CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

Cómo crear buenas claves

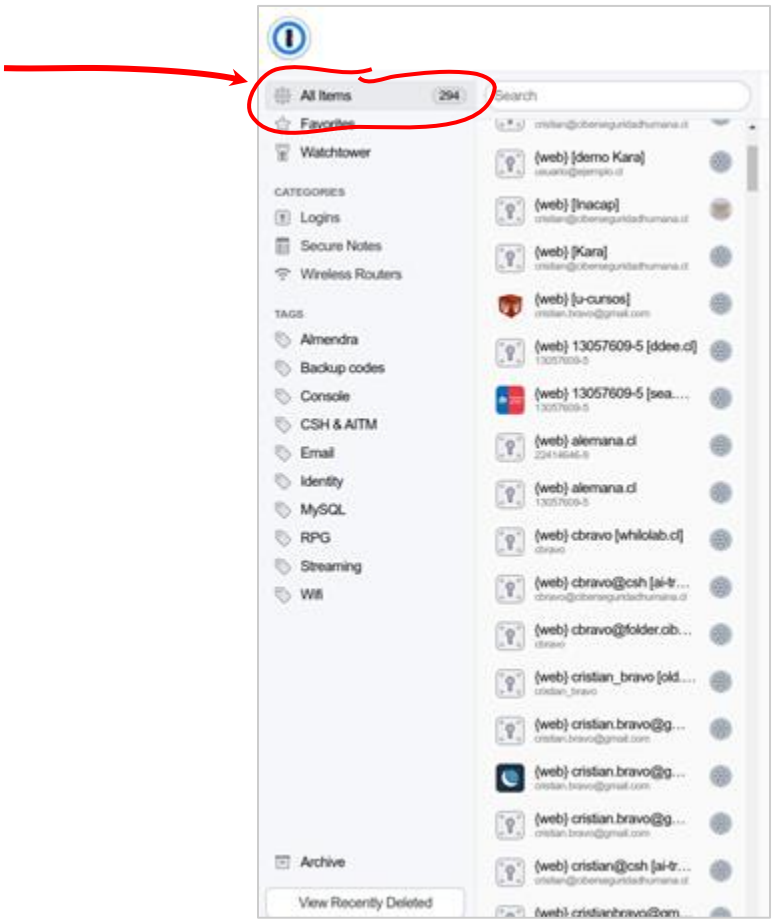
Cristian Bravo Lillo, Ph.D., Director CSIRT de Gobierno

cbravol@interior.gob.cl

¿Por qué es importante?

Las personas no podemos recordar tantas claves:

1. Usamos malas claves → adivinables fácilmente
2. Las guardamos en el email o en planillas Excel
3. Usamos la misma clave (con variaciones menores) para muchos lugares



¿Qué es una buena clave?

Fácil de recordar (por mí)

Difícil de adivinar (por otros)

Los atacantes saben lo anterior, así que…

- Prueban sistemáticamente variaciones de claves
- Si encuentran una clave, la prueban en otras cuentas tuyas
- Si se meten a tu computador, buscan emails con claves, o archivos Excel con claves.

¿Cómo evitar lo anterior?

1. Inventa claves con varias palabras aleatorias (passphrases)

[Intermedio con preguntas frecuentes]

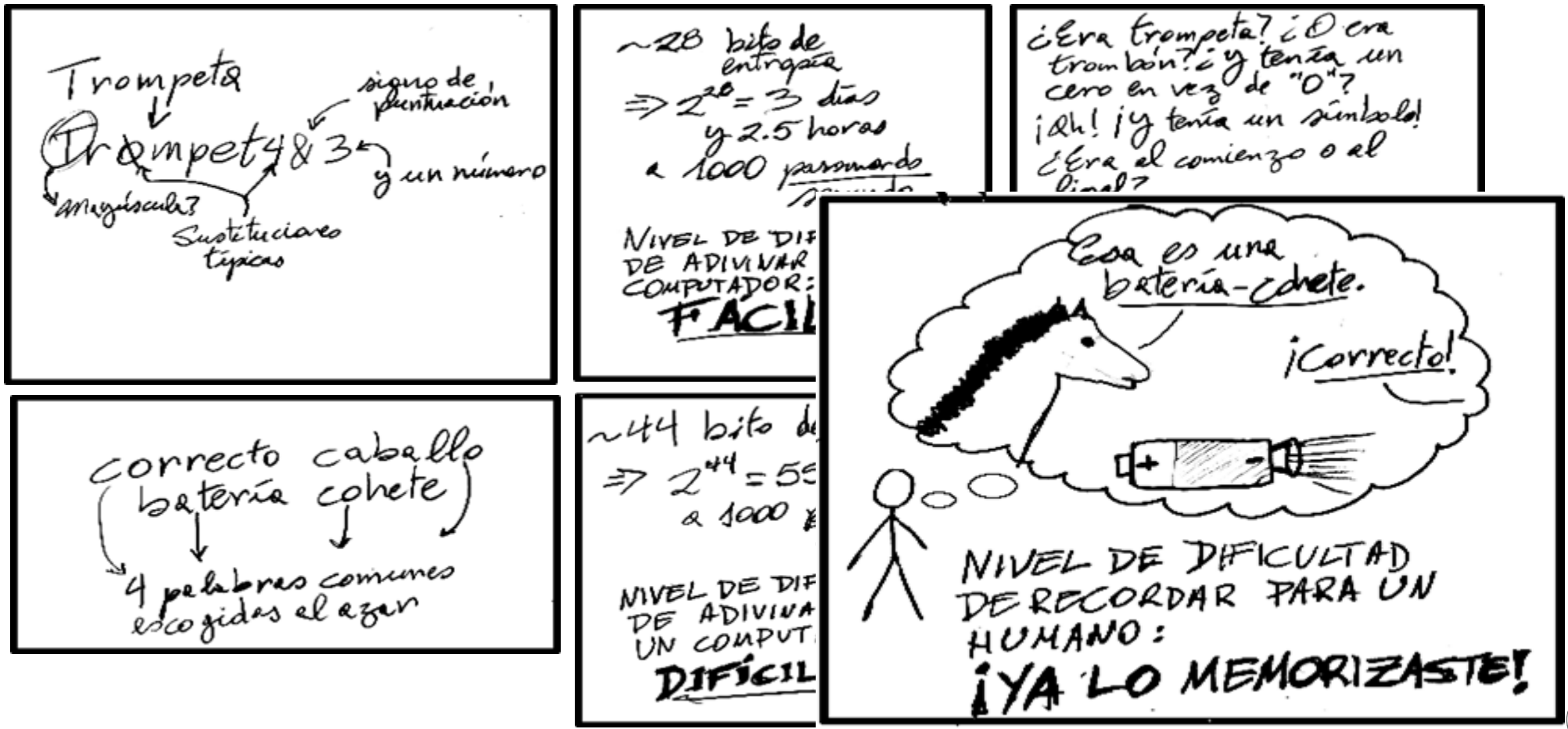
2. Usa una tarjeta de claves

3. Usa un gestor de claves

[Recomendación incómoda para terminar]

1

¿Qué es una passphrase?

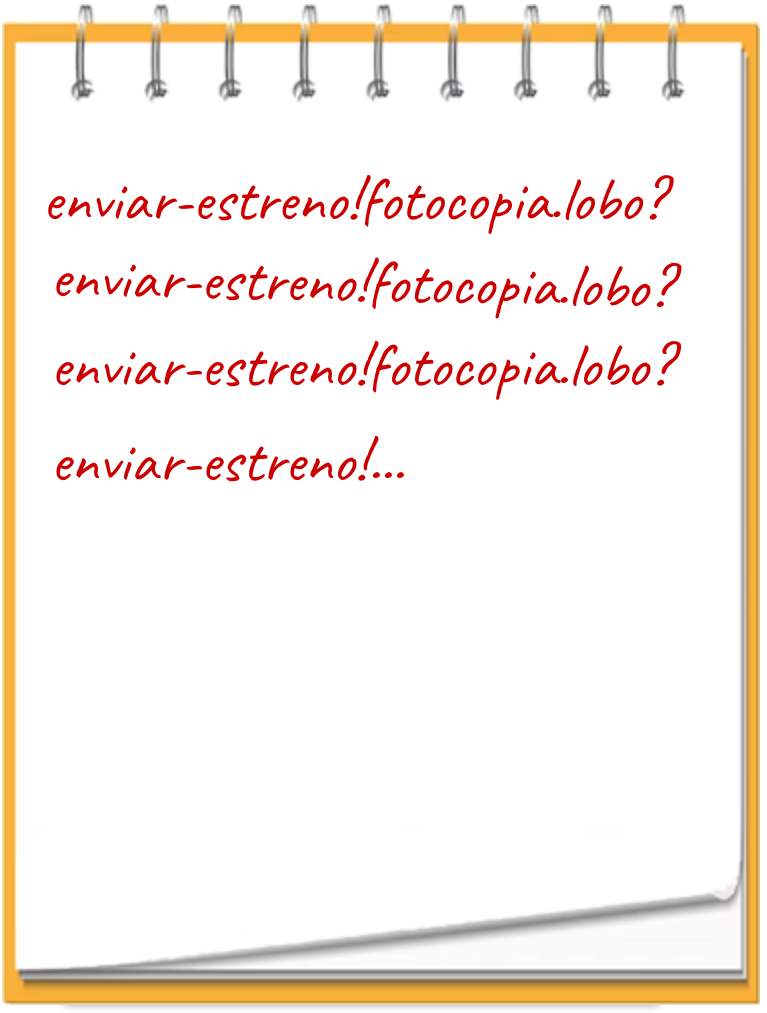


Basado en https://xkcd.com/936/

1

Ejercicio: inventa una passphrase

1. Anda a https://palabrasaleatorias.com
2. Escoge cuatro palabras al azar
3. Imagina una historia o inventa una imagen mental con esas palabras
4. Agrega símbolos de puntuación y/o números
5. Escríbela varias veces (en un papel que luego romperás)



2

¿Qué es una tarjeta de claves?

Es una tarjeta impresa que uno lleva en la billetera o cartera, con combinaciones aleatorias de letras y números.

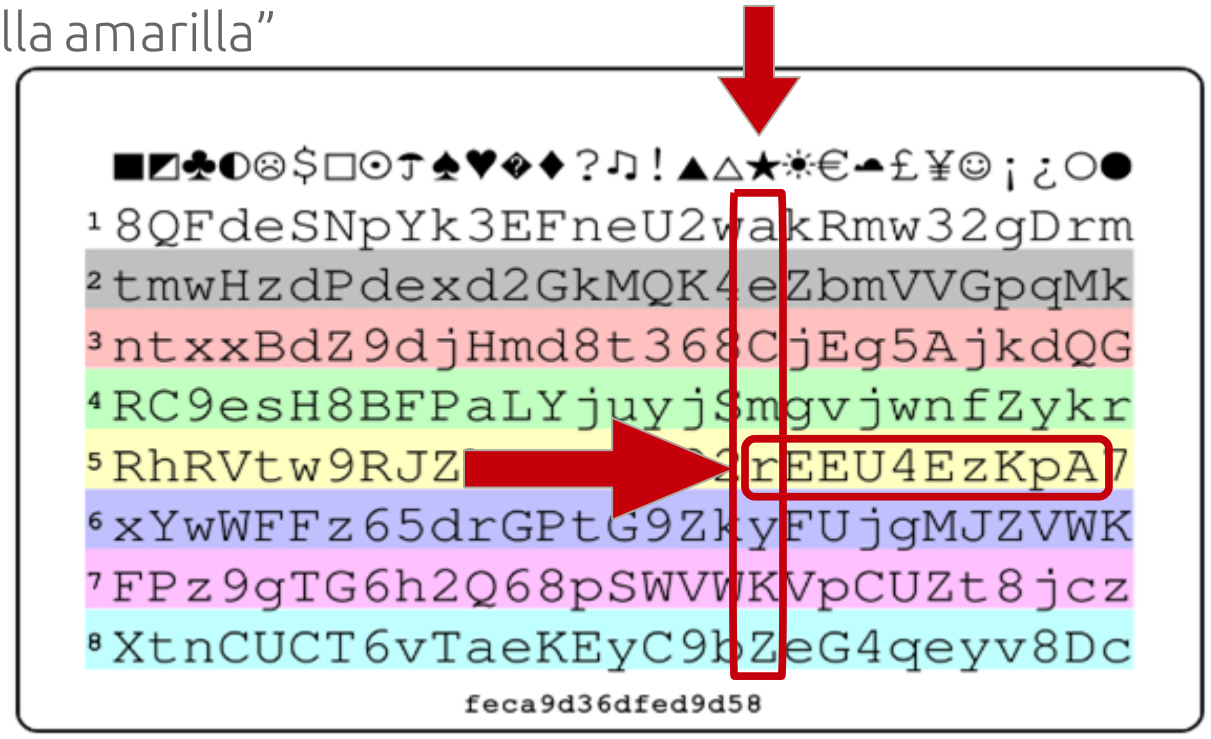
https://passwordcard.org

2

¿Cómo se usa una tarjeta de claves?

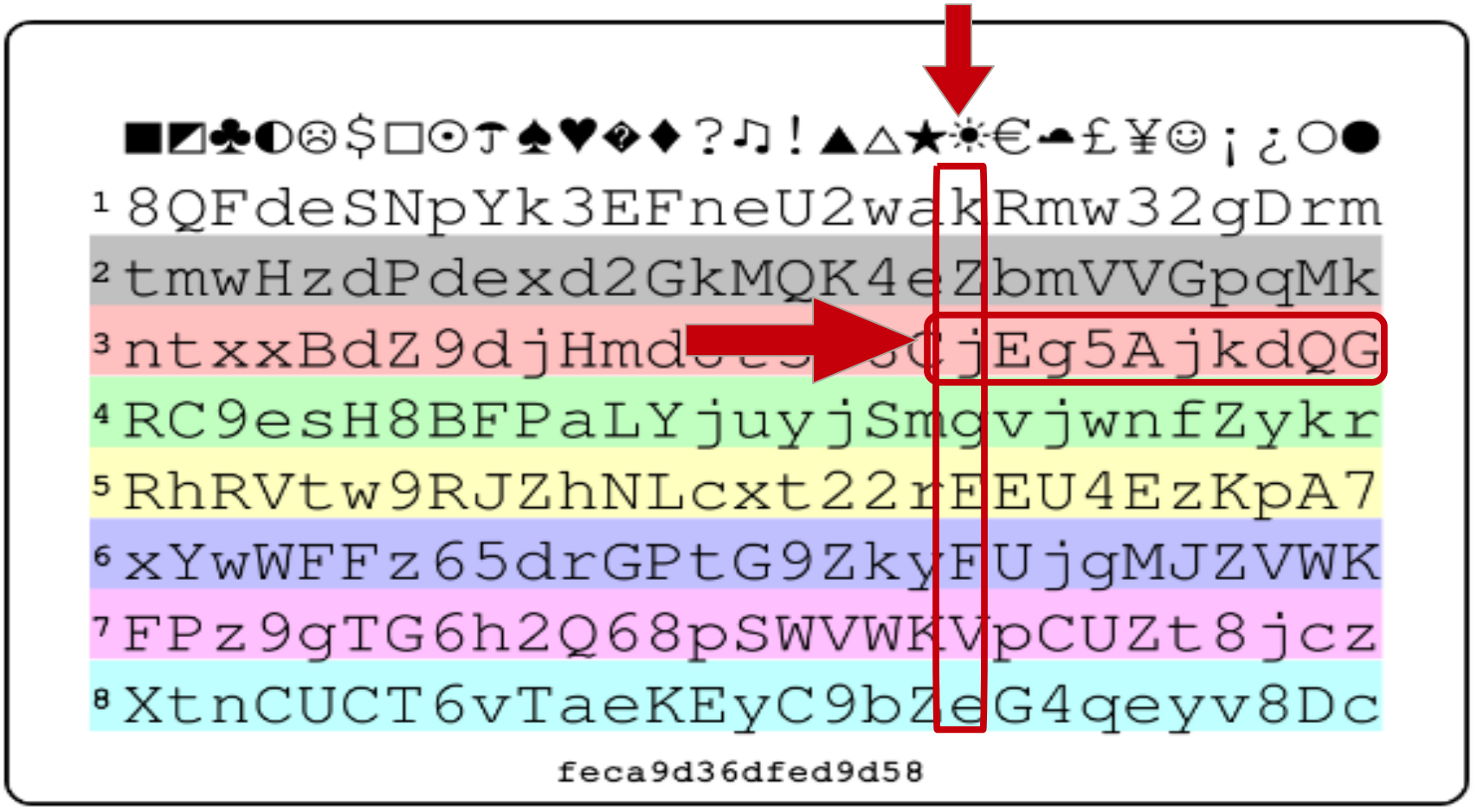
Se escoge de antemano un largo: por ejemplo, 10 caracteres

Para cada sitio que requiera username y password, escoges un símbolo y un color: p. ej., “estrella amarilla”



2

¿Cuál es la clave para "sol rojo", con 10 caracteres?



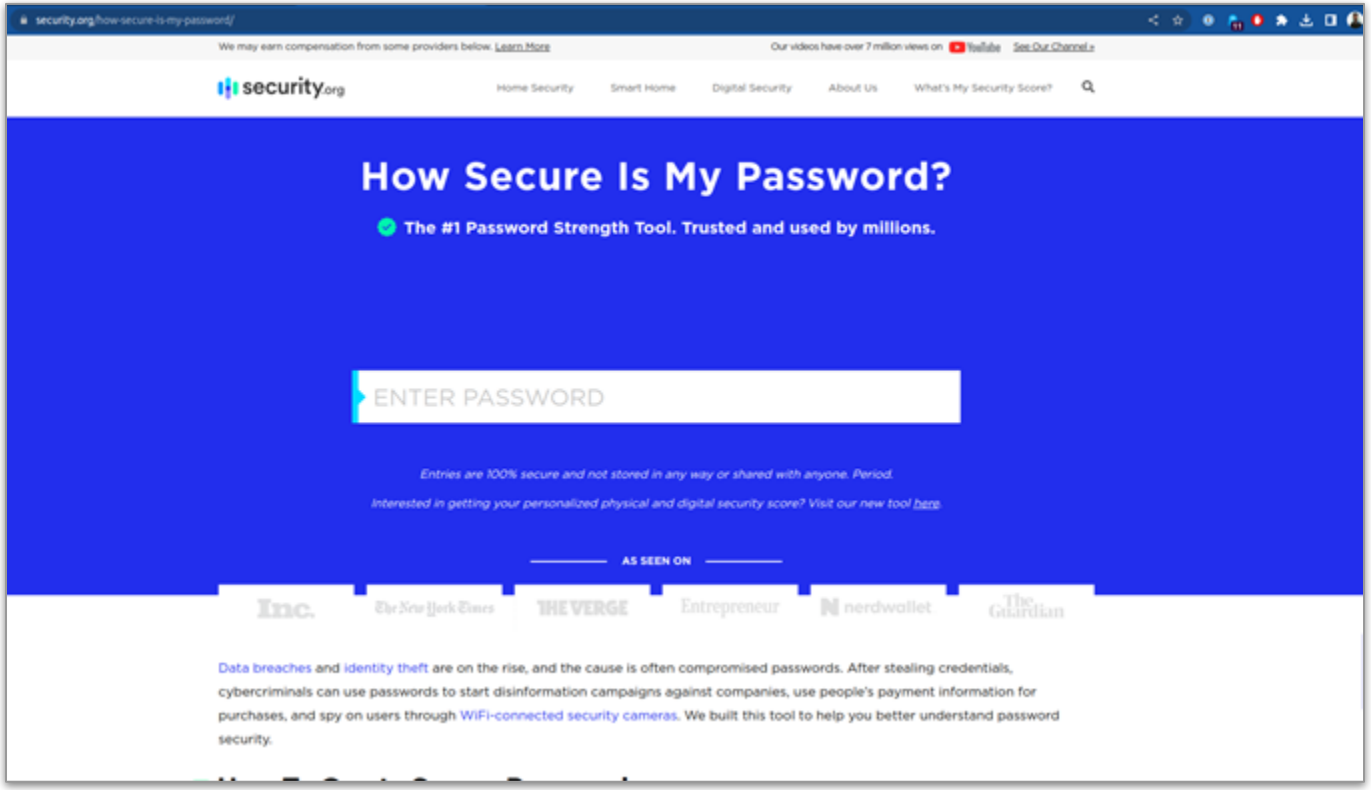
Preguntas frecuentes: “¿Es seguro escribir mis claves?”

Sí, siempre que:

1. No escribas en el mismo papel la cuenta a la que pertenece, y
2. Guardes el papel en un lugar “seguro”, como tu cartera o billetera.

¿Cómo sé si mi clave es buena?

Pruébala en https://www.security.org/how-secure-is-my-password/:



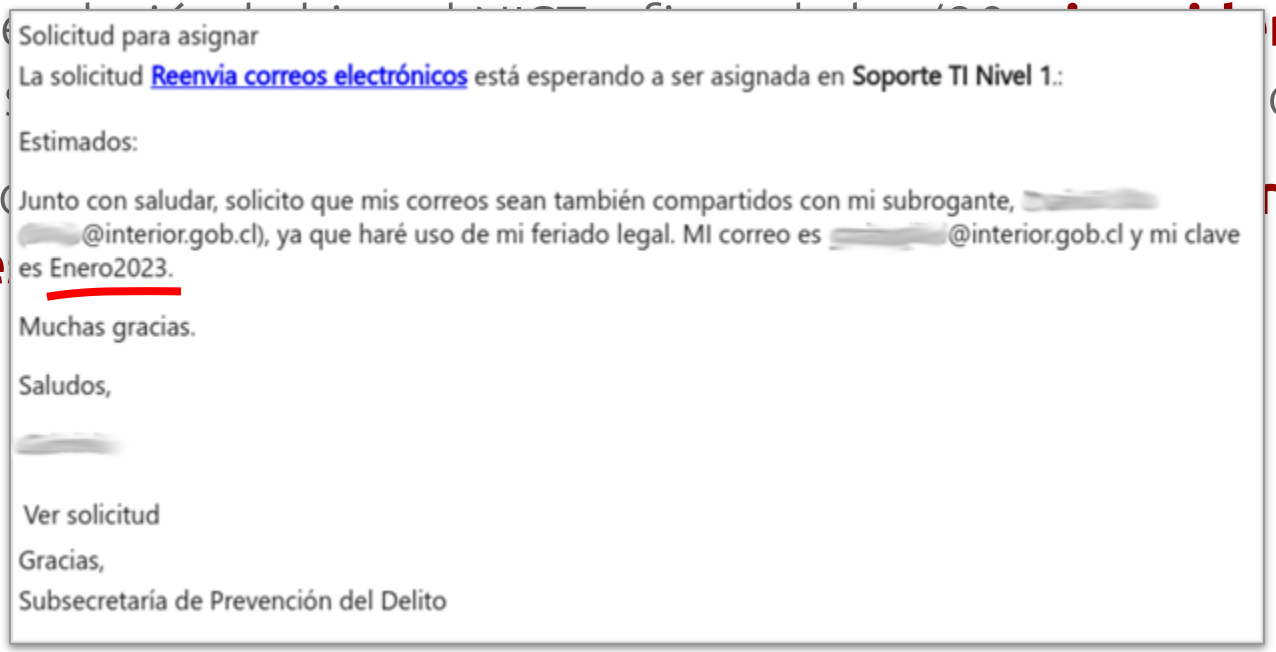
[Intermedio]

Preguntas frecuentes:
"¿Debo cambiar mis claves cada N meses?"

No, esa es una mala práctica.

Esta recome[illegible]**ncia**. Durante dos décadas[illegible]dación.

Hoy tenemo[illegible]**rds más predecible**[illegible]



Solicitud para asignar

La solicitud Reenvia correos electrónicos está esperando a ser asignada en **Soporte TI Nivel 1**.:

Estimados:

Junto con saludar, solicito que mis correos sean también compartidos con mi subrogante, [redacted]@interior.gob.cl), ya que haré uso de mi feriado legal. MI correo es [redacted]@interior.gob.cl y mi clave es Enero2023.

Muchas gracias.

Saludos,

[redacted]

Ver solicitud

Gracias,

Subsecretaría de Prevención del Delito

Preguntas frecuentes:
"¿Es seguro guardar mis claves en el email, o en Excel?"

El correo electrónico sin encriptar es muy inseguro. Nunca guardes ni envíes nada confidencial en el correo.

Nunca envíes claves por correo electrónico. Si es necesario, usa WhatsApp o Signal.

Nunca guardes tus claves en archivos en tu computador o teléfono. Eso es lo primero que busca un atacante.

3

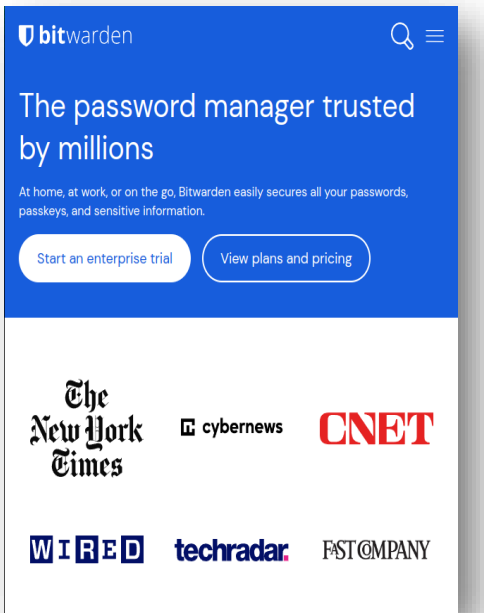
¿Qué es un gestor de claves?

Es un sitio/app que genera passwords aleatorios para cada sitio/app que requiera una clave:

https://1password.com/es

https://www.dashlane.com/es

https://bitwarden.com/



3

¿Hay alternativas locales para los desconfiados?

Por supuesto. Sin embargo, hay que balancear usabilidad vs. confidencialidad:

http://keepass.info

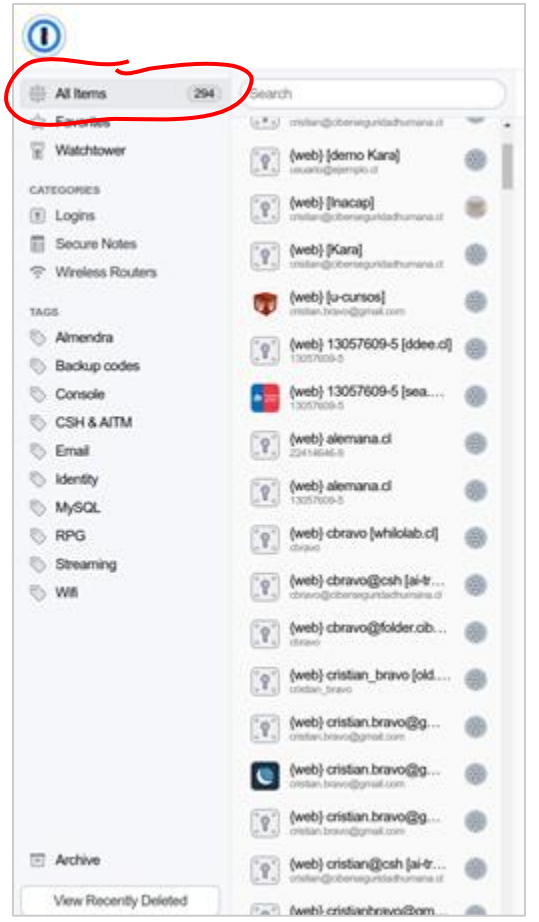
¿Por qué es importante usar un gestor de claves?

Una persona promedio tiene 25 cuentas con passwords, tipea 8 passwords al día, tiene 6.5 passwords, y cada password es compartido entre casi 4 sitios [Florencio y Herley 2007]

La recomendación de expertos es tener un password distinto para cada sitio/app/servidor

En la práctica es imposible recordar tantos passwords

Hoy es imprescindible tener y saber usar bien un gestor de claves



3

¿Ventajas y desventajas?

¿Ventajas?

- Hay que recordar una sola clave, no 300
- Generan claves aleatorias para cada sitio
- Ingresan claves de forma automática en los sitios que uno visita (y esto es muy cómodo)
- No se dejan engañar por sitios de phishing
- Algunos ofrecen 2FA integrado

¿Desventajas?

- La clave maestra tiene que ser realmente buena
- Para expertos, es molesto abrir el browser para una clave por CLI

3

“Pero ¿qué pasa si pierdo acceso al gestor de claves?”

Existe una tendencia fuerte a mantener las mismas malas claves que uno tiene, por si “pierdo acceso al gestor”.

Los gestores están hechos para hacer fácil recuperar el acceso: muchos generan una hoja de emergencia para imprimir.

Reemplaza tus claves por textos aleatorios → **¡no necesitas recordar tus claves de memoria!**

3

¿Y qué pasa si lo uso en mi teléfono?

Muchos gestores de clave tienen aplicaciones para laptop y teléfono, y sincronizan el contenido de ambos.

En el teléfono y en un Mac, permiten acceder a tus claves a través de biometría.

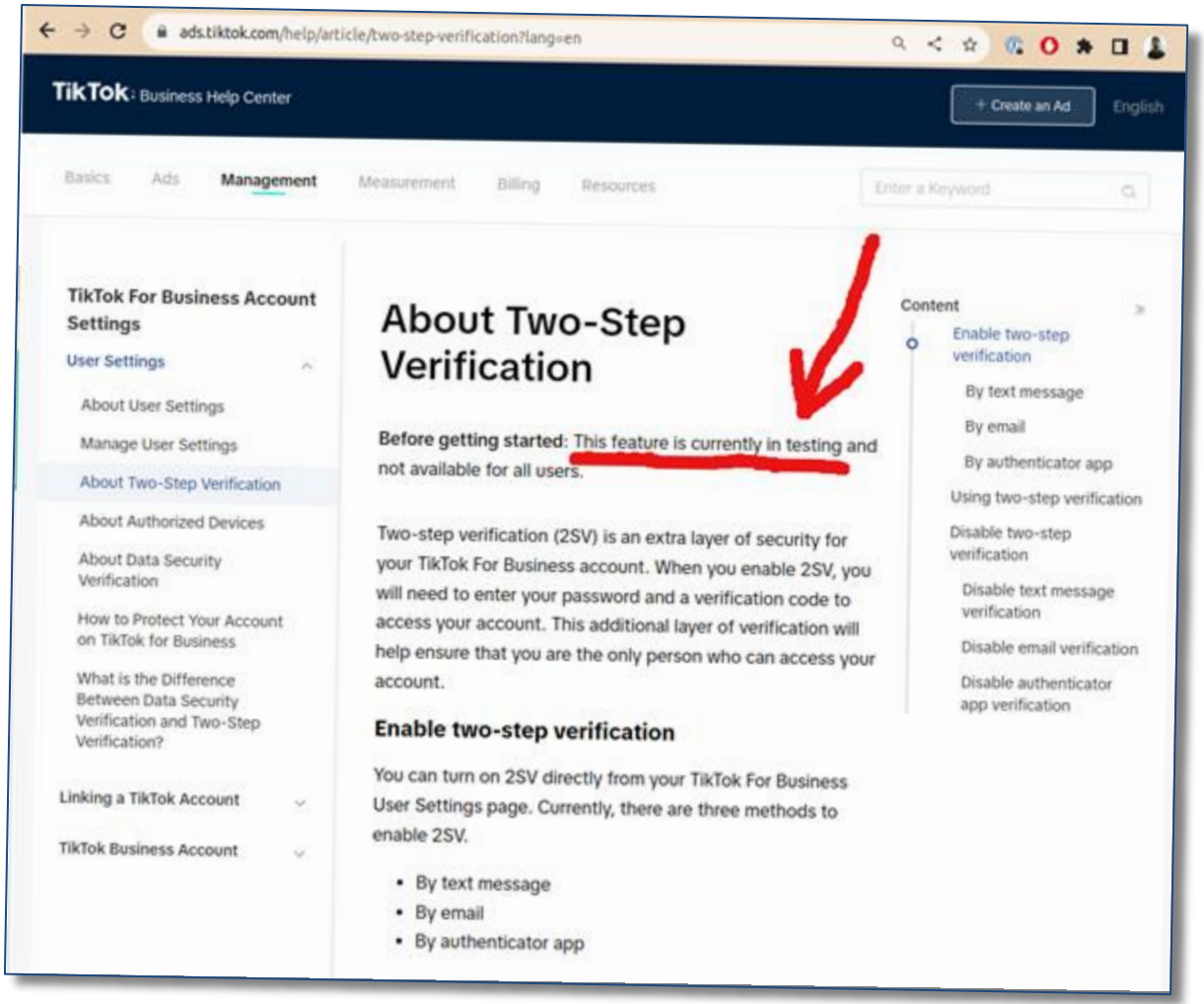
[Recomendación incómoda]

Usa doble factor de autenticación

- Es un método para restringir acceso a una cuenta:
  - Con mensajes de texto
  - Con email
  - Con passwords de una sola vez (e.g., Time-based One Time Password, o TOTP), con aplicaciones como Google Authenticator, Authy, Microsoft Authenticator
- La mayor parte de los bancos lo utilizan (algunos sólo para ciertas operaciones, como transferencias)
- La mayor parte de los servicios en línea más populares lo ofrecen de manera obligatoria: Gmail, LinkedIn, Instagram, etc.

[Recomendación incómoda]

¿Y TikTok…?



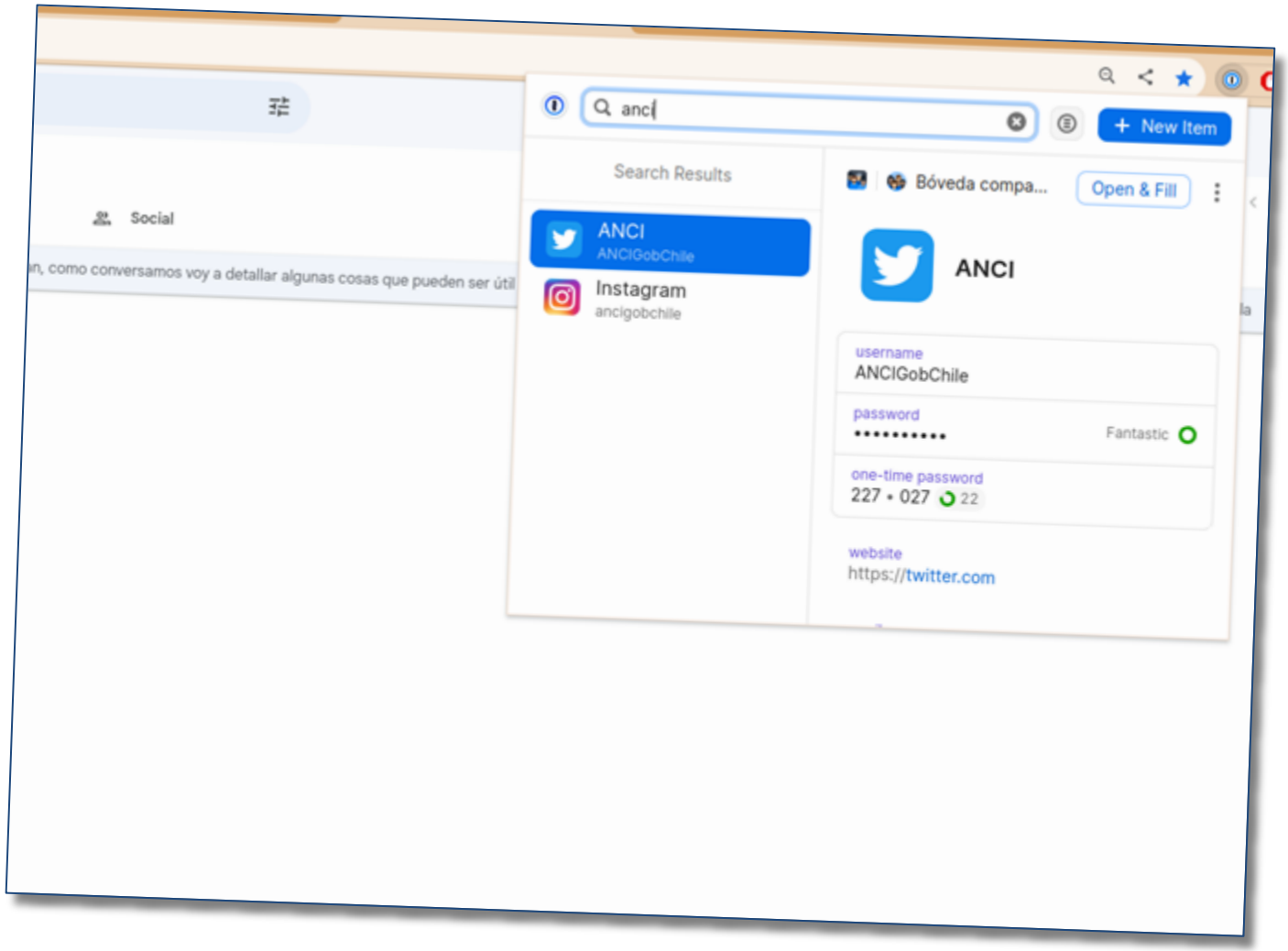
[Recomendación incómoda]

¿Por qué usar doble autenticación?

- Si alguien quiere meterse a una cuenta protegida, tiene que:
  - Saber tu clave (la puede haber adivinado o robado)
  - Tener tu teléfono
- Hoy la mayor parte de las cuentas están “conectadas”: se usan como respaldo para acceder a otras cuentas.
- Algunos gestores de clave (e.g., 1password) te permiten guardar 2FA además de claves.

[Recomendación incómoda]

Algunos gestores de clave también guardan TOTPs



¿Cómo evitar lo anterior?

1. Inventa claves con varias palabras aleatorias (passphrases)

2. Usa una tarjeta de claves

3. Usa un gestor de claves

[Intermedio con preguntas frecuentes]

[Recomendación incómoda para terminar]

¡Muchas gracias!

Cristian Bravo Lillo, Ph.D.
cbravol@interior.gob.cl