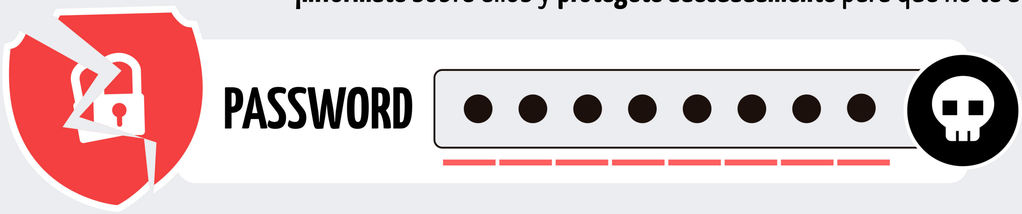
Ataques a las contraseñas

¡**Infórmate** sobre ellos y **protégete adecuadamente** para que no te afecten!



Conocer cuáles son las estrategias que usan los ciberdelincuentes para intentar robar contraseñas nos ayuda a protegernos mejor de posibles ataques y amenazas

¿Qué tipos de ataques existen?

Fuerza bruta

Consiste en adivinar la contraseña a base de ensayo y error.
Los ciberdelincuentes prueban distintas combinaciones al azar, conjugando nombres, letras y números, hasta que dan con el patrón correcto.

Ataques de diccionario

Un software se encarga automáticamente de intentar obtener la contraseña.
Empiezan con letras simples como "a", "AA" o "AAA" y, progresivamente, va probando con palabras más complejas.

Phishing

Una de las técnicas más utilizadas por los cibercriminales para robar contraseñas y nombres de usuario.
Se engaña a la víctima para que rellene un formulario fraudulento que suplanta a un servicio con sus credenciales de inicio de sesión.

Ataque keylogger

La víctima instala el malware en su equipo al hacer clic en un enlace o descargar un archivo de Internet.
Una vez instalado, el keylogger captura todas las pulsaciones del teclado, incluyendo las contraseñas, y se las envía a los ciberdelincuentes.

¿Cómo proteger nuestras contraseñas de estos ataques?

Contraseñas complejas

Utilizar más de 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales.

Contraseñas diferentes

No reutilizar contraseñas, usa contraseñas diferentes para distintos servicios.

Cambiar con regularidad

Dependiendo de la criticidad de la información que maneje el servicio, se establecerá una mayor o menor periodicidad para el cambio de contraseña.

Pero ¿qué es la ingeniería social?

La ingeniería social es muy utilizada por los ciberdelincuentes y se trata de técnicas de engaño y manipulación para hacerse con los datos de los usuarios. Toma nota de los siguientes consejos para no caer en trampas:

No reveles nunca información personal ni datos confidenciales (credenciales, números de tarjetas de créditos, cuentas bancarias, etc.) por teléfono, email o redes sociales, podrían estar suplantando la identidad de alguna empresa o servicio.

Ten cuidado al compartir información. Evita exponerte en Internet y en redes sociales publicando información personal (número de teléfono, dirección, hábitos, etc.). Éstos facilitan el trabajo a los ciberdelincuentes, si quieren, por ejemplo, adivinar tu contraseña.

Verifica los ficheros adjuntos y enlaces. No los descargues ni accedas a ellos si desconoces su contenido, aunque provengan de un contacto conocido, podrían tratarse de un Keylogger u otro malware.

Utiliza el sentido común y recuerda que en Internet el mejor sistema de seguridad eres tú

Mantente al día con nuestras campañas de concienciación para estar informado. ¡Es nuestra mejor defensa!

www.osi.es

OSI Oficina de Seguridad del Internauta
@osiseguridad
osiseguridad
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD