



CONSEJOS BÁSICOS CIBERSEGURIDAD EN CONTRASEÑAS



Una contraseña segura es la principal barrera que impide que te hackeen la mayoría de tus cuentas en línea.

Principales amenazas en las contraseñas



Ataques por fuerza bruta

Ejecuta pruebas automatizadas de ensayo y error hasta encontrar los caracteres correctos de las credenciales



Hackeo basado en diccionario

Programas automatizados para probar y generar millones de palabras clave posibles, como nombres de pila o palabras comunes, hasta encontrar la combinación.



Ataques phishing

Método que utilizan los hackers para robar contraseñas y nombres de usuario, que consiste en engañar a la víctima para que rellene un formulario falso, donde inicia sesión.



Ataques malware

El malware es un software dañino que se puede instalar en un dispositivo sin el conocimiento o el consentimiento del usuario.



Ataques de ingeniería social

Implican el uso de técnicas de manipulación para engañar a las personas para que revelen información confidencial, como contraseñas

Recuerda que las contraseñas que utilizas en tus sistemas son la principal barrera para de seguridad. Debes introducir contraseñas fuertes que blinden tu información profesional y personal.

El hacker intentará hacerse con tus credenciales para acceder a tu información. Conocer los principales ataques y protegerse con una buena contraseña te ayudarán a fortalecerte frente a futuras amenazas.



CONSEJOS BÁSICOS CIBERSEGURIDAD EN CONTRASEÑAS

¿Cómo evitar una mala gestión de las contraseñas?

No compartas tus contraseñas con nadie

Si lo haces, dejará de ser secreta y estarás dando acceso a tu privacidad

No utilices la misma contraseña en diferentes servicios

Siempre claves diferentes para servicios diferentes

Utiliza gestores de contraseñas

Si te cuesta memorizar las contraseñas o utilizas muchos servicios, apóyate en estos programas, son muy útiles y sencillos de manejar

Asegúrate de que son robustas

Están formadas por al menos 8 caracteres: mayúsculas, minúsculas, números, caracteres especiales...

Cuidado con las preguntas de seguridad

Si las utilizas, que sólo tú y nadie más sepa las respuestas

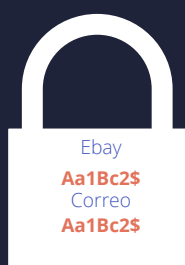
Tus contraseñas deben ser...



Secretas



Robustas



No Repetidas



Cambiadas Periódicamente

Utiliza contraseñas únicas para cada servicio, no las compartas. Usa contraseñas robustas o programas de generación de contraseñas y ten cuidado con las preguntas de seguridad. Actualiza tu contraseña de forma periódica.



CONSEJOS BÁSICOS CIBERSEGURIDAD EN CONTRASEÑAS

¿Qué tan segura es mi contraseña?

1 ¿Es larga?

Intenta que tenga un mínimo de 8 - 12 caracteres



2 ¿Es difícil de adivinar?

Debes evitar las secuencias del estilo ("1234", "abcde") porque las pueden hackear con fuerza bruta en segundos. También evita las palabras comunes por la misma razón.



3 ¿Usas tipos de caracteres variados?

Las minúsculas, mayúsculas, los símbolos y los números pueden formar parte de la contraseña. La variedad puede aumentar lo segura que es tu contraseña.



4 ¿Evita los sustitutos obvios de los caracteres?

Por ejemplo, usar el número "0" en lugar de la letra "O"

password_

5 ¿Las has usado antes?

Reutilizar las contraseñas compromete las cuentas, haz que siempre sean diferentes entre sí.



123456789



A23cM1s6w



password



p@ssw0rd

Evita secuencias fáciles de números, usa contraseñas largas, no repetidas, que contengan secuencias de texto y números, mayúsculas, minúsculas y caracteres especiales.