



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

Cómo crear buenas claves

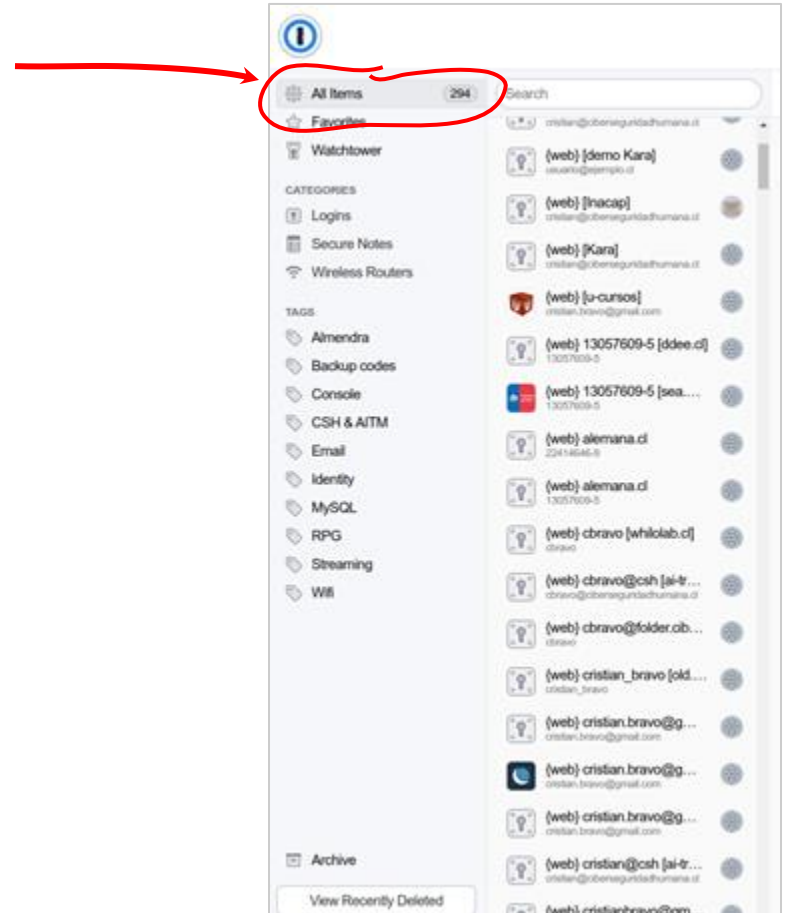
Cristian Bravo Lillo, Ph.D., Director CSIRT de Gobierno

cbravol@interior.gob.cl

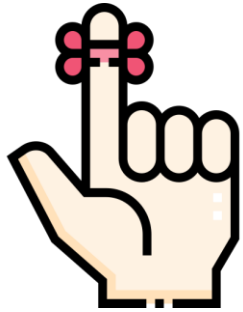
¿Por qué es importante?

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?



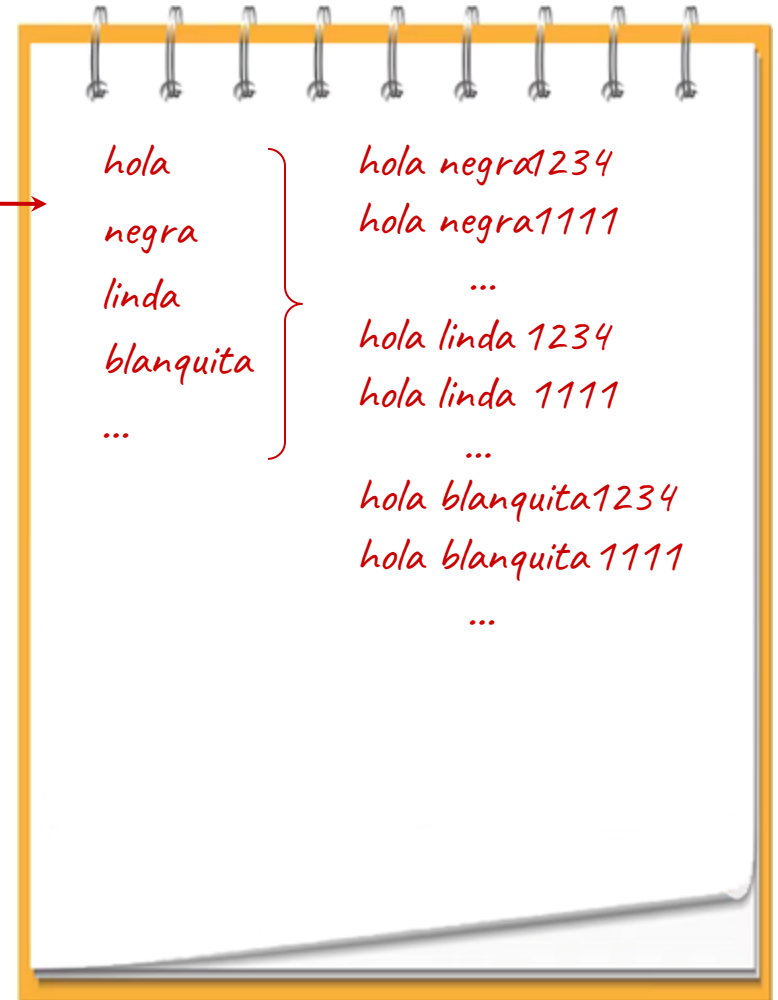
Fácil de
recordar
(por mí)

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)

2

Usa una tarjeta de claves

3

Usa un gestor de claves

[Intermedio con preguntas frecuentes]

[Recomendación incómoda para terminar]

¿Qué es una passphrase?

Trompeta
 ↓
 Trompeta4&3
 ↑
 mayúscula? signo de puntuación
 Sustituciones típicas y un número

~28 bits de entropía
 $\Rightarrow 2^{28} = 3$ días
 y 2.5 horas
 a 1000 passwords
 /segundo

NIVEL DE DIF. DE Adivinar COMPUTADOR:
FACIL

¿Era trompeta? ¿O era trombon? ¿y tenía un cero en vez de "0"?
 ¡Ah! ¡y tenía un símbolo!
 ¿Era al comienzo o al final?

correcto caballo
 batería cohete
 ↓
 4 palabras comunes escogidas al azar

~44 bits de entropía
 $\Rightarrow 2^{44} = 59$
 a 1000 passwords
 /segundo

NIVEL DE DIF. DE Adivinar UN COMPUT.
DIFICIL

Esa es una batería-cohete.
 ¡Correcto!

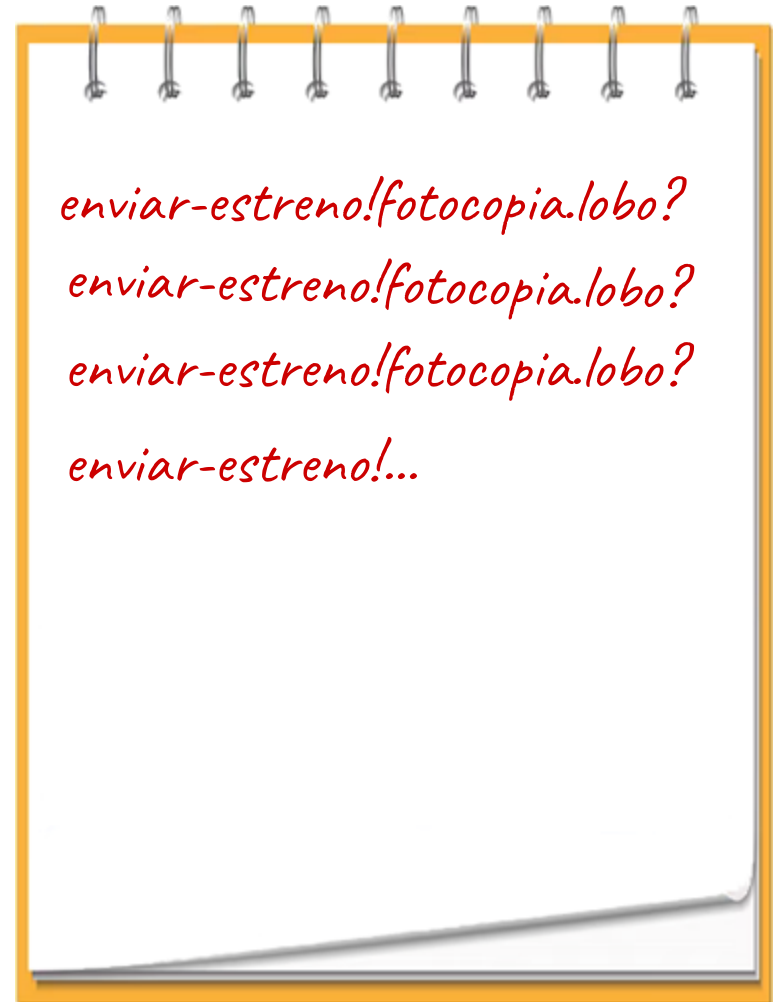
NIVEL DE DIFICULTAD DE RECORDAR PARA UN HUMANO:
¡YA LO MEMORIZASTE!



1

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)

Ejercicio: inventa una passphrase



2

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

¿Qué es una tarjeta de claves?



<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”

■ ▣ ♣ ○ ⊕ \$ □ ⊙ ↑ ♠ ♥ ♦ ◆ ? ♪ ! ▲ △ ★ ☆ € ¬ £ ¥ ☺ ; ¿ ○ ●

¹ 8QFdeSNpYk3EFneU2wakRmw32gDrm

² tmwHzdPdxd2GkMQK4eZbmVVGpqMk

³ ntxxBdZ9djHmd8t368CjEg5AjkdQG

⁴ RC9esH8BFPaLYjuyj\$mgvjwnfZykr

⁵ RhRVtw9RJZ → rEEU4EzKpA7

⁶ xYwWFFz65drGptG9ZkyFUjgMJZVWK

⁷ FPz9gTG6h2Q68pSWVWKVpCUZt8jcz

⁸ XtncUCT6vTaeKEyC9bZeG4qeyv8Dc

feca9d36dfed9d58

2

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

■ ▣ ♣ ○ ⊗ \$ □ ⊙ † ♠ ♥ ♦ ♠ ? ♪ ! ▲ △ ★ ☀ € ₣ £ ¥ ☺ ; ¿ ○ ●

1 8QFdeSNpYk3EFneU2wakRmw32gDrm
2 tmwHzdPdexd2GkMQK4eZbmVVGpqMk
3 ntxxBdZ9djHmdces5QjEg5AjkdQG
4 RC9esh8BFPaLYjuyjSmgvjwnfZykr
5 RhRVtw9RJZhNLCxt22rFEU4EzKpA7
6 xYwWFFz65drGptG9ZkyFUjgMJZVWK
7 FPz9gTG6h2Q68pSWVWKVpCUZt8jcz
8 XtncUCT6vTaeKEyC9bZeG4qeyv8Dc

feca9d36dfed9d58

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.



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



“¿Debo cambiar mis claves cada N meses?”

No, esa es una mala práctica.

Esta recomendación ha existido durante dos décadas.

Hoy tenemos

predecible



encia. Durante la implementación.

ds más

“¿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:

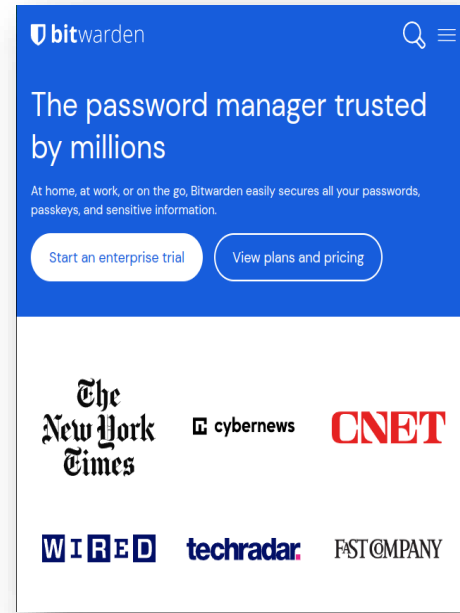
<https://1password.com/es>



<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>



The screenshot shows the official website for KeepPass Password Safe. The page layout includes a top header with the logo and 'OSI certified' badge, a left-hand navigation menu, and a main content area. The main content area features a 'Latest News' section with a sub-screenshot of the application's interface, which displays a list of entries with columns for Name, Username, Password, URL, and Notes.

Name	Username	Password	URL	Notes
Keepass 2.34	Keepass 2.34	Keepass 2.34	Keepass 2.34	Keepass 2.34
Keepass 2.33	Keepass 2.33	Keepass 2.33	Keepass 2.33	Keepass 2.33
Keepass 2.32	Keepass 2.32	Keepass 2.32	Keepass 2.32	Keepass 2.32
Keepass 2.31	Keepass 2.31	Keepass 2.31	Keepass 2.31	Keepass 2.31
Keepass 2.30	Keepass 2.30	Keepass 2.30	Keepass 2.30	Keepass 2.30
Keepass 2.29	Keepass 2.29	Keepass 2.29	Keepass 2.29	Keepass 2.29
Keepass 2.28	Keepass 2.28	Keepass 2.28	Keepass 2.28	Keepass 2.28
Keepass 2.27	Keepass 2.27	Keepass 2.27	Keepass 2.27	Keepass 2.27
Keepass 2.26	Keepass 2.26	Keepass 2.26	Keepass 2.26	Keepass 2.26
Keepass 2.25	Keepass 2.25	Keepass 2.25	Keepass 2.25	Keepass 2.25
Keepass 2.24	Keepass 2.24	Keepass 2.24	Keepass 2.24	Keepass 2.24
Keepass 2.23	Keepass 2.23	Keepass 2.23	Keepass 2.23	Keepass 2.23
Keepass 2.22	Keepass 2.22	Keepass 2.22	Keepass 2.22	Keepass 2.22
Keepass 2.21	Keepass 2.21	Keepass 2.21	Keepass 2.21	Keepass 2.21
Keepass 2.20	Keepass 2.20	Keepass 2.20	Keepass 2.20	Keepass 2.20
Keepass 2.19	Keepass 2.19	Keepass 2.19	Keepass 2.19	Keepass 2.19
Keepass 2.18	Keepass 2.18	Keepass 2.18	Keepass 2.18	Keepass 2.18
Keepass 2.17	Keepass 2.17	Keepass 2.17	Keepass 2.17	Keepass 2.17
Keepass 2.16	Keepass 2.16	Keepass 2.16	Keepass 2.16	Keepass 2.16
Keepass 2.15	Keepass 2.15	Keepass 2.15	Keepass 2.15	Keepass 2.15
Keepass 2.14	Keepass 2.14	Keepass 2.14	Keepass 2.14	Keepass 2.14
Keepass 2.13	Keepass 2.13	Keepass 2.13	Keepass 2.13	Keepass 2.13
Keepass 2.12	Keepass 2.12	Keepass 2.12	Keepass 2.12	Keepass 2.12
Keepass 2.11	Keepass 2.11	Keepass 2.11	Keepass 2.11	Keepass 2.11
Keepass 2.10	Keepass 2.10	Keepass 2.10	Keepass 2.10	Keepass 2.10
Keepass 2.9	Keepass 2.9	Keepass 2.9	Keepass 2.9	Keepass 2.9
Keepass 2.8	Keepass 2.8	Keepass 2.8	Keepass 2.8	Keepass 2.8
Keepass 2.7	Keepass 2.7	Keepass 2.7	Keepass 2.7	Keepass 2.7
Keepass 2.6	Keepass 2.6	Keepass 2.6	Keepass 2.6	Keepass 2.6
Keepass 2.5	Keepass 2.5	Keepass 2.5	Keepass 2.5	Keepass 2.5
Keepass 2.4	Keepass 2.4	Keepass 2.4	Keepass 2.4	Keepass 2.4
Keepass 2.3	Keepass 2.3	Keepass 2.3	Keepass 2.3	Keepass 2.3
Keepass 2.2	Keepass 2.2	Keepass 2.2	Keepass 2.2	Keepass 2.2
Keepass 2.1	Keepass 2.1	Keepass 2.1	Keepass 2.1	Keepass 2.1

3

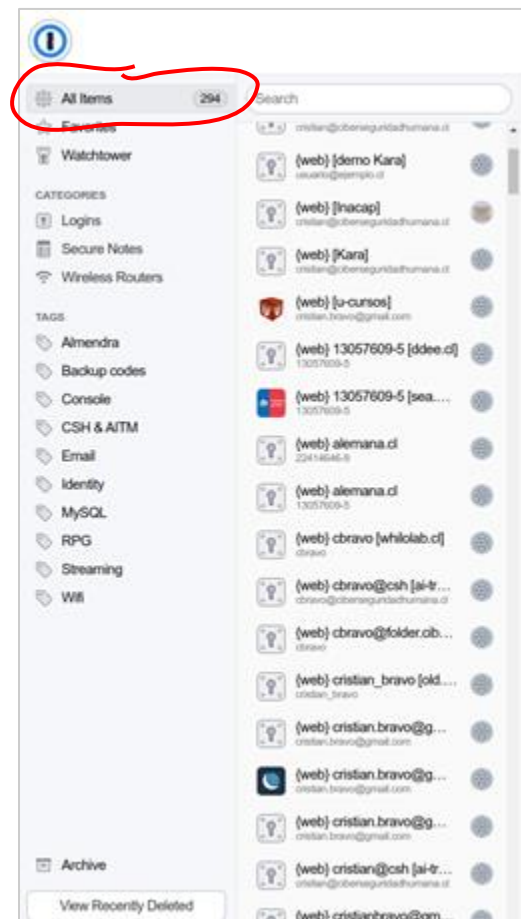
¿Por qué es importante usar un gestor de claves?

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

¿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.

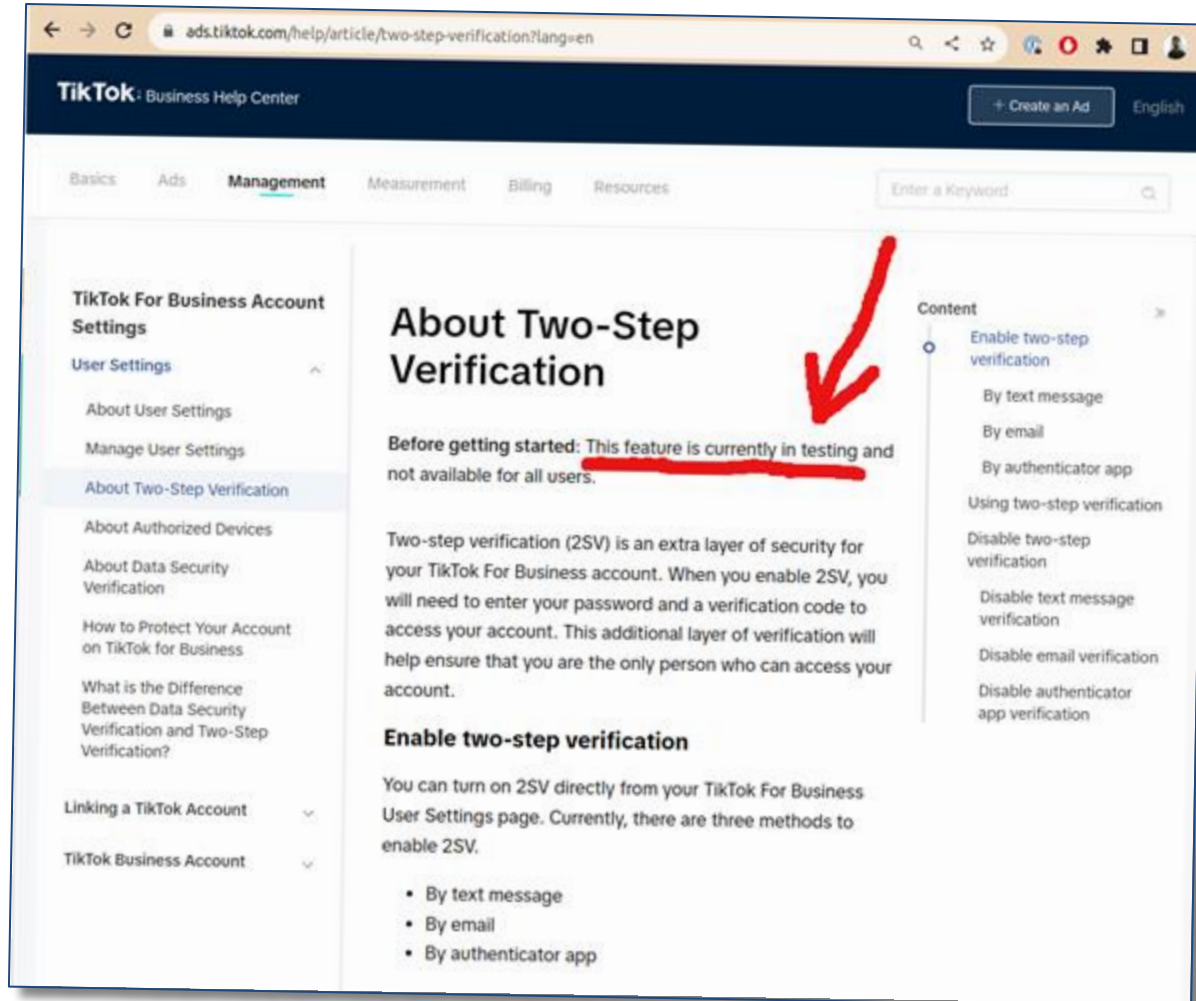
En el teléfono y en un Mac, permiten acceder a tus claves a través de biometría.

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...?



The screenshot shows the TikTok Business Help Center page for "About Two-Step Verification". The page is in English and has a dark blue header with the TikTok logo and "Business Help Center". A navigation bar includes "Basics", "Ads", "Management", "Measurement", "Billing", and "Resources". A search bar is present with the placeholder "Enter a Keyword".

The main content area is titled "About Two-Step Verification". A red arrow points to the text: "Before getting started: This feature is currently in testing and not available for all users.". Below this, the text explains that Two-step verification (2SV) is an extra layer of security for TikTok For Business accounts, requiring a password and a verification code. It lists three methods to enable 2SV: By text message, By email, and By authenticator app.

The left sidebar contains a "TikTok For Business Account Settings" menu with options like "User Settings", "About User Settings", "Manage User Settings", "About Two-Step Verification", "About Authorized Devices", "About Data Security Verification", "How to Protect Your Account on TikTok for Business", "What is the Difference Between Data Security Verification and Two-Step Verification?", "Linking a TikTok Account", and "TikTok Business Account".

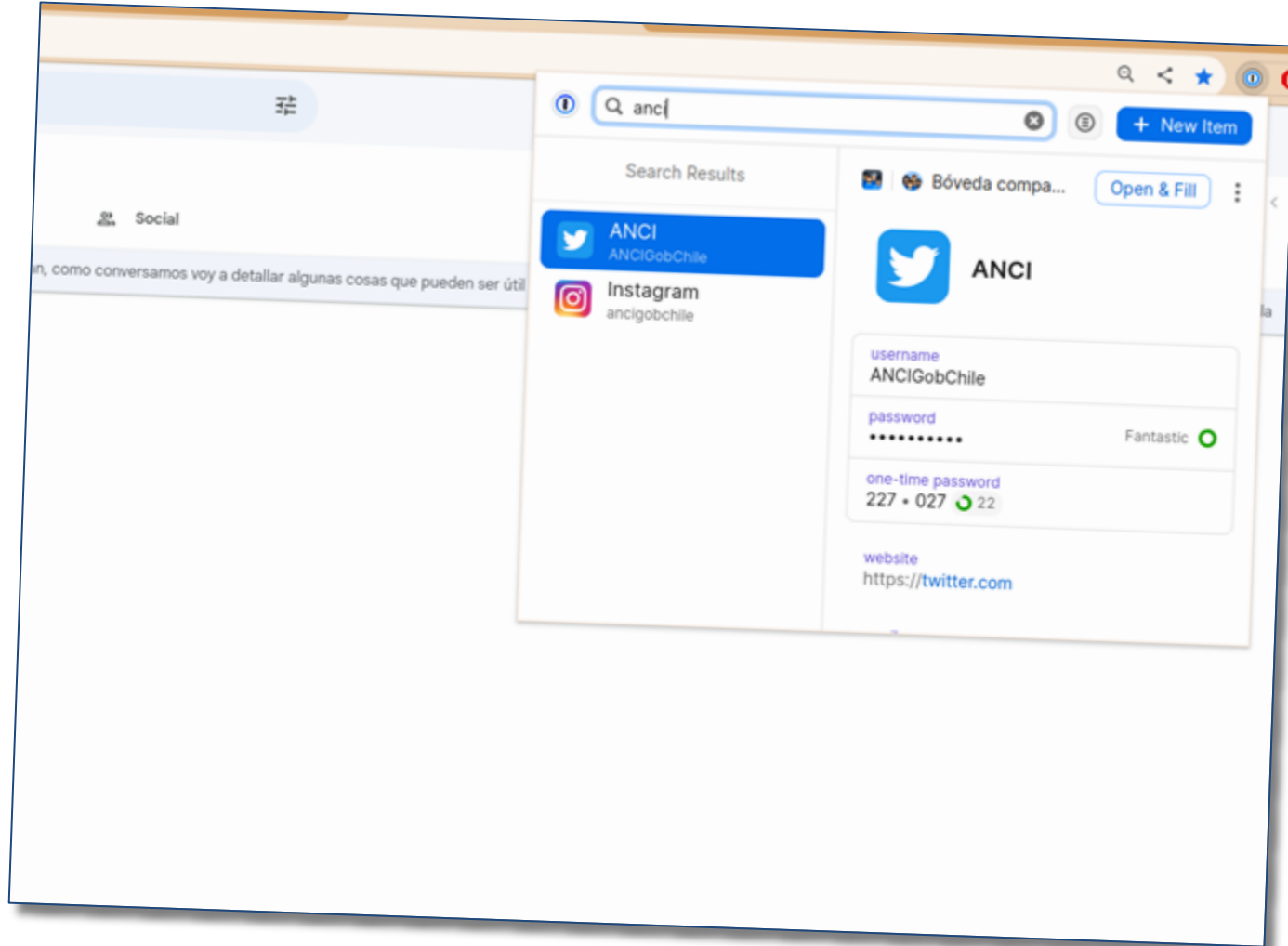
The right sidebar, titled "Content", lists various sub-topics: "Enable two-step verification", "By text message", "By email", "By authenticator app", "Using two-step verification", "Disable two-step verification", "Disable text message verification", "Disable email verification", and "Disable authenticator app verification".

¿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 TOTP



¿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