Escuela Tecnológica
Instituto Técnico Central
Establecimiento Público de Educación Superior

Sistema de Gestión de Seguridad de la Información

Protección Estratégica ante Posibles Ataques Cibernéticos

Ing. Angela A. Pulido – Líder del SGSI

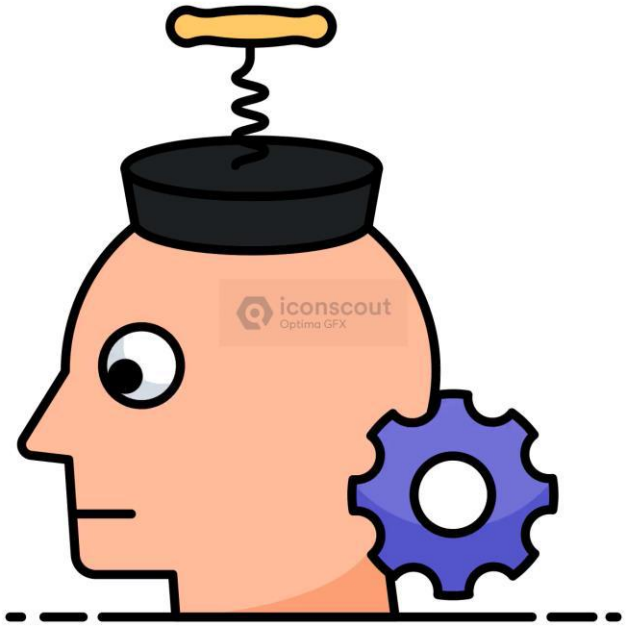
Ing. Angelica Rojas – Contratista de Ciberseguridad

Junio de 2025

Reacreditación
Programas Académicos
ETITC

Introducción a la seguridad Informática

- Fundamentos de la ciberseguridad
- Importancia en un mundo interconectado
- Desafíos que enfrentamos en la era digital



Temas:

- ✓ Ingeniería social
- ✓ Phishing
- ✓ Ataque mediante redes sociales
- ✓ Fuerza bruta
- ✓ Smishing
- ✓ Malware
- ✓ Gusanos
- ✓ Troyano

INGENIERÍA SOCIAL

Técnica de manipulación psicológica utilizada para engañar a las personas y hacer que revelen información confidencial.

PHISHING

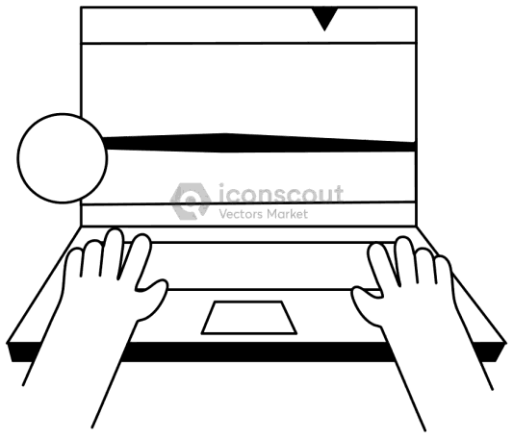
Un ataque sencillo, efectivo y muy peligroso

¿Por que el nombre
"Phishing" (Pesca)?
Proponiendo la forma en que los atacantes "pescan" información confidencial de los usuarios.

¿Que es?
En un método de ataque cibernético en el que los delincuentes intentan engañar a los usuarios para que revelen información confidencial, como contraseñas o datos bancarios. Por lo general, esto se hace a través de correos electrónicos aparentemente legítimos que solicitan a los destinatarios que ingresen sus datos en sitios web falsos. Estos sitios falsos suelen imitar a las páginas reales de instituciones financieras o servicios en línea

Como lo hacen?

Los ciberdelincuentes suelen enviar mensajes **falsos** que contienen enlaces a sitios web **fraudulentos**. A menudo se hacen pasar por empresas reconocidas, amigos o contactos de confianza para engañar a la víctima.

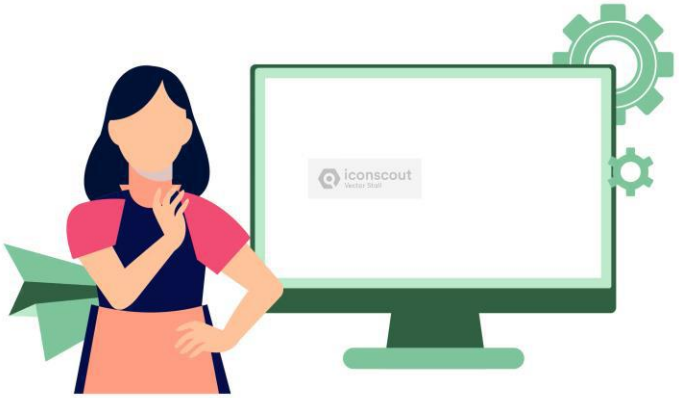


ATAQUES MEDIANTE REDES SOCIALES:

Los principales ataques son:

- **Link falso:** Se envía un link que al hacer clic dirige a la victima a un sitio diseñado para actividades ilegales, como la descarga de un malware o robo de la información personal o credenciales.

Ataques mediante redes sociales:



- **Fake news** (noticias falsas).

Es información o historias que son fabricadas y difundidas con la intención de engañar, desinformar o manipular a las personas por su contenido falso.

Ataques mediante redes sociales:

- **Complementos falsos o extensiones maliciosas**: Son programas adicionales que se instalan en navegadores web con la apariencia de proporcionar alguna funcionalidad útil, pero son usados para recopilar datos personales, descargar malware, redirigir a sitios web maliciosos o realizar acciones perjudiciales para la experiencia de navegación y seguridad del usuario.

Fuerza bruta :

- Es un método de ataque que consiste en probar todas las combinaciones posibles para descifrar contraseñas. Usan direcciones de correo o de usuario que han sido registradas en paginas maliciosas.

Smishing:

- Ataque mediante mensajes de texto fraudulentos con el objetivo de engañar a las personas y obtener información confidencial como contraseñas, números de cuenta bancaria o robar dinero.
- Los delincuentes suelen hacerse pasar por instituciones financieras o empresas legitimas para conseguir que las personas revelen su información personal

Malware

- Un malware es un tipo de software malicioso creado para infiltrarse, dañar o robar información de un sistema informático sin el consentimiento del usuario.

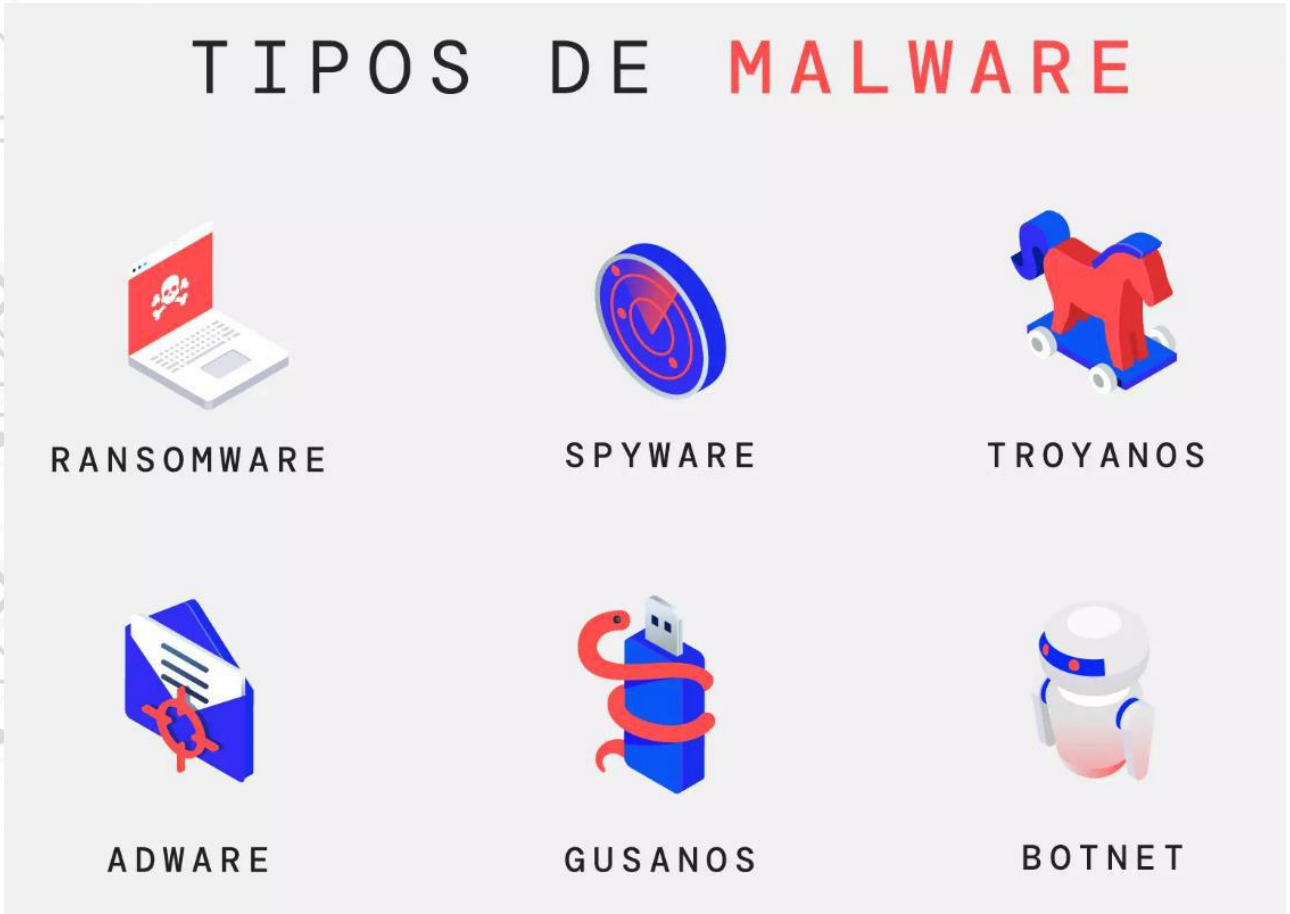


Imagen tomada de: https://www.deltaprotect.com/blog/tipos-de-malware

Ramsomwere

Gusanos :

- Son programas maliciosos que se propagan rápidamente a través de una red sin necesidad de ser descargados. Una vez infectan un sistema, pueden causar daños y se replican para propagare a otros dispositivos

Troyano :

- Malware que se disfraza como programa legitimo para engañar a los usuarios. Una vez se ejecuta en el sistema, puede causar daños y robar información confidencial a la victima

Conclusiones :

La seguridad cibernética es un esfuerzo colectivo, por lo que es importante educarse continuamente sobre las mejores practicas de seguridad y estar atento ante posibles amenazas

“No te confíes”

Recomendaciones:

- Estar atentos siempre, para no ser el eslabón mas débil de la cadena.
- Compartir su conocimiento, así se puede evitar que mas personas sen victimas de un ataque cibernético.
- Conviértase en el cyberguardian de su comunidad.
- Si no estas seguro, pregunta.

Escuela Tecnológica
Instituto Técnico Central
Establecimiento Público de Educación Superior

Reacreditación
Programas Académicos
ETITC

Esp. Angela A. Pulido – Líder del SGSI
Ing. Angelica Rojas– Prof. de Ciberseguridad