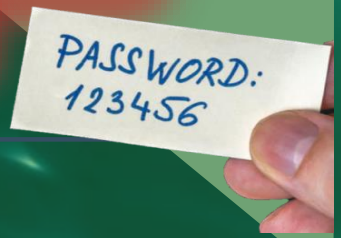
Consecuencias de tener contraseñas débiles



Vulnerabilidad a ataques de fuerza bruta: Las contraseñas débiles son fáciles de adivinar mediante ataques de fuerza bruta, donde los atacantes intentan todas las combinaciones posibles de caracteres hasta que encuentran la contraseña correcta. Esto puede dar lugar al acceso no autorizado a tus cuentas y dispositivos.

Riesgo de acceso no autorizado: Si alguien obtiene acceso a tu dispositivo o cuenta debido a una contraseña débil, podría robar tus datos personales, financieros o confidenciales, comprometiendo tu privacidad y seguridad.

Riesgo de robo de identidad: El acceso a cuentas en línea a través de contraseñas débiles puede permitir a los atacantes robar tu identidad y realizar actividades fraudulentas en tu nombre, como abrir cuentas bancarias, realizar compras o cometer ciberdelitos.

Pérdida de datos: Si un atacante obtiene acceso a tu dispositivo o cuentas, podría borrar o corromper tus datos, lo que podría originar una pérdida irreparable de información importante, como fotos, documentos y archivos personales.

Daño reputacional: Las violaciones de seguridad debidas a contraseñas débiles pueden dañar tu reputación personal o profesional, ya que la pérdida de datos o la filtración de información confidencial pueden afectar a ti o a tu empresa de manera negativa.

El uso de contraseñas débiles en dispositivos digitales puede tener una serie de consecuencias negativas, ya que la seguridad de tus datos y sistemas digitales depende, en gran medida, de la fortaleza de las contraseñas que utilizas.

¿Cómo es de segura tu contraseña?

¿En cuantos dispositivos y cuentas usas la misma contraseña?

REALIZADO POR LA UNIDAD DE COORDINACIÓN DE CIBERSEGURIDAD

Dirección General de la Guardia Civil

Unidad de Coordinación de Ciberseguridad

C/ Guzmán El Bueno 110 – 28003 Madrid

www.guardiacivil.es – Telf.: 900.101.062

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

Contraseñas Seguras

¡Tú tienes la clave!

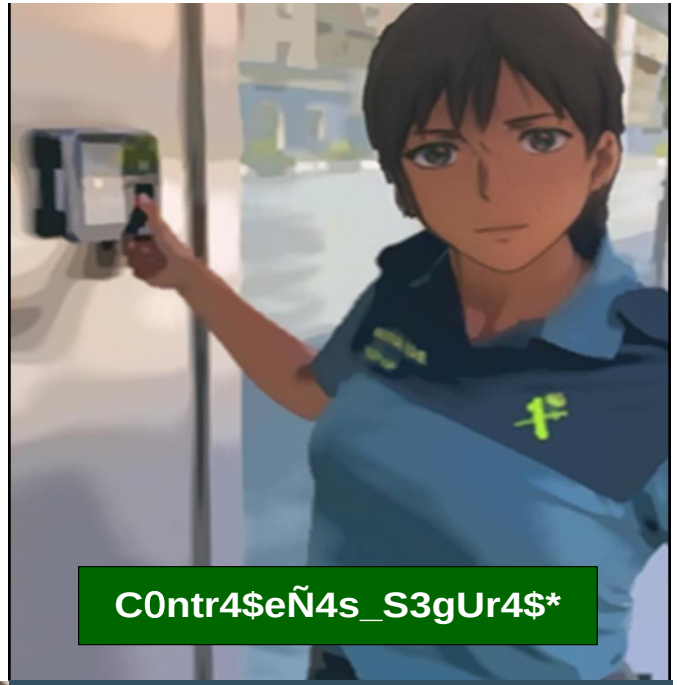
Unidad de Coordinación de Ciberseguridad

Aprendamos sobre contraseñas

Longitud: Utiliza contraseñas largas, preferiblemente de al menos 12 caracteres, las contraseñas cortas son más fáciles de averiguar por otras personas.

Combinación de caracteres: Incluye letras mayúsculas, minúsculas, números y símbolos especiales en tu contraseña (@, #, $, etc.).

Evita información personal: No uses datos personales como tu nombre, fecha de nacimiento o palabras fáciles de adivinar.



Distintas contraseñas para distintos servicios: No uses la misma contraseña para múltiples cuentas.

Autenticación de dos factores (2FA): Habilita la autenticación de dos factores, cuando sea posible, para añadir una capa adicional de seguridad.

Mantén tus contraseñas seguras: No compartas tus contraseñas con nadie y guárdalas en un lugar seguro, o utiliza una herramienta de gestión de contraseñas para generar y almacenar contraseñas de forma segura.

Cambia contraseñas periódicamente: Es importante cambiar tus contraseñas regularmente.

No compartas tus contraseñas: al hacerlo aumentas considerablemente las posibilidades de que caigan en malas manos.

Siguiendo estos consejos podrás mejorar la seguridad de tus contraseñas y proteger tus cuentas en línea.