; BRIGNOLI, 2003).

- Identificar a autoria dos ataques, assim como sua seriedade, estragos causados e responsáveis pelo incidente.
- Divulgar o mais rápido possível o acontecimento ocorrido para que o mesmo incidente não ocorra em outras áreas da empresa.

- Tomar as medidas necessárias para restaurar aquilo que foi afetado como, por exemplo, mudar senhas, trocar funcionários, aumentar o nível de controle.
- Contatar os órgãos de segurança para que o fato seja registrado, assim como tentar entrar em contato com os responsáveis pelos ataques.

Esse capítulo apresentou alguns dos procedimentos que creio ser fundamentais na criação de uma política de segurança da informação que procura se proteger de ataques de engenharia social, não devendo ser considerada como uma lista completa de procedimentos, até mesmo porque isso varia de acordo com o planejamento de cada empresa, ou seja, esses procedimentos são uma base para a criação de uma política de segurança que se ajuste as necessidades peculiares de cada empresa.

4. TIPOS DE FRAUDES USANDO A ENGENHARIA SOCIAL, SUAS TÉCNICAS E MEIOS UTILIZADOS

Nesse capítulo, serão abordadas as várias técnicas usadas pelos engenheiros sociais, assim como os meios utilizados para alcançarem o objetivo de enganar suas vítimas.

4.1. MEIOS MAIS COMUNS PARA ATACAR

Os engenheiros sociais utilizam-se normalmente dos seguintes meios para atacar suas vítimas: (POPPER; BRIGNOLI, 2003).

- Telefone convencional ou VoIP (voz sobre IP): O engenheiro social usa suas técnica e habilidades passando-se por alguém para ludibriar a vítima.
- Internet: Coletar informações sensíveis dos usuários como, por exemplo, login e senha ao serem digitados.
- Intranet: Tem por objetivo acessar remotamente algum microcomputador da rede com o objetivo de se passar por alguém.
- E-mail: Enviar e-mails falsos para induzir a vítima a clicar em links que instalarão vírus, Cavalos de Troia ou redirecionarão para páginas falsas que capturam dados digitados.
- Pessoalmente: Tentar persuadir a vítima.
- Chats: Tentar se passar por outra pessoa nas salas de bate-papo.

- Fax: Obter informações primárias para posteriormente fazer um ataque melhor elaborado.
- Correio convencional: Envia correspondências ou cartas falsas para as vítimas. É um método considerado nada atual, mas é muito utilizado para enganar pessoas mais antigas ou idosas.
- Spyware: É um software espião que monitora o microcomputador sem que a vítima perceba.
- Redes P2P (Peer-to-Peer): Essa é uma tecnologia que permite o compartilhamento de arquivos entre diversos computadores. O atacante usa essa tecnologia para espalhar vírus, Cavalos de Troia e muitas outras pragas, além de claro oferecer ajuda para suas vítimas a fim de trapaceá-las.
- Redes Sociais: Os sites de relacionamento são cada vez mais utilizados pelos usuários. O que muitos deles talvez não saibam é que esses sites deixam um rastro das informações de maneira que pessoas mal intencionadas podem se passar por outras pessoas, camuflando assim sua real identidade. Isso contribui bastante para o sucesso de um ataque de engenharia social.

4.2. TÉCNICAS DE ATAQUE MAIS COMUNS

Abaixo, encontram-se as técnicas e métodos de ataque mais comuns usados pelos engenheiros sociais: (POPPER; BRIGNOLI, 2003).

- Pesquisa: Essa tática concerne no colhimento de materiais com a finalidade de descobrir quem são as pessoas que guardam as informações desejadas. O próximo passo será procurar meios para absorver as informações desejadas dessas pessoas.
- Personificação e impostura: A personificação se baseia na criação de um personagem. Um exemplo clássico é aquele em que o engenheiro social faz uma ligação passando-se por alguém da área de informática da empresa e diz precisar da senha da pessoa ou se passar por um assistente da presidência ou gerencia e pedir informações em nome do seu chefe. Muitos engenheiros sociais chegam a estudar padrões de fala e o tipo de linguagem utilizada por suas vítimas, pois cada organização possui suas próprias linguagem e expressões. Isso acontece porque ao conversar com alguém utilizando a mesma linguagem, se torna mais fácil persuadi-lo, pois a vítima se sente mais segura. Em grandes empresas é difícil

conhecer todos os funcionários e devido a isso, normalmente a vítima acaba cedendo.

- Divisão de responsabilidades: A técnica da divisão de responsabilidades também é bem comum e se resume em convencer os funcionários a compartilharem as senhas com o objetivo de dividirem determinadas tarefas ou responsabilidades.
- Spoofing: Uma nova técnica utilizada é o chamado Spoofing do número telefônico, que tem por objetivo defraudar o sistema de identificação de chamadas, fazendo com que o número exibido pelo identificador de chamadas seja aquele desejado pelo fraudador.
- E-mails falsos: Essa técnica é uma das mais comuns aplicadas pelos engenheiros sociais para conseguirem dados alheios como, por exemplo, senhas, contas bancárias, cartões de crédito e etc. Normalmente esses e-mails falsos abordam assuntos que estão em alta na mídia, atualizações de segurança, recuperação de dados bancários, promoções, premiações ou qualquer outro assunto que venha despertar a curiosidade da vítima para que ela seja persuadida a clicar em links que instalarão vírus, cavalos de troia ou direcionarão para páginas falsas, que capturarão os dados da vítima ao serem digitados.
- Phishing: Criação de sites falsos que possuem o endereço muito parecido com o site original, tirando assim proveito de erros de digitação comuns. Ao digitar informações nesse site, automaticamente os dados são enviados para os criminosos. Por isso a importância de ter certeza se o site é verdadeiro antes de enviar qualquer informação.
- Engenharia Social Inversa: A engenharia social inversa é uma técnica mais avançada e que exige muito mais preparação e pesquisa. Nessa técnica os papéis se invertem. O atacante finge ser uma autoridade, de maneira que os funcionários passarão a pedir informação para ele, até chegar um ponto que o criminoso extraíra informações valiosas sem que ninguém desconfie.
- Footprint: Essa técnica tem por objetivo maior descobrir informações a respeito de algumas tecnologias usadas pela empresa, referentes principalmente ao acesso remoto, Internet e extranet. Essa técnica utiliza-se de softwares especiais para coletar as informações desejadas e é normalmente utilizada quando o invasor não consegue absorver as informações desejadas através de outras técnicas de persuasão devido à falta de conhecimento por parte das vítimas a respeito do assunto desejado pelo invasor.

- Vasculhamento do lixo: Por incrível que pareça, o vasculhamento do lixo da empresa é um dos grandes métodos usados por esses criminosos para conseguirem acessar informações sensíveis, pois muitas empresas não se preocupam com o destino do seu lixo ou sequer utilizam máquinas fragmentadoras ou trituradoras de papel para que os diversos documentos sigilosos não sejam recuperados por pessoas mal intencionadas.
- Olhar pessoas digitando: Essa técnica tem por objetivo descobrir as senhas das pessoas enquanto elas digitam no teclado.
- Programação neurolinguística: Essa técnica se baseia em imitar o jeito de ser da vítima como, por exemplo, sua maneira de falar, se expressar, gestos e entre outros, por um determinado tempo para assim confundi-la, de maneira a formar certa intimidade, deixando a vítima pensar que está no comando da situação. Até que a partir de certo momento, o engenheiro social passa a comandar o diálogo sem que a vítima sequer perceba, capturando assim as informações desejadas. (JUNIOR, 2006).

Kevin Mitnick também ressalta que:

É prática comum pedir que um colega ou subordinado faça um favor. Os engenheiros sociais sabem como explorar o desejo natural das pessoas de ajudar e fazer parte de uma equipe. Um atacante explora esse traço humano positivo para enganar empregado desavisado para que executem ações que o coloquem mais perto de seu objetivo. É importante entender esse conceito simples para que você reconheça quando outra pessoa está tentando manipulá-lo. (MITNICK; SIMON, 2003, p. 163).

5. DICAS PARA NÃO SER MAIS UMA VÍTIMA DA ENGENHARIA SOCIAL

De acordo com (PEIXOTO, 2006, p. 20).

Se todo funcionário fosse tão questionador como uma criança, demonstrando interesse nos mínimos detalhes, ouvindo mais, estando fortemente atento a tudo à sua volta, e principalmente fazendo o uso dos poderosos “por quês”, com certeza as empresas transformariam os frágeis cadeados em legítimos dispositivos dificultantes de segurança da informação.

5.1. COMO SE PROTEGER

O bom senso é fundamental nesses casos. Fique bastante atento com relação a qualquer tipo de abordagem, independente do meio utilizado, como por exemplo, *e-mails*, telefone e etc. Não forneça informações confidenciais como, por exemplo, senhas. Já nos casos de mensagens que tentam induzir a clicar em links contidos no *e-mail* ou em alguma página da *Internet*, a melhor coisa a fazer é entrar em contato com o remetente do *e-mail* ou com a instituição se for o caso, para certificar-se a respeito do assunto. (COMITÊ GESTOR DA INTERNET NO BRASIL, 2006).

Esses são alguns dos maiores erros cometidos dentro do ambiente corporativo que aumentam potencialmente o risco de se tornar uma vítima da engenharia social: (PEIXOTO, 2006)

- Mencionar senha por telefone é um erro gravíssimo, pois antes de disponibilizar qualquer tipo de informação, deve-se saber com quem se fala e de onde fala, além de conferir através de aparelhos identificadores de chamada se o telefone de origem da ligação está realmente batendo com o mencionado. Também é importante conferir o motivo pelo qual solicitaram determinada informação. Lembrando que existe uma técnica já abordada no capítulo anterior chamada *Spoofing*, que faz com que o número exibido pelo identificador de chamadas seja aquele desejado pelo fraudador. Portanto, não é seguro confiar somente nessa informação para ter certeza que o solicitante é realmente quem diz ser;
- Visitantes terem acesso à área interna na empresa, obtendo contato com as informações confidenciais;
- Entrega de informações sem o devido conhecimento real de quem as está levando;
- Entrada de pessoas não autorizadas ou principalmente sem identificação, com portas abertas e expostas à entrada de qualquer um;
- Recebimento de informações digitais (disquete, CD etc.) sem o prévio conhecimento da procedência (de onde realmente vem e de quem vem e do que se trata), sem fazer primeiramente uma inspeção do material recebido em algum lugar ou equipamento que não comprometa a empresa ou organização;
- Descarte incorreto de material que se acha inútil, como por exemplo, não triturar documentos antes de jogá-los fora e de preferência em diversas lixeiras ou o descarte de disquetes, CDs e outros, sem eliminar definitivamente as informações contidas neles;

- Gavetas abertas, de fácil acesso a documentos.
- Jogo via *internet* ou mesmo por disquetes, *Pen-drives* ou CD-ROM são passíveis de conter armadilhas, como ativação de *worms*, *cavalos de troia*, *vírus* e dentre outros perigos que se escondem por trás dos envolventes jogos, ou diversões oferecidas;
- Deixar expostos arquivos de *backup*, não guardando em lugar seguro e confiável, além de demonstrar explicitamente que é um *backup*.
- Nome de usuário e senhas expostas para qualquer um que passar ver e ter acesso.
- *Disquetes*, *Pen-drives*, *CDs*, documentos, material particular como bolsas, carteiras em cima da mesa ou expostos, com grande facilidade de alguém se apoderar ou ter acesso, principalmente se as portas ou janelas ficam sempre abertas.
- Programas, documentos digitais gravados em *disquete* ou *CDs*, não sendo devidamente guardados em lugares seguros onde somente aqueles que podem ter realmente acesso seriam portadores da informação;
- Computador ligado exibindo informações confidenciais como senha, *login* de usuário, códigos fontes;
- Acessos a sites indevidos, não confiáveis, ou fora das políticas de trabalho da empresa;
- Computador ligado e, sobretudo, *logado* com a senha e nome de algum usuário esquecidinho, deixando o uso da máquina disponível para alguém não autorizado.
- Sistema de alarme desativado, desligado ou inoperante, em caso de alguma urgência ou emergência;
- *Softwares* em lugar não seguro; bem como livros, apostilas etc., que contenham informações que sirvam como um facilitador em trazer palavras de cunho técnico de modo a disponibilizar id, senhas, sejam elas *default* ou não;
- Enfeites, como vasos, quadros, dentre outros, servindo como mera distração, fugindo do habitual e tradicional *layout* de arranjo do ambiente de trabalho, podendo ser alvo de suspeita, pois atrás desses “enfeites” podem estar guardados, escondidos ou implantados sistemas de escuta, gravadores, dentre outros

pequenos sistemas que podem colher informações ditas ou vivenciadas naquele ambiente. Paranoias e neuroses à parte, todo cuidado é pouco;

“Quanto aos riscos inerentes aos fatores humanos, podem-se destacar como exemplo os seguintes controles:” (SÊMOLA, 2003 citado por PEIXOTO, 2006, p. 53).

- Seminários de sensibilização;
- Cursos de capacitação;
- Campanhas de divulgação da política de segurança;
- Crachás de identificação;
- Procedimentos específicos para demissão e admissão de funcionários;
- Termo de responsabilidade;
- Termo de confidencialidade;
- *Softwares* de auditoria de acessos;
- *Softwares* de monitoramento e filtragem de conteúdo;

As práticas acima citadas ajudarão a minimizar a possibilidade da empresa se tornar mais uma vítima da engenharia social.

Podemos constatar na visão de (PEIXOTO, 2006, p. 54)

A maior prova para se ter certeza de que você será a próxima vítima da engenharia social é simplesmente subestimar o praticante desta arte. Mas como ao certo saber quem é afinal o engenheiro social naquele dado momento, lugar ou situação? Não saberá, na primeira instância. Apenas desconfiará de algum suspeito à medida que você vá adquirindo conhecimento das técnicas padrões e revolucionárias da engenharia social. E assim percebendo algumas “gafes” do engenheiro social, deixará a incerteza para então capturar o alvo certo.

Abaixo, mais algumas dicas para manter seu computador seguro ao acessar a *Internet*. (SISTEMA DE COOPERATIVAS DE CRÉDITO DO BRASIL, [200-?]).

- Instale um bom programa de antivírus e, pelo menos uma vez por semana, faça uma verificação completa do computador;
- Use sempre cópia original do programa de antivírus, pois as cópias “piratas” geralmente já estão infectadas e não funcionam corretamente;
- Configure seu antivírus para procurar por atualizações diariamente;
- Use seu antivírus para verificar todo arquivo baixado antes de abri-lo ou executá-lo pela primeira vez;
- Cópias originais do Windows são mais seguras e são atualizadas periodicamente pela Microsoft;
- Mantenha o sistema operacional do seu computador e seus programas sempre atualizados para protegê-los contra as falhas de segurança, que são descobertas todos os dias;
- Somente instale programas de fontes confiáveis. Evite os serviços de compartilhamento (por exemplo: Kazaa, Bittorrent, Limeware, Emule, etc.). Eles são uma das principais fontes de disseminação de programas nocivos;
- Não abra *e-mails* e arquivos enviados por desconhecidos;
- Não abra programas ou fotos que dizem oferecer prêmios;
- Cuidado com os *e-mails* falsos de bancos, lojas e cartões de crédito;
- Jamais abra arquivos que terminem com PIF, SCR, BAT, VBS e, principalmente, os terminados com EXE e COM;
- Se você desconfiar de um *e-mail* recebido, mesmo quando enviado por pessoa conhecida, cuidado, pois pode ser um *e-mail* falso;
- Verifique se o endereço que está aparecendo em seu navegador é realmente o que você queria acessar;
- Não confie em tudo o que vê ou lê;
- Não autorize instalação de software de desconhecidos ou de sites estranhos;

- Antes de clicar em um link, veja na barra de status do navegador se o endereço de destino do link está de acordo com a descrição do mesmo;
- Sempre desconfie de ofertas e sorteios dos quais não tenha prévio conhecimento.
- Ao realizar compras pela *Internet* procure por sites reconhecidamente seguros;
- Se for utilizar o seu cartão de crédito ou tiver que fornecer dados bancários, verifique se a página acessada utiliza tecnologia de criptografia, ou seja, o endereço da página acessada deve começar com “https” e deve aparecer o ícone de um cadeado na barra de status (parte inferior) ou à direita da caixa do endereço, dependendo do navegador. Uma observação importante a ser feita, é que *Crackers* colocam imagens de cadeados para fazer com que os usuários pensem que o site é seguro, mas na realidade não é.
- Se você desconfiar de um site de compra, deixe-o de lado e compre em outro lugar.
- Ao preencher qualquer cadastro seja ele virtual ou não, só forneça informações de extrema necessidade.
- Não acredite em todos os *e-mails* sobre vírus, principalmente aqueles de origem duvidosa que trazem anexo arquivo para ser executado, prometendo solucionar o problema;
- Jamais acredite em pedidos de pagamento, correção de senhas ou solicitação de qualquer dado pessoal por *e-mail*. Comunique-se por telefone com a instituição que supostamente enviou o *e-mail* e confira o assunto.
- Nunca realize operações bancárias ou transações pela *internet* que possuam informações pessoais de lugares públicos como, por exemplo, LAN-Houses, pois computadores públicos muitas vezes contêm códigos maliciosos, instalados por pessoas mal-intencionadas, capazes, por exemplo, de registrar tudo o que você digitar no teclado, facilitando a quebra de sigilo dos seus dados confidenciais.

Os mecanismos de busca da *Internet* indexam um número enorme de páginas Web e outros recursos. *Crackers* podem usar esses mecanismos para fazer ataques anônimos, procurar por vítimas e adquirir o conhecimento necessário para montar um poderoso ataque contra a rede. Os mecanismos de busca são perigosos em grande parte porque usuários são descuidados. Além disso, os mecanismos de busca podem ajudar a evitar a identificação dos *Crackers*. Mecanismos de busca tornam a descoberta de máquinas

expostas quase sem esforço. Nos últimos anos, os mecanismos de busca têm recebido uma grande quantidade de atenção negativa por expor informações confidenciais. Como resultado, o mais “interessante” que são as consultas, não retorna mais resultados úteis. (MCCLURE; SCAMBRAY; KURTZ, 2009, p. 553, tradução nossa).

A tabela abaixo exhibe as áreas de risco da empresa, a tática do invasor e a respectiva estratégia de combate, para assim evitar ser mais uma vítima. (POPPER; BRIGNOLI, 2003).

Tabela 2 – Áreas de Risco, Táticas e Estratégias

Área de Risco	Tática do invasor	Estratégia de Combate
Suporte de Informática	Representação e persuasão	Desenvolver na empresa uma política de mudança frequente de senhas e treinar os demais funcionários para nunca passarem senhas ou outras informações confidenciais por telefone;
Entrada de edifícios	Acesso físico não autorizado;	Treinar os funcionários da segurança para não permitirem o acesso de pessoas sem o devido crachá de identificação e mesmo assim fazer uma verificação visual;
Escritórios	Caminhar pelo ambiente;	Não digitar senhas na presença de pessoas estranhas, a não ser que você consiga fazer isso rapidamente;
Suporte telefônico	Usar de disfarces na hora de solicitar ajuda aos atendentes, geralmente se passando por outra pessoa;	Os atendentes devem solicitar sempre um código de acesso, para só então prestarem o suporte solicitado;
Escritórios	Caminhar pelos corredores à procura de salas desprotegidas;	Todos os visitantes devem ser acompanhados por um funcionário da empresa;
Sala de correspondência	Inserção de mensagens falsas;	Fechar e monitorar a sala de correspondência;
Sala dos	Instalam programas analisadores de	Manter sala dos servidores

servidores	protocolo para conseguirem informações confidenciais, além da remoção de equipamentos;	sempre trancada, e o inventário de equipamentos atualizado;
Central telefônica	Roubar acesso a linhas telefônicas	Controlar chamadas para o exterior e para longas distâncias, e recusar pedidos de transferências suspeitas;
<i>Internet e intranet</i>	Criar e/ou inserir programas na <i>Internet</i> ou <i>intranet</i> para capturar senhas;	Criar senhas fortes e fazer uso consciente da mesma, alterando-a periodicamente.
Depósito de lixo	Vasculhar o lixo;	Guardar o lixo da empresa em lugar seguro, triturar todo tipo de documento, e destruir todo o tipo de mídia magnética fora de uso;

Tabela 2 – Áreas de Risco, Táticas e Estratégias

Área de Risco	Tática do invasor	Estratégia de Combate
Escritório	Roubar documentos importantes;	Manter os documentos confidenciais fora do alcance de pessoas não autorizadas, de preferência em envelopes fechados.

Fonte: (POPPER; BRIGNOLI, 2003).

Quase todos esses ataques poderiam ser evitados se o empregado alvo seguisse estas etapas:

- Verificar a identidade da pessoa para ter certeza se ela é realmente quem diz ser.
- Certificar se a pessoa realmente possui autorização.
- Ficar sempre atento ao ser abordado por alguém, principalmente se você não conhece a pessoa. Independente se a abordagem foi feita através do telefone, carta ou *e-mail*, não forneça informações sensíveis, pessoais ou até mesmo da organização onde trabalha.
- Não clicar em *links* antes de verificar a autenticidade da solicitação. Várias são as vítimas de *e-mails* falsos. Para não ser mais uma vítima dessa armadilha, entre em

contato com a fonte da solicitação seja ela uma pessoa, empresa, órgão público e etc.

- A melhor coisa a fazer enquanto estiver navegando na *Web* é ser cauteloso e manter o antivírus e detectores de pragas virtuais em geral sempre atualizados.
- Escolher senhas fortes e não compartilhar com outras pessoas.

5.1.1. Elaborando senhas fortes

Com relação à elaboração de senhas:

“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 apud POPPER; BRIGNOLI, 2003, p. 4-5).

Isso pode ser reforçado pela seguinte opinião:

“Muitos usam como senha, palavras que existem em todos os dicionários, seus apelidos, ou até mesmo o próprio nome que, com um software gerenciador de senhas, é possível decifrá-las em segundos.” (VIRINFO, 2002 apud POPPER; BRIGNOLI, 2003, p. 4).

Para um engenheiro social, uma senha forte será aquela composta por uma sequência aleatória de caracteres. Os seguintes critérios podem ajudar sua senha a se tornar forte: (MICROSOFT CORPORATION, 2006).

- Escolha senhas longas, pois para cada caractere adicionado, maior será a proteção. A quantidade mínima de caracteres recomendável é oito para uma senha segura. O ideal seria no mínimo quatorze caracteres.
- Uma frase secreta é fácil de lembrar e por ser mais longa, será mais seguro ainda.
- A combinação de letras, números e símbolos ajudam bastante a aumentar a força da senha. Quanto maior a variedade de caracteres, mais poderosa será a senha.

- Quanto menor a variedade de caracteres maior deverá ser a senha. Uma senha que possui quinze caracteres composta somente por letras e números aleatórios é cerca de 33.000 vezes mais forte do que uma senha de oito caracteres que é composta por elementos de todo o teclado. É lógico que uma senha ideal possui vários tipos de caracteres diferentes e ao mesmo tempo é longa.
- Use a tecla "Shift", pois sua senha será muito mais forte se você combinar os símbolos gerados através dessa tecla.
- Use frases ou palavras que você lembre com facilidade, mas que ao mesmo tempo seja difícil de alguém adivinhar.

Vejamos alguns passos para criar sua senha forte:

- 1) Escolha uma frase fácil de lembrar como por exemplo. "**Meu filho Carlos tem três anos**" ou então utilize a primeira letra de cada palavra que ficaria assim "**mfctta**".
- 2) Uma ótima opção se o sistema aceitar é a utilização de espaços entre as palavras ou caracteres.
- 3) Lembre-se de que quanto maior e mais complexas as combinações forem, mais forte será a senha, então ao invés de usar "**mfctta**" como no primeiro exemplo, pode-se usar "**MfcTtA**", "**Meu FilhO CarLos tem 3 aNos**" ou "**MeuFilhO KrlOs t&m 3 @no\$.**". Essa é a oportunidade de usar a imaginação.

Teste sua senha em um verificador de senhas. Este é um recurso que ajuda a medir a força da sua senha. (MICROSOFT CORPORATION, [200-?]).

Estratégias para evitar senhas fracas

- Evite escolher sequencias repetidas como, por exemplo: "**123456**", "**3333333**", "**abcdefg**" ou letras próximas no teclado.
- Evite também substituições semelhantes como, '**1**' no lugar de 'i' ou '@' no lugar de 'a', como em "**M1cr0\$0ft**" ou "**Senh@**", lembrando que essas substituições podem sim se tornar fortes mais somente quando combinadas com vários outros caracteres.
- Não use nome de *login*, data de aniversário, parte do nome, número de documentos, informações de familiares, pois informações pessoais e de familiares são as primeiras a serem testadas pelos invasores.

- Também não use palavras encontradas em dicionários, pois existem *softwares* sofisticadíssimos que utilizam essa técnica, e inclusive palavras de trás para frente, erros comuns de digitação, substituições e até mesmo aquelas palavras que um adulto consciente jamais falaria perto das crianças.
- Use uma senha diferente para cada site ou sistema. Pois se você utiliza a mesma senha para tudo e alguém descobrir, todas as outras também serão descobertas e a catástrofe será bem maior.

O objetivo maior dessas dicas é minimizar ou dificultar ao máximo a possibilidade de um ataque de engenharia social. Pois segundo o próprio Kevin Mitnick, considerado o maior entendido do assunto:

“A verdade é que não existe uma tecnologia no mundo que evite o ataque de um engenheiro social” (MITNICK; SIMON, 2003, p. 195).

O próprio Mitnick considerado o maior especialista em engenharia social do qual se tem notícias, em uma das suas raras vindas ao Brasil no final do ano de 2003, concedeu uma entrevista para a Information Week Brasil, onde declarou que foi vítima de engenharia social ao receber uma ligação de um jornalista dizendo que havia conversado com seu editor. Desatento, Mitnick confiou na palavra do jornalista e deu uma entrevista sobre o livro. Depois, quando a reportagem foi publicada o editor de Mitnick ligou para ele furioso, pois toda a estratégia para o lançamento do livro *The Art of Deception* (A arte de enganar) havia sido prejudicada por causa da entrevista, que o editor não havia autorizado. (PEIXOTO, 2006).

CONCLUSÃO

O presente artigo procurou abordar a engenharia social de maneira a esclarecer o que realmente é essa prática tão utilizada nos dias atuais para alcançar algum objetivo através da trapaça. Assim como a importância que a informação tem para as organizações e a necessidade de protegê-la.

A maioria dos incidentes envolvendo a segurança da informação está diretamente ligada ao fator humano, pois este está totalmente relacionado com a segurança da informação. A segurança da informação tem um início e termina nas pessoas. Segurança da informação está mais relacionada com processos do que com a própria tecnologia. Por isso não adiantará nada investir pesado em tecnologia e deixar de lado o fator humano. A conscientização é fundamental, sem ela a empresa corre um risco enorme, pois as vulnerabilidades humanas são evidentes e bem exploradas pelos engenheiros sociais.

O artigo atingiu os objetivos estabelecidos, que eram colaborar como um instrumento de conscientização a respeito do tema proposto, mostrando ao leitor o quanto as pessoas são manipuladas e ludibriadas nos dias de hoje através da engenharia social. Fazer também com que o leitor possa identificar um suposto ataque de engenharia social e, sobretudo reconheça o próprio engenheiro social através de suas características marcantes. Expor também procedimentos básicos que não podem de maneira alguma ficar de fora de uma política de segurança para treinamento e conscientização dos funcionários. E finalmente dar dicas ao leitor que podem ajudá-lo a não cair nas armadilhas do engenheiro social e assim não vir a se tornar mais uma vítima dessa prática.

Conforme proposto no início, o artigo procurou não abordar a parte técnica da segurança da informação que envolve abordagens a respeito de códigos, protocolos e etc. Buscou sim abordar bem os métodos e técnicas utilizadas pelos intrusos para roubarem informações e comprometerem a segurança da informação.

Espero ter alcançado as expectativas do leitor e ter também contribuído de alguma maneira para a difusão do conhecimento adquirido através dessa pesquisa que resultou na criação do artigo proposto.

REFERÊNCIAS

ALLEN, Malcolm. Social Engineering: A Means to Violate a Computer System. **SANS Institute InfoSec Reading Room**. [S.l.], 13 f., june./dec. 2006. Disponível em: . Acesso em: 20 ago. 2010.

ARAUJO, Eduardo E. de. **A VULNERABILIDADE HUMANA NA SEGURANÇA DA INFORMAÇÃO**. 2005. 85 f. Monografia (Graduação)– Faculdade de Ciências Aplicadas de Minas, União Educacional Minas Gerais S/C LTDA, Uberlândia, 2005. Disponível em: . Acesso em: 14 out. 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**: tecnologia da informação: técnicas de segurança - código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005. 120 p. Disponível em: < <http://xa.yimg.com/kq/groups/21758149/952693400/name/ABNT+NBR+ISO+IEC+17799+-+27001-2005++Tecnologia+da+Informa%C3%A7%C3%A3o++T%C3%A9cnicas+de+Seguran%C3%A7a+-+C%C3%B3digo+de+Pr%C3%A1tica+para+a+Gest%C3%A3o>>. Acesso em: 24 set. 2010.

COMITÊ GESTOR DA INTERNET NO BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança. **Cartilha de Segurança para Internet**. São Paulo, 2006. 95 p. Disponível em: . Acesso em: 23 ago. 2010.

ERICKSON, Jon. **Hacking**: the art of exploitation. San Francisco: No Starch Press, 2003.

FONSECA, Paula F. **Gestão de Segurança da Informação**: O Fator Humano. 2009. 16 f. Monografia (Especialização)– Redes e Segurança de Computadores, Pontifícia Universidade Católica do Paraná, Curitiba, 2009. Disponível em: . Acesso em: 24 ago. 2010.

JUNIOR, Guilherme. **Entendendo o que é Engenharia Social**. [S.l.: s.n.], 2006. Disponível em: . Acesso em: 5 set. 2010.

MARCELO, Antonio; PEREIRA, Marcos. **A Arte de Hackear Pessoas**. Rio de Janeiro: Brasport, 2005.

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. **Hacking exposed 6**: network security secrets & solutions. [S.l.]: The McGraw-Hill Companies, 2009.

MICROSOFT CORPORATION. **Ajude a proteger suas informações pessoais com senhas fortes**. [S.l.:s.n.], 2006. Disponível em: . Acesso em: 20 ago. 2010.

MICROSOFT CORPORATION. **Verificador de senha**. [S.l.:s.n.], [200-?]. Disponível em: . Acesso em: 20 ago. 2010.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003.

MITNICK, Kevin D.; SIMON, William L. **The art of intrusion**: the real stories behind the exploits of hackers, intruders, and deceivers. Indianapolis: Wiley Publishing, 2005.

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

PILARES da segurança da informação. Disponível em: . Acesso em: 31 out. 2010.

PIPKIN, Donald L. **Halting the hacker**: a practical guide to computer security. 2nd ed. Upper Saddle River: Pearson Education, 2003.

POPPER, Marcos Antonio; BRIGNOLI, Juliano Tonizetti. **ENGENHARIA SOCIAL**: Um Perigo Eminente. [2003]. 11 f. Monografia (Especialização)– Gestão Empresarial e Estratégias de Informática, Instituto Catarinense de Pós-Graduação – ICPG, [S.l.], [2003]. Disponível em: . Acesso em: 19 ago. 2010.

PRESCOTT, Roberta. **Fator humano**: um dos pilares da segurança da informação. [S.l.:s.n.], 2007. Disponível em: . Acesso em: 03 out. 2010.

RUSSELL, Ryan. **Stealing the network**: how to own the box. Rockland: Syngress Publishing, 2003.

SANTOS, Luciano A. L. **O impacto da engenharia social na segurança da informação**. 2004. 82 f. Monografia (Especialização)– Universidade Tiradentes, Aracaju, 2004. Disponível em: . Acesso em: 14 out. 2010.

SCHWARTAU, Winn. **Engenharia social**: pessoas ainda são elo mais fraco. [S.l.:s.n.], 2010. Disponível em: . Acesso em: 15 out. 2010.

SILVA, Elaine M. da. **Cuidado com a engenharia social**: Saiba dos cuidados necessários para não cair nas armadilhas dos engenheiros sociais. [S.l.:s.n.], 2008. Disponível em: . Acesso em: 20 out. 2010

SILVA, Maicon H. L. F. da; COSTA, V. A. de S. F. **O fator humano como pilar da Segurança da Informação**: uma proposta alternativa. Serra Talhada (PE), 2009. Disponível em: . Acesso em: 31 out. 2010.

SISTEMA DE COOPERATIVAS DE CRÉDITO DO BRASIL; CONFEDERAÇÃO NACIONAL DE COOPERATIVAS DE CRÉDITO. **Cartilha de Segurança da Informação**. [S.l.:s.n.], [200-?]. Disponível em: . Acesso em: 24 ago. 2010.

SKYLAN: technology. Disponível em: . Acesso em: 31 out. 2010.