About Me

OWASP
The Open Web Application Security Project

- Marco Castro mcastro@sefin.gob.hn
  - ➢ Ethical Hacker, Network Security Administrator y Cobit Foundation
  - ➢ Oficial de Seguridad de la Informacion en la Secretaría de Finanzas

OWASP
The Open Web Application Security Project

Temario

- Introducción
- ¿Qué es la Ingeniería Social?
- Factores Claves
- ¿Qué es lo que busca el hacker?
- Veamos un ejemplo
- Conozcamos al maestro
- Categoría de Ataques
- Medidas de Mitigación
- Conclusiones

OWASP
The Open Web Application Security Project

De Acuerdo a Balabit, Febrero de 2016

	USA	EU	
1	81%	83%	**SOCIAL ENGINEERING** (e.g. phishing)
2	62%	63%	**COMPROMISED ACCOUNTS** (e.g. weak passwords)
3	51%	54%	**WEB-BASED ATTACKS** (e.g. SQL/command injection)
4	33%	43%	**CLIENT SIDE ATTACKS** (e.g. against doc readers, web browsers)
5	23%	17%	**EXPLOIT AGAINST POPULAR SERVER UPDATES** (e.g. OpenSSL, Heartbleed)
6	21%	16%	**UNMANAGED PERSONAL DEVICES** (e.g. lack of BYOD policy)
7	15%	13%	**PHYSICAL INTRUSION**
8	11%	10%	**SHADOW IT** (e.g. users' personal cloud-based services for business purposes)
9	9%	10%	**MANAGING THIRD PARTY SERVICE PROVIDERS** (e.g. outsourced infrastructure)
10	6%	6%	**TAKE ADVANTAGE OF GETTING DATA PUT TO THE CLOUD** (e.g. IAAS, PAAS)

OWASP
The Open Web Application Securi

Introducción

¿Cuál es el activo más importante para la organización?

A: Información

B: Instalaciones

C: Procesos

D: Hardware

OWASP
The Open Web Application Security Project

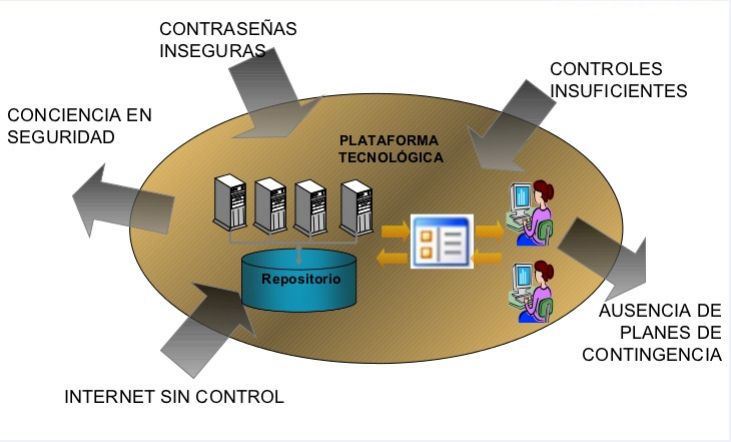
Introducción

Amenazas

Introducción

OWASP
The Open Web Application Security Project

Vulnerabilidades



OWASP
The Open Web Application Security

¿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**?

OWASP
The Open Web Application Security Project

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.

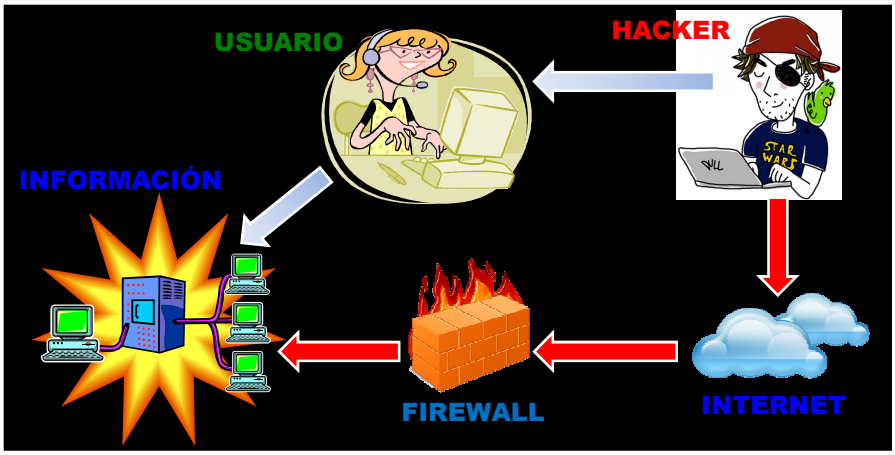
* Basada en Computadoras
  - Phishing

* Basada en Contacto Humano
  - Presencial
  - Telefónico
  - Etc…

¿Qué es la Ingeniería Social?

OWASP
The Open Web Application Security Project

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



Factores Claves

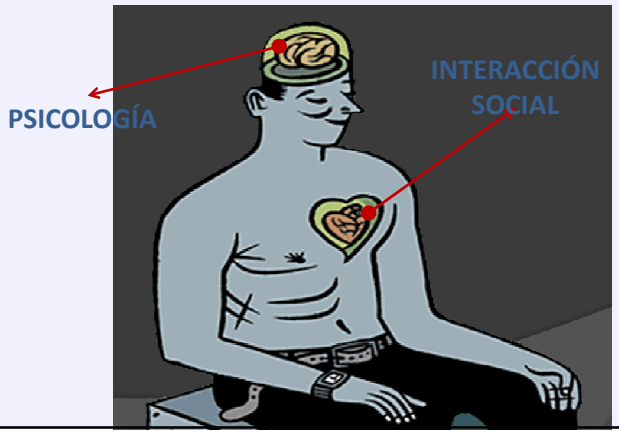
OWASP
The Open Web Application Security Project

- Es Mas fácil que tratar de hackear un sistema con códigos y algoritmos
- No es necesario violar o burlar sistemas de detección de intrusos o firewalls
- Las herramientas para utilizar son gratis o de muy bajo costo
- Sin registro y con 100 % de efectividad aprox.
- Porque las personas son la vulnerabilidad mas grande en cualquier Empresa

Factores Claves

OWASP
The Open Web Application Security Project

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



¿Que es lo que busca el hacker?

OWASP
The Open Web Application Security Project

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…

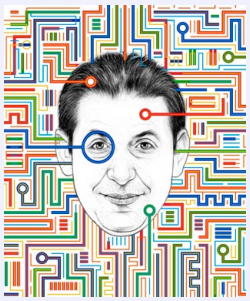
OWASP
The Open Web Application Security Project

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…

OWASP
The Open Web Application Security Project

Kevin Mitnick (El Cóndor) es uno de los hackers más famosos del mundo, que se especializó en el arte de manipular a las personas para que hicieran lo que el quería y obtener información confidencial. Su primera incursión en el *hacking* lo tiene a los 16 años cuando penetra el sistema administrativo de su colegio.



En 1981 accede al Sistema COSMOS (*Computer System for Mainframe Operation*)

En 1994 accede al computador personal de Tsutomu Shimomura (*Netcom On-Line Communications*)

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

Conozcamos al maestro…

OWASP
The Open Web Application Security Project

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

* Todos queremos ayudar.

* El primer movimiento es siempre de confianza hacía el otro.

* No nos gusta decir "NO".

* A todos nos gustan que nos alaben.

Categoría de Ataques

OWASP
The Open Web Application Security Project

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

OWASP
The Open Web Application Security Project

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.

Phishing (Morder el Anzuelo)

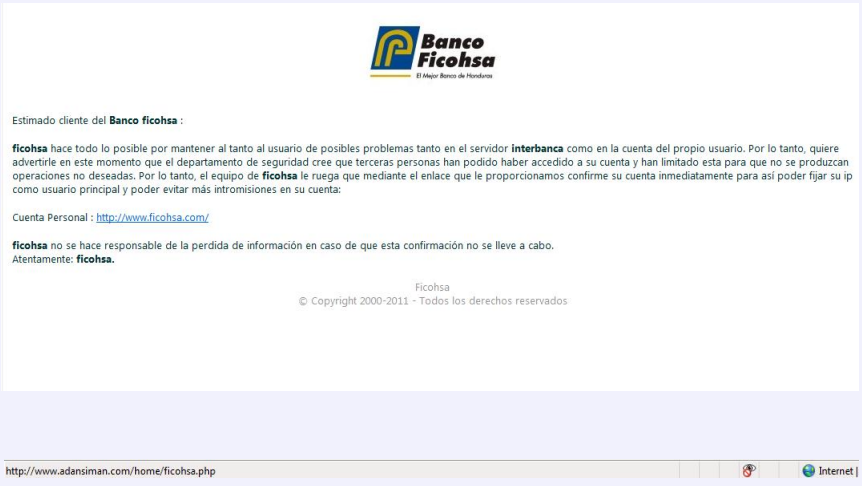
OWASP
The Open Web Application Security Project

Una de las principales vulnerabilidades es que muchos usuarios utilizan la ***misma contraseña*** para diferentes servicios.

Una técnica conocida es a través de ***formularios o pantallas de login falsas***. Donde se le pide al usuario que valide sus datos de acceso sobre un sitio Web manipulado por el atacante.

Ejemplo de Phishing

OWASP
The Open Web Application Security Project



Drive by Infection (Infecciones Dirigidas)

OWASP
The Open Web Application Security Project

Cuando uno descarga "***soluciones de seguridad***" desde sitios Web es posible infectarse con diferentes variedades de **Malware** o **Troyanos**.

A)- Intencionalmente: Aceptando la descarga desde el sitio Web.
B)- Involuntariamente: Explotando una vulnerabilidad en el navegador (0 day).

Email

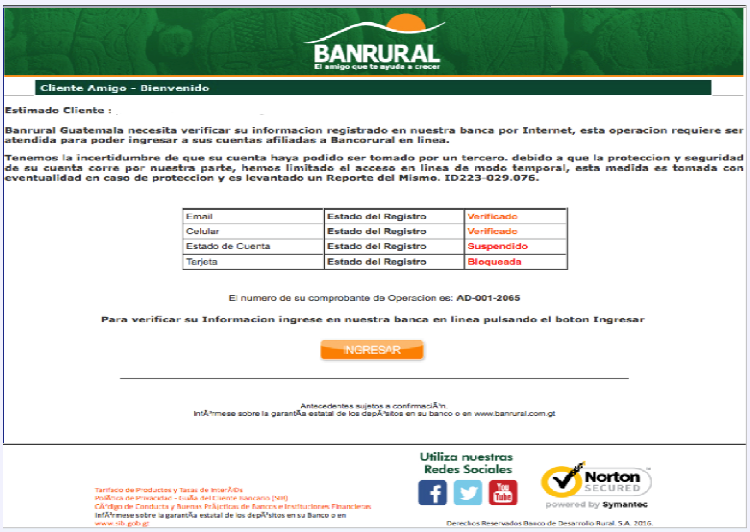
OWASP
The Open Web Application Security Project

Los emails enviados pueden contener información interesante para los usuarios y ser bastante llamativos como la ***imaginación*** lo permita. Desde fotos de famosas hasta *cómo construir un reactor nuclear*.

En los archivos adjuntos pueden existir ***virus***, ***gusanos***, **backdoors**, etc. permitiendo tener acceso total al atacante.

Email

OWASP
The Open Web Application Security Project



BANRURAL
El amigo que te ayuda a crecer

Cliente Amigo - Bienvenido

Estimado Cliente :

Banrural Guatemala necesita verificar su informacion registrado en nuestra banca por Internet, esta operacion requiere ser atendida para poder ingresar a sus cuentas afiliadas a Bancorural en linea.

Tenemos la incertidumbre de que su cuenta haya podido ser tomado por un tercero. debido a que la proteccion y seguridad de su cuenta corre por nuestra parte, hemos limitado el acceso en linea de modo temporal, esta madida es tomada con eventualidad en caso de proteccion y es levantado un Reporte del Mismo. ID223-029.076.

Email	Estado del Registro	Verificado
Celular	Estado del Registro	Verificado
Estado de Cuenta	Estado del Registro	Suspendido
Tarjeta	Estado del Registro	Bloqueada

El numero de su comprobante de Operacion es: AD-001-2065

Para verificar su Informacion ingrese en nuestra banca en linea pulsando el boton Ingresar

INGRESAR

Antecedentes sujetos a confirmaciÃ³n
IntÃ©rmese sobre la garantÃa estatal de los depÃ³sitos en su banco o en www.banrural.com.gt

Utiliza nuestras Redes Sociales

Norton SECURED powered by Symantec

Tarifario de Productos y Tasas de InterÃ©s
mÃ©dicas de Privacidad - Guía del Usuario Bancario (NIP)
CÃ³digo de Conducta y Buenas PrÃ¡cticas de Bancos e Instituciones Financieras
IntÃ©rmese sobre la garantÃa estatal de los depÃ³sitos en su Banco o en
www.sib.gob.gt

Derechos Reservados Banco de Desarrollo Rural, S.A. 2016

Categoría de Ataques

OWASP
The Open Web Application Security Project

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.

Dumpster Driving (Contenedor de Basura)

OWASP
The Open Web Application Security Project

También conocido como "***Trashing***" (***Buscar en la Basura***), es otro método de Ingeniería Social. Mucha información puede ser encontrada en la basura.

Ejemplos: Anotaciones, Manuales, Políticas, Memos, **CONTRASEÑAS**!

Shoulder Surfing (Espiar por encima del Hombro)

OWASP
The Open Web Application Security Project

Consiste en entablar una conversación y realizar ***notas mentales*** sobre las teclas que presiona el usuario al momento de ingresar sus datos de acceso a un sistema.

Categoría de Ataques

OWASP
The Open Web Application Security Project

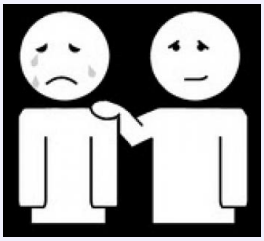
ATAQUES DE SIMPATÍA

- 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.



Curiosidad (Hardware)

OWASP
The Open Web Application Security Project

El atacante deja un ***dispositivo de almacenamiento*** como pendrive, CD, memoria flash en un lugar donde pueda ser encontrado, mientras espera a que la víctima introduzca el dispositivo para infectarse con el código malicioso.

A través de la ***curiosidad*** humana es posible llevar a cabo este tipo de ataque.

Suplantación de ID

OWASP
The Open Web Application Security Project

Consiste en caracterizar a una persona, un rol. Generalmente los roles más empleados son ***soporte técnico*** y ***gerente***, etc.

En empresas grandes es difícil conocer a todos los empleados y falsificar las ID resulta Muy Simple!

Office Snooping (Espionaje en la Oficina)

OWASP
The Open Web Application Security Project

Muchos usuarios ***no dejan bloqueadas sus terminales*** cuando se levantan de sus escritorios o peor aún cuando se retiran del trabajo, por lo tanto es posible acceder a sus datos sin necesidad de identificarse.

Categoría de Ataques

OWASP
The Open Web Application Security Project

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.).*

Telefónico

OWASP
The Open Web Application Security Project

Un atacante llama por teléfono y trata de ***intimidar*** a alguien en la posición de autoridad o relevancia, de esa forma obtiene información.

Los Centros de Ayuda (***HelpDesk***) son generalmente vulnerables a este tipo de ataque.

Ingeniería Social Inversa

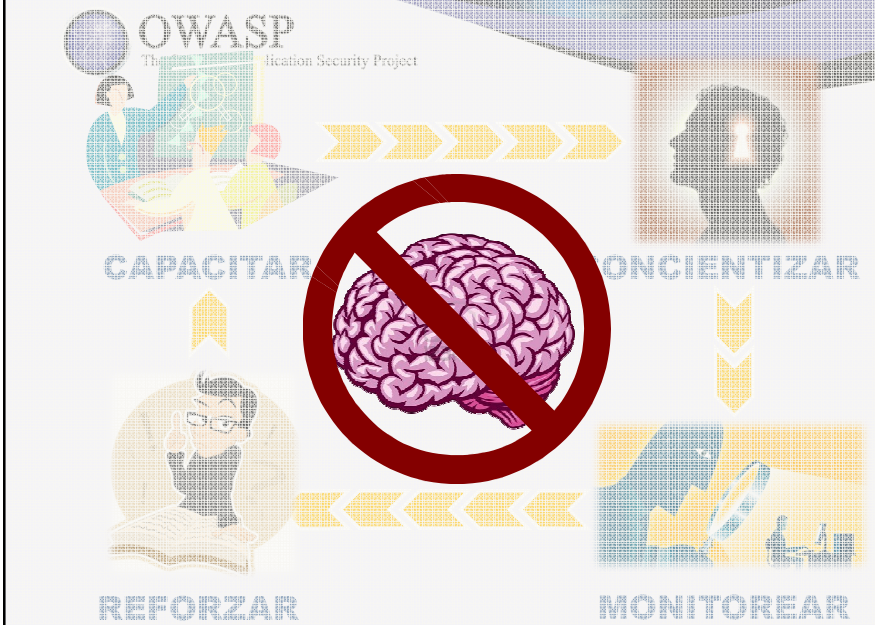
OWASP
The Open Web Application Security Project

Es el modo avanzado de la Ingeniería Social, conocido como "***Ingeniería Social Inversa***".

El atacante trata de parecer alguien de ***autoridad***, para que le pregunten a él y así obtener información.

Requiere mucha ***preparación***, ***investigación*** y saber relacionarse con las personas.

Medidas de Mitigación



Medidas de Mitigación

OWASP
The Open Web Application Security Project

Simples métodos para evitar un ataque:

» "***No***" es lo primero, en algunas situaciones puede ser flexible, disuasivo y eficaz. Los "NO" son más fuertes cuando estamos seguros de tener razón.

» ***Sí el conocimiento es un arma, la ignorancia es una armadura***. No dar mucha información o detalles sobre lo que nos preguntan.

» Las ***políticas*** son buenas defensas contra la ingeniería social.

» ***Lo mejor manera de aumentar nuestras defensas es disminuir la posibilidad de evadirlas***. Utilizar seguridad física, biometría y restringir el acceso físico.

Medidas de Mitigación

OWASP
The Open Web Application Security Project

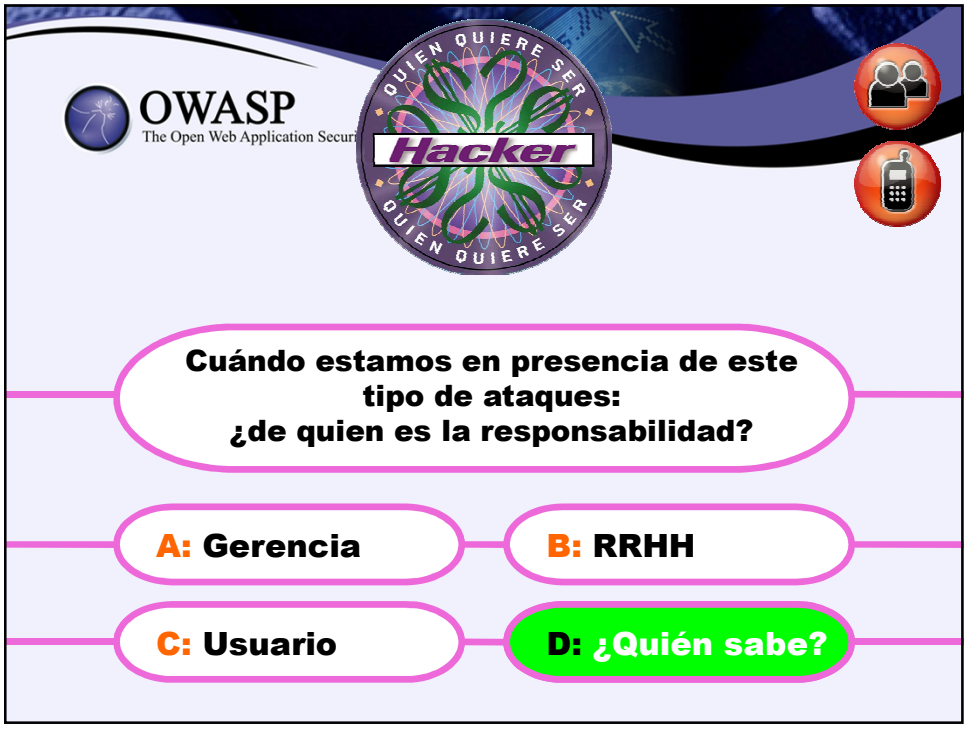
¿Cuál de las siguientes acciones NO es una medida de mitigación a la Ingeniería Social?

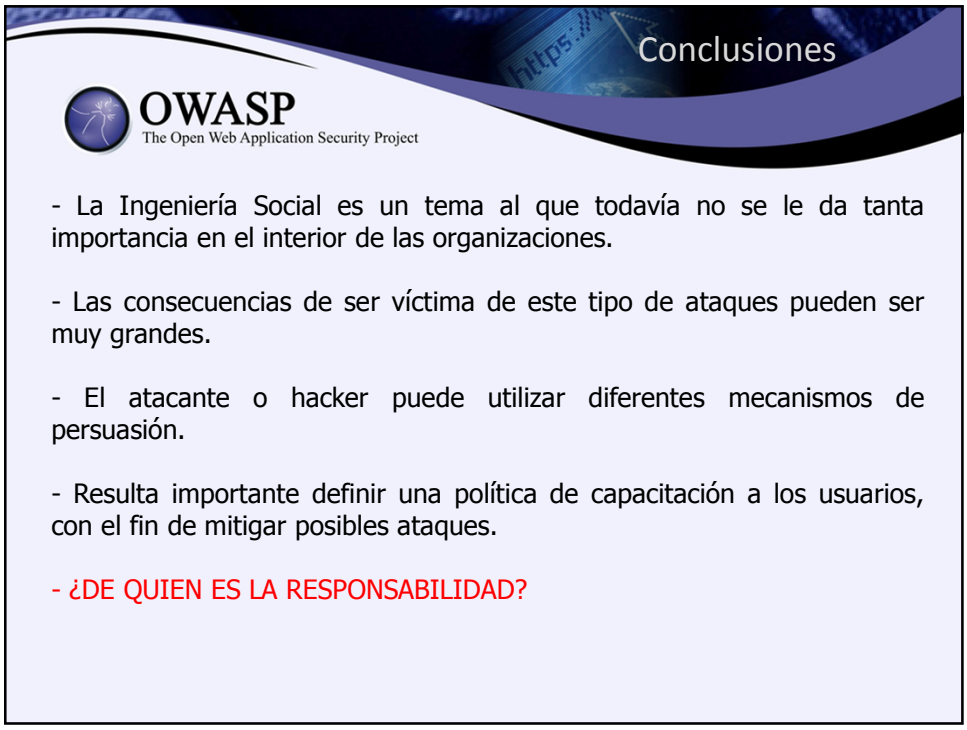
A: Capacitar

B: Documentar

C: Monitorear

D: Concientizar


OWASP
The Open Web Application Securi
QUIEN QUIERE SER
Hacker
QUIEN QUIERE SER
Cuándo estamos en presencia de este tipo de ataques: ¿de quien es la responsabilidad?
A: Gerencia
B: RRHH
C: Usuario
D: ¿Quién sabe?


Conclusiones
OWASP
The Open Web Application Security Project
- 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

OWASP
The Open Web Application Security Project

En un congreso de seguridad de información, 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

OWASP
The Open Web Application Security Project