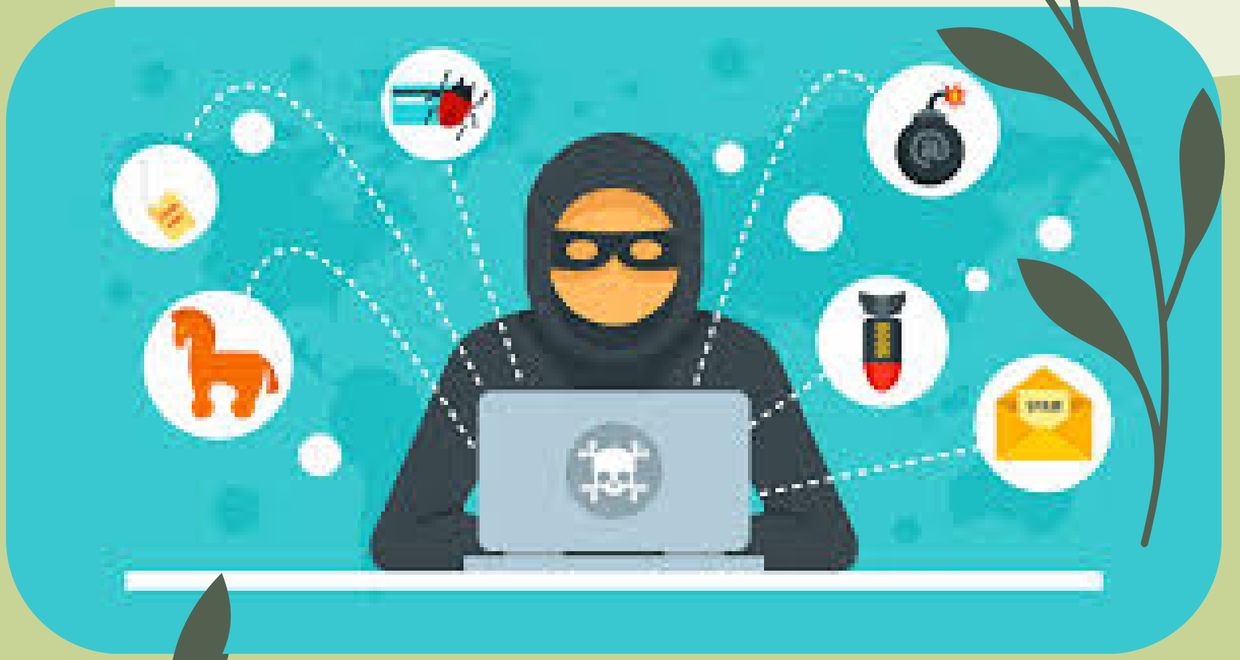
Amenazas informáticas

BORDON JAZMIN
MARTINA CANOSA
3° "A"

¿Que son las amenazas informáticas?

Las amenazas informáticas son riesgos que pueden afectar la seguridad y el funcionamiento de sistemas, redes y datos: van desde programas maliciosos (virus, troyanos, ransomware) y ataques de hackers hasta el robo de contraseñas, la ingeniería social y fallas técnicas o físicas que provocan pérdida o exposición de información. Estas amenazas buscan robar, alterar o bloquear acceso a datos y servicios, y pueden causar desde molestias menores hasta daños económicos y pérdida de confianza. Para reducirlas se usan medidas como copias de seguridad, contraseñas fuertes, actualizaciones y precaución con correos o enlaces sospechosos.

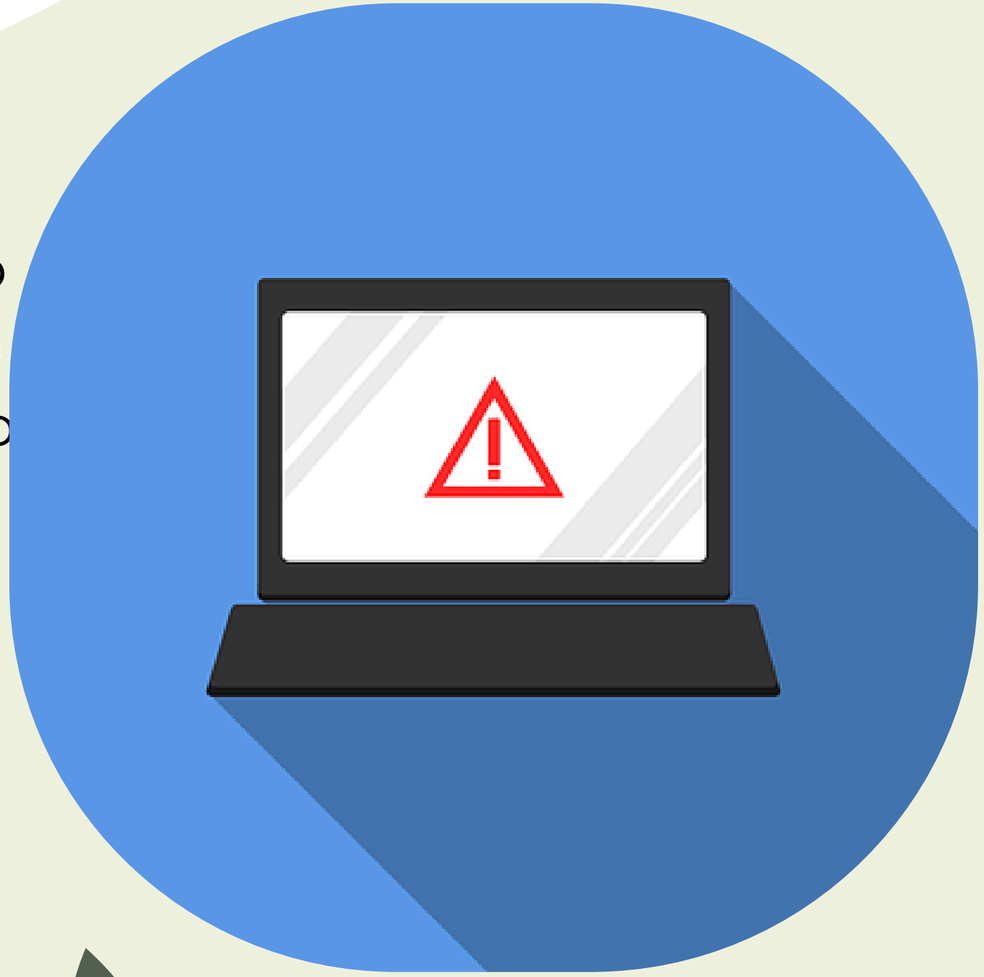


Ataques de contraseña

Un ataque de contraseña es cualquier intento de obtener, robar, adivinar o comprometer de cualquier otra forma las credenciales de inicio de sesión de un usuario. El objetivo es tener acceso no autorizado a sistemas, aplicaciones o datos que deberian estar protegidos con contraseña.

Denegación de servicio

Una denegación de servicio (DoS) es un tipo de ciberataque en el que un actor malicioso tiene como objetivo que un ordenado u otro dispositivo no esté disponible para los usuarios a los que va dirigido, interrumpiendo el funcionamiento normal del mismo.



Algunas características de los ataques de contraseña:

DESIFRAMIENTO DE CONTRASEÑAS

El desciframiento de contraseñas es cuando los cibercriminales utilizan programas y herramientas para obtener acceso no autorizado a las cuentas en línea.

ATAQUE DE FUERZA BRUTA

Un ataque de fuerza bruta es cuando los cibercriminales utilizan el software en un intento de adivinar las credenciales de inicio de sesión a través del método de prueba y error.

DIFUSIÓN DE CONTRASEÑA

El rociado de contraseñas, también llamado ataque de rociado de contraseñas, es cuando los cibercriminales utilizan una lista de contraseñas de uso común para intentar obtener acceso a varias cuentas en un dominio

ATAQUE DE DICCIONARIO

Un ataque de diccionario es un ataque de contraseñas que utiliza palabras y frases comunes del diccionario para comprometer las cuentas.

Algunas características de denegación de servicio:

CONSUMO DE RECURSOS

Un ataque DoS puede agotar recursos como ancho de banda, memoria, espacio en disco o poder de procesamiento, impidiendo que el sistema funcione correctamente.

FALSIFICACIÓN DE DIRECCIÓN IP

Algunos ataques DoS utilizan direcciónes IP falsificadas para ocultar la fuente del ataque y dificultar la dirección y bloqueo.

INTERRUPCIÓN DE LA COMUNICACIÓN

Los ataques pueden interrumpir la comunicación entre los usuarios y el servicio objetivo, impidiendo que puedan acceder o interactuar con el.

ATAQUES DISTRIBUIDOS

Los ataques DDoS, que son una variante de los ataques DoS, utilizan múltiples sistemas comprometidos (botnet) para lanzar el ataque, lo que los hace mas difíciles de mitigar.

¿Cómo prevenirlos?

- Utiliza contraseñas seguras y únicas.
- Implementar un administrador de contraseñas
- Implementar la autenticación multifactor.
- Implementa medidas de seguridad tanto en la red interna como en el hosting o proveedor de servicios.

Fuentes:

Trabajo práctico: amenazas informáticas

https://www.keepersecurity.com/blog/es/2024/01/12/types-of-password-attacks/

Muchas gracias