

Nuevos retos de Seguridad

la importancia del elemento humano

Alfredo Aranguren T. CISM, CISSP

De nada sirve invertir miles de dólares en tecnología, si el elemento humano que la opera y usa falla.

Es importantes proteger la información, no importando la manera en que esta se encuentre (digital, impresa, verbal).

Problemática Actual

- Mal manejo de documentos impresos.
 - Impresión desatendida.
 - Desecho de documentos
 - Escritorio limpio.

Dumpster Diving



Problemática Actual

- Mal manejo de dispositivos de accesos físicos
 - Otorgar accesos a personal no autorizado.



Piggybacking

Problemática Actual

- Uso de USB Drives
 - Uso promiscuo
 - Desconocimiento de medidas básicas de seguridad.
 - Confidencialidad
 - Integridad
 - Destrucción



Problemática Actual

- Shoulder Surfing
 - Bloqueo de equipo



Problemática Actual

- Phishing



Facebook Login

Email:

Password:

Remember me

[Login](#) or [Sign up for Facebook](#)

[Forgot your password?](#)

Problemática Actual

- Cartas cadenas, Scams
 - Robo de identidad
 - Fraudes

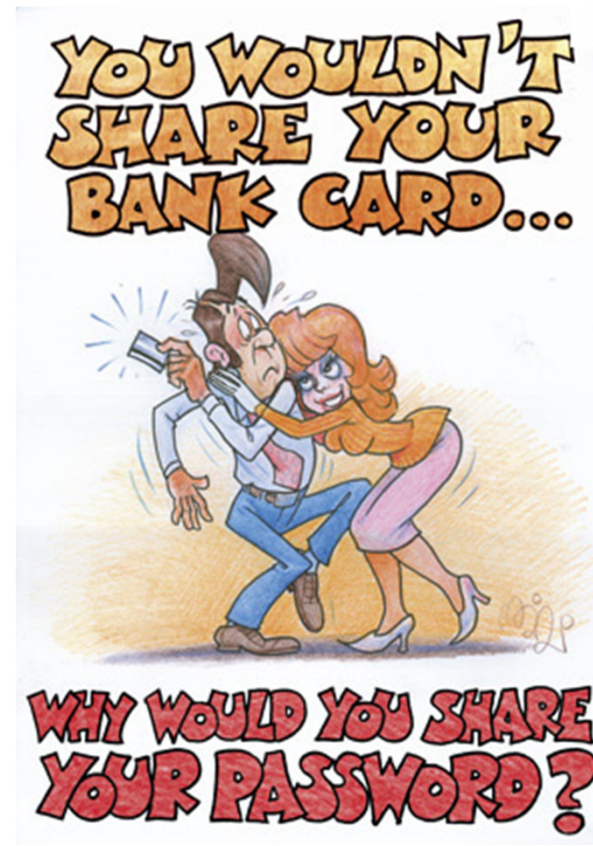
loan Department



"I need it to fly to Nigeria
to pick up my prize."

Problemática Actual

- Prestamos de cuentas y contraseñas
 - No repudiation



Problemática Actual

- Manejo de Información verbal
 - En sitios públicos
 - Fuera de la empresa
 - Con personas conocidas.



Principales amenazas 2011

- Vulnerabilidades en la aplicaciones
- Dispositivos móviles
- Virus y Gusanos
- Usuarios internos
- Hackers
- Cyberterrorismo
- Servicios en la nube
- Crimen organizado
- Ataques a redes sociales
- Phishing, Smishing, Vishing

Tendencias

- Los atacantes aumentarán el uso de tácticas de ingeniería social para darle vuelta a los controles de seguridad tecnológicos.
- Sus técnicas tomarán ventaja de factores psicológicos, tales como del deseo de tener más información, la necesidad de cumplir con normas sociales y en la propensión a obedecer a figuras de autoridad.
- Más organizaciones adoptarán los medios sociales como un aspecto fundamental de su estrategia de mercadotecnia.

Tendencias

- Las organizaciones tendrán dificultades para controlar las actividades en redes sociales de sus usuarios.
- Los atacantes continuarán tomando ventaja del poco entendimiento de las practicas de seguridad en redes sociales para defraudar a personas y organizaciones.
- El ser humano es el eslabón más débil, independientemente de como cambie la tecnología, los atacantes saben que siempre se puede engañar a los empleados.

Tendencias

- Las organizaciones empezarán a tomar acciones para asegurar al ser humano.
- La concientización ayudará a reducir la efectividad de los ataques y ayudará al usuario final a detectar un ataque.

Tendencias

- La redes sociales eventualmente remplazarán al correo como el vector primario para distribuir ligas y código malicioso aprovechando la falta de conocimiento del usuario.

¿Que Hacer?

- Un programa de concientización debe de ir enfocado a **crear una cultura, un hábito**.
- Los empleados deben de entender el **valor** que tiene la información y las **consecuencias** en caso de que la misma se vea comprometida.
- El soporte de la alta dirección es indispensable.
- Requiere la participación de diversas áreas (Comunicación corporativa, mercadotecnia)
- Manejo del lenguaje, simple es mejor. Use analogías.

¿Que Hacer?

- Use diferentes medios
- Piensa divertido
- Explica el porqué de la políticas.
- Las políticas deben de funcionar. (Walk your talk)

Los mandamientos de la seguridad

- Protege tu Equipo
- Tu usuario y contraseña son intransferibles... Cuídalos
- Haz uso adecuado de tu correo electrónico
- Mantén tu escritorio libre de información
- No Seas victima de fraude electrónico y Phishing
- Navega de manera segura
- Manejo de la información
- Protege las instalaciones
- Ante la duda... consulta

¿Porqué la ingeniería social es tan exitosa?

Porque no hay parches para la estupidez humana.



GRACIAS