

CURSOS  
INTERSEMESTRALES



PROTECO

# Seguridad

Introducción.

# Privacidad vs Anonimato vs Seguridad.

Es importante saber que estos conceptos son distintos y en algunos casos pueden llegar a ser contradictorios.



- PRIVACY -



- ANONYMITY -



- SECURITY -



# Privacidad.

Implica que nadie conozca tus acciones y mantener protegida tu información personal, va mayormente orientado al contenido (información).

Ej:

Historial clínico.

Datos personales.



PROTECO

# Anonimato.

Separar tus acciones de tu identidad. Las acciones (potencialmente) no son privadas.

No atribución.

Ej:  
Publicar mensajes  
en contra del regimen.



# Pseudo anonimato

Separar tus acciones de tu identidad. Más estas estarán ligadas a una segunda identidad.

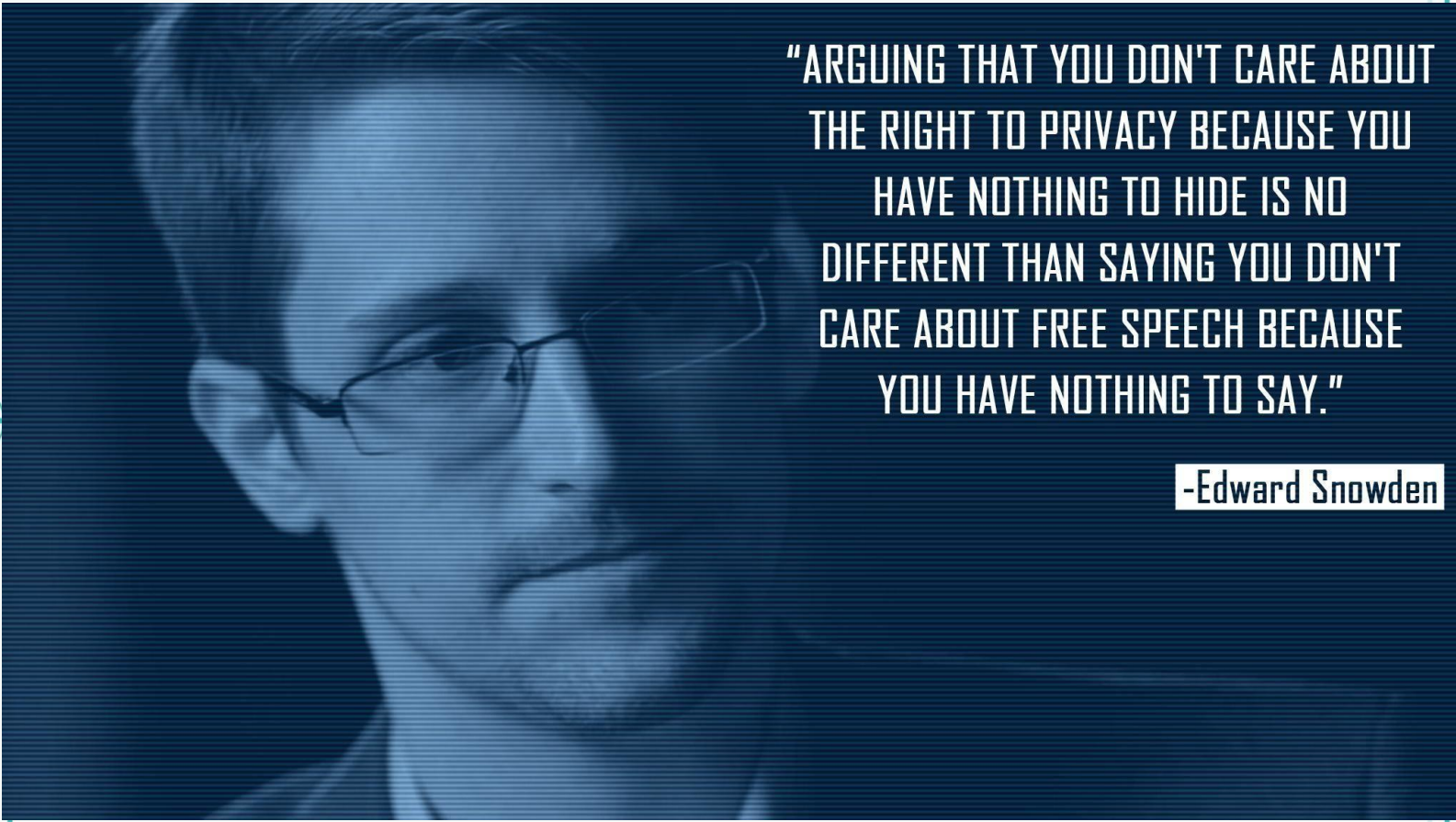
Ej:

Tener un nickname en un foro.

**MR. ROBOT**



# ¿No tengo nada que esconder?



"ARGUING THAT YOU DON'T CARE ABOUT  
THE RIGHT TO PRIVACY BECAUSE YOU  
HAVE NOTHING TO HIDE IS NO  
DIFFERENT THAN SAYING YOU DON'T  
CARE ABOUT FREE SPEECH BECAUSE  
YOU HAVE NOTHING TO SAY."

-Edward Snowden



PROTECO



# Mass Surveillance



PROTECO

# Mass Surveillance



PROTECO



# Seguridad.

¿Qué es la cyberseguridad?

Disciplina de manejo de riesgos. Que puede tener una solución tecnológica.

\*) Tecnológica (cifrados, acls, etc)

\*) Física (guardias, camaras, etc)

\*) Administrativa:  
(awareness, planes de contingencia)



PROTECO



## ¿Qué es la Seguridad informática?

“Conjunto de medios y técnicas implementadas para asegurar la integridad y la no difusión involuntaria de los datos ... entendiendo un conjunto de datos y recursos” (Agé M. ,2015)

Recursos:

- Físicos
- Lógicos
- Humanos



# ¿Qué no es seguridad?

¿Es necesariamente tecnológico? No

¿Existe por si mismo? No

¿Puedo tenerla al 100%? No

¿Es lo mismo para todos? No

¿Es una solución unica? No



# ¿Es fácil la seguridad?

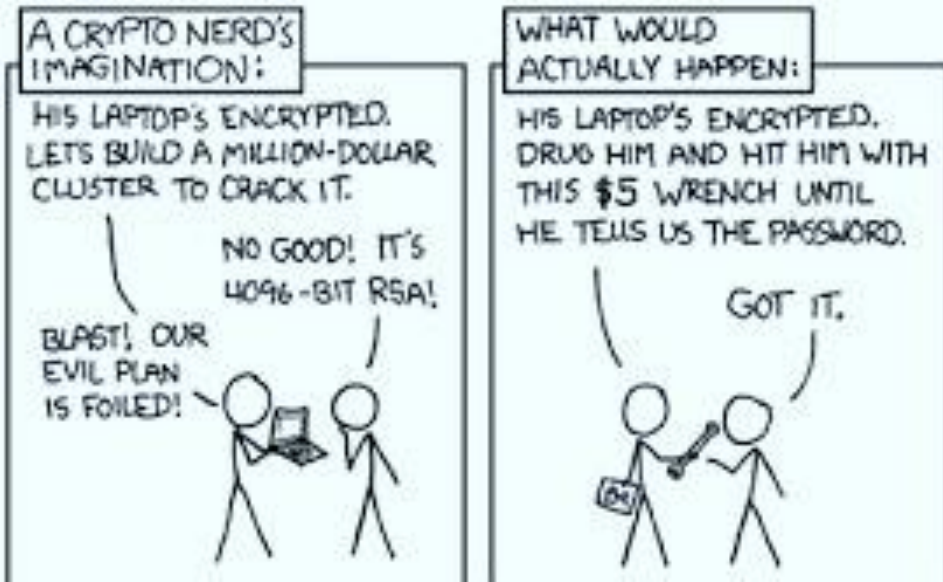
“Hoy no tuvimos suerte, pero recuerden  
que solo debemos tener suerte una vez,  
ustedes siempre tendrán que tener suerte”  
IRA en el brighton hotel bombing





# Mi empresa es muy pequeña.

- \*) 62 % de los ataques son a empresas pequeñas (IBM)
- \*) Security through obscurity no es la mayor estrategia. (STO)
- \*) Muchos ataques son automatizados, muchos ataques no tienen nada personal.
- \*) Un cybercriminal toma sólo por poder tomarlo.

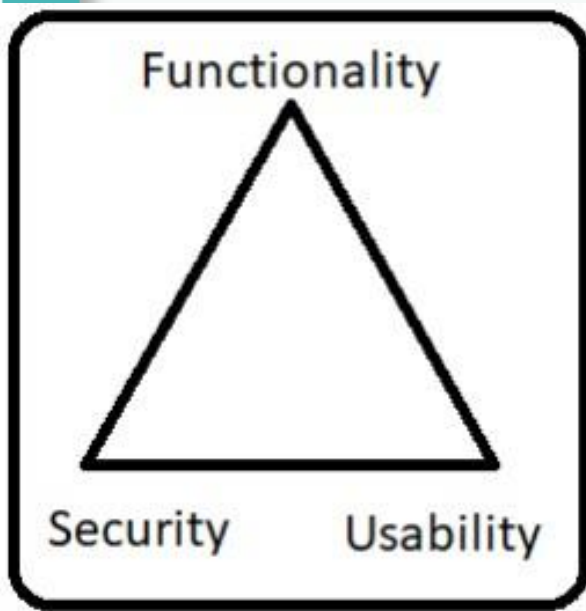




# Usability vs Security

Este es un tema bastante complejo.

Esta es la idea tradicional:



# Usability vs Security

Algunos autores critican el modelo anterior, y proponen que aunque en los extremos parece cierto, no lo es en el centro. Y no tiene porque estar peleadas ambas ideas.

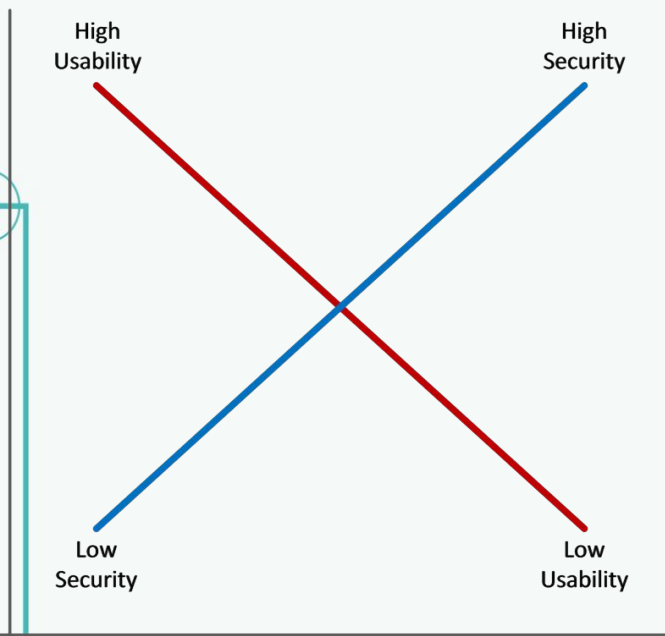


Figure 1: Security and usability tend to be inversely related



# Asset s

Una vez cubierta la importancia de la seguridad. ¿Qué es lo que queremos proteger?







# Vulnerabilidades

“Estado de configuración o defecto en un sistema que permite el uso de gente no autorizada mediante usos no intencionados violar las políticas de seguridad de un sistema. “ IETF Terminos similares: Security Bug





dependen de quienes



# Mitigar riesgos.

¿Porque no se eliminan los riesgos?

Siempre existirá el riesgo, y habrá situaciones en las cuales no se podrá erradicar completamente.

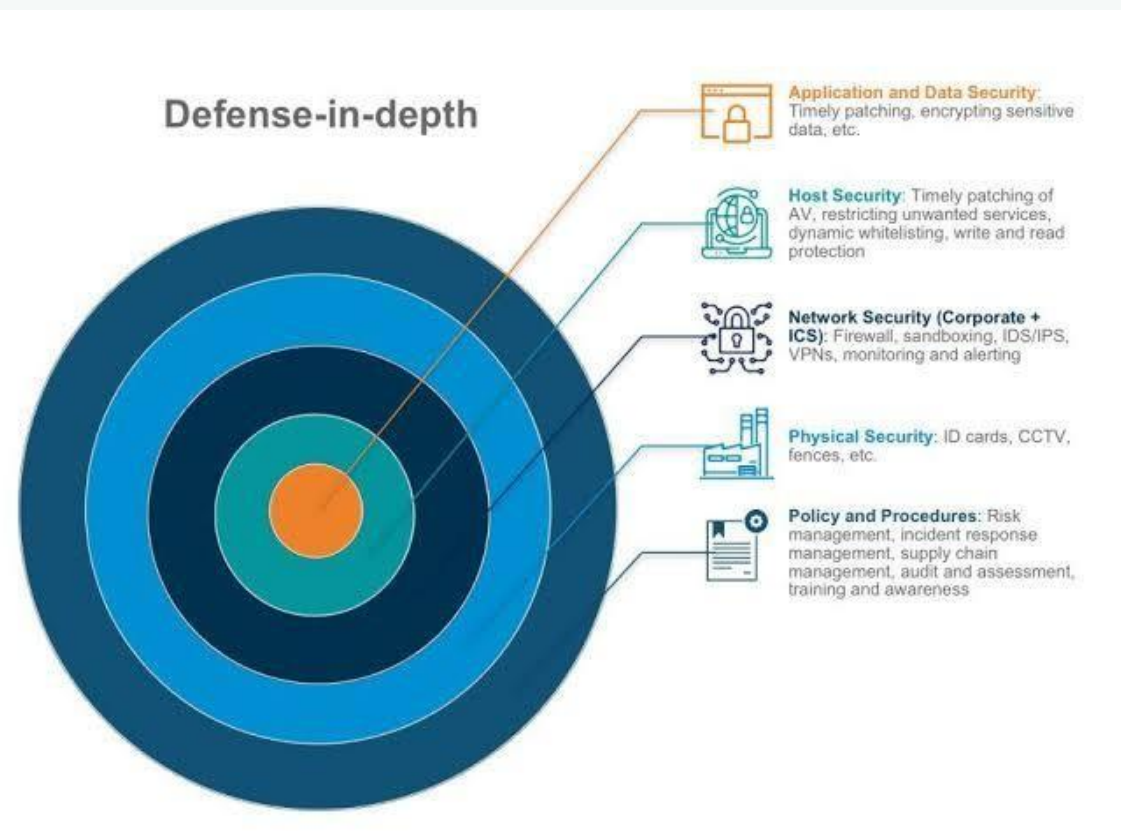
Depende de:

- \*) Nuestros assets.
- \*) Vulnerabilidades.



# Etapas de la seguridad.

Defense in Depth(Did): Consiste en tener múltiples capas de defensa, a modo de que el fallo de una pueda ser suplido por la siguiente.



# Etapas de la seguridad.

Ejemplos:

Prevención:

Actualizaciones, Firewalls, listas de control de acceso, etc.

Detección:

Antivirus, Monitorización, Logs, CanaryTokens, etc.

Recuperación:

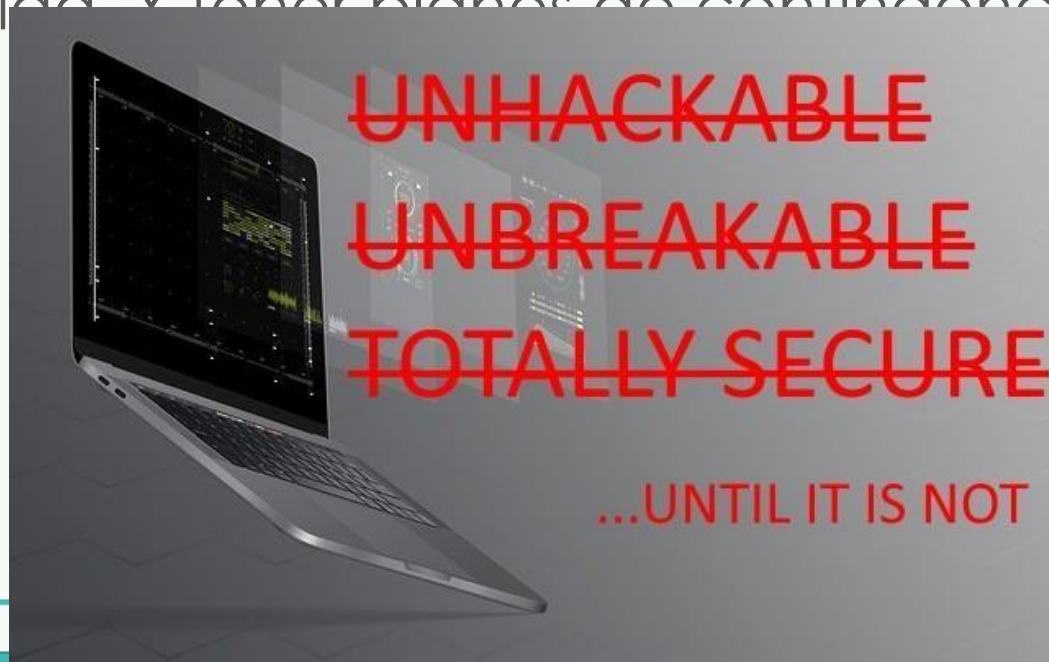
Anti-virus, respaldos, snapshots, respuestas automatizadas.



PROTECO

# Consideraciones:

- \*) No existe algo inhackeable
- \*) Mal manejo no es una cuestión de ser o no hackeados, sino de cuando.
- \*) A la primera intrusión, se acabó.
- \*) Debemos asumir que esta es una lucha perdida. Y tener planes de contingencia.





# Consideraciones:



# What's the Cost OF A CYBER ATTACK

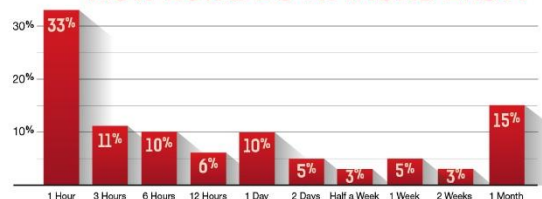
How much does a cyber-attack cost an organization? What are the business impacts? Radware conducted two surveys of IT professionals to find out.

## HOW WIDESPREAD ARE CYBER-ATTACKS?

**90%** of respondents reported experiencing an attack<sup>1</sup>.



## HOW LONG DO ATTACKS LAST?



## HOW MUCH DOES A CYBER-ATTACK COST?

A survey of U.S. and U.K. security executives found the following:



**36%** of U.S. respondents said an attack cost more than \$1 million<sup>2</sup>



**5%** said they spent more than \$10 million



**28%** of U.K. respondents said an attack cost more than £1 million<sup>2</sup>



**6%** said they spent more than £7 million

Average ransom paid in the U.S.  
**\$7,500**<sup>2</sup>



## TO PAY OR NOT TO PAY?

Nothing says "money" more than a ransom attack.



Average ransom paid in the U.K.  
**£22,000**<sup>2</sup>

## WHAT'S THE BUSINESS IMPACT?

Brand reputation, operational and revenue loss are the biggest.<sup>2</sup>

Brand Reputation Loss



Operational Loss



Revenue Loss



## CHANGES TO THWART SECURITY THREATS

Reduce the impact of a cyber-attack via policy/process change.<sup>2</sup>

Changes in Technology



Changes in C-Level Awareness



Changes in Knowledge/Education



## KNOWLEDGE IS POWER

Learn more at [www.ddoswarriors.com](http://www.ddoswarriors.com)

<sup>1</sup> 2015-2016 Global Application & Network Security Report  
<https://www.radware.com/inf-report-2015/>

<sup>2</sup> Security and the C-Suite: Threats and Opportunities  
<https://www.radware.com/c-suite-security-report-2016/>

# Modelos de seguridad:

CIA TRIAD.



PROTECO

# Introducción a la Seguridad Informática

Integridad:

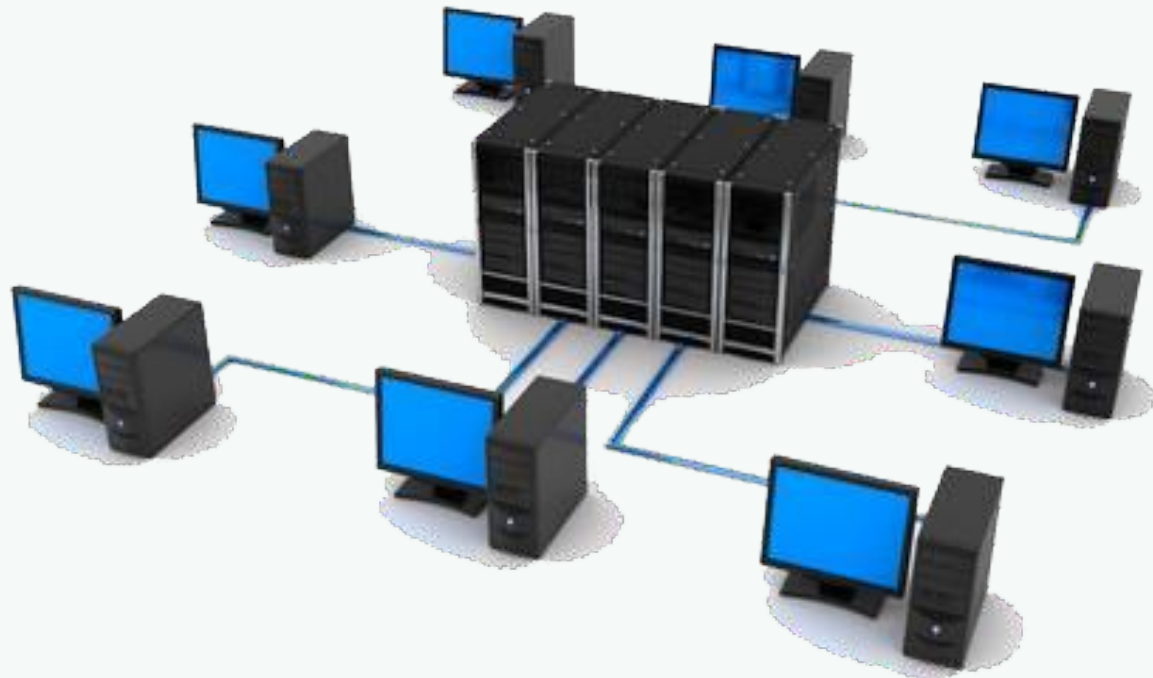
Evitar que los datos sufran cambios no autorizados.



# Introducción a la Seguridad Informática

Disponibilidad:

Continuidad operativa de una entidad y su accesibilidad mediante autorización.



PROTECO



# Introducción a la Seguridad Informática

Confidencialidad:

Protección contra la difusión no autorizada.  
Solo el emisor y el receptor deben entender el contenido del mensaje.



PROTECO

# Modelos de seguridad.

Parkerian Hexad (1998):



# Modelos de seguridad.

Parkerian Hexad (1998):

Autenticidad: Verificación del autor de algo.

Usabilidad: Facilidad de acceso o uso del propio producto. Ej: Encriptar un disco y perder la llave.

Se diferencia de la accesibilidad porque en este caso tienes acceso a tus datos, más no los puedes usar.



# Conceptos clave

Non repudation:

Permite que en un servicio de seguridad, se mantiene evidencia a modo que el locutor y transmisor de ciertos datos no puedan negar haber participado en la comunicación.

Esta puede orientarse a los varios aspectos de la comunicación.



PROTECO



# Zero trust-model

No confíes, evalúa. (Incluyéndote a ti mismo)

Menos confianza implica mayor seguridad.

Nunca confíes, siempre comprueba.

Todo tiene cierto nivel de riesgo  
(Debemos calcular si es asumible).

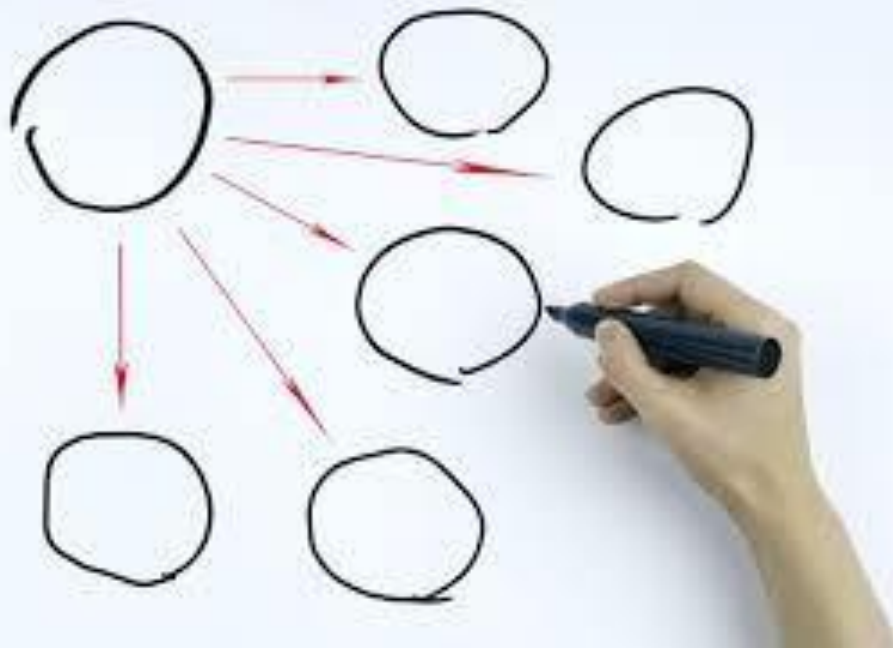


# Zero trust-model

Bueno, ¿y que debo hacer? Distribuye la confianza.

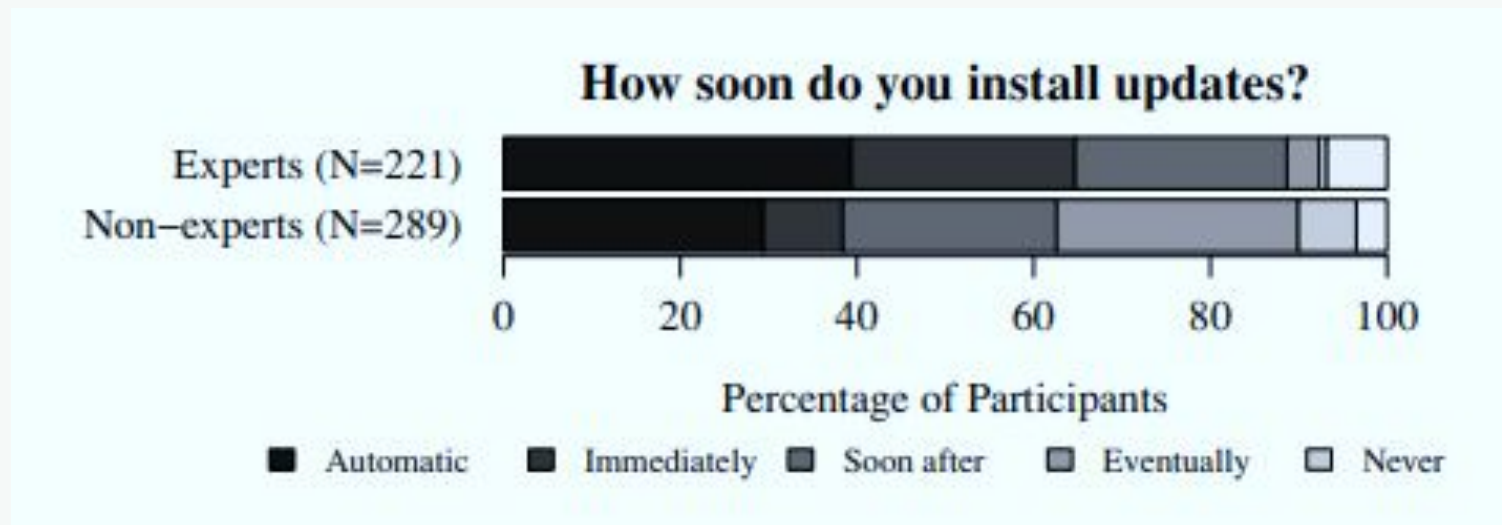
Ej:

Subir archivos a la nube, pero cifrados. De este modo estas distribuyendo tu confianza en la entidad que crea el cifrado v el servidor de almacenamiento.



# Expertos vs Usuarios comunes.

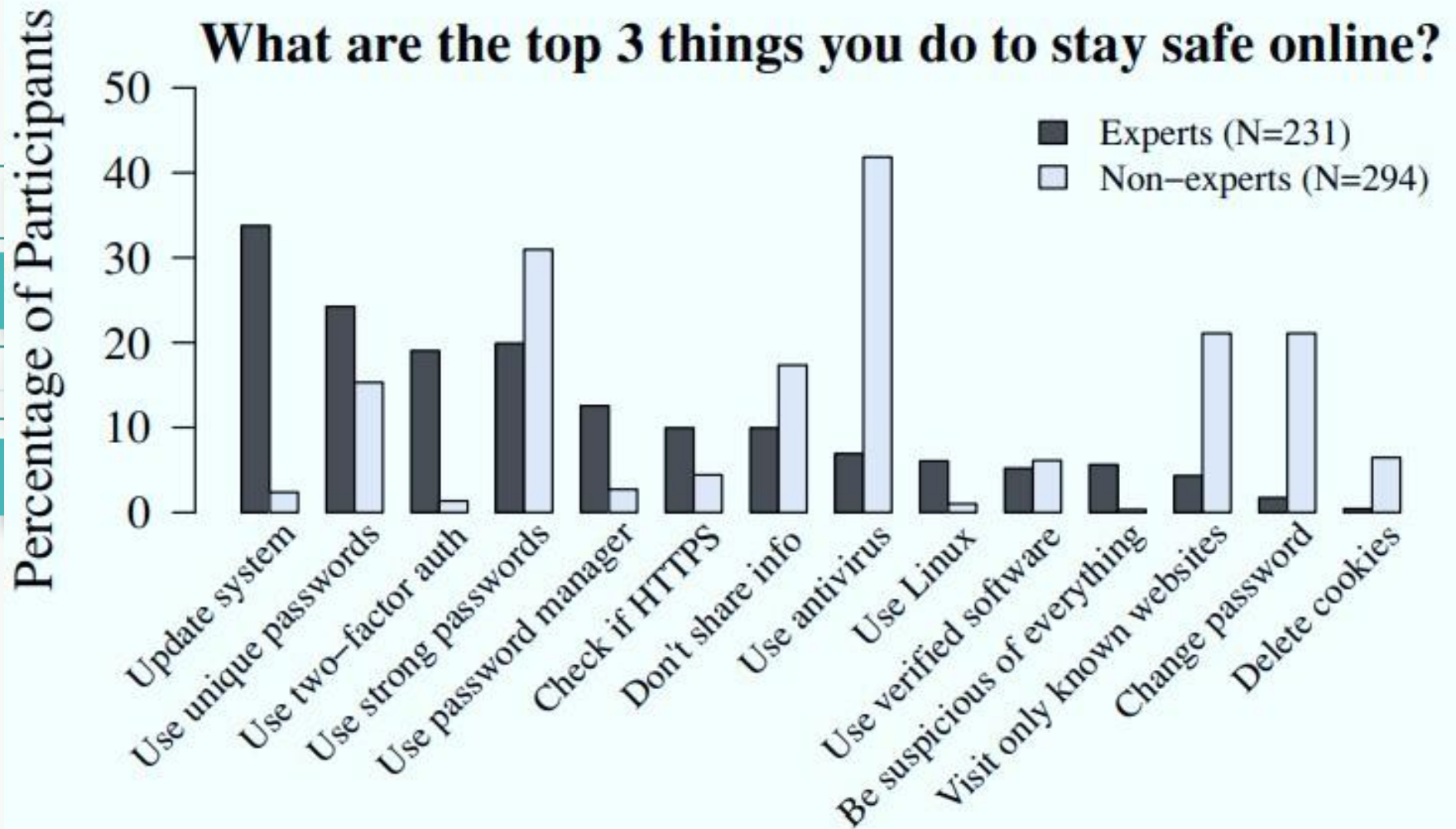
“No one can hack my mind” Estudio hecho por Google en 2015



Ejercicio mental.

¿Cuales son las principales 3 cosas que haces para estar seguro online?

# Expertos vs Usuarios comunes.





# Consideraciones

Al final del día, como usuario final tus tareas se limitan a:

- \*) Distribuir la confianza.

- \*) Actualizar a la brevedad (mejor de forma automática)

Hardening: Endurecer reduciendo las vulnerabilidades y el attack Surface.



Hacker:

- Persona que se deleita en tener un conocimiento íntimo de la tecnología.(IETF)  
Sus acciones van ligada al conocimiento.  
“Hago lo que hago solo para aprender como funciona el sistema telefónico” (Captain Crunch)



# Cracker

- Cracker:

Individuo cuyos intereses van hacia acceder a un sistema sin autorización. Comúnmente maliciosos. Suelen ser opuestos a hackers(IETF)

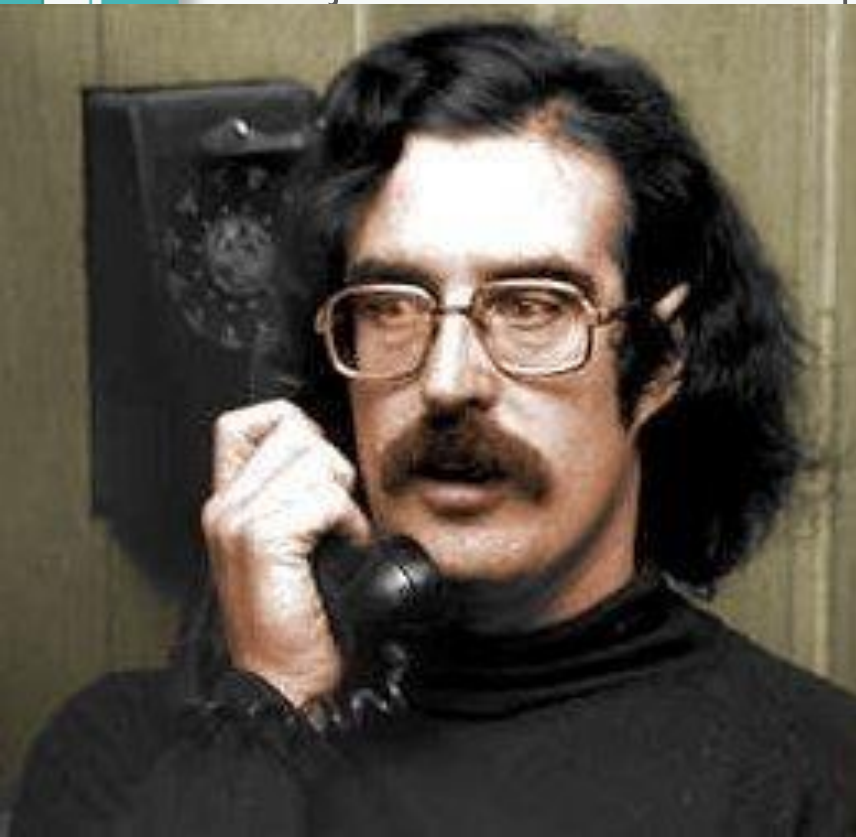
Suelen actuar por intereses económicos.



# Phreaker

- Phone freak: Alguien con altos conocimientos de tecnología telefónica. Tiene raíces en la modificación de frecuencias (frequency)

Ej: John Thomas Draper.



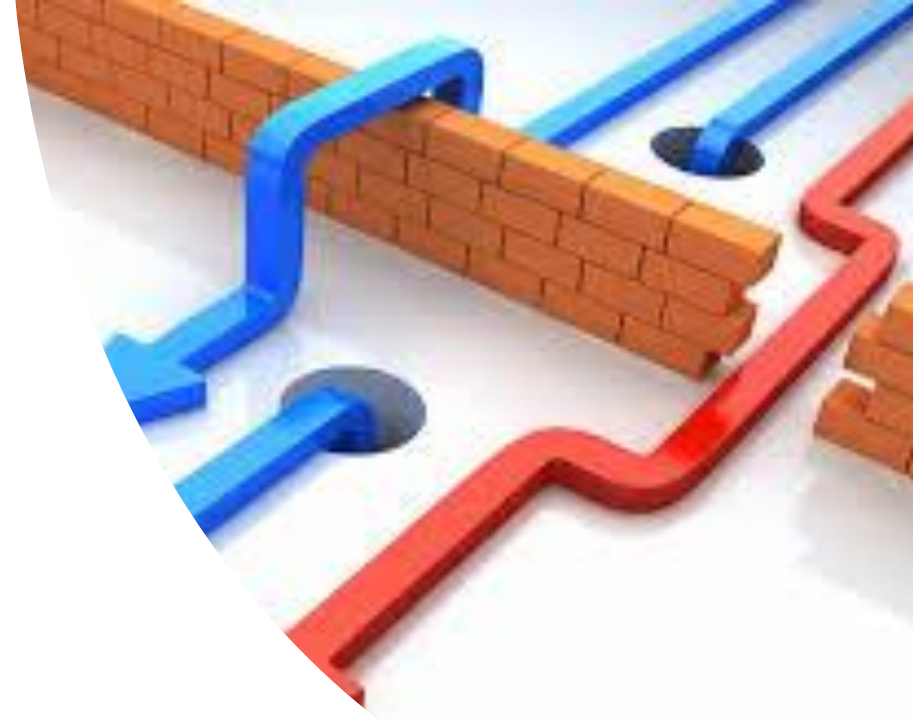
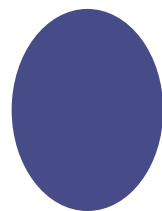
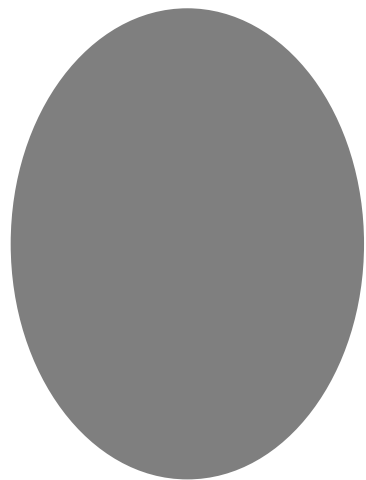


# Hacktivista

Persona cuyas acciones se ven dictadas por una causa y no necesariamente por motivos económicos. Su moral se ve determinada por su causa, y no necesariamente son cybercriminales.

Ej: Aaron Swartz (Lucho contra Sopa)



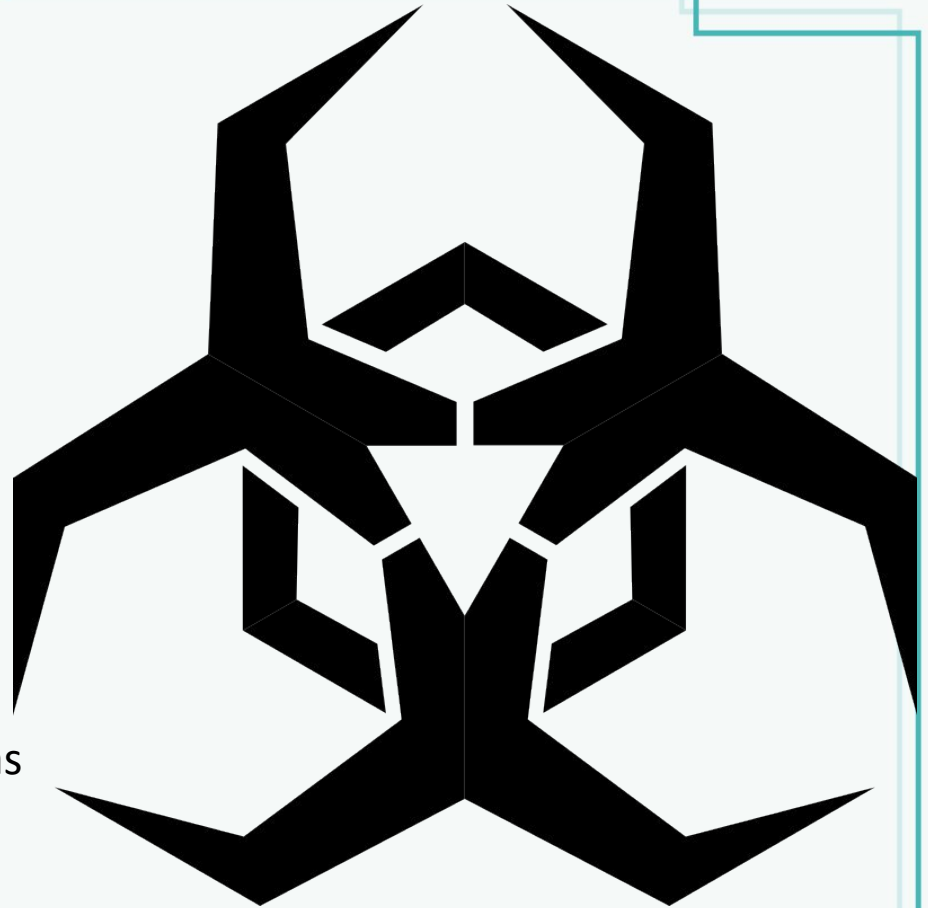


# Introducción a la Seguridad Informática

Vulnerabilidades

# Introducción a la Seguridad Informática

- Amenazas:
  - Naturales:
    - Incendio
    - Terremoto
    - Huracanes
  - Humanas:
    - Malicioso
    - No malicioso
  - Lógicas:
    - Puertas traseras
    - SW incorrecto
    - Malware



# Introducción a la Seguridad Informática

Malicious Software (Malware):

Diseñado para causar daño a un equipo o red.  
Actúa en contra de los deseos del usuario de la computadora.



# Introducción a la Seguridad Informática

Virus:

Adherido a un ejecutable, puede producir copias de si mismo e insertarse en otros programas. No se activará por si mismo.

Ej:

Antichrist

Stinky Cheese

Macro virus

Codigo Rojo.





# Introducción a la Seguridad Informática

Worms:

Son autosuficientes, no requieren de ayuda humana o de otro programa para propagarse.

Ej:

Stuxnet (Destrucción de centrifugadoras para enriquecer uranio en Irán).

Code shikara



# Introducción a la Seguridad Informática

Rootkits:

Modifica el sistema operativo para que el malware este oculto del usuario. Evitan la identificación e intentos de ser removidos.

Ej:

SuckIT

Adore

Hacker Defeder



# Introducción a la Seguridad Informática

Ransomware:

Amenaza al usuario con publicar su información o bloquear el acceso a esta a menos que se pague un rescate.

Ej:

Jisut

Slocker

WannaCry



PROTECO



# Introducción a la Seguridad Informática

Troyanos o caballos de troya:

SW que parece legítimo, suelen crear puertas traseras o utilizar rootkits. No se suelen replicar a si mismos, sino mediante interacción de usuarios.

Ej:  
Beast  
Darkgoose



# Introducción a la Seguridad Informática

Spyware:

Software malicioso que se ejecuta en secreto en una computadora e informa a un usuario remoto.

Apunta la información confidencial y puede otorgar acceso remoto a los depredadores.



PROTECO



# Introducción a la Seguridad Informática

Keyloggers:

Software o hardware que permite la acción de grabar (registrar / logging) las teclas presionadas en un teclado.



Los datos pueden ser recuperados por la persona que opera el programa de registro.

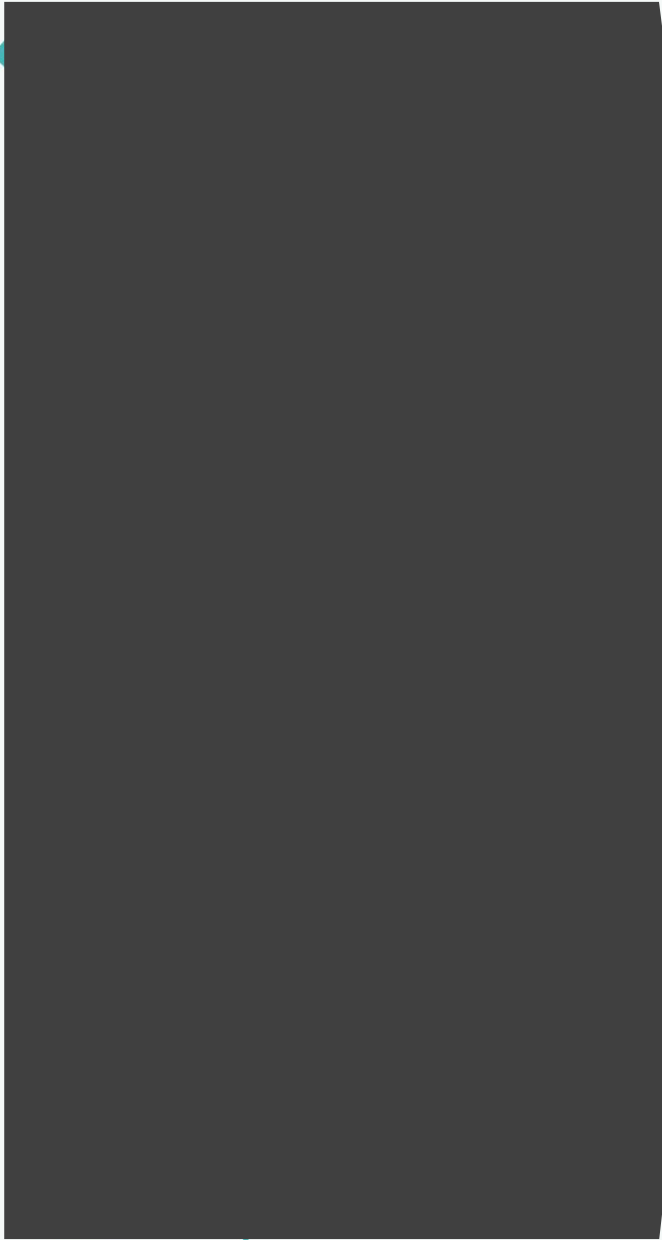
# Introducción a la Seguridad Informática

## DDOS:

Un ataque de denegación de servicio distribuido, es el bombardeo de solicitudes de datos simultáneas a un servidor central. El atacante genera estas solicitudes desde múltiples sistemas comprometidos.

Al hacerlo, el atacante espera agotar el ancho de banda de Internet o la RAM del objetivo. El objetivo final es bloquear el sistema del objetivo e interrumpir su negocio.





Los ataques Man-in-the-middle (MitM) ocurren cuando los atacantes se insertan en una transacción de dos partes. Una vez que los atacantes interrumpen el tráfico, pueden filtrar y robar datos.

Dos puntos de entrada comunes para los ataques MitM:

1. En una conexión Wi-Fi pública no segura, los atacantes pueden insertarse entre el dispositivo de un visitante y la red. Sin saberlo, el visitante pasa toda la información a través del atacante.
2. Una vez que el malware ha infringido un dispositivo, un atacante puede instalar un software para procesar toda la información de la víctima.

# Zero Days

Vulnerabilidad que es desconocida para el responsable de un software. Hace alusión a que lleva 0 días desde su descubrimiento.



# Ingenieria Social

Arte de obtener información de una persona, mediante técnicas como influir, manipular, personificar, etc.

Más puede existir en un entorno de completo consentimiento.





# Ingenieria Social



Christopher Hadnagy:  
Un ejemplo claro  
serían los gobiernos  
y políticos  
estructurando sus  
palabras para crear  
el mayor impacto en  
sus discursos, que  
podría ser algo tan  
bueno como malo.



## Social Engineering

### TYPES OF ATTACKS

PHISHING



SPEAR PHISHING



VISHING



SMISHING



MINING SOCIAL MEDIA



LEARN MORE



[www.vasco.com/crontosign](http://www.vasco.com/crontosign)

# Ingenieria Social

## Phising:

- Práctica de enviar comunicaciones fraudulentas que parecen provenir de una fuente confiable. Suele hacerse por correo electrónico.
- El objetivo es robar datos confidenciales como tarjetas de crédito e información de inicio de sesión, o instalar malware en la máquina de la víctima.

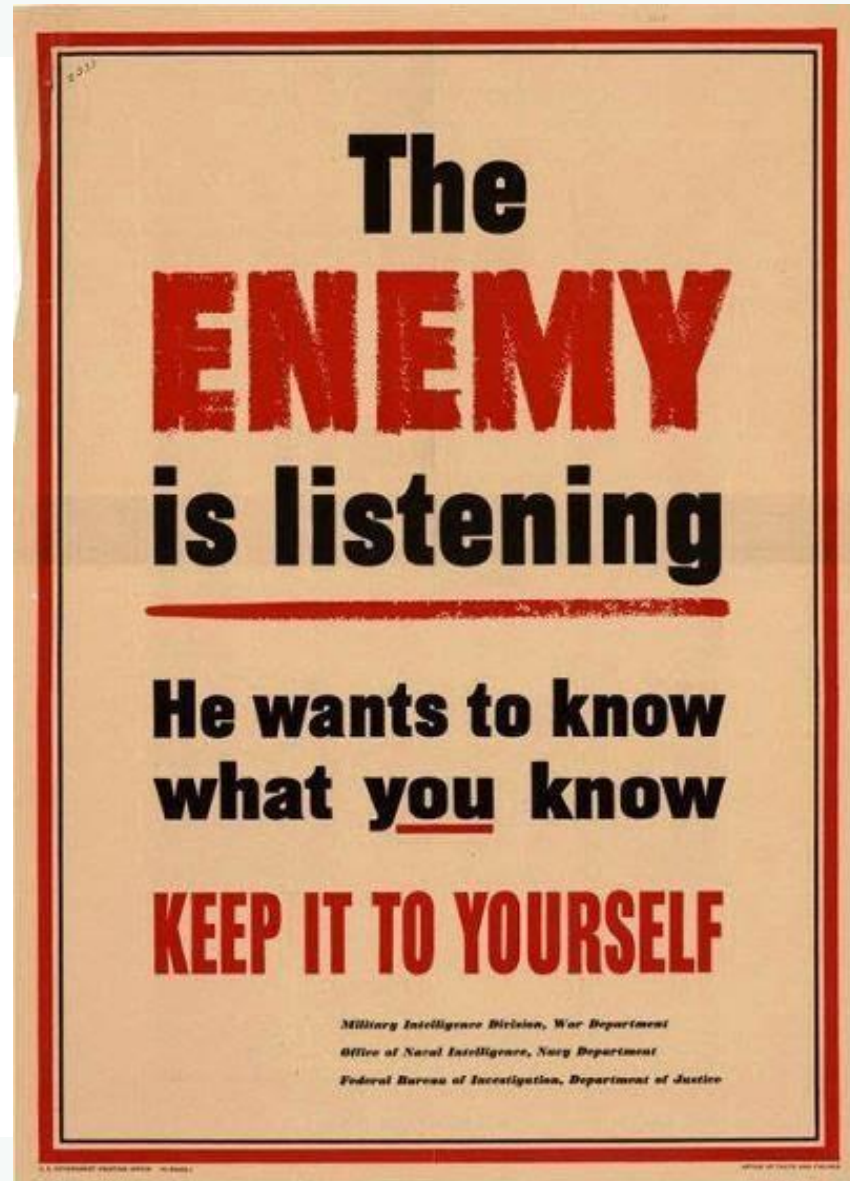


## Tipos de ataques Phishing:

- Spear phishing: Se dirige a individuos específicos en lugar de a un amplio grupo de personas.
- Whaling: Cuando los atacantes van tras un "pez gordo" como un CEO, se llama caza de ballenas.



OPSEC  
(Operations  
Security)





# OPSEC (Operations Security)

- La seguridad de las operaciones (OPSEC) es un proceso que identifica información crítica para determinar si las acciones amistosas pueden ser observadas por sistemas adversarios de inteligencia.
- Determina si la información obtenida por adversarios podría interpretarse como útil para ellos.



# OPSEC (Operations Security)

## 10 Rules of Opsec-

1. Keep your mouth shut (doesn't tell yours plan )
2. Trust No one (hack alone)
3. Never Contaminate identities
4. Be uninteresting



# OPSEC (Operations Security)

5. Be Paranoid now
6. Know your limitations
7. Minimize Information(no log - specially browsing history)
8. Be Professional
9. Employ Anti-Profiling
10. Protect Your assets(Do Encryption)

## THERE ARE TWO RULES IN OPSEC

1. NEVER GIVE OUT ALL THE INFORMATION

2. [REDACTED]

## OPSEC in a nutshell

- Keep your mouth shut
- Guard secrets
  - Need to know
- Never let anyone get into position to blackmail you