Para proteger tus cuentas en sitios web y servicios importantes como el correo electrónico y las plataformas bancarias, es clave implementar prácticas seguras de creación y gestión de contraseñas.

Aquí algunos pasos esenciales para hacerlo:

1. **Utiliza contraseñas fuertes y únicas**

- Longitud : Las contraseñas seguras suelen tener al menos 12 caracteres.
- Variedad de caracteres : Incluye letras mayúsculas, minúsculas, números y símbolos especiales (como `!`, `@`, `#`, etc.).
- Evita palabras comunes : No uses palabras sencillas o comunes como "password123" o "abc123", ya que son fáciles de adivinar.
- No repitas contraseñas : Cada cuenta debe tener una contraseña única, de forma que si una es comprometida, no afecte a las demás.

Una contraseña segura podría parecer algo como: `aB9$xRt@3g6^J`.

La razón de porqué se recomiendan contraseñas con variedad de caracteres y al menos 12 caracteres es por la resistencia frente a ataques de fuerza bruta (probar con un ordenador todas las combinaciones posibles), aproximadamente hay en español 100 caracteres diferentes, por tanto una contraseñas de 12 posiciones tiene $100^{12}=10^{24}$ = mil trillones. Para romper ese código con fuerza bruta se necesitaría probar $(10^{201} – 1)*(100/99)$ combinaciones que es un número extremadamente grande (un uno seguido de 201 ceros).

2. **Utiliza un gestor de contraseñas.**

El generar y gestionar contraseñas tan grandes y con caracteres tan extraños hace casi obligatorio el usar un gestor.
Un gestor de contraseñas es una aplicación que guarda todas tus contraseñas en un solo lugar, protegido por una "contraseña maestra". Algunos de los más recomendados son LastPass , **Bitwarden** y 1Password.

- Ventaja : Te permite recordar solo una contraseña maestra en lugar de todas, y el gestor genera contraseñas seguras y únicas automáticamente.

- Acceso en todos tus dispositivos : La mayoría de los gestores ofrecen **sincronización** en varios dispositivos, lo cual es muy conveniente.

3. **Activa la autenticación de dos factores (2FA)**

- La autenticación de dos factores agrega una capa extra de seguridad, ya que, además de tu contraseña, requiere un segundo paso de verificación (como un código enviado a tu teléfono o generado por una aplicación como Google Authenticator o Authy).

- Esto significa que incluso si alguien obtiene tu contraseña, no podrá acceder sin este segundo factor.

4. **Evita compartir contraseñas y utiliza dispositivos de confianza**

- No compartas tus contraseñas con nadie y evita ingresar a tus cuentas en dispositivos públicos o compartidos.
- Siempre revisa que la URL del sitio comience con https y que tenga un candado en la barra de dirección. Esto indica que la conexión es segura.
-**Evita guardar contraseñas en el navegador , es una practica muy común y que facilita mucho la vida a un hacker.**

5. **Cambia tus contraseñas regularmente.**

- Cambia tus contraseñas al menos cada 6-12 meses en sitios sensibles, como el correo electrónico y bancos.
- Si sospechas de una posible filtración o vulnerabilidad, cambia tu contraseña de inmediato.

6. **Consejos para recordar la contraseña maestra**

- Puedes crear frases de contraseña usando palabras aleatorias que tengan un significado especial para ti o sean fáciles de recordar, pero no obvias para otros.
Ejemplo: `¡Coche+Sol123Libro%`, que mezcla palabras con símbolos y números.

Implementar estas prácticas reduce considerablemente el riesgo de accesos no autorizados y protege tu información personal.

Próximo capitulo: "El gestor de contraseñas"