

OUTROS TRABALHOS EM:  
[www.projetoderedes.com.br](http://www.projetoderedes.com.br)

**CENTRO UNIVERSITARIO DO MARANHÃO – UNICEUMA**  
**CURSO DE ANÁLISE E DESENVOLVIMENTO DE SISTEMAS**  
**SEGURANÇA E AUDITORIA DE SISTEMAS**

**SEGURANÇA DA INFORMAÇÃO:**  
**ENGENHARIA SOCIAL E BIOMETRIA**

*Arthur Fernandes de Oliveira*

*Guilherme Augusto*

*Maria Angélica Costa Bezerra da Silva*

*São Luís*

*2012*

*Arthur Fernandes de Oliveira*

*Guilherme Augusto*

*Maria Angélica Costa Bezerra da Silva*

**SEGURANÇA DA INFORMAÇÃO:  
ENGENHARIA SOCIAL E BIOMETRIA**

*Trabalho apresentado a Professora Msc. Alessandra  
da disciplina Segurança e Auditoria de Sistemas do  
curso de Análise e Desenvolvimento de Sistemas.*

*São Luís*

*2012*

## Sumário

1 – Introdução .....	4
2 – O que é a engenharia social?.....	5
2.1 – Vulnerabilidades .....	5
2.2 – Tipos de ataques.....	5
2.3 – Meios de ataque .....	6
2.4 – Técnicas .....	6
2.5 – Prevenção.....	7
3 – Biometria.....	8
3.1 – O que é a biometria? .....	9
3.2 – Biometria na segurança da informação .....	9
3.3 - Como funciona?.....	10
3.4 – Reconhecimento.....	10
3.5 – Tipos de identificação .....	11
5 – Conclusão.....	13
Referências.....	14

## **1 – Introdução**

Com o número de ataques a sistemas de informação aumentando, gradualmente várias medidas tecnológicas para evitá-los foram tomadas. Assim, os responsáveis pelos ataques estão mudando de foco.

Entretanto, ainda existem várias técnicas disponíveis para que um usuário mal intencionado encontre brechas nas defesas de segurança de informação de uma empresa. Dentre estas, a abordagem humana, mais conhecida como engenharia social é a mais peculiar e também a mais difícil de prever e controlar.

Este trabalho tem o objetivo de descrever a engenharia social, suas várias formas, suas técnicas e como elas exploram as falhas humanas causando impacto nas empresas. Também abordaremos como a biometria – uso de características biológicas para identificação - pode ser uma solução válida contra alguns tipos de ataques da engenharia social.

## 2 – O que é a engenharia social?

Chama-se de engenharia social o conjunto de técnicas usadas para manipular pessoas de modo que elas tomem ações ou divulguem informações confidenciais. Ao contrário de fraudes comuns, o objetivo do atacante é ganhar acesso ou dados de um sistema.

O termo engenharia é usado por ser uma prática que se baseia em uma série de táticas e informações e age sobre o aspecto “social” do ser humano. Ela se vale das fraquezas do homem para burlar as camadas de segurança que foram implementadas.

### 2.1 – Vulnerabilidades

Um sistema pode ter sua segurança comprometida por vulnerabilidades, são elas: físicas, naturais, hardware, software, mídias, comunicação e humanas. Dentre as falhas humanas exploradas pela engenharia social estão:

- **Vontade de ser útil** – o ser humano quer se sentir útil e procura ser prestativo quando uma ocasião apropriada surge;
- **Buscar amizades/afeto** – Ao ser elogiado, torna-se mais aberto a fornecer informações;
- **Dividir responsabilidades** – Desejo de compartilhar o peso de alguma tarefa;
- **Persuasão** – Capacidade de convencer o outro;
- **Insatisfação** – O descontentamento pode levar funcionários a cederem informações.

Existem várias outras características humanas que podem ser usadas, tudo vai depender do tipo de ataque e da técnica usada.

### 2.2 – Tipos de ataques

Ataques deste tipo de prática são divididos em duas categorias: diretos e indiretos.

- Os ataques diretos são aqueles que exigem interação direta entre o engenheiro social e a sua vítima, o que pode ser feito através um telefonema ou pessoalmente, por exemplo. Eles requerem mais elaboração, planejamento e eloquência por parte do engenheiro social;

- Os ataques indiretos são realizados através de ferramentas específicas e não requer a presença do atacante, como envio de vírus, e-mails falsos, etc.

Em qualquer um dos dois tipos o ciclo de ataque é o mesmo:

Reunir informações → Estabelecer relacionamento → Exploração → Execução

## 2.3 – Meios de ataque

Os seguintes meios podem ser utilizados em um ataque de engenharia social (mais de um meio ou uma combinação deles poderá ser utilizado):

- **Telefone** – Para coletar dados ao se passar por outra pessoa da empresa;
- **Internet** – Para angariar informações para planejamento ou para o ataque em si;
- **Intranet** – Permite o acesso de computadores da rede interna da empresa para passar-se por alguém da empresa através de suas credenciais;
- **E-mail** – Envio de e-mails falsos para induzir a vítima a instalar vírus ou ceder informações restritas;
- **Chats** – Para estabelecer vínculos afetivos e ganhar confiança da vítima;
- **Pessoalmente** – Fazendo uso de persuasão direta;
- **Fax** – Obtenção de informações privilegiadas e falsificação de documentos;
- **Correio convencional** – Envio de correspondência falsa ou interceptação de documentos;
- **Spyware** – Envio de um programa espião para o computador da vítima a fim de coletar informações;
- **Redes P2P** – Usar a rede de compartilhamento para a disseminação de vírus e trojans.
- **Redes Sociais** – Rastrear informações pessoais da vítima para preparação e planejamento do ataque.

Estes são os meios mais comuns, mas não são os únicos. O meio depende da necessidade e da criatividade do engenheiro social.

## 2.4 – Técnicas

Existem duas categorias principais para dividir as técnicas empregadas na engenharia social: As baseadas em tecnologia e as não baseadas em tecnologia. As primeiras são as que fazem uso de ferramentas tecnológicas, como e-mail, por exemplo. As não baseadas em tecnologia não utilizam recursos avançados contando apenas com a presença do engenheiro social.

- **Pesquisa** – Coleta de dados para saber quem detém a informação buscada;
- **Personificação ou impostura** – Fazer-se passar por outra pessoa;
- **Divisão de responsabilidades** – Convencer funcionários a compartilharem tarefas a fim de ceder acesso à informação;
- **Spoofing** – Consiste em boicotar o sistema telefônico a fim de simular que a ligação está sendo feita do número de um determinado departamento da empresa, por exemplo;
- **E-mails falsos** – Envio de e-mails que simulam ser de instituições oficiais ou autoridades para induzir ao erro ou divulgação de informações;
- **Phishing** – Criação de sites falsos, idênticos aos originais para obtenção de dados da vítima;
- **Engenharia social inversa** – O atacante finge ser alguém com autoridade e conhecimento para extrair as informações da vítima;
- **Footprint** – Investigação para saber mais informações da empresa. Pode ser colhida através de software específico;
- **Vasculhamento de lixo** – Procurar no lixo da empresa por documentos importantes;
- **Espionagem** – Observar pessoas digitando, ouvir comentários;
- **Programação neurolinguística** – Consiste em imitar os gestos da vítima a fim de ganhar confiança.

## 2.5 – Prevenção

O conhecimento é a melhor arma na prevenção deste tipo de ataque. É preciso que se fique atento a qualquer tipo de abordagem via e-mail, carta onde somos induzidos a tomar qualquer ação que revele informações e dados importantes.

Deve-se sempre estar atento quando lhe for solicitado informações sensíveis como, por exemplo, números de cartões de crédito, senhas e etc. por pessoas estranhas. A vítima antes de tudo deve verificar a autenticidade da ligação que esta recebendo, do crachá que o atacante apresentou e etc.

Nunca fornecer informações pessoais, de empresas e etc. antes de identificar e constatar a autenticidade do pedido. Por várias vezes, vítimas recebem e-mails contendo links falsos, informações não verdadeiras ou até mesmo solicitações de cadastro em empresas fantasmas. Para não cair nestas armadilhas a vítima deve, por exemplo, entrar em contato com a instituição que lhe

fez a solicitação de cadastro, como por exemplo bancos, receita federal e etc., para garantir assim uma autenticidade do pedido, nunca clicar sobre links recebidos através de spams e etc.

Atualmente as empresas que querem evitar esse tipo de ataque, estão investindo alto em treinamento de funcionários, a fim de evitar a vazão de informações sobre a estrutura da empresa.

O treinamento, estabelecimento da política de segurança da informação na empresa, baseia-se em educar os funcionários a sempre certificar-se de que a pessoa a quem vai fornecer as informações é realmente quem diz ser, a tomarem cuidado com o lixo pois este é uma grande fonte de informações, desconfiarem de pessoas em chats e etc.

Esta política de segurança da informação da empresa deve conter dentre outros tópicos, planos e ações de segurança como, por exemplo, plano de proteção física, continuidade dos negócios, análise de riscos, ações de engenharia, plano de contingência, plano de conscientização de todos os colaboradores, mesmo os terceirizados e etc.

Basicamente tudo se resume em reeducar toda a corporação a fim de implantar uma nova cultura cem por cento abrangente, cem por cento, pois qualquer falha põe novamente a corporação em risco iminente.

### **3 – Biometria**

A necessidade de autenticação / identificação de usuários em uma rede de computadores é o principal aspecto para a segurança da informação e está associada à possibilidade de acesso restrito a uma determinada área ou serviço da rede, ou seja, se não for possível identificar uma pessoa que esteja tentando acessar um sistema, nenhum outro tópico de segurança fará sentido.

O aumento de serviços em rede, por exemplo, e-mail, ERP, Internet, entre outros e a necessidade de segurança em áreas estratégicas é a motivação para implantar um sistema de autenticação e identificação confiável e pouco intrusivo.

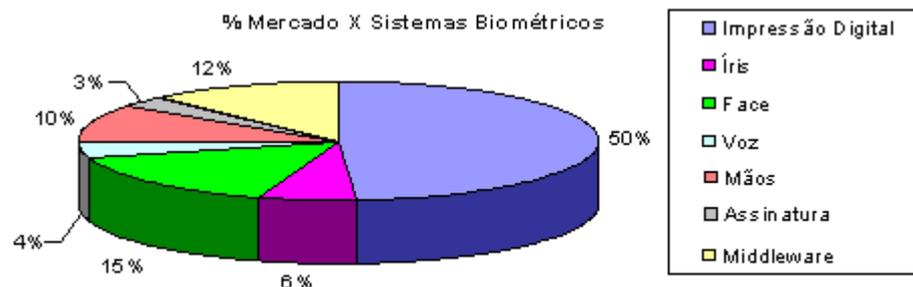
A forma mais popular para registrar pessoas em quase todo o mundo é a impressão digital e as fotografias, que são registradas em fichas e permitem a identificação sem grandes dificuldades. Entretanto, esses métodos têm sido questionados quanto aos problemas de segurança, quer sejam de ordem institucional, governamental ou mundial.

### 3.1 – O que é a biometria?

A biometria pode ser definida como a ciência da aplicação de métodos de estatística quantitativa a fatos biológicos, ou seja, é o ramo da ciência que se ocupa da medida dos seres vivos (do grego bio = vida e métron = medida). Resumindo, a biometria é a autenticação / identificação de um indivíduo pelas suas características biológicas e comportamentais.

Como mencionado, a necessidade de autenticação / identificação está associada à possibilidade de acesso restrito a um determinado bem ou serviço. A autenticação / identificação pode ser realizada de várias formas: por aquilo que se possui (crachá, cartão magnético), por aquilo que se sabe (senha) ou por aquilo que se é, através das características biométricas, tais como: íris, voz, impressão digital e outras.

Na biometria, os identificadores são obtidos a partir de singularidades pertencentes às características biológicas e/ou comportamentais do indivíduo. Esta técnica apresenta a vantagem de usar características únicas, sem a necessidade do indivíduo possuir objetos ou memorizar algo. Ele é autenticado / identificado por aquilo que é.



Fonte: International Biometric Group's Biometric Market Report 2000

**Figura 1 – Mercado dos principais sistemas biométricos comerciais**

### 3.2 – Biometria na segurança da informação

A biometria pode ser utilizada em um sistema de informação para resolver dois problemas importantes: a identificação e o acesso de usuários à rede de computadores.

Os sistemas biométricos utilizados na segurança em uma rede de computadores buscam verificar a identidade de um indivíduo (identificação) através das características únicas inerentes a

essa pessoa por meio de processos automatizados. Essas características podem ser físicas (olhos, mão, etc.) e / ou comportamental (modo como assina um documento, por exemplo).

No controle de acesso, os sistemas biométricos permitem que um indivíduo possa ser autenticado na rede sem a necessidade de uma senha ou outro dispositivo físico (crachá, cartão eletrônico, etc.), ou ainda (e mais usualmente) em combinação com estes.

### 3.3 - Como funciona?

A autenticação biométrica envolve duas fases: registro no sistema (coleta de dados) e reconhecimento da característica biométrica. Para isso é necessário primeiramente que todos os usuários sejam cadastrados através de um dispositivo de entrada de dados, geralmente um scanner, microfone, leitor óptico ou outro meio eletrônico, para colher a representação digital (a amostra biométrica ou "live scan") que será usada na verificação do indivíduo.

O cadastramento envolve o indivíduo que irá fornecer uma amostra de sua característica biométrica, sendo que essa característica-chave será usada pelo sistema para gerar um modelo biométrico. A amostra é convertida para um algoritmo matemático que então é criptografado. Cada vez que o usuário requerer um acesso ao sistema, uma verificação / autenticação será realizada e a amostra da característica particular do indivíduo será comparada com o modelo biométrico armazenado no banco de dados.

### 3.4 – Reconhecimento

Os procedimentos de reconhecimento do usuário por meio da biometria podem ser aplicados de duas formas:

- **Um-para-um** – o sistema simplesmente compara a característica biométrica apresentada com a informação registrada no banco de dados para aquele usuário;

- **Um-para-muitos** – o sistema efetua a busca em todo o banco de dados, comparando as informações fornecidas até que seja encontrado ou não um registro idêntico aquele fornecido.

Quando a verificação da informação é positiva, o usuário terá acesso assegurado ao sistema, senão, será bloqueado.

### 3.5 – Tipos de identificação

Hoje em dia, existem várias características biológicas que podem ser usadas em um processo de identificação por biometria. Vejamos as principais:

- **Impressão digital:** o uso de impressão digital é uma das formas de identificação mais usadas. Consiste na captura da formação de sulcos na pele dos dedos e das palmas das mãos de uma pessoa. Esses sulcos possuem determinadas terminações e divisões que diferem de pessoa para pessoa. Para esse tipo de identificação existem, basicamente, três tipos de tecnologia: óptica, que faz uso de um feixe de luz para ler a impressão digital; capacitiva, que mede a temperatura que sai da impressão; e ultrassônica, que mapeia a impressão digital através de sinais sonoros. Um exemplo de aplicação de identificação por impressão digital é seu uso em catracas, onde o usuário deve colocar seu dedo em um leitor que, ao confirmar a identificação, liberará seu acesso;
- **Retina:** a identificação por retina é um dos métodos mais seguros, pois analisa a formação de vasos sanguíneos no fundo do olho. Para isso, o indivíduo deve olhar para um dispositivo que, através de um feixe de luz de baixa intensidade, é capaz de "escanear" sua retina. A confiabilidade desse método se deve ao fato da estrutura dos vasos sanguíneos estarem relacionadas com os sinais vitais da pessoa. Sendo mais direto, o dispositivo leitor não conseguirá definir o padrão da retina de uma pessoa se esta estiver sem vida;
- **Íris:** a identificação por meio da íris é uma forma menos incômoda, pois se baseia na leitura dos anéis coloridos existentes em torno da pupila (o orifício preto do olho). Por essa combinação formar uma "imagem" muito complexa, a leitura da íris é um formato equivalente ou mais preciso que a impressão digital. Por nem sempre necessitar da checagem do fundo do olho, é um método mais rápido de identificação. A preferência por identificação da íris também se baseia no fato desta praticamente não mudar durante a vida da pessoa;
- **Geometria da mão:** este também é um método bastante usado. Consiste na medição do formato da mão do indivíduo. Para utilizá-lo, a pessoa deve posicionar sua mão no dispositivo leitor sempre da mesma maneira, do contrário as informações de medidas poderão ter diferenças. Por esse motivo, os dispositivos leitores contêm pinos que indicam onde cada dedo deve ficar posicionado. Esse é um dos métodos mais antigos que existe, porém não é tão preciso. Em contrapartida, é um dos meios de identificação mais

rápidos, motivo pelo qual sua utilização é comum em lugares com muita movimentação, como universidades, por exemplo;

- **Face:** neste método a definição dos traços do rosto de uma pessoa é usada como identificação. É um processo que se assemelha em parte com a leitura da geometria das mãos, mas considera o formato do nariz, do queixo, das orelhas, etc.;
- **Voz:** a identificação por voz funciona através da dicção de uma frase que atua como senha. O usuário deverá informar a um reconhecedor a tal frase sempre que for necessário sua identificação. O entrave dessa tecnologia é que ela deve ser usada em ambientes sem ruídos, pois estes podem influenciar no processo. Além disso, se o indivíduo estiver rouco ou gripado sua voz sairá diferente e poderá atrapalhar sua validação. Por esta razão, a identificação por voz ainda é pouco aplicada;
- **Assinatura:** esse tipo de identificação consiste na comparação da assinatura com uma versão gravada em um banco de dados. Além disso, é feita a verificação da velocidade da escrita, a força aplicada, entre outros fatores. É um dos mecanismos mais usados em instituições financeiras, embora não se trate completamente de um método biométrico.

É importante frisar que todos esses métodos possuem alguns entraves que os fazem necessitar de aperfeiçoamento ou, dependendo do caso, da aplicação de outra solução. Por exemplo, na identificação por retina, a pessoa que estiver usando óculos deve retirá-lo; na identificação por face, um ferimento ou um inchaço no rosto pode prejudicar o processo; na identificação da geometria da mão, um anel também pode trazer problemas; na identificação por voz, ruídos externos, rouquidão ou até mesmo uma imitação da voz de um indivíduo pode pôr em dúvida o procedimento; na comparação de assinaturas, o estado emocional da pessoa pode atrapalhar e há ainda o fato da escrita mudar com o passar do tempo.

## 5 – Conclusão

A engenharia social é o jeito mais fácil para um hacker ganhar acesso a um sistema – e um dos mais comuns. Ainda assim milhares de empresas ao redor do mundo investem sua segurança apenas em camadas tecnológicas de defesa, esquecendo-se do treinamento básico de seus funcionários para evitar que o fator humano comprometa toda uma estrutura.

A biometria nos oferece uma alternativa para diminuir os ataques da engenharia social quando assumem a forma da impostura. Entretanto, ainda há muito que ser melhorado e não se trata de uma tecnologia plenamente livre de problemas, como exemplificamos.

Mas há várias pesquisas em desenvolvimento que visam diminuir os erros da identificação biométrica e também estudos sobre como educar melhor o usuário para que não se torne vítima frequente da engenharia social.

## Referências

CANEDO, JOSÉ ALBERTO. **Biometria**. Disponível em:

<<http://www.forumbiometria.com/biometria.html>> Acesso em: 30 mar. 2012.

SILVA, CLEVERTOM. **Segurança através da biometria**. Disponível em:

<[http://www.gestorseg.com/academico/trabalhos/1342\\_A\\_SEGURANCA\\_ATRAVES\\_DA\\_BIOMETRIA%28SEGET%29.pdf](http://www.gestorseg.com/academico/trabalhos/1342_A_SEGURANCA_ATRAVES_DA_BIOMETRIA%28SEGET%29.pdf)> Acesso em: 30 mar. 2012.

\_\_\_\_\_. Engenharia social (Segurança da informação). Disponível em:

<[http://pt.wikipedia.org/wiki/Engenharia\\_social\\_%28seguran%C3%A7a\\_da\\_informa%C3%A7%C3%A3o%29](http://pt.wikipedia.org/wiki/Engenharia_social_%28seguran%C3%A7a_da_informa%C3%A7%C3%A3o%29)>. Acesso em: 30 mar 2012.

\_\_\_\_\_. Segurança da informação vs. Engenharia Social – Como se proteger para não ser mais uma vítima. Disponível em: <<http://monografias.brasilecola.com/computacao/seguranca-informacao-vs-engenharia-social-como-se-proteger.htm>>. Acesso em: 30 mar 2012.

**OUTROS TRABALHOS EM:**

**[www.projeteredes.com.br](http://www.projeteredes.com.br)**