

ISO 27000, conjunto de mejores prácticas, para desarrollar, implementar, y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)

↳ descansa en políticas de seguridad

ISO 27032 Gestión de la Ciberseguridad (4 elementos)

- 1.- Seguridad en las Redes
- 2.- Seguridad en Internet
- 3.- Seguridad de la Información
- 4.- Seguridad de las aplicaciones

ISO 37001 Lucha contra el Soborno en las organizaciones: Una oferta

(según el punto 3.1) { promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor}

Dinamarca el más limpio, México 26 de Corrupción en 2023 era 126.  
2024  
31

Eugene Kaspersky → Presencia importante gracias a sus laboratorios, presencia en 195 países. Lucha contra el cibercrimen

La proliferación de dispositivos móviles unido al home office

- información a todas partes
- Se facilitan el trabajo y actividades diarias
- Añade una nueva fisura en la Seguridad informática

Higiene cibernética: Acciones que las personas usuarias de todo tipo de dispositivos TI realizan para mejorar su Seguridad en línea y mantener un sistema saludable

Externas pretende destruir → Amenaza toda clase de malware

Internas vulnerabilidades debilidad

# Peligro todo aquél que puede ocasionar un daño

# Riesgo probabilidad de realización (amenaza + vulnerabilidad)

5 Acción que se realiza en contra alguien o algo para destruir o hacer daño.

V	U	L	N	E	L	I	G	R	O	R	A	P	A	T	A	Q	U	E	B	I	C	S	L	T	G	I	O	D	A	M	E	N	A	Z	A	D													
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40										
horizontalmente	abajo																																																
Acción que se realiza en contra alguien o algo para destruir o hacer daño.	Todo aquello que puede ocasionar daño:	Defecto o falla de seguridad en los sistemas, y que pueden aprovechar los maleantes para sus fines ilícitos:	Consecuencia o efecto producido por un ataque:	Posibilidad de que se produzca un contratiempo y con ello alguien o algo sufra perjuicio o daño:																																													
5	2	1	3	4	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50

## Fuentes de amenaza

- Factor humano
- Hardware
- Red
- Tipo lógico
- Desastres Naturales

Riesgo → Situación en que puede darse la posibilidad de que se produzca un contratiempo o una desgracia, y de que alguien o algo sufra perjuicio o daño

La suma de : amenaza + vulnerabilidad → Aumenta o disminuye el riesgo para que se dé un ataque.

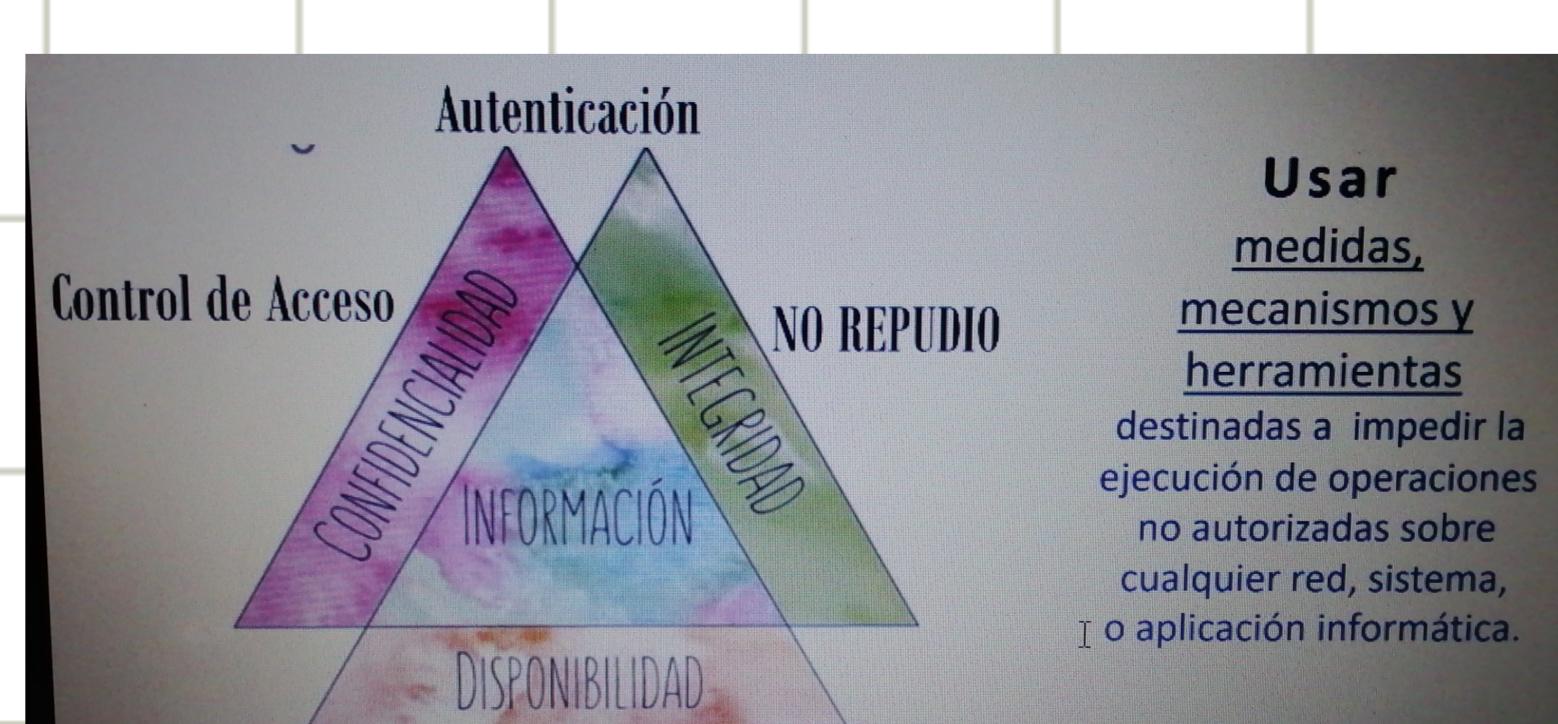
**Retos de Ciberseguridad :** Prevención → Tener buenas prácticas de Seguridad  
Mecanismos y herramientas de seguridad  
Administración de la información

Operación → Responsabilidad de todos, el conjunto de actividades establecidas para dar cumplimiento a las medidas preventivas por usuarios, creadores

Recuperación → Plan de Emergencia cuando falla la prevención y operación

Programas de Sensibilización

El mayor Reto es evitar cualquier acción, intencional o no que comprometa la información



## Tema 2.2 Perfil del ciberatacante

Personas cometan delitos  
computadora no

↳ Grandes conocimientos en la tecnología y lo ocupan para hacer delitos en el mundo virtual

Sin conocer al adversario, motivaciones y capacidades, es difícil desarrollar una estrategia de ciberseguridad porque te estarías enfrentando a un enemigo invisible.

- Comodidad  
+ Seguridad

¿Qué se quiere proteger?

¿De qué se quiere proteger?

¿Cómo se va a proteger?

Objetivo es obtener una visión completa del valor de los activos y las consecuencias de que se vea comprometida su triada de seguridad, y con ello identificar amenazas, riesgos y vulnerabilidades para evitar ataques.

¿Quiénes son cibercriminales? R: Emplados deshonestos, personas que "buscan oportunidades", proveedores (intercambio de info)

R: Aquellas personas que realizan actividades delictivas/filícitas en Internet

Dr. Lee Hadlington → Estudia como actúa un cibercrimenante



Artículo publicado en 2020

FOMO = Fear of Missing Out

Los que tienen FOMO a alta esa porque tienen una baja conciencia de la seguridad de la información

↳ Miedo a perderse algo, sensación de ansiedad

- Reducir tiempo de uso de redes sociales

- Reflexionar sobre su uso

- Vivir en el presente

- Establecer prioridades

- Cuidar autorestima

# Perfil de Cibertacante

- 1.- Niveles altos de impulsividad
- 2.- Persona antisocial
- 3.- Pasa por alto las normas
- 4.- Falta de empatía
- 5.- Tener deseo de poder y control
- 6.- Observador y metódico

¿Hacker = cibertacante? → Depende para que lo usa, yo soy hacker :O, por lo que se de tecnología muchos temas con los que podrían entrar a sistemas)

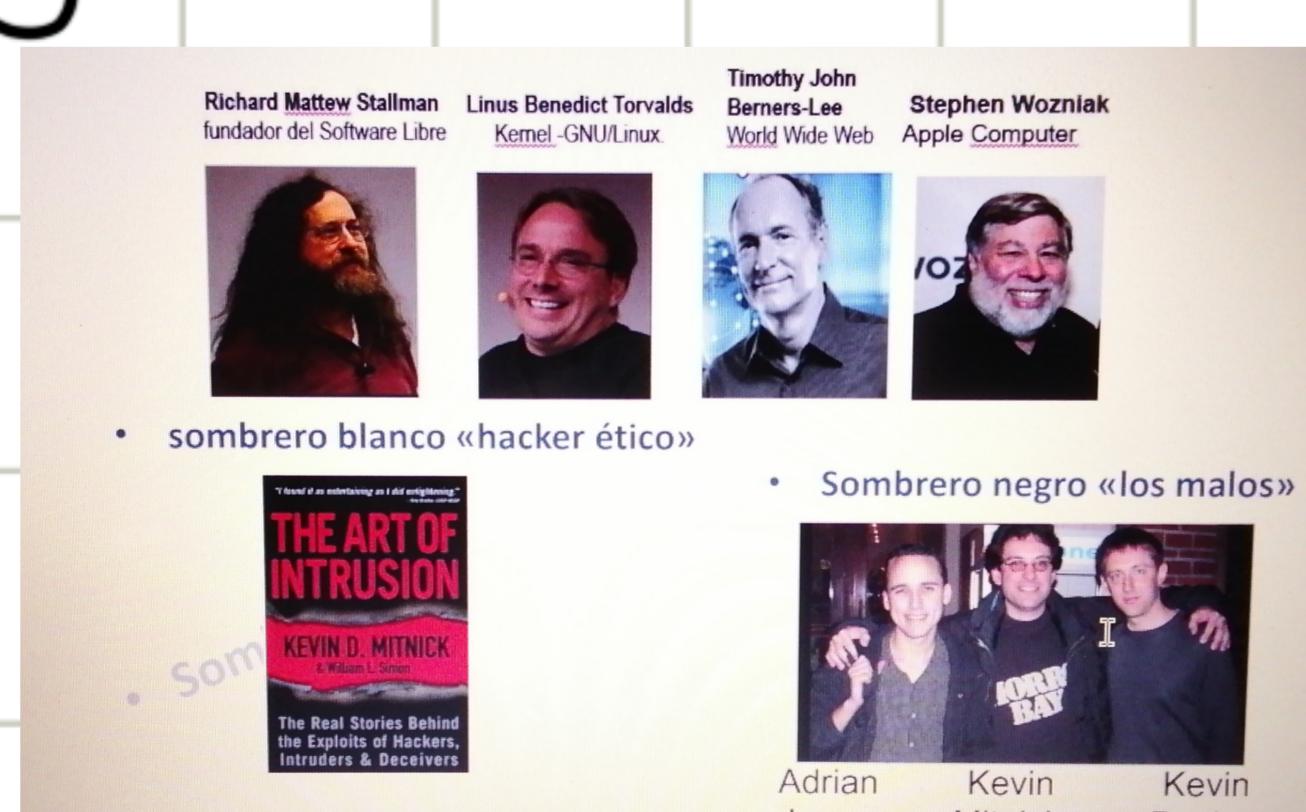
↓  
Perfil

- Curiosidad como fuente de conocimiento, apasionados por la búsqueda
- Pasión y adicción → Modo hack: Disfrutar el momento de estar frente a una computadora y sentirse cómodos y libres
- Motivación: Cada hacker, bueno o malo, tiene un motivo para hacer lo que hace

Tipos de Hacker: Personas con grandes conocimientos de informática

- Uno puede utilizarlos para acceder a los activos y obtener un beneficio en su reputación o económico
- Dos tiene ética ambigua y se mueve entre bien o mal
- Tres evalúa sistemas de seguridad y aplicaciones buscando vulnerabilidades o problemas de seguridad para solventarlos

Personas expertas en programación, que dedican su tiempo a desarrollar software y difundir información que pueda ser utilizada por otras personas.



- Ingeniería Social: Técnicas psicológicas para engañar a las personas, para que entreguen datos

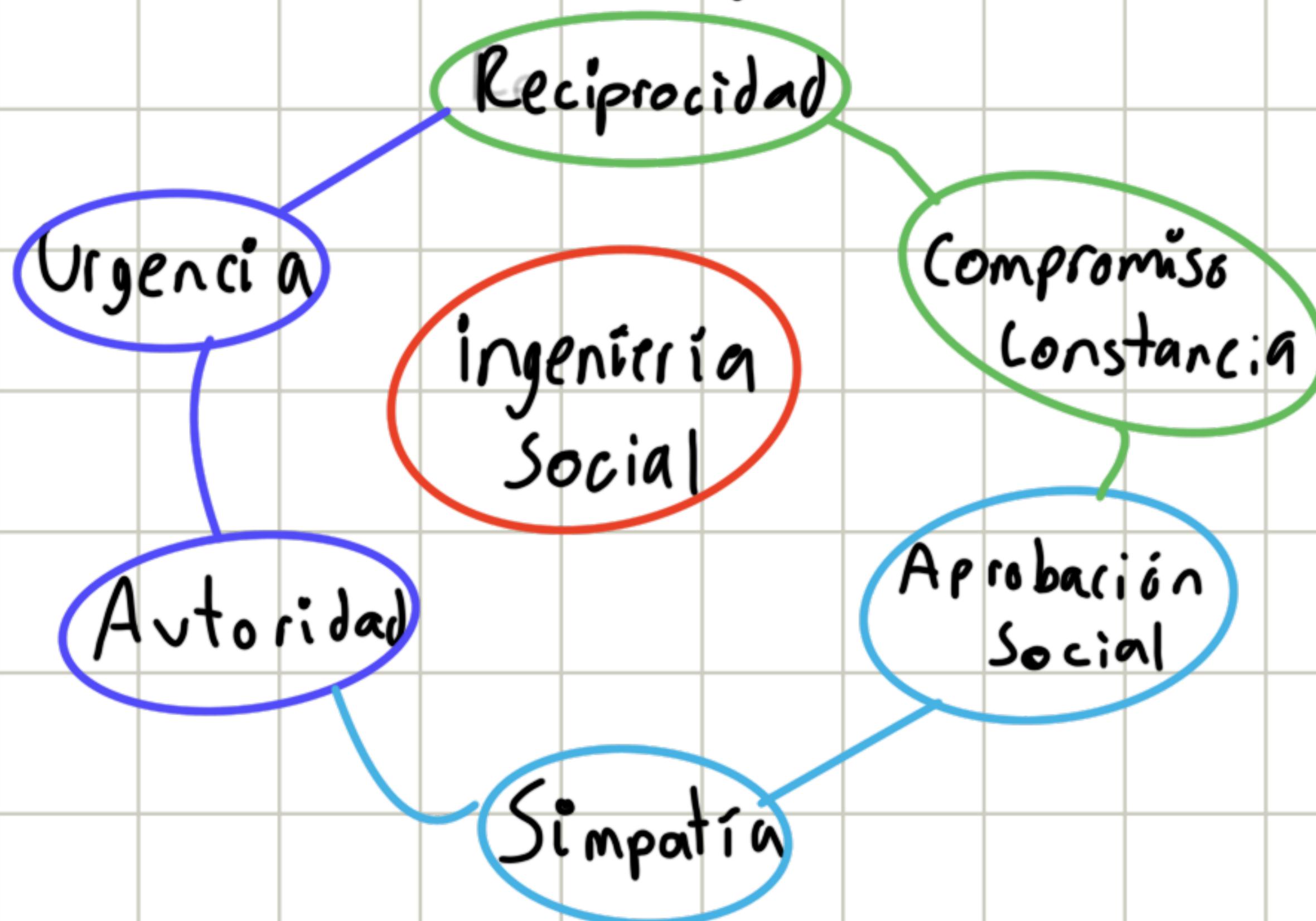
confidenciales

- Brad Sagarin → Técnicas que las personas utilizan para manipular

El eslabón más débil → El usuario (Falta de conocimiento y conocimiento, errores humanos, sobre confianza en la tecnología, comportamiento predictivo y ser susceptibles a la ingeniería social)

Casos Reales de estafa → Sofía nino Rivera

## 6 principios de la Ingeniería Social



- Similares a las estrategias de venta
- Se utilizan para ganar la confianza de una persona y después engañarla

Técnicas de la Ingeniería Social : Baiting, Scareware

Baiting, Scareware, email, sms, smishing, voz, vishing