Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

STELA MARTORINI

Engenharia Social: Como acontece e como evitar

Americana, SP

2012

Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

STELA MARTORINI

Engenharia Social: Como acontece e como evitar

Trabalho de conclusão de curso apresentado a Faculdade de Tecnologia de Americana como parte das exigências do Curso de Tecnologia em Segurança da Informação para obtenção do título de Tecnólogo em Segurança da Informação.

Orientador: Professor Edson Roberto Gaseta

Americana, SP

2012

FACULDADE DE TECNOLOGIA DE AMERICANA

STELA MARTORINI - RA 40191013005

Engenharia Social: Como acontece e como evitar

Monografia aprovada como requisito parcial para obtenção do título de Tecnólogo em Segurança da Informação do curso de Segurança da Informação da Faculdade de Tecnologia de Americana.

Banca Examinadora

Orientador: _____
Professor Edson Roberto Gaseta - FATEC

Professor Convidado: _____
Professor Alexandre Garcia Aguado - FATEC

Presidente da Banca: _____
Professor Carlos Henrique Rodrigues Sarro - FATEC

Americana, 27 de Novembro de 2012

Dedico aos nobres.

Aos nobres famililares, nobres amigos, nobres companheiros, nobres de alma e aos nobres de coração.

“Uma corrente é tão forte quanto seu elo mais fraco.”

Thomas Reid

RESUMO

MARTORINI, Stela. **Engenharia Social:** como acontece e como evitar. 2012. 52f. Trabalho acadêmico (Graduação) – Faculdade de Tecnologia de Americana, Americana.

Na sociedade atual, a informação é considerada um dos ativos mais importantes das organizações, e junto com seu crescente valor, novas ameaças surgem. Dispositivos de segurança são criados e aperfeiçoados diariamente em uma tentativa de amenizar os ataques às informações e consequentemente os danos causados por eles. Porém, uma técnica que visa obter acesso às informações confidenciais sem ter que burlar os dispositivos de segurança da organização aparece no cenário atual e é considerada uma grande ameaça, a chamada Engenharia Social. Sendo assim, este trabalho explora o conceito de Engenharia Social, expondo como ela pode acontecer dentro das organizações e quais ações podem ser tomadas pelo departamento responsável pela segurança da informação para amenizar esse tipo de ameaça.

Palavras-chave: Engenharia Social. Segurança da Informação. Programa de Conscientização.

ABSTRACT

MARTORINI, Stela. **Engenharia Social:** como acontece e como evitar. 2012**.** 52f. Trabalho acadêmico (Graduação) – Setor de TI. Faculdade de Tecnologia de Americana.

In today's society, information is considered one of the most important assets of organizations, and with its increasing value, new threats arise. Safety devices are created and improved daily in an attempt to mitigate the attacks on information and therefore the damage caused by them. However, a technique that seeks access confidential information without having to cheat the security features of the organization appears in the current scenario and is considered a big threat, called Social Engineering. Thus, this work explores the concept of Social Engineering, exposing how it can happen within organizations and what actions can be taken by the security information responsible department to mitigate such threats.

Keywords: Social Engineering. Information Security. Awareness Program.

Lista de Figuras

LISTA DE SÍMBOLOS

@	Arroba

SUMÁRIO

INTRODUÇÃO

Antigamente, quando o homem descobriu o valor das coisas e passou a trocá-las por outros bens, sal e depois dinheiro, não sabia que de certa forma a informação seria a nova moeda da era digital. (MARCELO e PEREIRA, 2005)

Atualmente, a informação representa a inteligência competitiva dos negócios por estar integrada com os processos, as pessoas e as tecnologias e é reconhecida como ativo crítico para a continuidade operacional e saúde de uma organização. (SÊMOLA, 2003)

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste aumento da interconectividade, a informação está exposta a uma grande variedade de ameaças e vulnerabilidades. (NBR ISO/IEC 17999, 2005)

A preservação da segurança dessas informações não é de total responsabilidade dos dispositivos de tecnologia, grande parte dessa responsabilidade deve ser atribuída aos colaboradores da organização que têm acesso as informações, e que infelizmente, na maioria das vezes não estão preparados para lidar e reconhecer situações de risco.

Conhecendo o valor das informações e o elo mais fraco do sistema que as compõem foi desenvolvida uma técnica chamada Engenharia Social, onde o sujeito que a utiliza visa obter acesso a informações confidenciais sem ter que burlar a segurança dos ativos da organização.

Este trabalho tem como objetivo apresentar o conceito de Engenharia Social, destacando como ela acontece em um ambiente corporativo e como pode ser evitada.

Para a elaboração deste trabalho foram consultados três livros sobre Engenharia Social, além de artigos publicados em *websites* e trabalhos

acadêmicos sobre o assunto. Durante a pesquisa foram selecionados alguns livros para o embasamento científico e referência bibliográfica deste.

Este trabalho foi estruturado em capítulos iniciais que apresentam o que é Engenharia Social e como ela acontece. Sendo o capítulo um, uma breve introdução sobre o conceito de falsa ideia de segurança presente nas pessoas nos dia de hoje; o segundo capítulo introduz o conceito de Engenharia Social e apresenta o perfil de um Engenheiro Social, as ferramentas e os traços comportamentais explorados por ele e o terceiro trata sobre os tipos de Engenharia Social e as formas de abordagem utilizadas pelos Engenheiros Sociais quando se trata de Engenharia Social Voluntária.

A segunda parte deste trabalho tem como foco apresentar ações que podem evitar a Engenharia Social em ambientes corporativos, sendo o capítulo quatro uma apresentação dos pontos principais para evitar os ataques de Engenharia Social, tendo como foco a realização de treinamentos e programas de conscientização, além de métodos para avaliar se os programas estão realmente sendo efetivos. Um estudo de caso é apresentado no capítulo cinco seguido da conclusão do trabalho.

1 A FALSA IDEIA DE SEGURANÇA

Em um mundo cheio de crimes, violências, homicídio, roubos de identidade, clonagem de cartões de crédito entre todas as outras formas de se apoderar de algo que por lei e direito não é seu, é natural nascer entre a sociedade a necessidade de se sentir seguro e isso leva muitas pessoas a buscarem uma falsa ideia de segurança.

É o caso do responsável proprietário de uma casa, a qual foi instalada uma cerca elétrica, um sistema de alarme para detecção de intrusos, além de um cadeado de fechadura conhecido como sendo à prova de roubo instalado na porta da frente para proteger sua esposa, seus filhos e sua casa. Agora ele está certo de que tornou sua família muito mais segura com relação a intrusos. Mas e o intruso que quebra uma janela ou descobre o código que abre a porta da garagem? Ou o criminoso que consegue a sua senha do banco através de *websites* falsos? E o ladrão que descobre o número do seu celular e simula um sequestro contra sua filha para conseguir seu dinheiro através de um resgate? (MITNICK e SIMON, 2003)

Infelizmente, estes tipos de ataques são frequentes e as pessoas raramente percebem que estão sendo vítimas. Nesses casos, nem mesmo o melhor e mais eficiente sistema de segurança consegue deter o criminoso. Não importa o nível de segurança que o proprietário da casa acredita possuir, nunca haverá garantia da sua total segurança. Isto acontece porque, como explica Mitnick e Simon (2003), o elo mais fraco da segurança é o fator humano.

Da mesma forma que o proprietário da casa no exemplo acima acredita que sua casa está protegida de invasões, muitos profissionais da tecnologia da informação conservam a mesma errônea ideia de que tornaram suas organizações imunes aos ataques porque usaram produtos padrões de segurança, como por exemplo, antivírus, *firewalls*, sistemas de detecção de intrusos *(Intrusion Detection Systems),* sistemas de prevenção de intrusos *(Intrusion Prevention Systems)* ou dispositivos avançados de autenticação, tais como: *tokens*, biometria, leitura facial ou de retina, entre outros.

> A segurança é apenas uma ilusão, que fica mais defasada ainda quando entram em jogo a credulidade, a inocência ou a ignorância dos seres humanos (...). Todos que acham que os produtos de segurança sozinhos oferecem a verdadeira segurança estão fadados a sofrer da chamada ilusão da segurança. (MITNICK e SIMON, 2003).

2 ENGENHARIA SOCIAL

> *"- Receias, acaso, que esteja envenenada? - disse a mulher - Olha, vou comer a metade da maçã e tu depois poderás comer o resto para veres que deliciosa é ela."*
>
> *Branca de Neve - Irmãos Grimm*

As técnicas que compõe um ataque de Engenharia Social nos são apresentadas desde cedo e podem ser facilmente encontradas no nosso dia-a-dia. Muitas vezes elas não são utilizadas com o objetivo de um estrago mais profundo, porém, todos nós já utilizamos, ou fomos vítimas dessas técnicas.

Quando crianças, as primeiras estórias infantis que nos apresentam, já contêm uma dose de persuasão e tentativa de enganação das inocentes protagonistas. Nos deparamos, por exemplo, com o caso da bruxa má, que consegue convencer a Branca de Neve a morder a maçã envenenada que a levará ao sono eterno, da mesma forma que o Lobo Mau rouba a identidade de alguém que a Chapeuzinho Vermelho confia, a avó, para conseguir janta-la.

Neste trabalho, será estudado o termo Engenharia Social designado às práticas utilizadas a fim de se obter informações sigilosas ou importantes de organizações, pessoas ou sistemas de informações. Essas técnicas consistem em explorar as fragilidades encontradas nos seres humanos para conseguir chegar até a informação que lhe interessa sem passar pelos dispositivos de segurança.

2.1 Definição

Levando-se em conta o significado das palavras supostamente separadas, têm-se:

Engenharia: Aplicação do conhecimento científico e empírico, e certas habilitações específicas, à criação de estruturas, dispositivos e processos para converter recursos naturais em formas adequadas ao atendimento das necessidades humanas. (FERREIRA, 1993)

Social: Da sociedade, ou relativo a ela. (FERREIRA, 1993)

Analisando os termos em conjunto, o termo “Engenharia” foi atribuído porque as práticas da Engenharia Social constroem táticas de acesso a sistemas e informações sigilosas de forma indevida e “Social” porque utiliza de pessoas que trabalham e vivem em uma sociedade, ou seja, em grupos organizados. (SANTOS, 2004)

> A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter informações com ou sem o uso da tecnologia da informação. (MITNICK e SIMON, 2003).

2.2 Perfil do Engenheiro Social

O Engenheiro Social combina a falsa ideia de segurança presente nas organizações, a credulidade do ser humano e as suas técnicas de persuasão para obter sucesso nos seus ataques.

De acordo Mitnick e Simon (2003), quando você combina uma inclinação para enganar as pessoas com os talentos da influência e persuasão você chega ao perfil de um Engenheiro Social.

O Engenheiro Social é do tipo dinâmico, comunicativo, expressivo e seguro de si. Esse tipo de pessoa transborda confiança no que diz, por isso, é muito difícil não acreditar nas estórias que eles contam e se sentir à vontade para ajudá-los.

2.3 Ferramentas mais utilizadas pelo Engenheiro Social

De acordo com Peixoto (2006), as principais ferramentas utilizadas pelo praticante da Engenharia Social são:

a) Telefone ou VoIP (voz sobre IP): É a técnica mais utilizada pelos engenheiros sociais e consistem em assumir uma identidade falsa por meio de ligação telefônica. Exemplo: Engenheiro Social passar-se por um *help-desk*.

b) Internet (coleta de informações): Utilização de sites com identificação e senha padrão fornecidos pelo próprio sistema, sites clonados ou via FTP, Orkut, *Facebook*, registro.br, Google, dentre outros.

c) Intranet (acesso remoto): Esta técnica é a mais utilizada por funcionários insatisfeitos, como estes já possuem um conhecimento do ambiente corporativo alvo, a invasão fica mais fácil. Através de acesso remoto, praticam Engenharia Social, utilizando o endereço IP de uma determinada máquina da rede, passando por usuários autorizados, para quebrarem a integridade e a confidencialidade de sistemas.

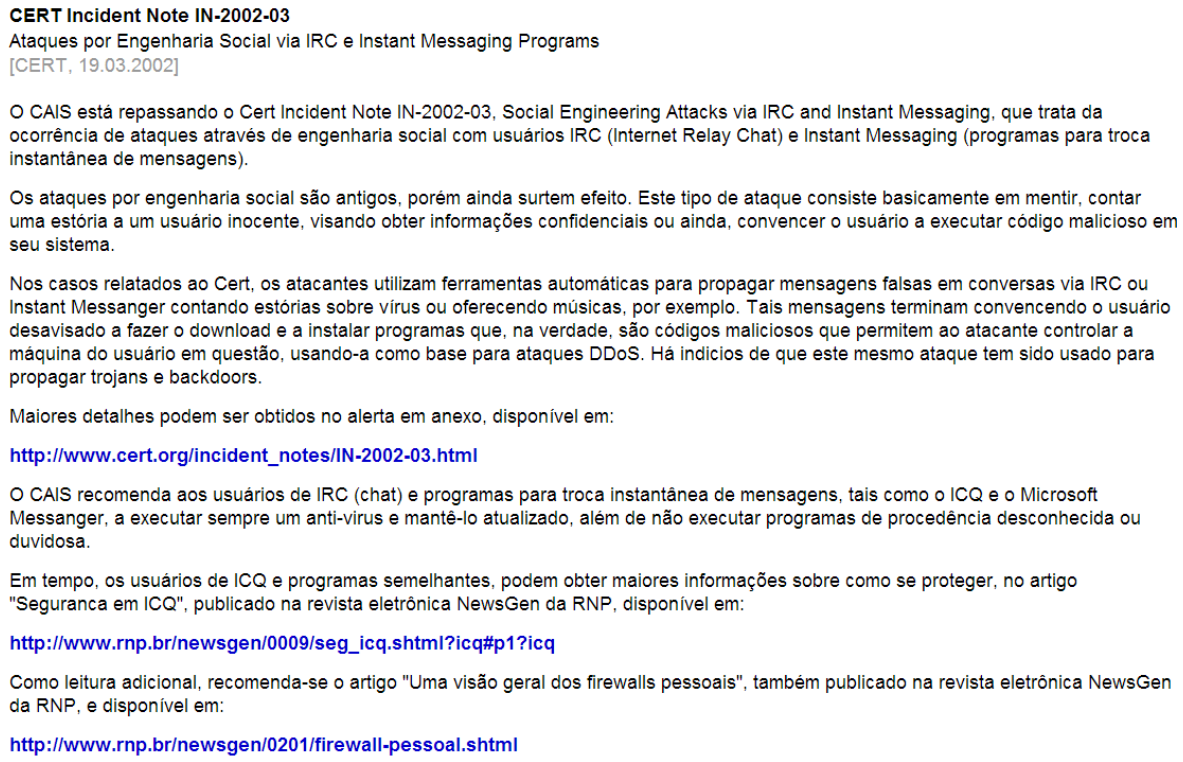
d) *E-mail Phishing Scam*: Nesta técnica, o Engenheiro Social envia mensagens eletrônicas induzindo a vítima a acessar um determinado *link*, que propiciará o preenchimento de seus dados em um formulário ou a instalação de um programa ofensivo. Neste tipo de fraude, o criminoso faz-se passar por uma entidade credível ou de confiança do usuário, para que fique mais fácil a obtenção das informações.

e) Pessoalmente (*In Person Social Engineering*): Engenheiro Social faz-se passar por alguém que na verdade ele não é. Adota toda uma encenação e

como um verdadeiro artista busca manipular a vítima de forma a ser bastante convincente no que diz. Esse tipo de ataque ganha mais força quando o atacante já conhece literalmente o território no qual vai pisar, mas, sobretudo, já tem consigo informações que lhe conferem subsídios para persuadir a vítima, valendo-se às vezes até mesmo das informações ditas como confidenciais. Alguns recursos a favor do Engenheiro Social seriam: sedução, intimidação, dramaticidade e credibilidade.

f) *Chats* (bate-papo): Fazer-se passar por alguém que na verdade não é fica muito mais fácil pelos canais de bate-papo. Além de tudo, com o envio de fotos o ataque fica bem mais atrativo e sedutor. Exemplo: Messenger.

O site da RNP (Rede Nacional de Ensino e Pesquisa), junto ao CAIS (Centro de Atendimento a Incidentes de Segurança) publicou em 2002 um alerta sobre um Incidente que foi reportado pelo CERT.org (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança) sobre ataques por Engenharia Social via IRC (*Internet Relay Chat*) e *Instant Messaging Programs.*



CERT Incident Note IN-2002-03
Ataques por Engenharia Social via IRC e Instant Messaging Programs
[CERT, 19.03.2002]

O CAIS está repassando o Cert Incident Note IN-2002-03, Social Engineering Attacks via IRC and Instant Messaging, que trata da ocorrência de ataques através de engenharia social com usuários IRC (Internet Relay Chat) e Instant Messaging (programas para troca instantânea de mensagens).

Os ataques por engenharia social são antigos, porém ainda surtem efeito. Este tipo de ataque consiste basicamente em mentir, contar uma estória a um usuário inocente, visando obter informações confidenciais ou ainda, convencer o usuário a executar código malicioso em seu sistema.

Nos casos relatados ao Cert, os atacantes utilizam ferramentas automáticas para propagar mensagens falsas em conversas via IRC ou Instant Messanger contando estórias sobre vírus ou oferecendo músicas, por exemplo. Tais mensagens terminam convencendo o usuário desavisado a fazer o download e a instalar programas que, na verdade, são códigos maliciosos que permitem ao atacante controlar a máquina do usuário em questão, usando-a como base para ataques DDoS. Há indicios de que este mesmo ataque tem sido usado para propagar trojans e backdoors.

Maiores detalhes podem ser obtidos no alerta em anexo, disponível em:

http://www.cert.org/incident_notes/IN-2002-03.html

O CAIS recomenda aos usuários de IRC (chat) e programas para troca instantânea de mensagens, tais como o ICQ e o Microsoft Messanger, a executar sempre um anti-virus e mantê-lo atualizado, além de não executar programas de procedência desconhecida ou duvidosa.

Em tempo, os usuários de ICQ e programas semelhantes, podem obter maiores informações sobre como se proteger, no artigo "Seguranca em ICQ", publicado na revista eletrônica NewsGen da RNP, disponível em:

http://www.rnp.br/newsgen/0009/seg_icq.shtml?icq#p1?icq

Como leitura adicional, recomenda-se o artigo "Uma visão geral dos firewalls pessoais", também publicado na revista eletrônica NewsGen da RNP, e disponível em:

http://www.rnp.br/newsgen/0201/firewall-pessoal.shtml

Figura 01 – Nota de Incidente do CERT. Alerta sobre ataques por Engenharia Social via IRC e *Instant Messaging Programs*. Fonte: (CERT.br, 2002)

g) Cartas/Correspondências: Método utilizado para atacar vítimas mais idosas ou que tenham resistência à tecnologia. O ataque consiste em enviar documentos pedindo alguma ação da vítima. Nesses casos, para tornar o ataque mais real, o atacante utiliza logomarcas de organizações públicas ou privadas conhecidas.

h) *Spyware:* Como define Amanda Xavier (2008) em sua publicação no site tecmundo, *spywares* são programas espiões, isto é, sua função é coletar informações sobre uma ou mais atividades realizadas em um computador. No caso da Engenharia Social, o atacante utiliza destes programas mal feitores para coletar informações confidenciais pessoais ou de organizações e, com elas, praticar atividades ilegais.

Exemplo: Engenheiro social envia e-mail contendo *spyware*, passando-se por integrante do departamento de segurança de um banco, apresentando um link para uma possível atualização do *Internet Banking*. Quando o mouse é

posicionado em cima do link, pode-se observar que o endereço correspondente não tem ligação alguma com o site da instituição financeira em questão (vide Figura 03).

Figura 02 – Exemplo de e-mail contento *spyware*. E-mail falso que direciona o usuário para o download e instalação de um software malicioso. Fonte: (MARTORINI, 2012).

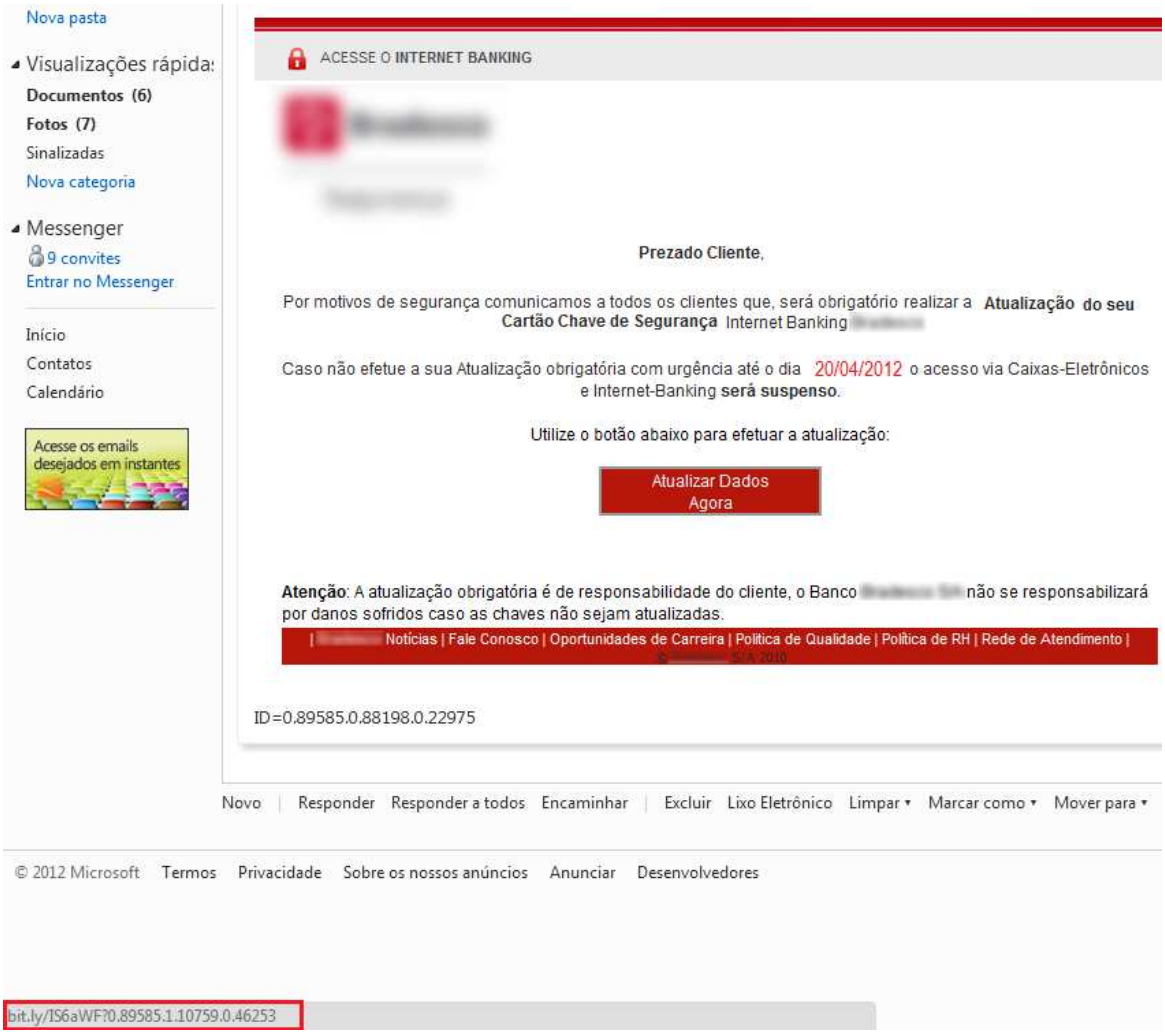


Figura 03 – Exemplo de e-mail contento *spyware*. E-mail falso que direciona o usuário para um link que não é de propriedade de Banco em questão, induzindo o usuário a instalar um software malicioso. Fonte: (MARTORINI, 2012).

i) Mergulho no lixo ("*Dumpster diving*"): São inúmeras as informações, dos mais variados tipos, que se encontram no lixo (cadernetas com informações pessoais, senhas, telefones, números de documentos, informações sobre eventos, cursos, relatórios patrimoniais, manuais com instruções internas da empresa, informações dos funcionários, papel timbrado da empresa, etc) e estas, às vezes, são cruciais na construção de um ataque de Engenharia Social.

j) Surfar sobre os ombros: É o ato de observar a vítima ao digitar no teclado do computador suas senhas ou outras informações a fim de roubá-las. Essa parte exige boa memorização e discrição do Engenheiro Social. Algumas

aplicações são exemplos reais de como se pode executar Engenharia Social, devido a alguns recursos por eles oferecidos, como envio de mensagens, demonstração de IP's ou nomes, enfim, a comunicação propriamente estabelecida já pode ser um fator favorável ao Engenheiro Social.

k) P2P (*Peer-to-Peer*): Tecnologia empregada para estabelecer comunicação entre inúmeros computadores, como uma rede, onde cada estação possui capacidades e responsabilidades equivalentes.

2.4 Traços comportamentais e psicológicos explorados pelo Engenheiro Social

De acordo com Maslow (1968), as necessidades de segurança, filiação, relações de amor e respeito só podem ser satisfeitas por outras pessoas, isto é, somente de fora da pessoa. Isso significa uma considerável dependência do ambiente.

Maslow (1968) também explica que uma pessoa nessa posição dependente não se pode dizer, realmente, que governa a si mesma ou que exerce o controle do seu próprio destino. Ela deve estar vinculada às fontes de suprimento das satisfações necessárias. Os desejos, caprichos, regras e leis dessas fontes governam a pessoa e têm de ser apaziguados, para que ela não ponha em risco as suas fontes de abastecimento.

Em certa medida, a pessoa deve ser sensível à aprovação, afeição e boa-vontade de outras pessoas. Isso é o mesmo que dizer que ela deve adaptar-se e ajustar-se, sendo flexível e receptiva, e modificando-se para se harmonizar à situação externa. (MASLOW, 1968)

É exatamente nesse cenário de dependência externa que o Engenheiro Social se aproveita da necessidade do ser humano de se ajustar ao ambiente em

que ela trabalha ou vive e aplica suas técnicas. Dentre os traços comportamentais e psicológicos explorados pelo Engenheiro Social, temos os principais:

a) Vaidade pessoal e/ou profissional: Marcelo e Pereira (2005) afirmam que o ser humano adora se sentir à vontade com outro e melhor ainda se este for “inferior” a ele. Um dos grandes pontos que o Engenheiro Social pode explorar é o ego de seus alvos.

O ser humano costuma ser mais receptivo quando recebe uma avaliação positiva e favorável, como elogios, tornando-se mais vulnerável a ataques de Engenharia Social.

b) Autoconfiança: A maioria das pessoas supõe que não será enganada, com base na crença de que a probabilidade de ser enganada é muito baixa, elas possuem uma autoconfiança muito grande, principalmente os colaboradores que já estão na empresa há muito tempo e conhecem todos os processos e procedimentos da mesma. (MITNICK e SIMON, 2003)

c) Formação Profissional: O ser humano busca valorizar as habilidades adquiridas na sua formação profissional, buscando o controle em uma comunicação, execução ou apresentação seja ela profissional ou pessoal, visando o reconhecimento pessoal inconscientemente em primeiro plano.

d) Vontade de ser útil: O ser humano, comumente, procura agir com cortesia, ajudando os outros quando necessário. Ele não nega a ajuda porque acredita que um dia pode ser ele quem esteja em uma situação complicada e precise da ajuda do colega de trabalho.

e) Busca por novas amizades: Como afirmaram Marcelo e Pereira (2005), explorar os sentimentos de carência e de amizade é uma das formas mais comuns desses invasores.

O ser humano costuma se agradar quando se comunica com alguém dinâmico e que o faça sentir bem, principalmente em um ambiente estressante de trabalho, tornando-se mais vulnerável e suscetível a fornecer informações, com o intuito de estabelecer amizades com o outro indivíduo.

f) Propagação da responsabilidade: Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades, o que o ajuda a não ver problemas em dividir informações com outros supostos colegas de trabalho.

g) Persuasão: Compreende quase uma arte a capacidade de persuadir pessoas, onde se busca obter respostas específicas. Isto é possível porque as pessoas possuem as características comportamentais, citadas acima, que as tornam vulneráveis à manipulação.

3 TIPOS DE ENGENHARIA SOCIAL

Podemos classificar a Engenharia Social em Involuntária e Voluntária.

3.1 Engenharia Social Involuntária

É aquela que todos nós praticamos sem saber que se trata de Engenharia Social. São ações e atitudes que temos, em relação ao outro visando obter algum tipo de informação que nos será útil no futuro.

Um exemplo de Engenheiros Sociais Involuntários são os nossos pais. Desde sempre, eles conseguem nos convencer através de histórias, motivos e justificativas muito bem desenvolvidas a fazermos aquilo que eles acreditam que seja o melhor para nós. (MITNICK e SIMON, 2003)

Outro exemplo de Engenharia Social involuntária é a técnica utilizada em ambientes sociais, que está relacionada à conquista do outro de uma forma geral. Involuntariamente passamos a buscar informações da pessoa desejada por intermédio de amigos, parentes, redes sociais, entre outros.

Após recolher as informações sobre o "alvo", como por exemplo, o estilo de música que ele gosta, os lugares que frequenta, os livros que interessam e os filmes preferidos, nós nos sentimos seguros para abordá-lo, e a partir disso, conquistar a confiança e/ou interesse daquela pessoa para iniciarmos o relacionamento desejado. (REGINALDO, SANTOS e ESPADONI, 2010)

3.2 Engenharia Social Voluntária

Trata-se do tipo de Engenharia Social em que este trabalho está focado. Esta é a forma maléfica de utilizar as técnicas de Engenharia Social e está

associada à maioria dos casos, sendo utilizada por pessoas que buscam violar sistemas, obter informações de forma desonesta, objetivando lucros pessoais ou empresariais. (REGINALDO, SANTOS e ESPADONI, 2010)

Afirmar que esse tipo de ataque é o mais frequente nos dias de hoje e possuem maior efetividade é inviável, visto que não existem dados estatísticos específicos sobre esse tipo de ataque. Isso acontece porque dificilmente uma pessoa se dá conta de que foi vítima de um ataque de Engenharia Social ou ajudou como coadjuvante, a não ser que as consequências desse ataque reflitam diretamente em algo visível pela vítima. Por exemplo, no caso de uma pessoa física, algum valor alto ser debitado da sua conta sem o conhecimento do mesmo. No caso de pessoa jurídica, um projeto de um produto inovador ser lançado por uma empresa concorrente. Às vezes, mesmo que a vítima se dê conta do ataque, ela o omite para não denegrir sua imagem ou a imagem da organização.

Entretanto, em um gráfico publicado no site do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) em abril de 2012, sobre os incidentes reportados ao CERT.br entre os meses de Janeiro e Março de 2012, é possível identificar uma categoria a qual os ataques de Engenharia Social se encaixam.

Com 15,37% de incidentes reportados, a categoria "fraude", que de acordo com a legenda do site, "engloba todos os incidentes em que ocorre uma tentativa de obter vantagem" e "quaisquer esquemas utilizados para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras", ocupa o quarto lugar na lista das categorias de incidentes reportados. A Engenharia Social pode ser encaixada neste tipo de categoria, visto que sua técnica principal consiste em enganar um usuário para obter vantagem.

Incidentes Reportados ao CERT.br -- Janeiro a Março de 2012

Figura 04 – Gráfico de Incidentes reportados ao CERT.br. Gráfico dos tipos de ataques reportados entre o período de Janeiro e Março de 2012. Fonte: (CERT.br, 2012)

Legenda:

- ***Worm***: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede. (15,61%)
- **DoS** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede. (0,07%)
- **Invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede. (1,85%)
- ***Web***: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet. (9,01%)
- ***Scan***: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar

possíveis vulnerabilidades aos serviços habilitados em um computador. (31,67%)

- **Fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem. (15,37%)
- **Outros**: notificações de incidentes que não se enquadram nas categorias anteriores. (26.4%)

  Obs.: Vale lembrar que **não se deve confundir *scan* com *scam***. *Scams* (com "m") são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.

3.3 Formas de abordagem utilizadas pelo Engenheiro Social

3.3.1 Criando a Confiança

De acordo com Mitnick e Simon (2003), nós, como seres humanos, estamos todos sujeitos a ser enganados, porque a confiança das pessoas pode ser usada de forma errada se for manipulada de determinadas maneiras.

A confiança é um sentimento imprescindível que os Engenheiros Sociais precisam despertar em suas vítimas para que os ataques sejam realizados com sucesso. A questão é: como eles fazem para obter a confiança de alguém que nem se quer, em algumas situações, estão vendo pessoalmente?

Inicialmente o Engenheiro Social coleta o máximo possível de informações sobre o alvo, além de jargões comumente utilizados naquele ambiente que irá atacar. Quando o Engenheiro Social conhece a linguagem de uma empresa, sua

estrutura corporativa, bem como os departamentos existentes e suas funções, ele adquire credibilidade. E credibilidade leva à confiança. (MITNICK e SIMON, 2003)

Outro truque que o Engenheiro Social utiliza para adquirir a confiança do próximo é abusando do respeito hierárquico que existe dentro das organizações. Quando alguém se apresenta como “Secretária do Diretor”, “Gerente do Departamento de Finanças”, “Administrador de Sistemas” ou qualquer outro título que esteja um nível acima do seu, fica mais difícil negar ou até mesmo duvidar de qualquer solicitação que lhe é feita.

3.3.2 Quando as informações não são inofensivas

A maioria das invasões da segurança de uma empresa começa com o Engenheiro Social obtendo alguma informação ou algum documento que parece ser muito inocente, tão comum e sem importância que a maioria das pessoas da organização não vê motivo pelo qual ela deva ser protegida e restrita.

Esse tipo de informação, que é aparentemente inócua de posse de uma empresa, é cobiçada por um atacante de Engenharia Social porque ela pode ter um papel vital em seu esforço de se revestir de credibilidade, e como explorado no capítulo acima, credibilidade leva à confiança. (MITNICK e SIMON, 2003)

Para conseguir obter essas informações aparentemente sem valor, o Engenheiro Social envolve a vítima com muitas perguntas que não possuem relevância para ele e introduz entre elas, as perguntas que fornecerão o que ele realmente precisa.

Em um exemplo extraído do livro A Arte de Enganar, de Mitnick e Simon (2003), é possível observar como o Engenheiro Social consegue extrair essas informações.

> “ National Bank, Contas Novas, Chris,”.
> “ Olá Chris. Aqui é o Alex”, o interlocutor diz. “Eu sou um representante do serviço ao cliente da CreditChex. Estamos fazendo uma pesquisa para melhorar os nossos serviços. Você tem alguns minutos?”
> Ela concordou e o interlocutor continua:

> “Muito bem – qual o horário de funcionamento da sua filial?” Ela respondeu e continuou respondendo às suas perguntas.
> “Quantos empregados da sua filial usam o nosso serviço?”
> “Com que frequência você liga para nós com uma consulta?”
> “Qual dos nossos números 800 nós designamos para vocês usarem ao ligar para nós?”
> “Os nossos representantes são sempre educados?”
> “Qual o nosso tempo de resposta?”
> “Ha quanto tempo você trabalha no banco?”
> “Qual ID de Comerciante você está usando no momento?”
> “Você já encontrou alguma imprecisão nas informações que fornecemos?”
> “Se você tivesse alguma sugestão para melhorar o nosso serviço, qual seria?”
> E finalmente:
> “Você se importaria em preencher questionários periódicos se os enviássemos para sua filial?”
> Ela concordou, eles conversaram um pouco, o interlocutor desligou e Chris voltou ao trabalho.

Neste exemplo, o que o Engenheiro Social realmente gostaria de saber era o ID de Comerciante e a tática usada por ele foi incluir a pergunta mais importante entre aquelas sem relevância, para criar uma ideia de credibilidade, visto que se a pergunta fosse feita solta, fora do contexto, seria muito provável que a vítima desconfiasse.

3.3.3 Ataque Direto: simplesmente pedindo

As técnicas utilizadas pelos engenheiros sociais estão interligadas. Elas são como peças de um quebra-cabeça que quando unidas, fazem com que a estória contada pelo engenheiro faça sentido e não desperte a desconfiança nas vítimas. Nesse tipo de ataque direto, o Engenheiro Social primeiro adquire as informações que, aparentemente, são inofensivas. Com essas informações em mãos, ele consegue ganhar a confiança de alguém de dentro da empresa que pode fornecer os dados que ele realmente visa. E ele consegue obtê-los simplesmente pedindo.

3.3.4 Posso ajudar?

Ficamos agradecidos quando temos um problema e alguém com conhecimento, habilidade e disposição nos oferece ajuda. O Engenheiro Social entende isso e sabe como se aproveitar da situação. Ele cria uma teia para convencer a vítima de que ela tem um problema que na verdade não existe ou que ainda não aconteceu, mas que o atacante sabe que acontecerá porque ele vai causá-lo. Em seguida ele se apresenta como a pessoa que pode fornecer a solução.

Se a vítima acredita que você está tentando ajuda-la ou prestar-lhe algum tipo de favor, ela dificilmente hesitará em compartilhar as informações confidenciais que de outra forma teriam sido protegidas.

Neste tipo de técnica, os alvos preferidos do Engenheiro Social são os empregados novos porque eles ainda não conhecem a fundo os procedimentos e o que pode ou não fazer dentro da empresa e, para causar uma boa impressão, eles estão ansiosos para mostrar como são prestativos e como podem ser rápidos. Outro alvo importante neste tipo de ataque são os empregados mais antigos da empresa, principalmente aqueles que possuem certa resistência à tecnologia. (MITNICK e SIMON, 2003)

3.3.5 Você pode me ajudar?

Esta técnica é muito parecida com a “simplesmente pedindo”, pois se baseia no fato de estar também solicitando um pedido de informação. Uma das diferenças é a questão da utilização da dramaticidade juntamente com a disposição que a vítima tem em ajudar.

Um dos métodos mais poderosos utilizados pelos Engenheiros Sociais é o golpe simples de fingir que precisa de ajuda. O Engenheiro leva em conta que o funcionário, novo ou velho de casa, vendo o problema em que seu “companheiro

de trabalho” se encontra, se sensibilizará e não hesitará em cooperar e assim fornecer o que ele deseja. (PEIXOTO, 2006)

Essa disposição de ajudar um colega com um problema faz parte daquilo que lubrifica as engrenagens da indústria, e parte daquilo que torna os empregados de algumas organizações mais agradáveis de trabalhar do que os empregados de outras organizações. Mas essa disposição em ajudar pode ser uma grande vulnerabilidade que um Engenheiro Social explorará. (MITNICK e SIMON, 2003)

3.3.6 Engenharia Social Inversa

Esse tipo de ataque pode acontecer de duas formas:

1. O atacante cria um cenário onde a vítima tem um problema e entra em contato com ele para conseguir resolver;
2. Outra forma acontece quando o alvo reconhece o ataque e usa princípios psicológicos de influência para tirar o máximo possível de informações do atacante para que a empresa possa preservar os ativos que estão sendo visados pelos Engenheiros Sociais. (MITNICK e SIMON, 2003)

3.3.7 Engenharia Social na Internet

No capítulo 2 deste trabalho, a internet foi identificada como um recurso utilizado pelos Engenheiros Sociais para coletar informações sobre suas vítimas. Sendo assim, atualmente ela se tornou um território cheio de armadilhas prontas para a qualquer momento instalar um *malware*[1] em sua máquina.

1 Abreviação de *malicious software* - software malicioso. *Malware* é qualquer tipo de software indesejado, instalado sem o seu devido consentimento. (Microsoft)

Os *malwares* estão escondidos em documentos que aparentemente são inocentes como, por exemplo, uma planilha, uma foto ou até mesmo uma apresentação de slides, mas ele instala secretamente um programa não autorizado. Após esse *software* instalado máquina, ele pode transmitir para o atacante cada tecla digitada na máquina, incluindo senhas, número de cartão de crédito, entre outras informações confidenciais. (MITNICK e SIMON, 2003)

Essa técnica de tentar enganar uma pessoa induzindo-a a abrir uma mensagem ou um documento que instale um programa malicioso em sua máquina é chamada atualmente de *phishing.*

De acordo com a Cartilha de Segurança do Cert.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), *phishing* é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

O *phishing* ocorre por meio do envio de mensagens eletrônicas que:

- Tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um *site* popular;
- Procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
- Informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;
- Tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas *Web*.

Para atrair a atenção do usuário, as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, imagens de pessoas e assuntos em destaque no momento.

A Cartilha de Segurança do Cert.br também apresenta outros golpes de internet, dentre eles:

- **Furto de identidade (*Identity theft*):** É o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas. Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade.

- **Fraude de antecipação de recursos (*Advance fee fraud*):** A fraude de antecipação de recursos, ou *advance fee fraud*, é aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.

- ***Pharming*:** É um tipo específico de *phishing* que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (*Domain Name System*). Neste caso, quando você tenta acessar um site legítimo, o seu navegador Web é redirecionado, de forma transparente, para uma página falsa.

4 AÇÕES PARA EVITAR A ENGENHARIA SOCIAL

Mitnick e Simon (2003) afirmam que não existe uma tecnologia no mundo que evite o ataque de um Engenheiro Social. Entretanto, eles apresentam três itens que, quando combinados, conseguem amenizar a ameaça da Engenharia Social. São eles:

- Conscientização dos empregados para a segurança da informação;
- Educação e treinamento e
- Políticas de Segurança que definem as principais regras para o comportamento do empregado.

Este capítulo do trabalho dissertará sobre os dois primeiros tópicos, assumindo que as organizações já tenham uma política de segurança com suas diretrizes definidas, o trabalho será focado em como deve ser feita a conscientização, educação e treinamento dos funcionários para que eles aceitem que são responsáveis pela segurança das informações e se sintam motivados a protegê-las, tornando-se assim, alvos difíceis para ataques de Engenharia Social.

4.1 Políticas de Segurança

Deve-se ressaltar que a política de segurança da empresa precisa ser muito específica quanto às salvaguardas para proteger dados valiosos contra alguém que não seja conhecido pessoalmente como o remetente, para isso, é essencial a existência de procedimentos padronizados para a verificação da identidade de alguém que solicita informações.

Esses procedimentos devem ser uma extensão da política de segurança, e devem conter etapas claras para a verificação da identidade de um solicitante, com níveis diferentes de autenticação, dependendo do grau de confidencialidade das informações requisitadas. (MITNICK e SIMON, 2003)

4.2 Conscientização e Treinamento

De acordo com Mitnick e Simon (2003), as organizações devem não apenas definir por escrito as regras das políticas, mas também devem se esforçar para orientar todos os que trabalham com as informações corporativas ou com os sistemas de computadores para que eles aprendam e sigam essas regras.

> Todos são tão vulneráveis aos ataques de Engenharia social que a única defesa efetiva de uma empresa é educar e treinar o seu pessoal, dando-lhes a prática que precisam para identificar um Engenheiro Social. (MITNICK e SIMON, 2003).

O primeiro passo para que um programa de conscientização seja eficiente, é educar os funcionários através de treinamentos regulares. Após a realização dos treinamentos, é essencial a utilização de técnicas que reforcem dia-a-dia a importância de assumir uma postura responsável quando se lida com informações coorporativas.

Um programa de conscientização deve estar em constante atualização. Da mesma forma que os Engenheiros Sociais encontram novas técnicas, o setor responsável pelos treinamentos de Segurança de uma organização deve estar estudando e atualizando suas técnicas e métodos de conscientização dos funcionários. Para isto, é essencial realização de testes que avaliem se os programas estão ou não gerando os resultados esperados.

A Figura 05, baseada nas ideias de Mitnick e Simon, ilustra os principais passos para a construção e manutenção de um programa de conscientização sobre segurança da informação.

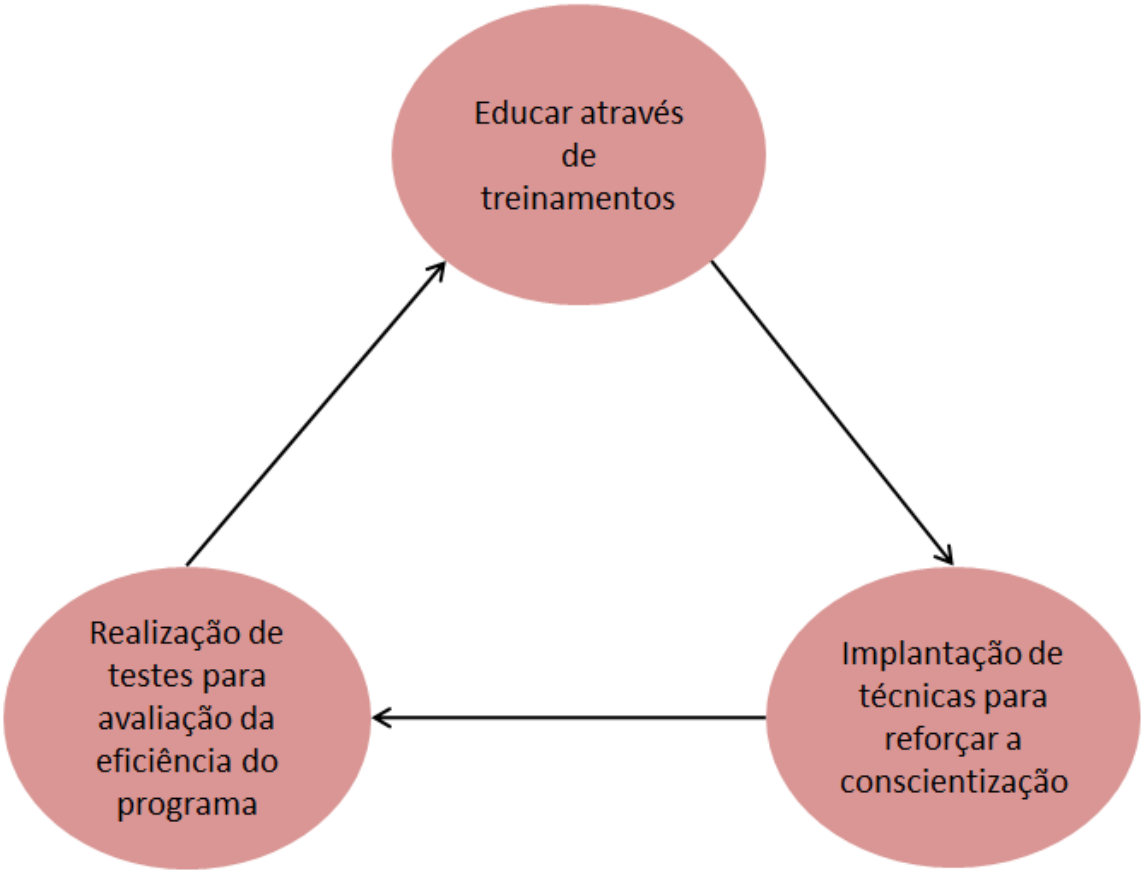


Figura 05 – Passos para a criação de um programa de conscientização. Abstração dos pontos principais para o desenvolvimento de um programa de conscientização eficiente. Fonte: (MITNICK e SIMON, 2003)

4.2.1 Criando programas de treinamento e conscientização

A primeira etapa do programa é fazer com que todos os funcionários tenham consciência de que existem pessoas desonestas que usarão a fraude para manipulá-las psicologicamente. Como explica Mitnick e Simon (2003), depois que as pessoas entendem melhor como podem ser manipuladas, elas conseguem com mais facilidade reconhecer um ataque que está para ser realizado.

A orientação básica que deve ser lembrada durante o desenvolvimento de um programa de treinamento e conscientização em segurança é que o programa precisa se concentrar em criar em todos os empregados a consciência de que a sua empresa pode ser atacada a qualquer momento e que uma perda de

informações confidenciais pode ameaçar não só a empresa, mas também as suas informações pessoais.

O programa de treinamento deve informar, prender a atenção e entusiasmar os aprendizes, motivando-os a querer entrar no programa e fazer sua parte para proteger os ativos de informações da organização. O objetivo é transformar a conscientização e o treinamento em segurança da informação em uma experiência interessante e interativa. As técnicas para que isso ocorra podem incluir:

1. Demonstração dos métodos da Engenharia Social por meio de dramatização.

Esta técnica pode ser utilizada para familiarizar os empregados dos principais métodos utilizados por um Engenheiro Social. De acordo com Mitnick e Simon (2003), são eles:

- Fingir ser um colega de trabalho;
- Fingir ser um empregado de um fornecedor, empresa parceira ou autoridade legal;
- Fingir ser alguém com autoridade;
- Fingir ser um empregado novo que solicita ajuda;
- Fingir ser um fornecedor ou fabricante de sistemas que liga para oferecer um patch ou uma atualização de sistema;
- Oferecer ajuda quando ocorrer um problema e, em seguida, faz o problema ocorrer para manipular a vítima a fazer com que ela ligue pedindo ajuda;
- Enviar um software ou patch grátis para que a vítima instale;
- Enviar um malware como um anexo de correio eletrônico;
- Usar uma janela pop-up falsa que pede para o usuário fazer o login novamente ou digitar uma senha;

- Capturar as teclas digitadas pela vítima com um sistema ou programa de computador;
- Deixar uma mídia portátil com software malicioso em algum lugar do local de trabalho;
- Usar jargão e terminologia interna para ganhar confiança;
- Oferecer um prêmio pelo registro em um site web com um nome de usuário e senha.

Além disso, é fundamental apresentar quais são os sinais que podem ser observados durante uma requisição, sendo possível identificar um ataque. Mitnick e Simon (2003) ressaltam os seguintes sinais:

- Recusa em dar um número de retorno;
- Solicitação fora do comum;
- Alegação de autoridade;
- Ênfase na urgência;
- Ameaça de consequências negativas em caso de não atendimento;
- Mostra desconforto quando questionado;
- Nome falso;
- Cumprimentos ou lisonja;
- Flerte.

2. Análise de ataques recentes em outras organizações, discutindo maneiras pela quais elas poderiam ter evitado o prejuízo.

3. Vídeos divertidos sobre segurança.

O programa prático de treinamento e conscientização sobre segurança das informações, principalmente relacionado aos ataques de Engenharia Social, que aborda aspectos do comportamento humano deve incluir:

- Uma descrição de como os atacantes usam as habilidades da Engenharia Social para enganar pessoas;
- Os métodos usados pelos engenheiros sociais para atingir seus objetivos;
- Como reconhecer um provável ataque de Engenharia Social;
- O procedimento para o tratamento de uma solicitação suspeita;
- A quem relatar as tentativas da Engenharia Social ou os ataques bem-sucedidos;
- A importância de questionar todos os que fazem uma solicitação suspeita, independente da posição ou importância que a pessoa alega ter;
- O fato de que os funcionários não devem confiar implicitamente nas outras pessoas sem uma verificação adequada;
- A importância de verificar a identidade e a autoridade de qualquer pessoa que faça uma solicitação de informação ou ação;
- O valor de informações aparentemente inofensivas, como nome de um servidor ou rede de computadores, e que essas informações podem dar a um atacante o conhecimento que ele precisa para ganhar a confiança ou encontrar a localização das informações que ele deseja.

4.3 Exemplos para reforçar a conscientização

A orientação básica que deve ser lembrada durante o desenvolvimento de um programa de treinamento e conscientização em segurança é que o programa precisa se concentrar em criar em todos os empregados a consciência de que a sua organização pode ser atacada a qualquer momento.

De acordo com Mitnick e Simon (2003), alguns exemplos para reforçar a concretização de um plano constante de conscientização podem incluir:

- O fornecimento de trabalhos, pesquisas, artigos para leitura voltada à Engenharia Social, para todos os funcionários;
- A inclusão de itens informativos nas circulares da organização: por exemplo, artigos, lembretes (de preferência itens curtos que chamem a atenção) ou quadrinhos;
- A colocação de uma foto do Empregado da Segurança do Mês;
- Pôsteres afixados nas áreas dos empregados;
- Notas publicadas no quadro de avisos;
- O fornecimento de lembretes impressos nos envelopes de pagamento;
- O envio de lembretes por correio eletrônico;
- O uso de proteções de tela relacionadas com segurança;
- A transmissão de anúncios sobre a segurança por meio dos sistemas de correio de voz;
- A impressão de etiquetas para o telefone com mensagens tais como “A pessoa que esta ligando é quem ela diz ser?”;
- A configuração de mensagens de lembrete que aparecem quando o computador é ligado, tais como “Criptografe as informações confidenciais antes de enviá-las”;
- A inclusão da conscientização para a segurança como o item padrão nos relatórios de desempenho dos empregados e nas análises anuais;
- A publicação na intranet de lembretes de conscientização para a segurança, talvez usando quadrinhos ou humor, ou alguma outra maneira que incentive as pessoas a lerem;
- O uso de um quadro eletrônico de mensagens na lanchonete, com um lembrete de segurança que seja trocado frequentemente;
- A distribuição de folhetos ou brochuras;

Toda precaução e divulgação quanto à segurança são válidos. Assim como as ameaças são constantes, os lembretes também devem ser constantes!

4.4 Teoria do reforço

De acordo com a Teoria do psicólogo norte-americano Skinner, o comportamento ou a motivação de um indivíduo é uma função das consequências daquele comportamento, se formos recompensados por nos comportar de certo modo, começaremos a fazer a ligação entre o comportamento apropriado e a recompensa.

A ideia principal dessa teoria é de que o reforço condiciona o comportamento, sendo que este é determinado por experiências negativas ou positivas. O reforço positivo se dá de várias formas tais como: premiações, promoções e até um simples elogio a um trabalho bem feito. São motivadores visto que incentivam o alto desempenho. O reforço negativo condiciona o funcionário a não se comportar de maneira desagradável, atuando através de repreensões chegando até a demissão. (BOWDITCH e BUONO, 1992)

Usando como base essa teoria, seria interessante recompensar os funcionários que identificam um ataque de Engenharia Social e conseguem evitá-lo, ou que promovem algum tipo de conscientização de segurança da informação no time. Resumindo, qualquer ação em prol da segurança e da efetividade do programa de conscientização deve ser reconhecido e recompensado.

Da mesma forma, um ato que facilite um ataque de Engenharia Social ou a quebra de alguma regra deve ser devidamente repreendido, para que estes sejam desmotivados.

4.5 Testes para avaliar a vulnerabilidade dos funcionários

O grau de efetividade dos treinamentos e dos programas de conscientização só pode ser determinado através de testes realizados contra os funcionários da organização. Neste caso, um aviso deve ser dado para que os funcionários tomem conhecimento dessa prática, eles precisam saber que em algum momento

podem receber uma ligação telefônica ou outra comunicação que usará as técnicas de um atacante como parte de tal teste.

Os resultados obtidos através dos testes não devem ser usados para punir, mas sim para definir a necessidade de treinamento adicional em algumas áreas. (MITNICK e SIMON, 2003)

Para a realização dos testes, a organização precisa usar a criatividade e a discrição. Preferencialmente, os testes devem ser realizados por funcionários que façam parte da equipe responsável pela Segurança da Informação. Alguns exemplos de testes podem incluir:

- Tentativa de obtenção de alguma informação inofensiva ou confidencial da organização através de uma ligação telefônica;
- Tentativa de obtenção de alguma informação inofensiva ou confidencial através de um serviço de mensagem instantânea;
- Criação de um perfil falso em um site de rede social que os funcionários da organização utilizem para tentativa de obtenção de dados sigilosos;
- Tentativa de *phishing* através do envio de inofensivas mensagens de e-mail que ao serem abertas emitem um alerta para a equipe de Segurança;

A partir destes testes será possível:

- Verificar se a “vítima” realmente segue as etapas para a verificação da identidade de um solicitante;
- Verificar o grau de resistência do funcionário com relação à persuasão;
- Encontrar quais áreas precisam de treinamento reforçado.

5 ESTUDO DE CASO

Como exemplo de um possível ataque de Engenharia Social, segue um diálogo entre um Engenheiro Social e um novo funcionário, conforme a legenda a seguir:

M: Mariana Silva (Nova funcionária)

F: Felipe (Engenheiro Social)

M: “Alô, Mariana. Em que posso ajudar?”

F: “Olá Mariana. Aqui é o Felipe do Departamento de Segurança da Informação, tudo bem com você?”

M: “Tudo sim Felipe e com você?”

F: “Tudo bem também. Você é nova por aqui?”

M: “Sou sim, hoje completa um mês.”

F: “E está gostando do trabalho?”

M: “Estou sim, muito!”

F: “Que bom! Alguém do nosso departamento já entrou em contato com você para te orientar sobre as melhores práticas de segurança da nossa organização?”

M: “Ainda não. “

F: “Bom, acho que esse vai ser o meu trabalho então! Gostaria de te alertar que não é permitido a instalação de *softwares* que não estejam na intranet. Isso porque não queremos nenhum problema com software sem licença de uso e também para evitar quaisquer problemas com software que tenha um *worm* ou um vírus.

M: “Sem problemas.”

F: “Você está ciente das nossas políticas sobre correio eletrônico?”

M: “Acho que não.”

F: “Bom, qual é o seu endereço de correio eletrônico atual?”

M: “marianas@xxxxxx.net”

F: “Seu nome de usuário é marianas também?”

M: “Não, é silvamari.”

F: “Certo. Queremos que todos os nossos empregados estejam cientes que pode ser perigoso abrir anexos de correio eletrônicos que não esteja esperando. Muito dos vírus são enviados e chegam em mensagens de correio eletrônico que parece vir de pessoas que você conhece. Assim sendo, se você receber alguma mensagem de correio eletrônico que o endereço não seja de alguém de dentro da organização, você não deve abrir o e-mail, deve simplesmente deletá-lo. Certo?”

M: “Certo.”

F: “Bom, a política da nossa organização diz que você tem de mudar sua senha a cada 90 dias, isso quer dizer que você ainda não trocou a sua primeira senha, mas precisamos ter certeza de que as pessoas estão usando senhas que não sejam muito fáceis de adivinhar. Por exemplo, nome de pai e mãe, nome de filho, data de aniversário, telefone residencial e assim por diante. E ela também deve conter: letras, números e símbolos. A sua senha possui tudo isso?”

M: “Ixi... Na verdade, não.”

F: “Que senha você está usando atualmente?”

M: “O nome da minha mãe: Cristiane.”

F: “Essa não é uma senha segura. Precisamos corrigir isso na sua próxima troca de senha. Podemos usar, por exemplo, uma fruta que você gosta.”

M: “Amora.”

F: “Isso, aí podemos trocar a primeira letra A pelo número 4 e o último A pelo @. O que você acha, muito mais difícil de adivinhar, certo?”

M: “Com certeza!”

F: “Certo, na próxima troca então, que será daqui a dois meses, lembre-se dessa senha, ok?”

M: “Ok. Obrigada Felipe.”

F: “Estou aqui para isso Mariana. A última dica, você tem um *software* de antivírus instalado no seu computador e é preciso mantê-lo atualizado. Tudo bem?”

M: “Claro, claro.”

F: “Bom, é isso então. Tenha um bom dia de trabalho, espero ter esclarecido algumas coisas pra você.”

M: “Ajudou muito! Obrigada, ótima dia para você também.”

F: “Até mais.”

M: “Até.”

5.1 Analisando a trapaça

Figura 06 – Mapa mental de um exemplo de ataque. Mapa mental de um exemplo de ataque de Engenharia Social onde o atacante consegue obter a senha do e-mail da vítima. Fonte: (MARTORINI, 2012)

Neste exemplo, o atacante utilizou de um título de respeito dentro da organização – membro do Departamento de Segurança da Informação – para conseguir credibilidade e assim adquirir a confiança do funcionário. Ele também disse que as senhas dentro da organização não podiam conter informações fáceis de adivinhar. Nesse ponto, o atacante criou um problema para o alvo, pois o alvo identificou que sua senha estava fraca. Sendo assim, para que o suposto membro do departamento de segurança pudesse ajudar, a nova funcionária compartilhou uma informação confidencial: sua senha de intranet.

5.2 Evitando a trapaça

Este é um caso mais difícil de lidar, pois a funcionária é nova na organização e ainda não está familiarizada com a política de segurança e as melhores práticas com relação à segurança da informação.

Em casos como este, o aconselhável é que seja realizado um programa de treinamento e conscientização para os funcionários novos antes que eles tenham acesso aos sistemas computacionais ou telefônicos da organização. O recomendável é que este treinamento seja realizado no primeiro ou segundo dia de trabalho do funcionário, para que antes de qualquer contato com as informações da organização, ele já esteja ciente da importância que é administra-las com cuidado.

O programa de treinamento e conscientização deve acontecer regularmente, para que as regras e dicas não caiam no esquecimento. De tempos em tempos, os funcionários - mesmos os mais velhos de casa - devem participar de treinamentos e programas de conscientização.

Para que os treinamentos não se tornem algo maçante, é importantíssimo que a equipe responsável pela criação e realização dos treinamentos esteja sempre renovando seus métodos e técnicas para cativar a atenção dos funcionários e incentivá-los a proteger o ativo mais importante da organização em que trabalha: a informação.

6 CONCLUSÃO

Com o aumento do valor das informações dentro do mundo comercial e econômico, novas técnicas de ataques para roubá-las surgem cada vez mais complexas e eficientes. Os dispositivos de segurança tentam acompanhar a crescente onda de tentativas a ataques dentro de organizações, tornando-se cada vez mais difíceis de serem burlados.

Porém, como visto neste trabalho, o Engenheiro Social não se intimida com os mecanismos de proteção física e lógica das informações, ele sabe muito bem onde atacar: no elo mais fraco dessa corrente, o ser humano.

Enquanto as informações forem controladas, usadas, manipuladas e acessadas por pessoas, elas estarão em constante ameaça e perigo de vazamento, principalmente porque indivíduos mal intencionados – os Engenheiros Sociais – encontrarão maneiras de obtê-las.

As organizações costumam investir em mecanismos físicos e lógicos para proteger as informações e acabam esquecendo-se de fortalecer aqueles que lidam dia e noite com suas informações: os funcionários. A melhor forma de fazê-lo é educando, educando e educando mais uma vez.

Os funcionários precisam entender o papel que possuem dentro de uma organização e o quão importante é manter protegido cada dado que circula dentro dela. Também precisam estar ciente do grau de estrago que o vazamento daquela informação pode ocasionar não só para a organização, mas para o próprio funcionário.

Depois de entender como devem lidar com as informações, eles precisam se sentir motivados a fazê-los, é nessa parte que entra a recompensa por alguma ação favorável pela segurança da informação ou a repreensão pela quebra de alguma regra.

Os treinamentos e programas de conscientização são formas de educar os funcionários, eles devem ser desenvolvidos com bastante cuidado, tentando

atender a todos os requisitos importantes para a organização, como também devem ser renovados constantemente, assim como os ataques são.

O ser humano é reconhecido pela capacidade de adaptar-se a diferentes ambientes e situações. Sendo assim, da mesma forma que ele é capaz de arquitetar ataques complexos de Engenharia Social, ele também é capaz de planejar diferentes técnicas para se proteger desses tipos de ataque. Essas técnicas podem ser desenvolvidas explorando as ferramentas do próprio Engenheiro Social: persistência, dinamismo e muita criatividade.

REFERÊNCIA BIBLIOGRÁFICA

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: ABNT, 2005.

ARRUDA, Felipe. **Engenharia Social:** o malware mais antigo do mundo. Disponível em <http://www.tecmundo.com.br/seguranca/8445-engenharia-social-o-malware-mais-antigo-do-mundo.htm>. Acesso em: 02 Julho 2012.
FERREIRA, Aurélio Buarque de Holanda. **Minidicionário da língua portuguesa**. 3 ed. - Rio de Janeiro: Nova fronteira,1993.

BOWDITCH, James L., BUONO, Anthony F**. Elementos de Comportamento Organizacional**. 1ª Ed. São Paulo: Pioneira, 1992.

CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). **Incidentes Reportados ao CERT.br -- Janeiro a Março de 2012.** Publicado em 19 de Abril de 2012. Disponível em <http://www.cert.br/stats/incidentes/2012-jan-mar/tipos-ataque.html>. Acesso em: 12 Setembro 2012.

CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). **Cartilha de Segurança para Internet: Golpes na Internet.** Disponível em < http://cartilha.cert.br/golpes/>. Acesso em: 16 Outubro 2012.

ESTÉS, Dra. Clarissa Pinkola. **CONTOS DOS IRMÃOS GRIMM.** Tradução Lya Wyler São Paulo: Rocco, 2005.

FERREIRA, Aurélio Buarque de Holanda. **Minidicionário da língua portuguesa**. 3 ed. - Rio de Janeiro: Nova fronteira,1993.

MARCELO, Antonio; PEREIRA, Marcos. **A Arte de Hackear Pessoas:** um guia para conhecer a Engenharia Social, os crimes digitais, os ataques de phishing e de como os novos criminosos estão atacando na Internet. Rio de Janeiro: Brasport, 2005.

MARTORINI, Stela*. Engenharia Social: como acontece e como evitar*. 2012**.** 52f. Trabalho acadêmico (Graduação) – Setor de TI. Faculdade de Tecnologia de Americana.

MASLOW, Abraham H. **Introdução à psicologia do ser**. Tradução Álvaro Cabral. Rio de Janeiro: Livraria Eldorado Tijuca LTDA, 1968.

MICROSOFT (Brasil). **O que é Malware?** Disponível em <http://www.microsoft.com/pt-br/security/resources/malware-whatis.aspx>. Acesso em 12 Setembro 2012.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar:** ataques de hackers: controlando o fator humano na segurança da informação. Tradução Kátia Aparecida Roque. São Paulo: Pearson Education, 2003.

PEIXOTO, Mário C. Pintaudi. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. São Paulo: Brasport, 2006.

REGINALDO, Eliana Ap; SANTOS, Laureci I. dos; ESPADONI, Suzely. *Engenharia Social: Seus Aspectos Tecnológicos e Humanos no Setor Público e Privado.* Trabalho de Conclusão de Curso (Mestrado em Segurança da Informação). São Paulo: Faculdade Impacta Tecnologia, 2010.

REZENDE, Denis Alcides; ABREU, Aline França. **Tecnologia da informação aplicada a sistemas de informação empresariais**. São Paulo: Atlas, 2000.

SANTOS, Luciano A. L. *O IMPACTO DA ENGENHARIA SOCIAL NA SEGURANÇA DA INFORMAÇÃO.* Monografia (Pós-graduação em Redes de Computadores). Aracajú: Universidade Tiradentes, 2004.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: Uma visão executiva. 1ª Ed. Rio de Janeiro: Campus, 2003.

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 < http://www.tecmundo.com.br/msn-messenger/1078-cuidado-com-a-engenharia-social.htm >. Acesso em: 20 Julho 2012

XAVIER, Andressa. **O que é Spyware?** Publicado em 2 de Julho de 2008. Disponível em <http://www.tecmundo.com.br/spyware/29-o-que-e-spyware-.htm#ixzz2368aL4Bt>. Acesso em 12 setembro 2012.

GLOSSÁRIO

Correio de Voz. Sistema centralizado de gerenciamento de mensagens telefônicas para um grande número de pessoas.

***Facebook*.** Site e serviço de rede social que foi lançada em 4 de fevereiro de 2004, operado e de propriedade privada da Facebook Inc..

FTP (*File Transfer Protocol*). O FTP é o protocolo de transferência de arquivos da Arquitetura Internet. Trata-se de um utilitário de uso interativo que pode ser chamado por programas para efetuar transferência de arquivo

Helpdesk. Serviço que visa o atendimento a reclamações de clientes. A central de Helpdesk atua como elo entre a empresa e seus clientes.

Instant Messaging Programs. Programas que funcionam com base em uma lista de pessoas com as quais você queira interagir e permite a troca de mensagens em tempo real para qualquer pessoa da lista, desde que ela esteja online.

Intrusion Detection Systems. O IDS é um sistema composto por sensores capazes de disparar um alarme caso algum evento determinado ou não esperado venha a acontecer em sua rede.

Intrusion Prevention Systems. O IPS possui a mesma função do IDS, com a diferença de que o possibilita bloqueios imediatos das intrusões.

IRC (*Internet Relay Chat*). Protocolo de comunicação utilizado na Internet. Ele é utilizado basicamente como bate-papo (chat) e troca de arquivos, permitindo a conversa em grupo ou privada.

***Link*.** É o "endereço" de um documento (ou de um recurso) na internet.

Orkut. O Orkut é uma rede social criada em 24 de Janeiro de 2004 com o objetivo de ajudar seus membros a conhecer pessoas e manter relacionamentos

Registro.br. Órgão responsável pelo registro e manutenção dos domínios .br.

Token. Dispositivos físicos que auxiliam o usuário quanto à segurança pessoal ao gerar uma senha temporária de proteção para as contas que ele utiliza.

Patch. Programa criado para atualizar ou corrigir um software.

Worm. Programa semelhante aos vírus, com a diferença de este ser auto replicante, ou seja, ele cria cópias funcionais de si mesmo e infecta outros computadores.