MÓDULO 5:
Protección de la privacidad digital

CONTENIDO 6: Familiarizarse con las formas de proteger los dispositivos

Este proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación refleja únicamente las opiniones del autor, y la Comisión no se hace responsable del uso que pueda hacerse de la información aquí difundida. 2022-1-TR01-KA220-VET-000088431

Co-funded by the European Union

Escáner de huellas dactilares

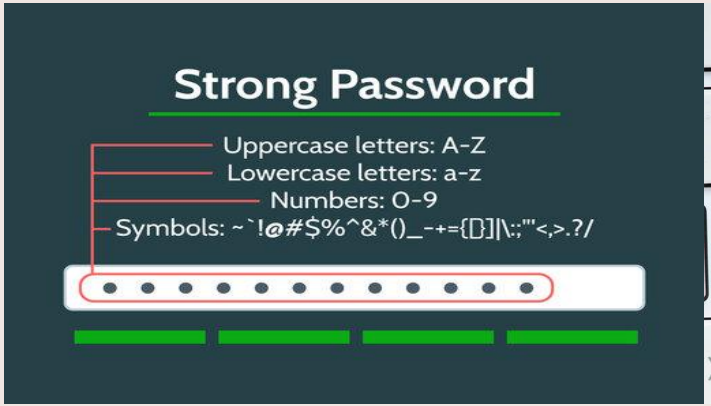
Los escáneres de huellas dactilares se han utilizado ampliamente en la tecnología actual para proporcionar a las personas seguridad cibernética. En la actualidad, casi todos los dispositivos móviles cuentan con esta funcionalidad, que puede establecer rápidamente una medida de seguridad básica.

Fuente: freepik

Co-funded by the European Union

Una contraseña segura

Los usuarios deben comprender la importancia de no solo confiar en las huellas dactilares, sino también de tener una contraseña segura que debe ser una combinación de letras mayúsculas y minúsculas, números y símbolos. Además, los usuarios deben evitar incorporar información personal en su contraseña al crear (por ejemplo, nombre, apellido, cumpleaños, etc.).



Fuente: freepik

Co-funded by the European Union

Al crear una contraseña, evita :

- Números consecutivos (por ejemplo, 1,2,3,4,5,6).
- Información personal como nombre, apodo, fecha de nacimiento, aniversario.
- Contraseñas cortas.
- Usar la misma contraseña durante mucho tiempo.
- Tener la misma contraseña para varias cuentas.

Fuente: freepik

Co-funded by the European Union

	
JoH/n1^D0e991	**JohnDoe1991**
,*j0hn91D0e.	John.Doe91
L0F+Pr0jeC+	LoftProject
D!GI//C0M&p	Digi.comp

Fuente: freepik

Co-funded by the European Union

Resumen

Hacer	• Utilice una contraseña diferente para cada servicio (es decir, JCU, Gmail, Dropbox, iTunes, etc.). • Use una frase de contraseña donde pueda, porque la longitud es más segura que la complejidad. • Utilice más de 4 números en un número PIN o código de acceso. • Cambie su contraseña periódicamente (anualmente sería un buen comienzo) o si cree que se ha visto comprometida.
No	• Utilice palabras simples o de diccionario (p. ej. Contraseña123, Townsville123) • Escriba su contraseña en una nota adhesiva y pégula en su monitor. • Utilice palabras fáciles de adivinar (por ejemplo, números de teléfono, fecha de nacimiento). • Dígale a cualquiera su contraseña, ¡esto incluye al personal de TIC!

Fuente: https://www.jcu.edu.au/information-and-communications-technology/secure-it/choosing-a-safe-password

Co-funded by the European Union

EJERCICIO

- Vamos a crear una contraseña segura juntos.
- Escriba primero su nombre y apellidos.
- Haga algunos cambios con él:
  - i → !
  - t → +
  - l → /
  - o → 0
- Haga algunas de las letras en mayúsculas.
- Añada caracteres como *.-', donde quiera.
- No olvide incluir números (no su cumpleaños!).

Co-funded by the European Union

Links útiles

- YouTube tutorial: cómo hacer una contraseña fuerte
- YouTube Vídeo: Seguro Te Conectás - Contraseña Segura. AGESIC
- Cómo crear una contraseña segura
- Consejos para crear una contraseña segura
- Huellas vs contraseñas

Referencias

- https://www.freepik.com/
- https://shorturl.at/x03ow
- https://shorturl.at/tKTIN