OPEN SHARE TECH

Ingeniería Social Digital

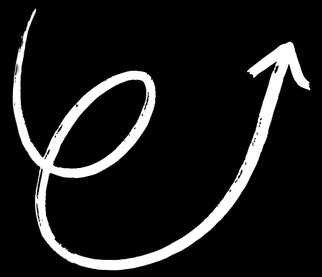
OPEN SHARE TECH

Qué es la ingeniería Social Digital

La ingeniería social digital es la acción del engaño o la manipulación para hacer que las personas den información, hagan clic en enlaces o descarguen cosas peligrosas.


¿Qué es el grooming?
Copy link
¿QUÉ ES
GROOMING?
Watch on YouTube

¿Qué es la ingeniería social?



01

Manipulación psicológica

La ingeniería social es una **técnica de manipulación** psicológica que busca obtener información a través de métodos engañosos y persuasivos.

02

Ejemplo común

Un desconocido crea una cuenta falsa haciéndose pasar por un adolescente amable. Empieza a ganarse la confianza del niño con mensajes o cumplidos. Luego, le pide que comparta información personal para seguir siendo amigos.

Técnicas comunes de ingeniería social

Phishing

Sitios o aplicaciones falsas que engañan para obtener datos.

Phishing


Apps
falsas


login.gmail.com.msg11.info/accounts2/ServiceLogin2.php?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fma
Google
URL FALSA
¿Es la primera vez que utilizas Gmail?
Gmail
La visión del correo electrónico de Google.
Gmail está basado en la idea de hacer que el correo electrónico resulte más intuitivo, eficiente y útil, e incluso divertido. Después de todo, Gmail tiene:
Mucho espacio
Más de 2757.272164 megabytes (y sigue en aumento) de almacenamiento gratuito.
Menos spam
Evita que los mensajes no deseados lleguen a la bandeja de entrada.
Acceso para móviles
Para leer mensajes de Gmail desde tu teléfono móvil, introduce http://gmail.com en el navegador web de tu móvil. Más información
Acceso
Nombre de usuario
@gmail.com
Contraseña
Acceso
¿No puedes acceder a tu cuenta?
Salir y acceder como otro usuario

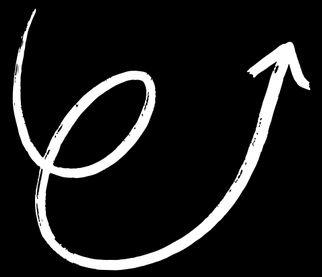
Técnicas comunes de ingeniería social

Pretexting

Historias inventadas se utilizan para conseguir información.

Pretexting
o
ataque de pretexto

Recopilan información relevante para la historia



Ejemplos

Soy amigo de tu papá, necesito su número.

Te ganaste una beca o celular

Soy tu maestro nuevo

Estafas a los abuelos

Suplantación de identidad

Definición

La suplantación de identidad es hacerse pasar por otra persona para obtener información.

Ejemplo

Un atacante puede llamar a alguien haciéndose pasar por alguien más.

Consecuencias

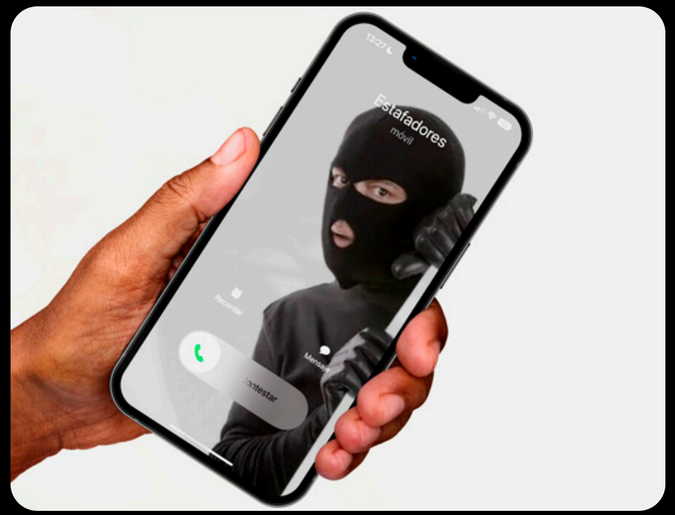
La suplantación de identidad puede llevar al robo de datos y a pérdidas financieras significativas.

Ataques digitales

Redes sociales

Los ataques en redes sociales son comunes y pueden comprometer información valiosa fácilmente.

Llamadas fraudulentas



Las llamadas fraudulentas engañan a las víctimas para obtener datos personales mediante manipulaciones.

Phishing

El phishing utiliza correos electrónicos falsos para robar información personal de manera efectiva. Compra de juegos falsos o cambio de contraseñas.

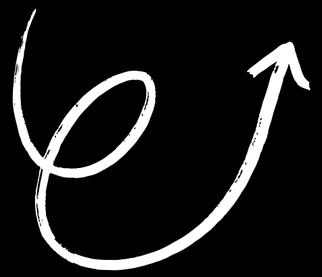
Técnicas comunes de ingeniería social

Baiting

Se ofrece algo atractivo para que la persona caiga en una trampa.

Baiting

Atraer con una recompensa falsa para robar información o controlar el dispositivo.



Descarga este programa para tener diamantes infinitos en Free Fire.

Haz clic aquí para ver quién visita tu perfil

Te regalamos stickers nuevos si bajas esta app

Técnicas comunes de ingeniería social

Grooming

Adultos que se hacen pasar por niños para ganarse la confianza.


Campaña sobre Grooming junto a Movistar
Copy link
Watch on YouTube

Riesgos y consecuencias de ataques de ingeniería social

Robo de cuentas o identidad

Exposición de fotos o información personal.

OPEN SHARE TECH

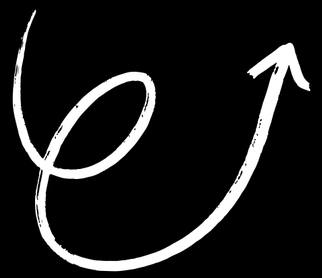
Riesgos y consecuencias de ataques de ingeniería social

Ciberacoso o chantaje

Pérdida de confianza o daño emocional.

OPEN SHARE TECH

Cómo protegerse y prevenir de la ingenieria social.



OPEN SHARE TECH

Conciencia

Fomentar **dudas sanas** sobre la información recibida.

Verificación

Confirmar la **identidad antes de compartir** información.

- No compartir contraseñas ni fotos privadas.
- Verificar quién te escribe o agrega en redes sociales.
- Desconfiar de enlaces sospechosos.

Apoyo

Contar a un adulto de confianza si algo incomoda.

Como docentes, somos los primeros modelos de comportamiento digital. Enseñamos no solo con palabras, sino con lo que compartimos

OPEN SHARE TECH

¿Qué tipo de ejemplo digital doy a los niños o adolescentes?

¿Qué publicaciones o comportamientos podrían imitar mis estudiantes?

¿He hablado con ellos sobre riesgos digitales o privacidad?

Leyes y normas relacionadas con seguridad y ciberseguridad en Guatemala:

OPEN SHARE TECH

1. **Decreto 39-2022: Ley de Prevención y Protección contra la Ciberdelincuencia**
2. **Iniciativa 6347: Ley de Ciberseguridad**
3. **Ley Marco del Sistema Nacional de Seguridad**
4. **Decreto 47-2008: Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas**
5. **Decreto 57-2008: Ley de Acceso a la Información Pública**
6. **Código Penal de Guatemala (Delitos informáticos y tecnológicos)**
7. **Ley para la Protección de Datos Personales y la Ley de Ciberseguridad y Seguridad de la Información**

Decreto 39-2022: Ley de Prevención y Protección contra la Ciberdelincuencia

- **Es la primera ley guatemalteca que regula directamente los delitos informáticos y las conductas en el entorno digital.**
- **Busca proteger la información, sistemas y datos frente a accesos no autorizados, fraudes digitales y ataques cibernéticos.**
- **Introduce tipos penales específicos como:**
  - **Acceso ilícito a sistemas informáticos.**
  - **Daño o destrucción de datos.**
  - **Suplantación de identidad digital.**
  - **Fraude informático.**
  - **Difusión no autorizada de información privada.**

Iniciativa 6347: Ley de Ciberseguridad

- **Busca crear un marco nacional de ciberseguridad, no solo penalizar delitos, sino prevenirlos y fortalecer la resiliencia digital del país.**
- **Propone la creación de:**
  - **CSIRT-GT (Equipo de Respuesta ante Incidentes Informáticos).**
  - **Fiscalía especializada en Ciberdelitos.**
  - **Centro Nacional de Ciberseguridad.**

Fomentar la educación y la cultura de ciberseguridad en escuelas y comunidades.

OPEN SHARE TECH

¡Gracias!