CREDENCIALES

EL TESORO MÁS BUSCADO

Las credenciales suponen la primera línea de defensa a nuestras cuentas, las cuales contienen nuestra información, y son una de las principales motivaciones de los ciberdelincuentes.

MÉTODOS DE OBTENCIÓN DE CREDENCIALES

FUERZA BRUTA

Se prueban combinaciones de forma indiscriminada hasta que se da con la credencial de acceso.
Se puede hacer uso de diccionarios con palabras relacionada con la víctima.

FILTRACIONES

Los diferentes servicios que usamos pueden tener incidentes de seguridad que comprometen y exponen datos de usuarios, incluyendo nuestras contraseñas.

INGENIERÍA SOCIAL

A través de distintas técnicas (Phishing, Smishing, Vishing...) buscan manipularnos, haciéndose pasar por una persona o una entidad, para que revelemos nuestra contraseña.

SPIDERING

Se basa en una técnica donde los ciberdelincuentes recopilan información pública sobre nosotros en la red con el objetivo de adivinar más fácilmente nuestras contraseñas.

CREDENCIALES

EL TESORO MÁS BUSCADO

¿CÓMO NOS PROTEGEMOS?

- **Hemos de crear contraseñas largas y complejas:** de al menos 12 caracteres alternando números (0-9), mayúsculas (A-Z), minúsculas (a-z) y caracteres especiales (¡, !, ¿, ?, @...).
- **Hemos de evitar el uso de información personal:** nombres de usuario, fechas de nacimiento o nombres de mascotas.
- **Hemos de evitar secuencias:** combinaciones como «123456» o «qwerty».
- **Hemos de cambiarlas regularmente:** sin usar reglas predecibles o secuencias relacionadas con la anterior, como «Septiembre2026!» -> «Octubre2026!».
- **Intentemos utilizar un gestor de contraseñas:** ayudan a almacenar y generar contraseñas de manera segura. NUNCA hemos de conservarlas por escrito.

CÓMO CREAR CONTRASEÑAS SEGURAS

1 ELEGIR

Elegimos un conjunto de palabras fáciles de recordar pero que no contengan información personal.

GirasolAmapola

2 COMBINAR

Combinamos las palabras para evitar que se encuentren en un diccionario pero siga siendo fácil de recordar.

Giramapola

3 PERMUTAR

Cambiamos algunos caracteres por símbolos y números para aumentar su complejidad.

Gir@map0la!

MFA

La autenticación de dos factores (*Multiple Factor Authentication*, MFA), consiste en añadir una segunda capa de protección en el acceso a las cuentas de usuario en los sistemas de información.

FACTOR 1

Algo que sabemos: usuario y contraseña

FACTOR 2

Algo que tenemos: código de verificación en el teléfono móvil

¡LA SEGURIDAD DIGITAL COMIENZA CONTIGO!

COFM

GOERTIS
Part of Telefónica Tech