



OWASP

The Open Web Application Security Project



TestGroup

INGENIERÍA SOCIAL: HACKING PSICOLÓGICO



Mayo - 2012

Gustavo Inzunza Rojas

Presentación

Gustavo Eduardo Inzunza Rojas



gustavo.inzunza@testgroup.cl



ginzunza



snootchie_

- Ingeniero en Computación e Informática
Universidad de Santiago de Chile
- Diplomado “Control, Seguridad y Auditoría Computacional”
Universidad de Santiago de Chile
- Test Manager
TestGroup

Introducción

Trojanos

Buffer OverFlow

DoS (*Denial of Service*)

Cross Site Scripting

Spyware

Virus

SQL Inyection

Pharming

DNS Name Prediction

Malware





¿Cuál es el eslabón más débil cuando hablamos de Seguridad de la Información?

A: Software

B: Internet

C: Usuario

D: Hardware

¿Qué es la Ingeniería Social?

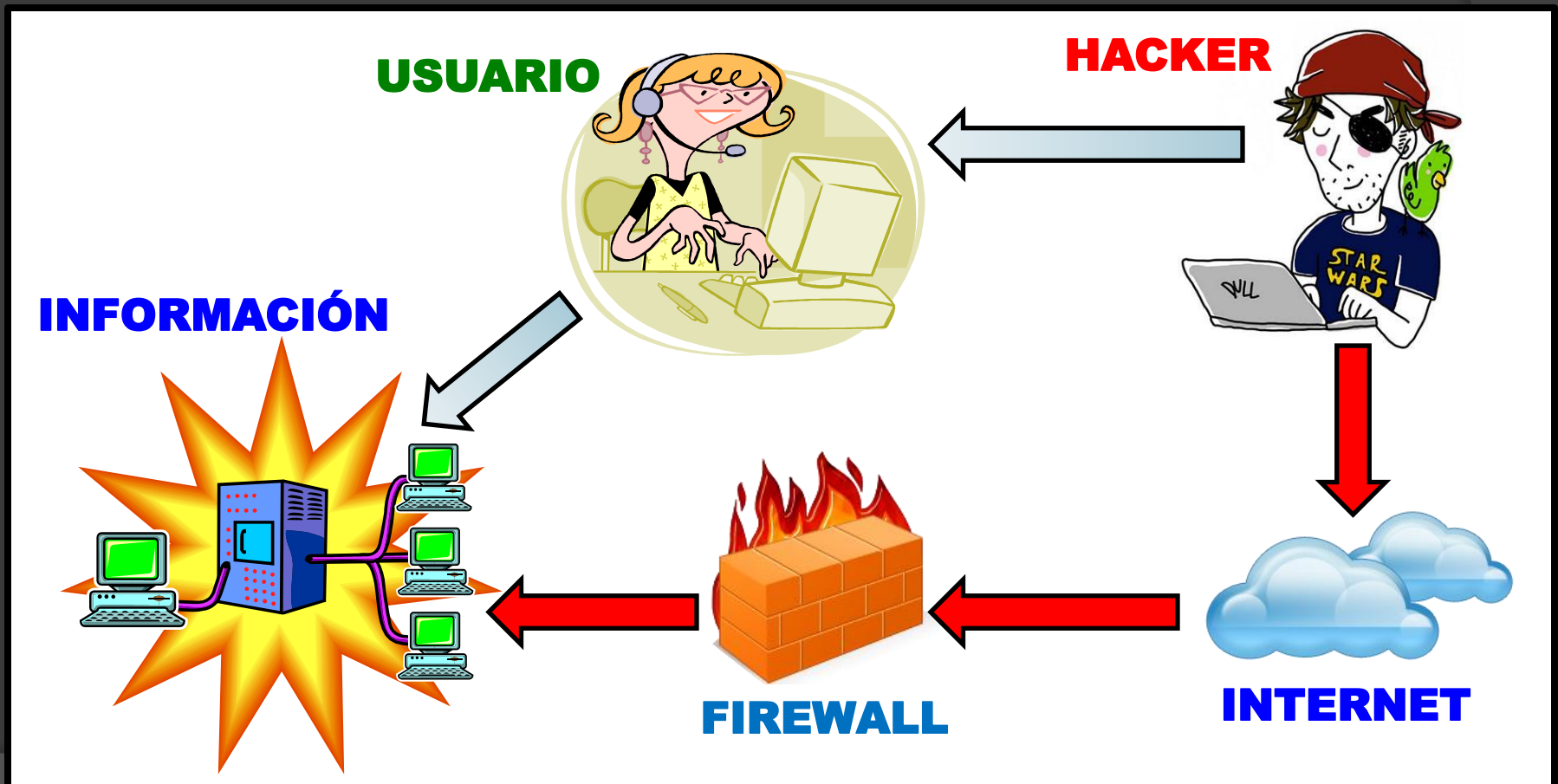
Conjunto de técnicas psicológicas y habilidades sociales (tales como: la influencia, la persuasión y la sugestión) implementadas hacia un usuario directa o indirectamente para lograr que éste revele información sensible o datos útiles sin estar conscientes de los riesgos que esto implica.

- * Basada en Computadoras
 - Phishing
- * Basada en Contacto Humano
 - Presencial
 - Telefónico
 - Etc...



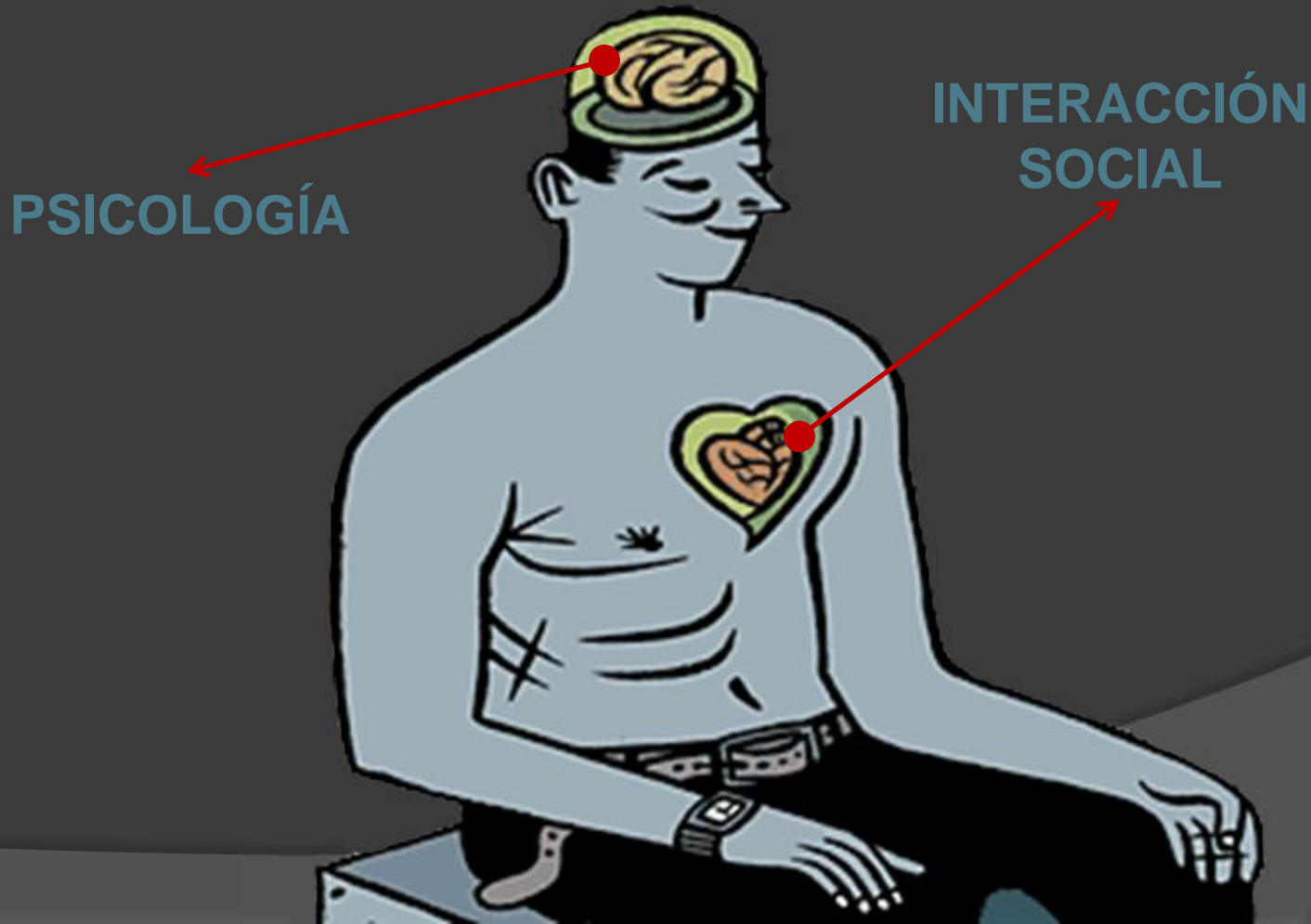
¿Qué es la Ingeniería Social?

Es bastante similar al hacking normal, con la única diferencia que no se interactúa con una máquina, sino con una persona.



Factores Claves

Al momento de entender la Ingeniería Social existen 2 puntos clave a tener en consideración.





¿Cuál es el activo más importante para la organización?

A: Información

B: Instalaciones

C: Procesos

D: Hardware

¿Que es lo busca el hacker?

El primer paso para comprender la importancia de protegerse respecto a estos ataques es determinar cual es el botín que persigue el hacker.

**Información
Confidencial**



¿Y cuál es el impacto?

- * Personal
- * Financiero
- * Imagen
- * Legal



Veamos un ejemplo...

Usuario: Hola?

Atacante: (*denotando prisa y fastidio*) Si, buenos días, habla Pedro de acá de Sistemas.

Usuario: Pedro?...de Sistemas?

Atacante: Si! (*con voz segura*) tienes algún problema con tu usuario de red?. Acá en la pantalla me figura que está presentando errores.

Usuario: Que yo sepa no...

Atacante: Quizás sea un error nuestro, a ver, dígame su nombre de usuario o identificador.

Usuario: Si...ehhhh...es "msilva".

Atacante: Ummm...segura?...déjame buscarlo en el listado de usuarios...Ok, acá está. ¿ahora deme su actual contraseña para cambiarla por una nueva?.

Usuario: Si... es "marcela80".

Atacante: Ok, muchas gracias. Hasta luego.

Conozcamos al maestro...

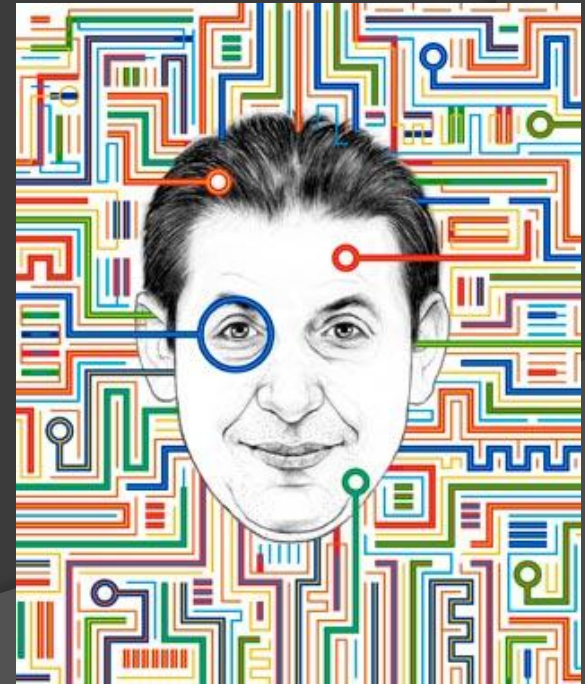
Kevin Mitnick (El Cóndor) es uno de los phreaker más famosos del mundo.

En 1981 accede al Sistema COSMOS (*Computer System for Mainframe Operation*). Obtiene listado de claves.

En 1983 obtiene acceso ilegal al ARPAnet para acceder a la red del Pentágono.

En 1994 obtiene la clave de Tsutomu Shimomura.

En 1995 es capturado por el FBI y condenado a 5 años de cárcel.



Conozcamos al maestro...

Fue acusado de robo de software y fraude electrónico.

Nokia

Novell

Sun Microsystems

Motorola

Apple

En 2002 edita el libro “The Art Of Deception”

En 2003 edita el libro “The Art Of Intrusion”



Conozcamos al maestro...

Según Mitnick la Ingeniería Social se fundamenta sobre cuatro conceptos básicos:

- * Todos queremos ayudar.
- * El primer movimiento es siempre de confianza hacia el otro.
- * No nos gusta decir “NO”.
- * A todos nos gustan que nos alaben.



Categoría de Ataques

Es posible separar la Ingeniería Social en 4 tipos de ataques:

Ataques Técnicos

Ataques al Ego

Ataques de Simpatía

Ataques de Intimidación



Categoría de Ataques

ATAQUES TÉCNICOS

- No existe contacto directo con las víctimas.
- El atacante utiliza emails, páginas web, boletines.
- El atacante simula ser una entidad reconocida y de confianza.
- Orientado a obtener información sensible de los usuarios.
- Altamente exitoso.



Categoría de Ataques

ATAQUES AL EGO

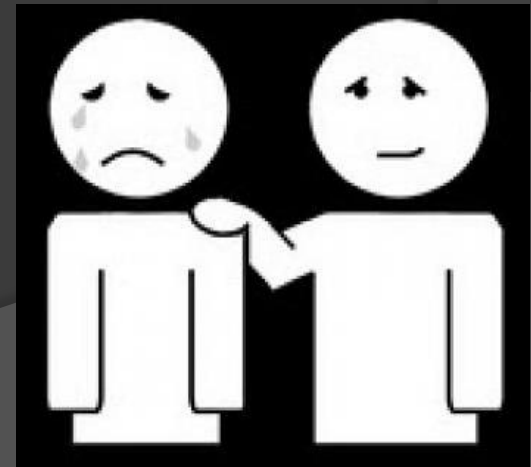
- El atacante apela a la vanidad y ego de la víctima.
- La víctima trata de probar su inteligencia y eficacia.
- Se busca que la víctima sienta que esta ayudando en un tema relevante (*y que posiblemente recibirá reconocimiento*).
- Usualmente la víctima nunca se da cuenta del ataque.



Categoría de Ataques

ATAQUES DE SIMPATÍA

- Se simula un escenario donde es urgente completar una tarea o actividad.
- Se apela a la empatía de la víctima.
- El atacante pide ayuda hasta que encuentra alguien que le pueda proporcionar lo que necesita.
- El atacante se muestra bastante desesperado, indicando que su trabajo está en juego si no completa su tarea.



Categoría de Ataques

ATAQUES DE INTIMIDACIÓN

- El atacante simula ser alguien importante en la organización.
- Trata de utilizar su autoridad para forzar a la víctima a cooperar.
- Si existe resistencia utiliza la intimidación y amenazas (*pérdida de empleo, multas, cargos legales, etc.*).





¿Cuál de las siguientes acciones NO es una medida de mitigación a la Ingeniería Social?

A: Capacitar

B: Documentar

C: Monitorear

D: Concientizar

Medidas de Mitigación



CAPACITAR



CONCIENTIZAR



REFORZAR



MONITOREAR



**Cuándo estamos en presencia de este
tipo de ataques:
¿de quien es la responsabilidad?**

A: Gerencia

B: RRHH

C: Usuario

D: ¿Quién sabe?

Conclusiones

- La Ingeniería Social es un tema al que todavía no se le da tanta importancia en el interior de las organizaciones.
- Las consecuencias de ser víctima de este tipo de ataques pueden ser muy grandes.
- El atacante o hacker puede utilizar diferentes mecanismos de persuasión.
- Resulta importante definir una política de capacitación a los usuarios, con el fin de mitigar posibles ataques.
- ¿DE QUIEN ES LA RESPONSABILIDAD?

Conclusiones

En un congreso “Access All Areas” de 1997, uno de los relatores decía:

"Aunque se dice que el único computador seguro es el que está desenchufado, los amantes de la ingeniería social gustan responder que siempre se puede convencer a alguien para que lo enchufe".



Preguntas

