

# Engenharia Social e o Fator Humano na Segurança da Informação

Setembro de 2004

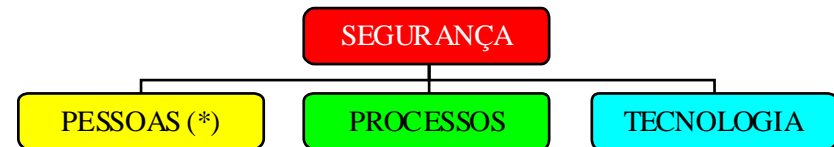
Por Marcelo Beltrão Caiado



*"Até mesmo um computador desligado pode ter seus dados roubados à distância. Basta que um engenheiro social habilidoso convença alguém a ligar o equipamento." Kevin Mitnick*

## Introdução

Qual é a maior **ameaça à segurança** dos bens de uma empresa ?



(\*) Também conhecido como "o elo mais fraco"

## Agenda

- Introdução
- O que vem a ser Engenharia Social
- Quem é o Engenheiro Social
- Como se proteger
- As perguntas de ouro
- Considerações finais
- Reflexões
- Sugestões Bibliográficas

## Introdução

**Hackers fazem uso de problemas de segurança. Engenheiros Sociais tiram vantagem de problemas na natureza humana.**

### **VISÃO EQUIVOCADA**

1. Achar que não vai ocorrer com você.
2. Questionar a importância do fator humano.
3. Acreditar que a tecnologia é uma panacéia.

### **VISÃO CORRETA**

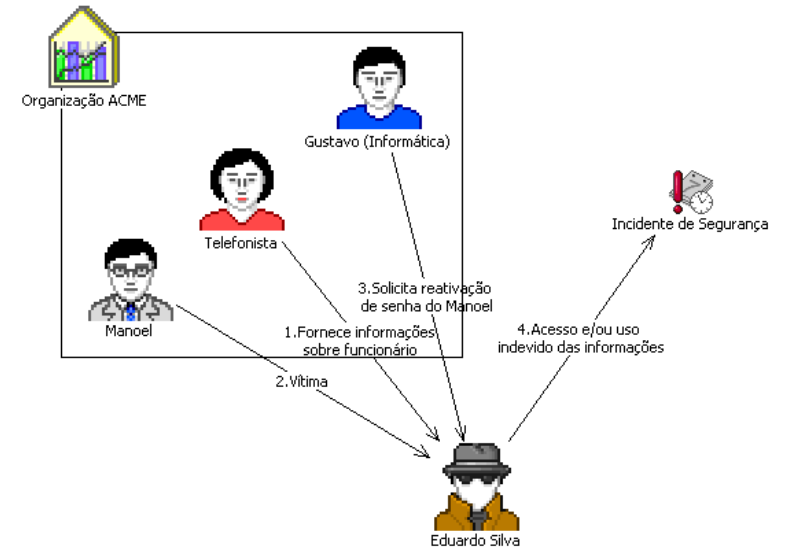
1. Agir preventivamente. Caso ocorra a abordagem de algum Engenheiro Social, detectar e não permitir o acesso a informações.
2. Inserir estratégias de segurança social como parte da defesa em profundidade.

# O que vem a ser Engenharia Social?

1. **A técnica da Engenharia Social.**  
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. Como o resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.
2. **Como age o Engenheiro Social.**  
Um mágico inescrupuloso que faz você olhar a sua mão esquerda enquanto com a mão direita rouba seus segredos.
3. **Um dos ataques mais sofisticados e com maior chance de alcançar o sucesso.**  
O Engenheiro Social consegue obter de uma pessoa algo que ela normalmente não faria para um estranho.

# O que vem a ser Engenharia Social?

## Simplesmente pedindo



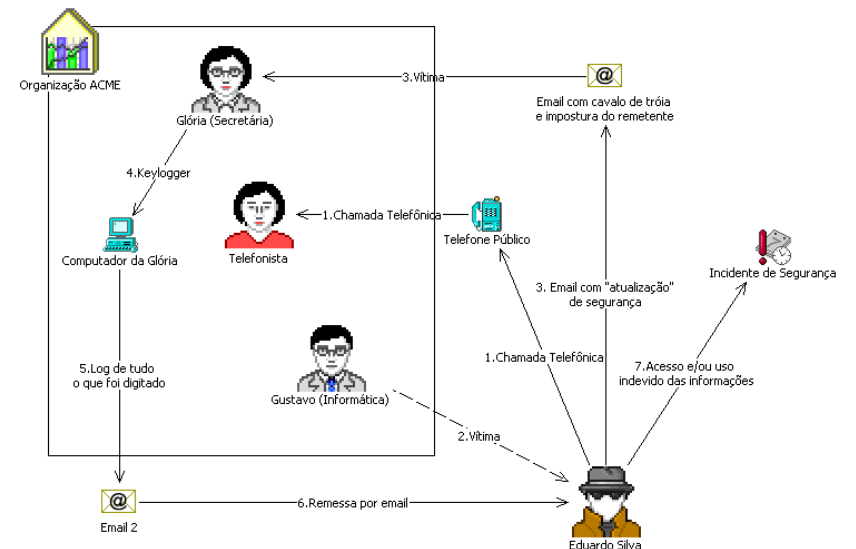
# O que vem a ser Engenharia Social?

## Principais Ataques

1. **Simplesmente Pedindo** - “Você pode me ajudar?”  
“Não estou conseguindo logar...”
2. **Criando a confiança** - “Posso ajudar?”  
“Você ganhou um sensacional...”
3. **Sites Falsos e Anexos Perigosos** - Scammers  
Joinners (Keyloggers e Trojans)
4. **Usando o Fator Psicológico** - Características da natureza humana

# O que vem a ser Engenharia Social?

## Criando confiança



## O que vem a ser Engenharia Social?

### Sites falsos e anexos perigosos



## O que vem a ser Engenharia Social?

### Características da Natureza Humana

#### Consistência

Parte do pressuposto de que ninguém deseja descumprir algo que havia prometido

#### Validação social

As pessoas tendem a cooperar quando isso parece estar de acordo com aquilo que as outras pessoas estão fazendo

#### Escassez

A cooperação surge na medida em que se acredita que um determinado recurso estará disponível por pouco tempo ou está em falta

## O que vem a ser Engenharia Social?

### Características da Natureza Humana

#### Autoridade

Quando alguém acredita que está lidando com um superior, não costuma questionar os pedidos

#### Afabilidade

Sendo gentil, uma pessoa acredita que estará fazendo amigos

#### Reciprocidade

Uma pessoa pode ser manipulada de forma a acreditar que alguém está lhe fazendo um favor, e desta forma irá procurar retribuir

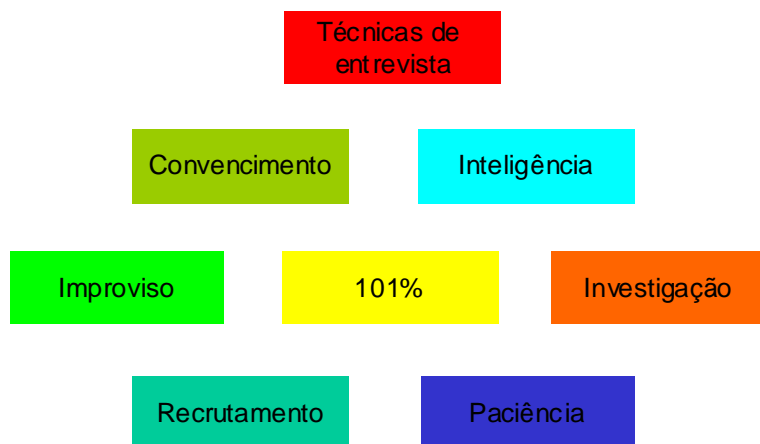
## Quem é o Engenheiro Social?

### Objetivos

1. Dinheiro
2. Acesso a recursos
3. Busca de vantagens
4. Vingança
5. Curiosidade
6. Guerra
7. Política
8. Divertimento
9. Reconhecimento

## Quem é o Engenheiro Social?

### Aptidões Pessoais



## Como se proteger?

### Identificando os sinais de um ataque

1. Recusa em dar um numero de retorno
2. Solicitação fora do comum
3. Alegação de autoridade
4. Ênfase na urgência
5. Alegação de autoridade
6. Ameaças de conseqüências negativas em caso de não atividade
7. Nome falso; lisonja; flerte; etc.

## Como se proteger?

### Fatores que deixam as empresas mais vulneráveis

1. Um número grande de empregados
2. Diversas instalações
3. Informações sobre o paradeiro dos empregados deixadas nas mensagens de correio de voz e email
4. Falta de treinamento e segurança
5. Nenhum plano ou grupo de resposta aos incidentes de segurança

## Como se proteger?

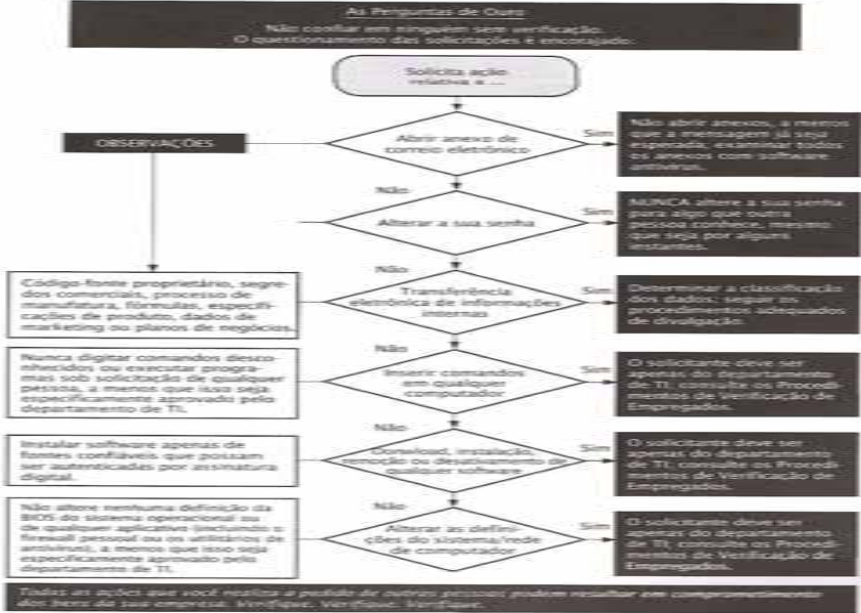
### Melhores Práticas

Capacitação de usuários e técnicos  
Conscientização  
Redundância de pessoas  
Adoção de Política de Segurança (política de senhas e instruções na guarda de informações)  
Classificação dos Dados  
Procedimentos de Verificação (autorização e autenticidade)

### REGRA

Os programas de capacitação e conscientização devem ser recorrentes (ISO 17799, Cap.VI).

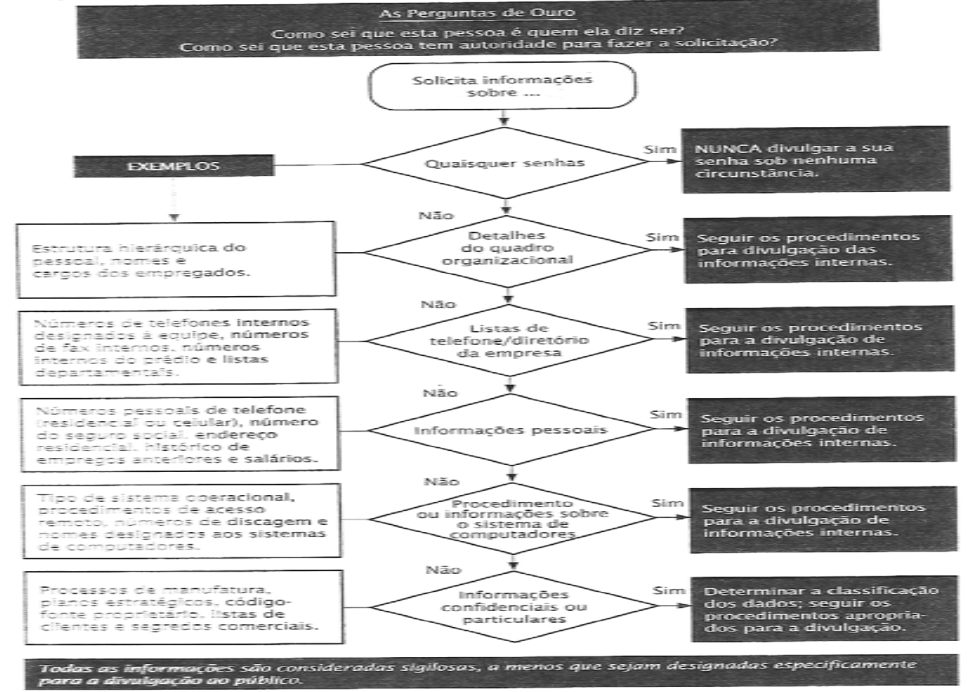
### Respondendo a uma solicitação de informações



### Considerações Finais

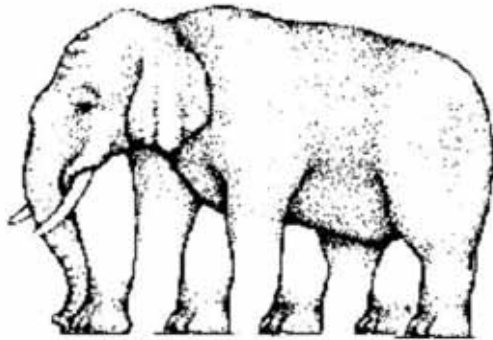
1. O usuário comum como vítima.
2. A Engenharia Social e a Justiça Brasileira
3. O difícil combate à Engenharia Social.

### Respondendo a uma solicitação de informações



### Reflexões

1. "Nada deve ser mais estimado do que a informação, mais bem pago do que a informação e nada deve ser mais confidencial do que o trabalho de coleta de informações". Sun Tzu, in *A Arte da Guerra*
2. "Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza sobre o primeiro". Albert Einstein



# Perguntas?

*marcelobc@pgr.mpf.gov.br*

---

## Sugestões Bibliográficas

1 <sup>o</sup>	<b>Livros</b>	A Arte de Enganar – Kevin Mitnick Você pode negociar qualquer coisa – Herb Cohen
2 <sup>o</sup>	<b>Filmes</b>	Caçada Virtual Prenda-me se for capaz A liga extraordinária
3 <sup>o</sup>	<b>Internet</b>	<a href="http://www.zdnet.com.au/insight/security/0,39023764,39149146,00.htm">http://www.zdnet.com.au/insight/security/0,39023764,39149146,00.htm</a> <a href="http://www.kuro5hin.org/story/2004/6/3/223758/2267">http://www.kuro5hin.org/story/2004/6/3/223758/2267</a>