



Cinco recomendaciones básicas de protección personal en ciberseguridad

Cristian Bravo Lillo, Director CSIRT de Gobierno

cbravol@interior.gob.cl



Las cinco recomendaciones

1. Gestiona tus claves
2. Presta atención a las direcciones
3. Presta atención a las redes wifi
4. Instala las actualizaciones de seguridad de tu computador/teléfono
5. Respalda tu información

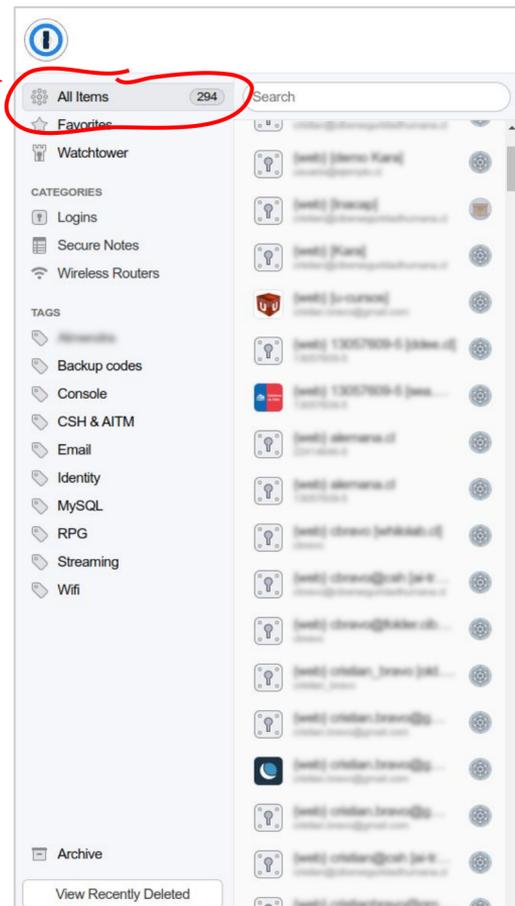
1 Gestiona tus claves

1 Gestiona tus claves

¿Por qué es importante?

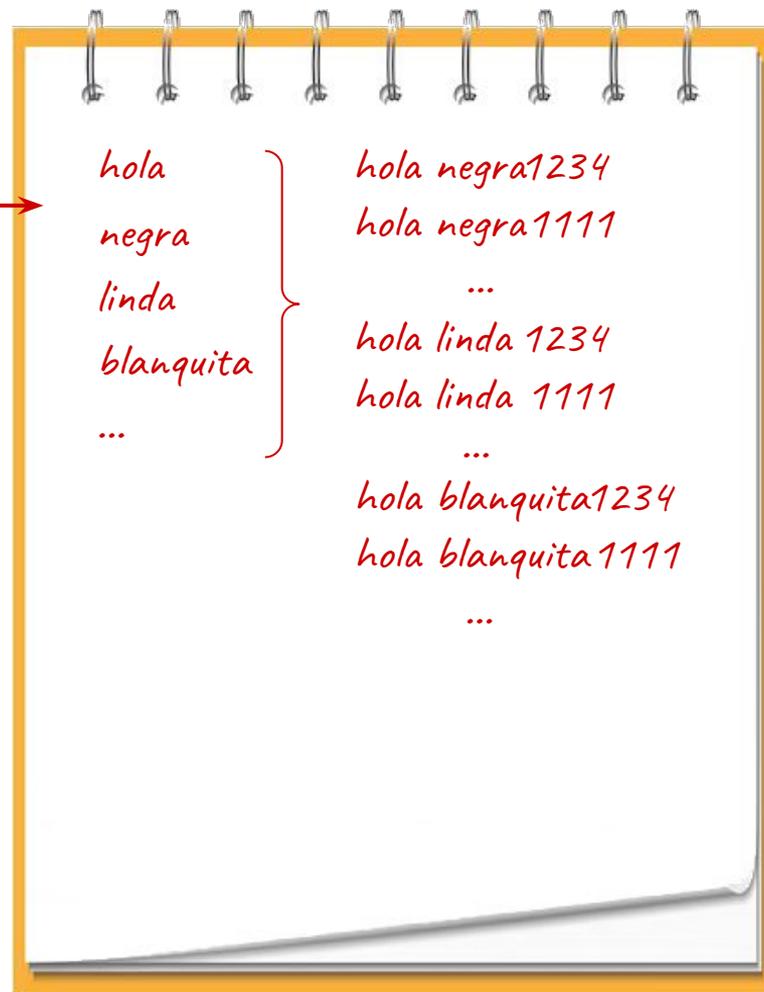
Las personas no podemos recordar tantas claves:

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



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.



1 Gestiona tus claves

¿Cómo evitar lo anterior?

Inventa claves con varias palabras aleatorias (passphrases)

Usa una tarjeta de claves

¿Qué es una passphrase?

Trompeta
 ↓
 Trompet4 & 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
 NIVEL DE DIFICULTAD DE Adivinar COMPUTADOR:
FÁCIL

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

correcto caballo
 batería cohete
 ↓
 4 palabras comunes escogidas al azar

~44 bits de entropía
 $\Rightarrow 2^{44} = 59$ años a 1000
 NIVEL DE DIFICULTAD DE Adivinar UN COMPUTADOR:
DIFÍCIL

Esa es una batería-cohete.
 ¡Correcto!
 NIVEL DE DIFICULTAD DE RECORDAR PARA UN HUMANO:
¡YA LO MEMORIZASTE!

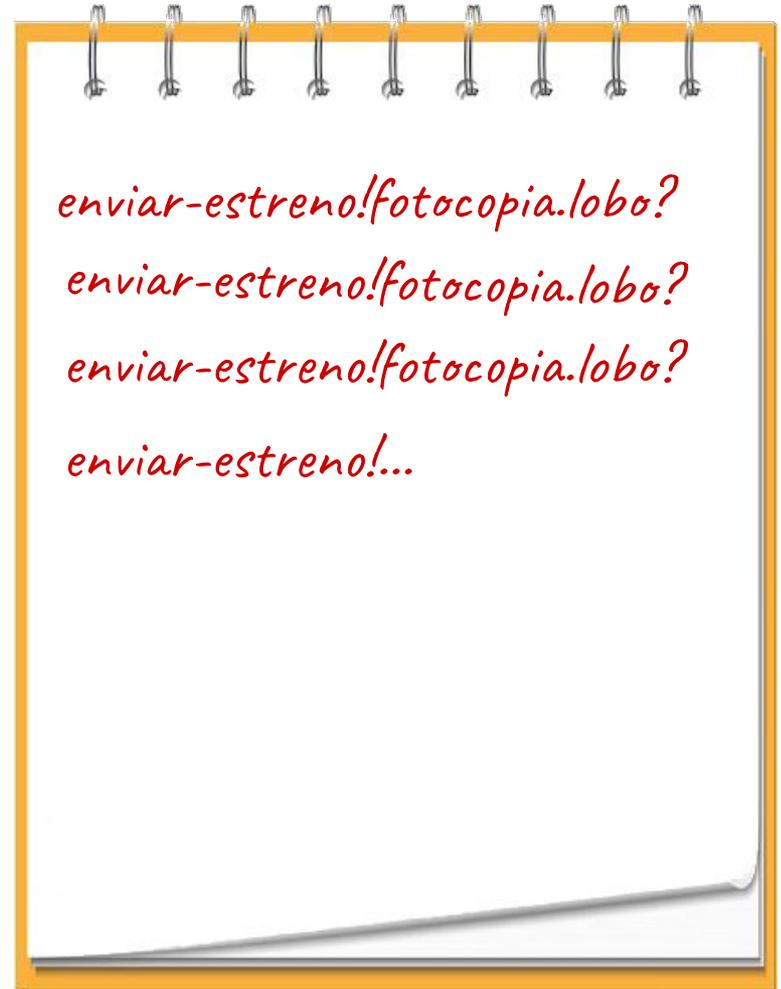


1

Gestiona tus claves

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)

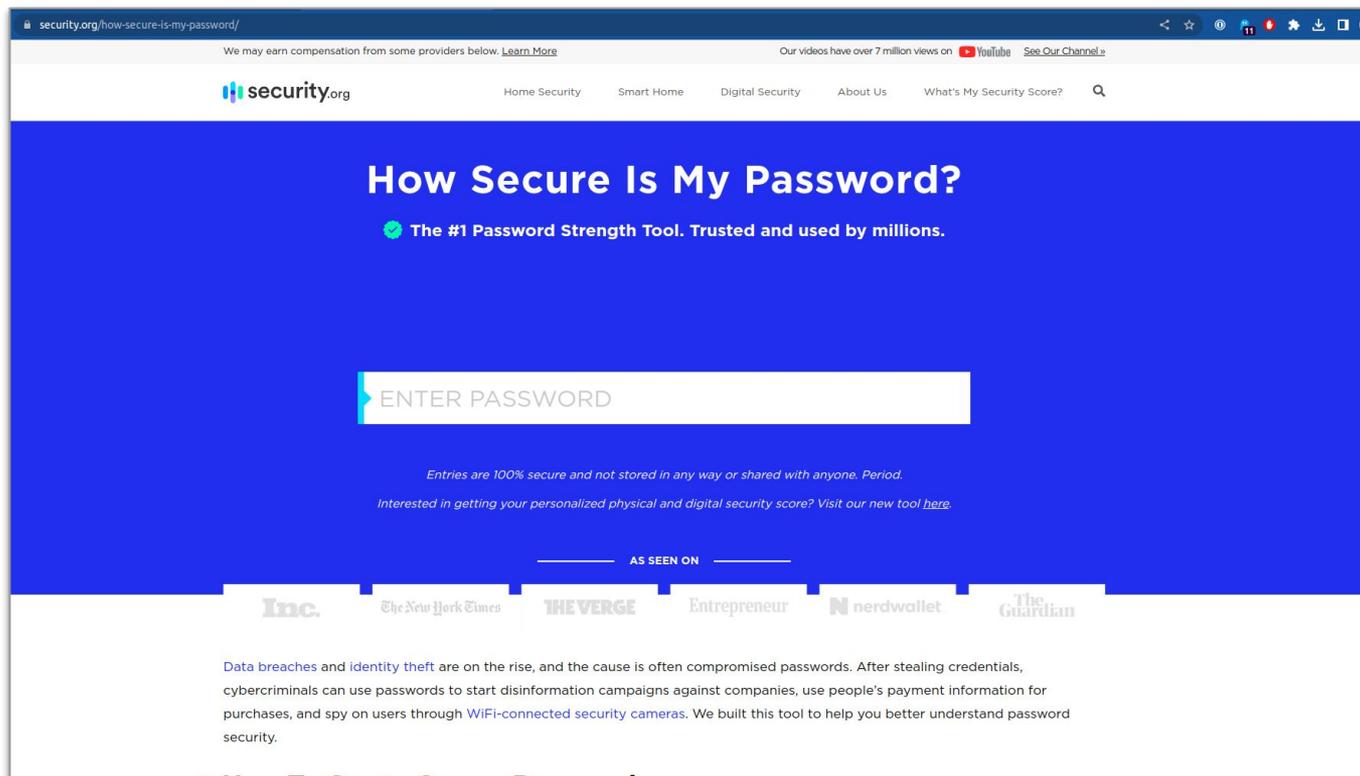
Ejercicio: inventa una passphrase



1 Gestiona tus claves

¿Cómo sé si mi clave es buena?

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



The screenshot shows the website [security.org/how-secure-is-my-password/](https://www.security.org/how-secure-is-my-password/). The page features a blue header with the security.org logo and navigation links: Home Security, Smart Home, Digital Security, About Us, and What's My Security Score?. The main content area has a large blue background with the title "How Secure Is My Password?" and a sub-headline "The #1 Password Strength Tool. Trusted and used by millions." Below this is a white input field labeled "ENTER PASSWORD". A small green checkmark icon is to the left of the sub-headline. Underneath the input field, there is a note: "Entries are 100% secure and not stored in any way or shared with anyone. Period." and a link: "Interested in getting your personalized physical and digital security score? Visit our new tool [here](#)". At the bottom, there is a section titled "AS SEEN ON" with logos for Inc., The New York Times, THEVERGE, Entrepreneur, Nerdwallet, and The Guardian. A paragraph of text at the very bottom explains the importance of password security in the context of data breaches and identity theft.

1 Gestiona tus claves

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>

¿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 ntxxBdZ9djHmd8t368CjEg5A jkdQG

4 RC9esH8BFPaLY juyjSmgvjwnfZykr

5 RhRVtw9RJZ → rEEU4EzKpA7

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.



1

Gestiona
tus claves

Preguntas frecuentes:

“¿Debo cambiar mis claves cada N meses?”

No, esa es una mala práctica.

Esta recomendación
dos décadas

Hoy tenemos
predicible

Solicitud para asignar

La solicitud [Reenvía 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

ncia. Durante
dación.

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.

2

Presta atención
a las direcciones

2 Presta atención a las direcciones

¿A qué nos referimos con “direcciones”?

A las direcciones URL y las direcciones de correo electrónico.

¿A qué poner atención? A que ambas sean legítimas:

1. **Cuando visitas un sitio web:** pon atención a la URL
2. **Cuando recibes un email:** pon atención a la dirección de correo

2 Presta atención a las direcciones

¿Porqué es importante aprender a distinguir direcciones?

En un sitio web, **todo es “falsificable”**, excepto la URL que muestra el navegador (hay formas, pero es más difícil).

En un email, **todo es falsificable**; pero la dirección del remitente es más difícil de falsificar.

2 Presta atención a las direcciones

Ejemplo: un email de phishing enviado a la Subsecretaría de Defensa desde un correo falso

zimbra

Mail Contacts Calendar

Found 51 results for: phishing

New Message

Basic Filters

- has attachment
- is flagged
- is unread

Advanced Filters

- Received from ...
- Sent to ...
- Date sent ...
- Attachments ...
- Size ...
- Status ...
- Tag ...
- Folder ...

Conditionals

Click to add before the selected bubble, or at the end. Note: AND is implied between adjacent terms.

AND OR NOT ()

De: zimbra <zimbra@sssdefensa.cl>

Fecha: 3 de julio de 2017, 04:54:22 CLT

Para: mrobledo@ssdefensa.cl

Asunto: Actualizacion de politicas de seguridad

Saludos cordiales, debido a varios intentos de ataques hemos actualizado nuestras politicas de seguridad para la seguridad de todas las cuentas de la Subsecretaria de Defensa, todos los usuarios deben conocer estas politicas de seguridad las cuales se encuentran: [AQUI](#)

TAMBIEN ME PERMITO ADJUNTAR MENSAJE MILITAR CON LAS DEBIDAS RECOMENDACIONES SOBRE POSIBLES CORREOS MALICIOSOS.....

ATTE.

Soporte de la Subsecretaria de Defensa

MES DE CSIR CIBERSEGU

18

2 Presta atención a las direcciones

Ejemplo: sitio de phishing en Subsecretaría de Defensa (continuación)



The screenshot shows a web browser window with the address bar displaying "Not secure | zimbra.ssdefensa.ml/a/login.html". The page content features the Zimbra logo, a yellow warning box with the text "Para poder configurar las opciones de seguridad de cuentas de Zimbra, tienes que verificar tu cuenta.", a password input field labeled "Contraseña:", a "Recordarme" checkbox, a "Continuar" button, and a version selector set to "Estándar (HTML)". A callout box points to the address bar with the text "zimbra.ssdefensa.ml/a/login.html".

2 Presta atención a las direcciones

Ejemplo: sitio de phishing en Subsecretaría de Defensa (continuación)

Inicio de sesión en el cl x

Not secure | zimbra.ssdefensa.ml/b/login.html

 zimbra

El nombre de usuario o la contraseña son incorrectos. Comprueba que no esté activada la tecla Bloq Mayús y vuelve a introducir el nombre de usuario y contraseña.

Contraseña:

Recordarme

Versión: [¿Qué es esto?](#)

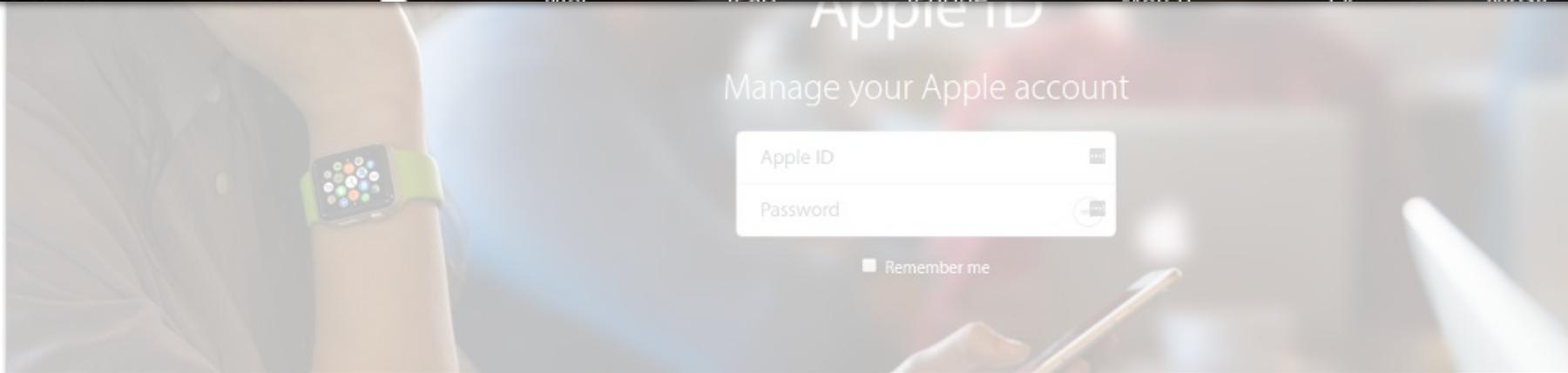
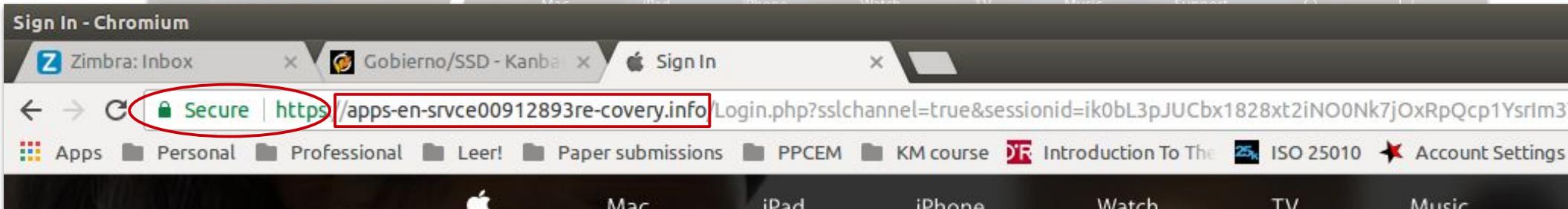
2 Presta atención a las direcciones

Ejemplo: sitio de phishing en Subsecretaría de Defensa (continuación)



2 Presta atención a las direcciones

Ejemplo: otro sitio de phishing en Subsecretaría de Defensa



2 Presta atención a las direcciones

¿Qué es una dirección URL?

Es una dirección única en el mundo para cada sitio web, documento, etc., en Internet. Tiene 4 partes:

- 1 Protocolo**, como http:// o https:// (no siempre se muestra)
- 2 Nombre de dominio**. Se lee de derecha a izquierda, y define quién controla el recurso.
- 3 Path (ruta)**. Se lee de izquierda a derecha, e indica dónde está el recurso dentro del dominio.
- 4 Parámetros**. Una serie de valores que permiten interactuar con el recurso (no siempre presentes).

https:// gob -> interior Esto es dentro del dominio

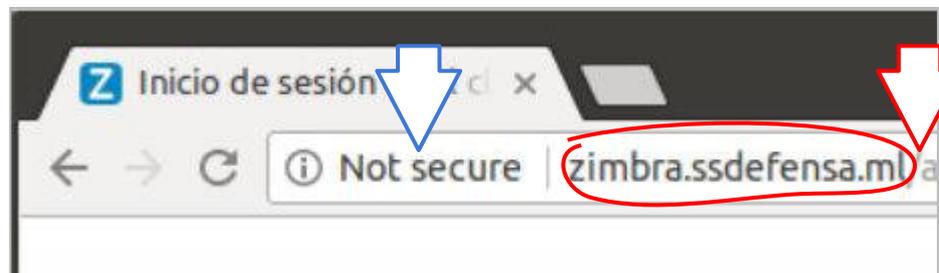


2 Presta atención a las direcciones

Asegúrate que el nombre de dominio sea legítimo y que la conexión sea segura

Cuando visites un sitio web, asegúrate que:

1. **El dominio sea legítimo** (depende de a dónde quieres ir)
2. **La conexión sea segura**



3 Presta atención a las redes wifi

3 Presta atención a las redes wifi

Todos nos conectamos a redes wifi.

Nuestros teléfonos y laptops recuerdan las wifis a las que se conectan.

Es trivial crear una red wifi con cualquier nombre, y no hay forma de saber qué hay detrás de ese nombre.

No importa que la conexión sea “segura”, porque el dueño de la Wifi puede mostrar cualquier cosa de forma segura.

¿Por qué es importante?



3 Presta atención a las redes wifi

Evita conectarte a redes wifi públicas

Una red wifi pública:

- Puede estar configurada para espiar el tráfico
- Puede estar intervenida para espiar el tráfico

Es imposible saber de antemano, así que evita conectarte → usar roaming desde tu teléfono es más seguro

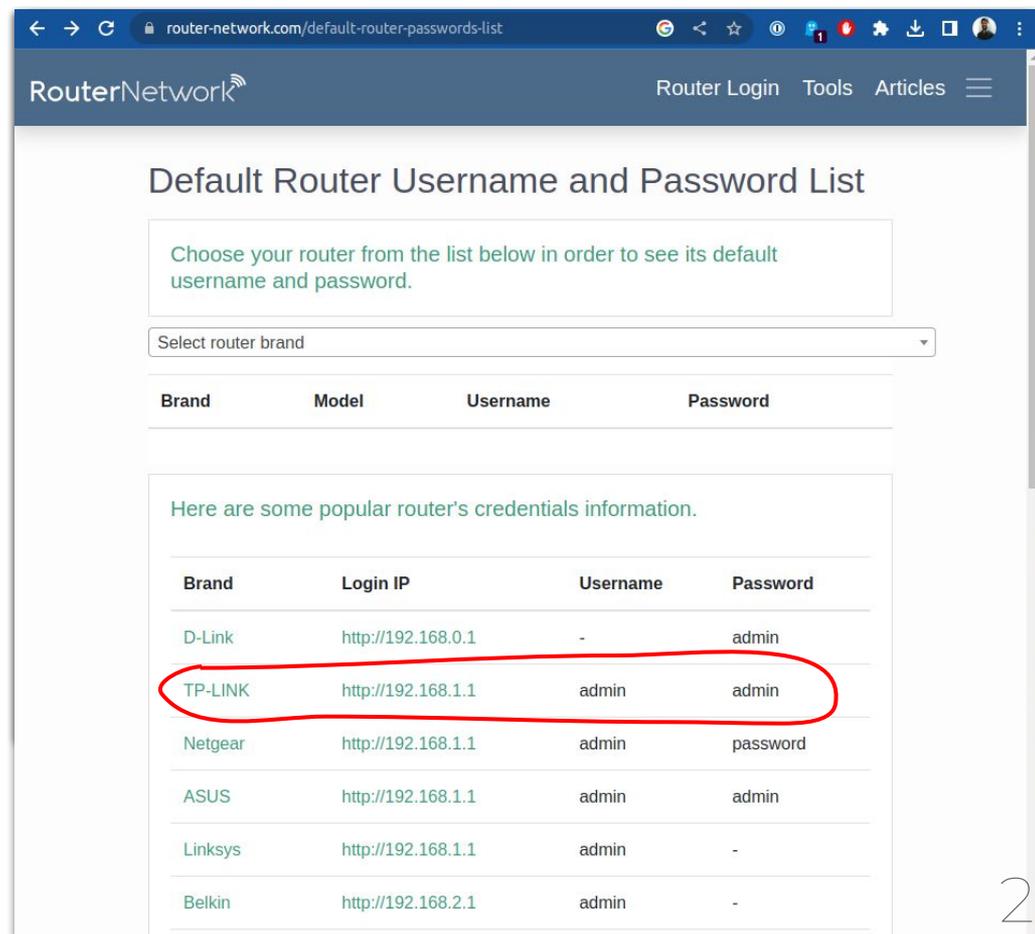


3 Presta atención a las redes wifi

Cambia la clave de administrador de tu router wifi

En tu casa, tu router wifi tiene dos claves:

- La clave de la red → a veces las personas la cambian
- La clave de administrador del router → **nadie la cambia**



The screenshot shows a web browser displaying the RouterNetwork.com website. The page title is "Default Router Username and Password List". Below the title, there is a text box that says "Choose your router from the list below in order to see its default username and password." and a dropdown menu labeled "Select router brand". Below this, there is a table with columns "Brand", "Model", "Username", and "Password". The table lists several router brands and their default credentials. The TP-LINK entry is circled in red.

Brand	Model	Username	Password
D-Link	http://192.168.0.1	-	admin
TP-LINK	http://192.168.1.1	admin	admin
Netgear	http://192.168.1.1	admin	password
ASUS	http://192.168.1.1	admin	admin
Linksys	http://192.168.1.1	admin	-
Belkin	http://192.168.2.1	admin	-

4

Instala actualizaciones de seguridad en computador y teléfono

4 Instala actualizaciones de seguridad en computador y teléfono

El 12 de mayo de 2017 ocurrió el ataque masivo conocido como WannaCry.

El gusano responsable del ransomware atacó computadores que no tenían instalado un parche de seguridad que

Microsoft había publicado un mes antes.

¿Por qué es importante instalar actualizaciones de seguridad?



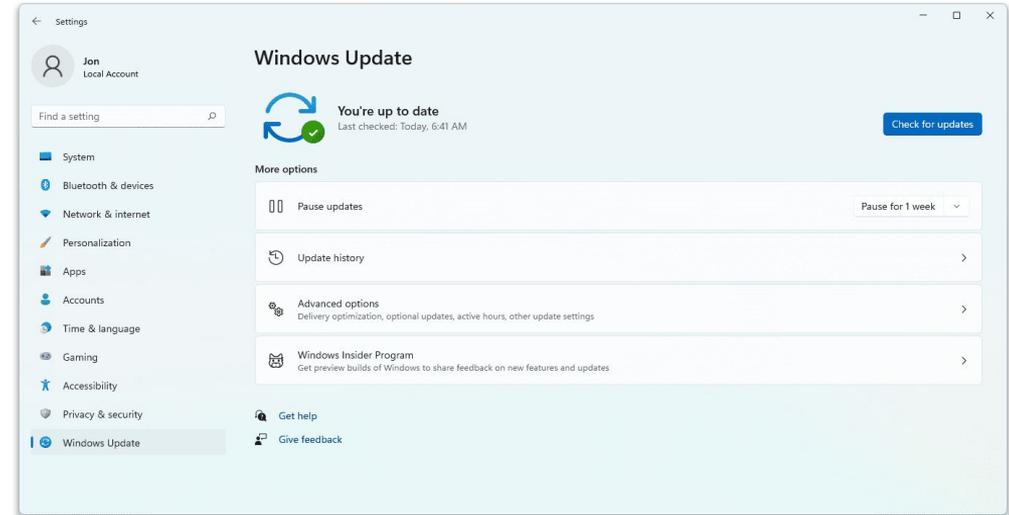
4 Instala actualizaciones de seguridad en computador y teléfono

Las actualizaciones de seguridad ayudan a corregir errores y fallas en el software que usamos.

Es posible configurar MS Windows para:

- Instalar actualizaciones de seguridad de forma automática
- Que no te moleste con actualizaciones en las horas de trabajo

¿Por qué es importante instalar actualizaciones de seguridad?



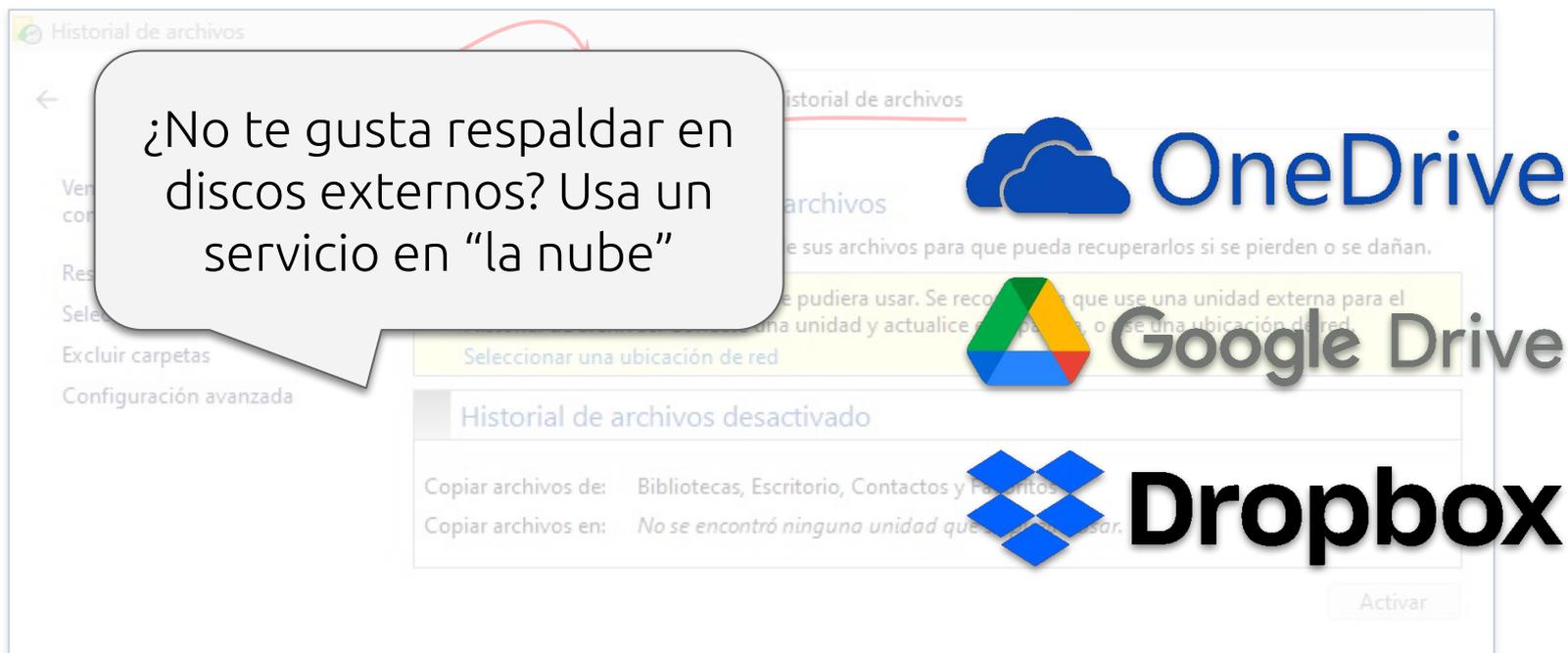
5 Respaldar tu información

5 Respalda tu información

Respalda tu información

Mantén toda la información importante (laboral y personal) respaldada → hay formas automáticas de hacerlo

¿No te gusta respaldar en discos externos? Usa un servicio en “la nube”



The image shows a screenshot of the Windows 'Historial de archivos' (File History) settings window. A speech bubble points to the settings, suggesting cloud storage as an alternative to external drives. Three cloud storage services are highlighted with their logos: OneDrive, Google Drive, and Dropbox. The OneDrive logo is blue, Google Drive is multi-colored, and Dropbox is blue. The text 'Historial de archivos desactivado' is visible, along with options to 'Copiar archivos de' and 'Copiar archivos en'. A red arrow points from the speech bubble to the 'Historial de archivos' title bar.

OneDrive

Google Drive

Dropbox

5 Respalda tu información

Es el mejor remedio contra:

- Hacking
- Ransomware
- Parejas despechadas
- Colegas enojados
- Etc., etc., etc.

Respalda tu información



¡Recuerda!

1. Gestiona tus claves
2. Presta atención a las direcciones
3. Presta atención a las redes wifi
4. Instala las actualizaciones de seguridad de tu computador/teléfono
5. Respalda tu información

¡Muchas gracias!

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

