

Cómo crear contraseñas seguras

Protege tus cuentas con contraseñas fuertes y únicas · Principiante

SmartGuys.biz · smartguys.biz

¿Por qué importan las contraseñas?

Una contraseña débil es como dejar la puerta de tu casa abierta. Los hackers usan programas que prueban miles de contraseñas por segundo. Si usas "123456" o tu fecha de nacimiento, tu cuenta puede ser robada en segundos.

Características de una contraseña segura

- Mínimo 12 caracteres (cuanto más larga, mejor).
- Mezcla letras mayúsculas y minúsculas: A, b, C...
- Incluye números: 3, 7, 9...
- Agrega símbolos: !, @, #, \$, %, &...
- No uses información personal: nombre, fecha de nacimiento, número de cédula.
- No uses palabras del diccionario: "perro", "casa", "amor".
- Usa una contraseña diferente para cada cuenta importante.

Método de la frase secreta

Una forma fácil de crear contraseñas fuertes y memorables es usar una frase:

- 1 Piensa en una frase que solo tú conozcas: "Mi perro Toby nació en 2018"
- 2 Toma la primera letra de cada palabra: MpTne2018
- 3 Agrega símbolos: MpTne2018!
- 4 Resultado: una contraseña de 10 caracteres fácil de recordar y difícil de adivinar.

• Ejemplo de contraseña fuerte

"Vivo en Guanacaste y tengo 3 vacas!" !" VeGyt3v! — 8 caracteres con mayúsculas, número y símbolo. Puedes hacerla más larga para mayor seguridad.

Contraseñas que NUNCA debes usar

- 123456 / 123456789 / 12345678
- password / contraseña / clave
- Tu nombre o el de un familiar
- Tu fecha de nacimiento (ej: 15031998)
- El nombre de tu mascota
- qwerty / abc123 / 111111

Gestores de contraseñas

Un gestor de contraseñas es una app que guarda todas tus contraseñas de forma segura. Solo necesitas recordar una contraseña maestra. Opciones gratuitas:

- Google Password Manager — integrado en Chrome y Android, completamente gratis.
- Bitwarden — gratuito, de código abierto, disponible en todos los dispositivos.
- iCloud Keychain — para usuarios de iPhone y Mac, viene incluido.

Verificación en dos pasos (2FA)

La verificación en dos pasos agrega una capa extra de seguridad. Además de tu contraseña, necesitas un código que llega a tu celular o email. Actívala en:

- Gmail: Configuración !' Seguridad !' Verificación en dos pasos.
- Facebook: Configuración !' Seguridad e inicio de sesión !' Autenticación en dos factores.
- WhatsApp: Configuración !' Cuenta !' Verificación en dos pasos.

Regla de oro

Nunca compartas tu contraseña con nadie, ni con personas que digan ser del soporte técnico de Google, Facebook o tu banco. Las empresas legítimas NUNCA te pedirán tu contraseña.