Ciberseguridad

16 ATAQUES CIBERNÉTICOS Y COMO PREVENIRLO

@saulruizplaza

Ciberseguridad

PISHING



Suplantan identidades para robar información sensible, como credenciales y datos bancarios, mediante correos electrónicos y sitios web falsos.

¿Cómo prevenirlo?

- Activar autenticación en **dos factores** (2FA).
- **Verificar** siempre el remitente y URL de los correos.

@saulruizplaza

Ciberseguridad

RANSOMWARE

Malware que cifra archivos y exige un rescate para desbloquearlos.

¿Cómo prevenirlo?

- **Backup** frecuente de datos.
- Antivirus **actualizado** y parches de seguridad al día.



@saulruizplaza

Ciberseguridad

MAN-IN-THE-MIDDLE (MITM)

El atacante intercepta y manipula las comunicaciones entre dos partes sin su conocimiento.

¿Cómo prevenirlo?

- Usar **HTTPS** y cifrado en las comunicaciones.
- **Evitar** redes Wi-Fi **públicas** y no seguras.



@saulruizplaza

Ciberseguridad

DDoS



Un ataque que utiliza múltiples sistemas comprometidos para inundar un servidor y hacerlo inaccesible.

¿Cómo prevenirlo?

- Implementar **protección** DDoS.
- Utilizar **firewalls** y técnicas de mitigación de tráfico.

@saulruizplaza

Ciberseguridad

SQL Injection



Ataque donde el atacante inyecta código SQL malicioso en una base de datos vulnerable.

¿Cómo prevenirlo?

- Usar sentencias SQL **parametrizadas**.
- **Validar** y sanitizar las entradas de los usuarios

@saulruizplaza

Ciberseguridad

SPYWARE



Malware que monitorea las actividades de un usuario para robar datos personales y confidenciales.

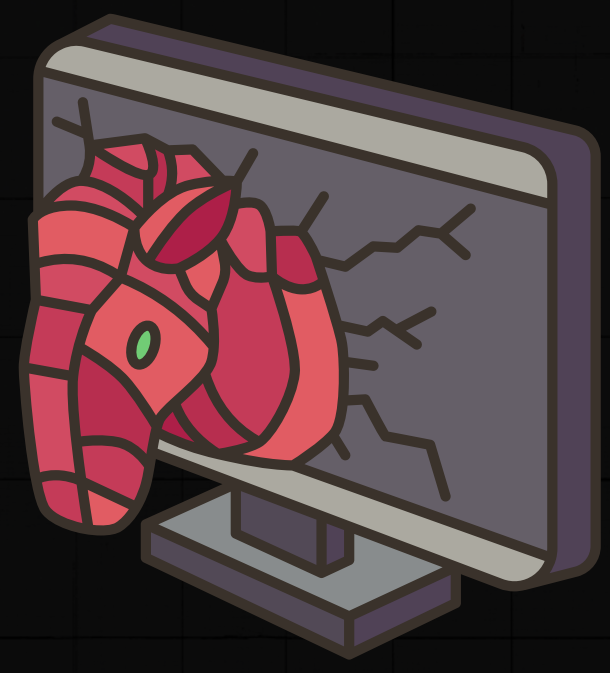
¿Cómo prevenirlo?

- Mantener **actualizado** el antivirus.
- No **descargar** software de fuentes no confiables.

@saulruizplaza

Ciberseguridad

CABALLO DE TROYA



Malware disfrazado de software legítimo que permite el acceso remoto a un sistema comprometido.

¿Cómo prevenirlo?

- Mantener **actualizado** el antivirus.
- No descargar software de fuentes no confiables.

@saulruizplaza

Ciberseguridad

KEYLOGGER

Software o hardware que registra las pulsaciones de teclas de un usuario, capturando información confidencial como contraseñas.

¿Cómo prevenirlo?

- **Antimalware** actualizado.
- Evitar dispositivos **desconocidos** en sistemas personales.



@saulruizplaza

Ciberseguridad

ATAQUE ZERO-DAY



Un ataque que explota vulnerabilidades desconocidas de software, antes de que el proveedor pueda emitir un parche.

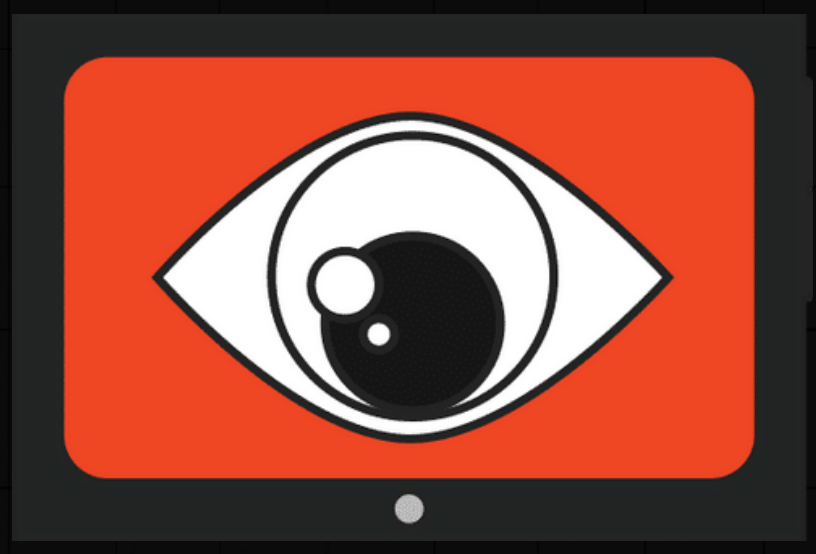
¿Cómo prevenirlo?

- Aplicar **parches** de seguridad lo antes posible.
- Mantener un **monitoreo** activo de vulnerabilidades

@saulruizplaza

Ciberseguridad

INSIDER THREAT



Un ataque perpetrado por un empleado o persona con acceso autorizado dentro de la organización.

¿Cómo prevenirlo?

- **Controlar** el acceso con el principio de mínimos privilegios.
- **Monitorear** y auditar el acceso interno a sistemas críticos.

@saulruizplaza

Ciberseguridad

CLICKJACKING

El atacante engaña al usuario para que haga clic en algo diferente a lo que cree, a través de un sitio web malicioso.

¿Cómo prevenirlo?

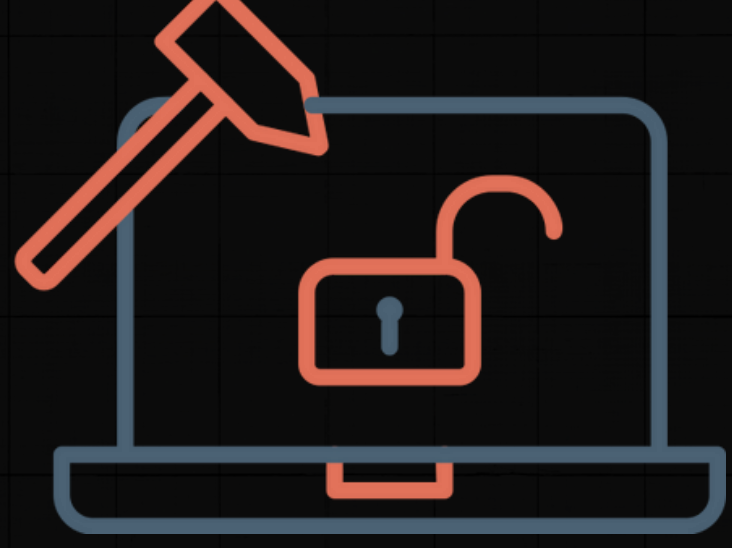
- Deshabilitar **iframes** externos no verificados.
- Utilizar **protecciones de seguridad** en los navegadores.



@saulruizplaza

Ciberseguridad

FUERZA BRUTA



Ataque donde el atacante prueba repetidamente combinaciones de contraseñas hasta encontrar la correcta.

¿Cómo prevenirlo?

- Implementar **autenticación multifactor** (MFA).
- Limitar los intentos de inicio de sesión.

@saulruizplaza

Ciberseguridad

PUERTA TRASERA



El atacante instala una puerta trasera en el sistema para poder acceder en el futuro sin ser detectado.

¿Cómo prevenirlo?

- **Monitorear** la actividad de la red.
- Asegurarse de **deshabilitar** puertos no utilizados.

@saulruizplaza

Ciberseguridad

DNS SPOOFING



Ataque donde el atacante manipula las respuestas del servidor DNS para redirigir a los usuarios a sitios web falsificados.

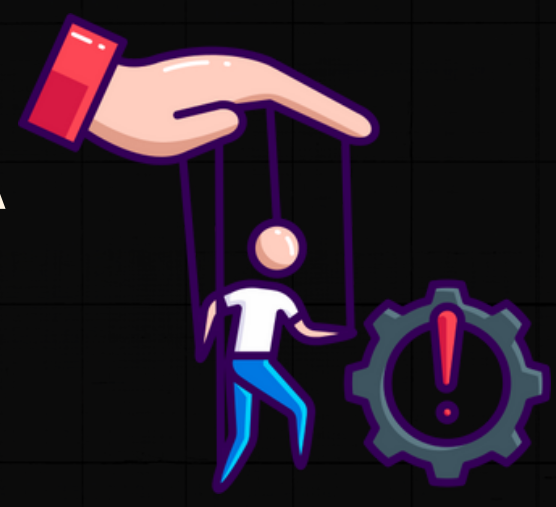
¿Cómo prevenirlo?

- Usar **DNSSEC** para asegurar las respuestas del servidor DNS.
- Validar las respuestas del DNS.

@saulruizplaza

Ciberseguridad

INGIENERÍA SOCIAL



Manipulación psicológica de individuos para que revelen información confidencial o realicen acciones que comprometan la seguridad.

¿Cómo prevenirlo?

- Entrenamiento continuo sobre **técnicas de ingeniería social.**
- **Verificar** siempre la identidad de la persona que solicita información confidencial.

@saulruizplaza

Ciberseguridad

PASSWORD CRACKING



El atacante intenta adivinar contraseñas utilizando herramientas automáticas que prueban diferentes combinaciones.

¿Cómo prevenirlo?

- Usar **contraseñas fuertes y únicas.**
- Cambiar regular las contraseñas

@saulruizplaza

Ciberseguridad

¿Te ha sido útil? Sígame y comparta este post con otras personas a las que pueda resultar útil.

@saulruizplaza