1. Contraseña que se ha tenido débil alguna vez 🡪1234 que al no tener una dificultad mayor es fácil de descifrar y su seguridad es baja
2. Contraseña posible de frase 🡪 WILSONALFONSOTARRIFACAPATAZ

Sustituyendo con caracteres especiales

W1L$0N@|F0N$0T@rriF@C@P@T@/=

Esto genera una traza de 20 longitud con caracteres no tan fáciles de predecir como lo es $, @, |, /, =

Diversidad de caracteres:

* Mayúsculas (W, L, F, C, P, etc.)
* Minúsculas (r, i, a, etc.)
* Números (1, 0)
* Símbolos especiales ($, @, |, /, =)

Al no tener un patron secuencial como seria la frase inicial aumenta la dificultad al hackear esta contraseña

**Establecer amenaza vector de ataque**

* **Origen de la entrada (correo, SMS, notificación por red social)**

¿Quién es el emisario del mensaje? - ¿Es una dirección sospechosa o desconocida?

¿Hay errores raros en el nombre o dominio (como g00gle.com en lugar de google.com)?

2. Contenido del mensaje

¿Te presionan para actuar rápido? ("¡Urgente!", "¡Última oportunidad!", "¡Tu cuenta será suspendida!")

¿Prometen cosas fuera de lo común? ("Ganaste un premio", "Ofrecemos empleo sin experiencia").

3. Tipo de archivo adjunto

¿El adjunto es un tipo de archivo peligroso? (por ejemplo, .exe, .bat, .scr, .js, .docm, .xlsm).

¿Un archivo ofimático que pide habilitar macros?

4. Análisis del archivo adjunto

¿El archivo adjunto tiene firmas conocidas de malware?

¿El archivo tiene scripts escondidos o ejecución automática?

5. Enlaces incluidos

¿Te lleva a una página de login falsa?

¿Los enlaces reales (pase el cursor sin hacer clic) coinciden con el texto?

6. Comportamiento sospechoso del sistema

Después de abrir el archivo, ¿la computadora actúa rara? (se pone lenta, aparecen ventanas extrañas, contactos reciben correos que no enviaste tú).

7. Fecha y contexto

¿El correo llegó en un horario raro o sin contexto? (por ejemplo, te mandan una factura cuando no has comprado nada).

Gestor de contraseña

Un gestor de contraseñas es un programa (aplicación o servicio web) que se encarga de:

Crear contraseñas automáticas muy fuertes y únicas (imposibles de adivinar para un hacker).

Guardar todas tus contraseñas en un archivo cifrado, como si fuera una bóveda súper segura.

Proteger esas contraseñas usando una única contraseña maestra que solo tú conoces.

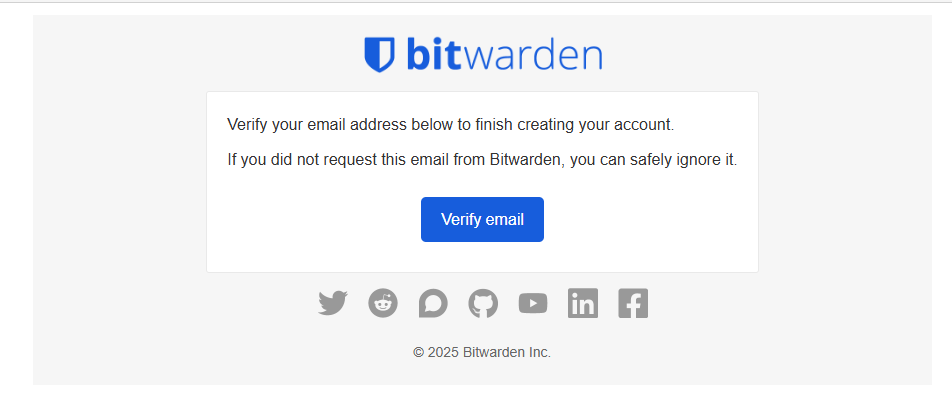
Recordar y autocompletar tus contraseñas cuando vayas a iniciar sesión en sitios web o aplicaciones.

Sincronizar tus contraseñas entre tus dispositivos (teléfono, computadora, Tablet), de manera cifrada.

Avisarte si alguna de tus contraseñas se ha filtrado en internet (en algunos casos).

Instalación de un gestor de contraseña

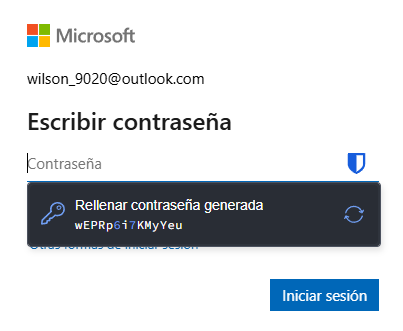
Lo primero es crear una cuenta en bitwarren donde le van a pedir un correo y su nombre, después tendra que verificar que su dirección es correcta y le enviaran un un email asi



Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

* Después de verificar el correo se crea una contraseña maestra la cual podemos ver en la imagen anterior



Aquí vemos la contraseña generada para ingresar sirve mas en el caso de registrarse en un sitio web para no tener que memorizar una gran cantidad de contraseñas y en casos como Outlook que si se olvida se puede perder el acceso