



Cinco consejos avanzados de ciberseguridad (para usuarios dedicados)

Cristian Bravo Lillo, Director CSIRT de Gobierno

cbravol@interior.gob.cl



Los cinco consejos básicos

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

Los cinco consejos avanzados

1. Usa un gestor de claves
2. Usa doble factor de autenticación
3. Mejora la privacidad
4. Instala sólo Apps “oficiales” en tu teléfono
5. Bloquea tu computador/teléfono

¿“Bloquea tu computador”?
¡Pensé que realmente
estábamos hablando de
cosas avanzadas!



1

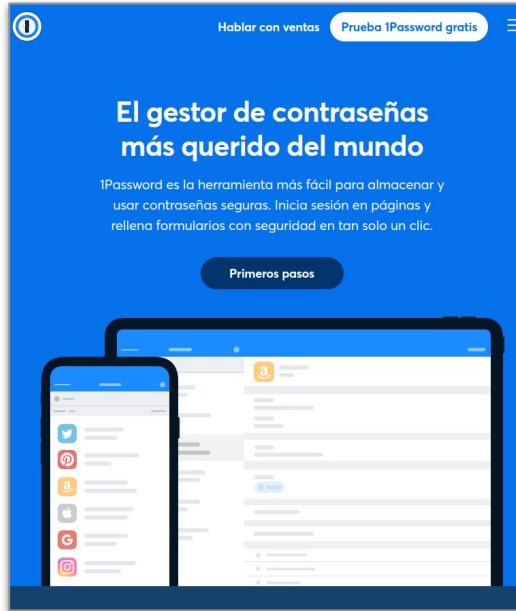
Usa un
gestor de
claves



¿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>



<http://keepass.info>



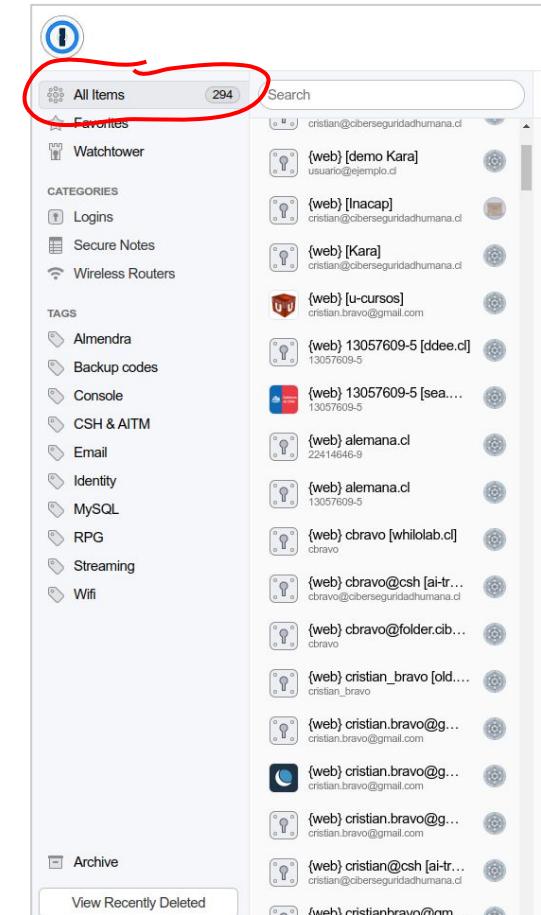
¿Por qué es importante usar un gestor de claves?

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



1

Usa un
gestor de
claves

¿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

¿Ventajas y desventajas?

¿Desventajas?

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

“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!**



The image shows a screenshot of the 1Password Emergency Kit. At the top, there is a red header with the 1Password logo and the text "1Password Emergency Kit". Below the header, it says "Created for Cristian Bravo Lillo on 1/4/2023". The main content area contains text and a list of steps. The text reads: "If you get locked out of your account, you'll need these account details to sign in — including your Secret Key, which we cannot access or recover for you." Below this, a list of three steps is provided: 1. Get your Emergency Kit off your computer and print out a copy. 2. Fill in your account password below so you don't forget it. 3. Store it somewhere safe (such as with your birth certificate, your will, or on your personal cloud storage). Below the list, there is a section titled "1Password Account Details" with fields for "SIGN-IN ADDRESS" (containing "https://my.1password.com"), "EMAIL ADDRESS" (containing "cristian.bravo@gmail.com"), and "SECRET KEY" (containing "A3-"). There is also a "PASSWORD" field with a red edit icon. To the right of the password field is a yellow key icon and a circular "Copy" icon. At the bottom left, there is a "Need help?" section with contact information: "Contact 1Password at: support@1password.com". At the bottom right, there is a "Setup Code" section with a QR code and the text: "Scan this code from the 1Password apps to set up your account quickly and easily."

¿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.



2 Usa doble
factor de
autenticación

2

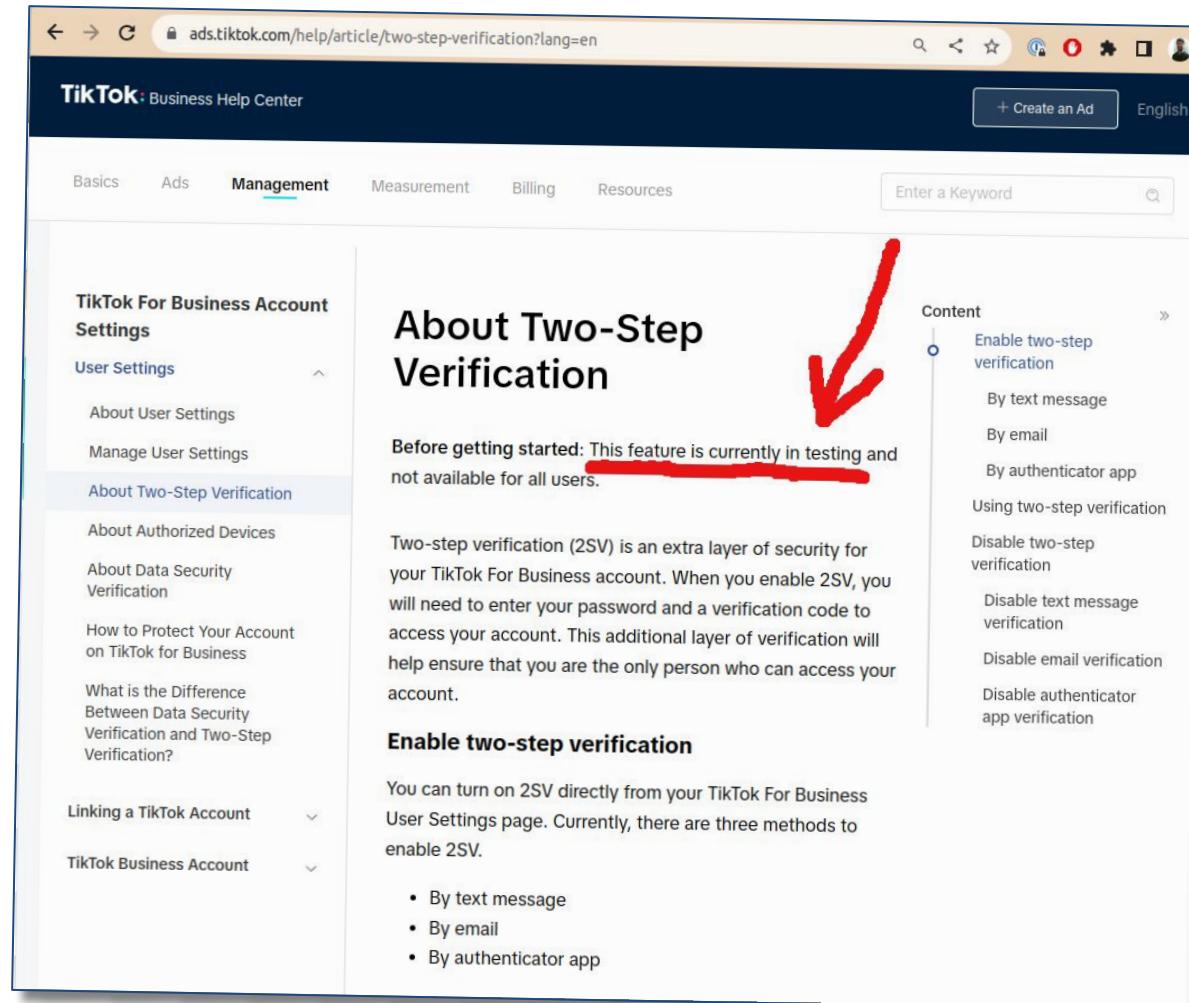
Usa doble
factor de
autenticación

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.

2 Usa doble factor de autenticación

¿Y TikTok...?



About Two-Step Verification

Before getting started: This feature is currently in testing and not available for all users.

Two-step verification (2SV) is an extra layer of security for your TikTok For Business account. When you enable 2SV, you will need to enter your password and a verification code to access your account. This additional layer of verification will help ensure that you are the only person who can access your account.

Enable two-step verification

You can turn on 2SV directly from your TikTok For Business User Settings page. Currently, there are three methods to enable 2SV.

- By text message
- By email
- By authenticator app

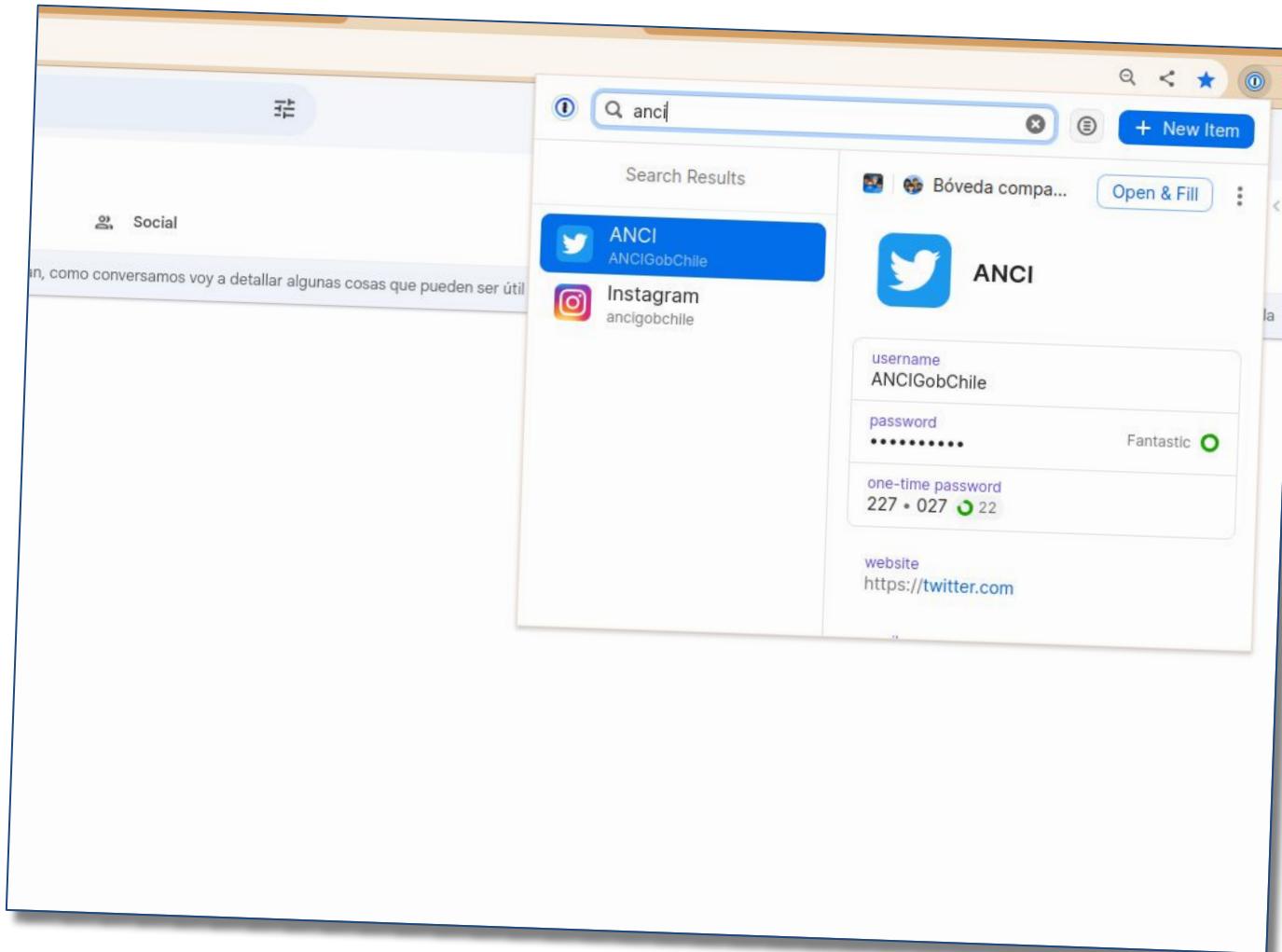
Content

- 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
- 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.

Algunos gestores de clave también guardan TOTPs



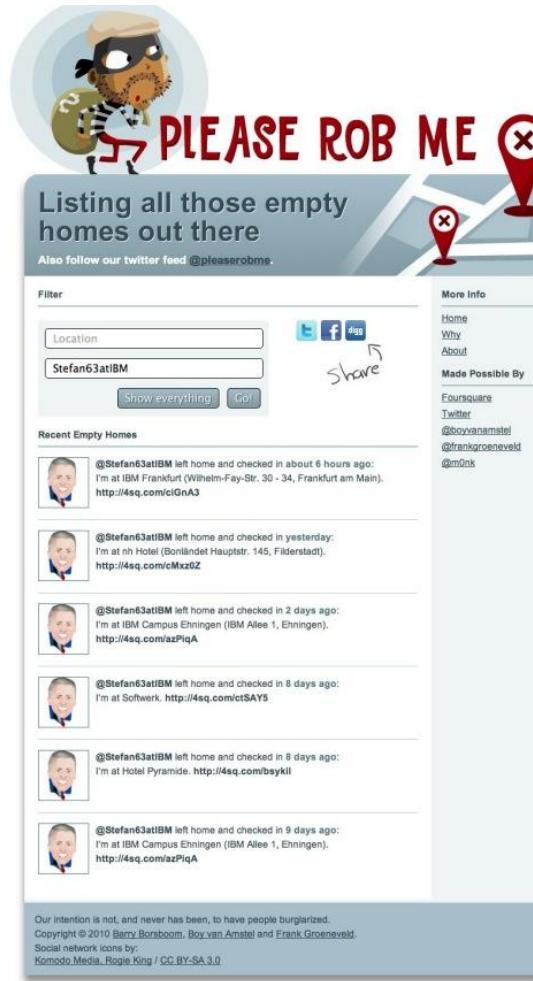
3

Mejora la
privacidad de
tu navegador



El 2010 apareció un sitio llamado pleaserobme.com.

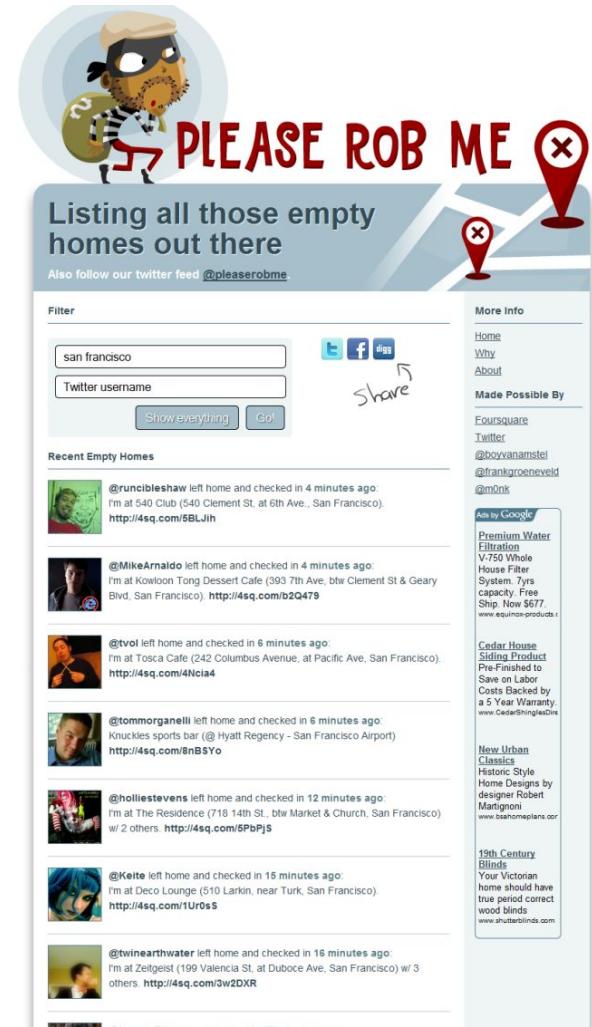
La privacidad también es ciberseguridad



The screenshot shows the homepage of [Please Rob Me](http://pleaserobme.com). The header features a cartoon illustration of a burglar with a mask and a sack, and the text "PLEASE ROB ME" in large red letters. Below the header, a sub-header reads "Listing all those empty homes out there". A "Filter" section includes a "Location" input field with "Stefan63atIBM" typed in, and "Show everything" and "Go!" buttons. To the right of the filter is a "Share" button with a social media icon. The main content area is titled "Recent Empty Homes" and lists several entries, each with a small profile picture, a tweet from the user, and a link to their location on Foursquare. The entries are as follows:

- @Stefan63atIBM left home and checked in about 6 hours ago: I'm at IBM Frankfurt (Wilhelm-Fay-Str. 30 - 34, Frankfurt am Main). <http://4sq.com/cIGnA3>
- @Stefan63atIBM left home and checked in yesterday: I'm at Hotel (Bonnlandet Hauptstr. 145, Filderstadt). <http://4sq.com/cMxzD2>
- @Stefan63atIBM left home and checked in 2 days ago: I'm at IBM Campus Ehingen (IBM Allee 1, Ehingen). <http://4sq.com/cPIqA>
- @Stefan63atIBM left home and checked in 8 days ago: I'm at Softwerk. <http://4sq.com/ctSAYS>
- @Stefan63atIBM left home and checked in 8 days ago: I'm at Hotel Pyramide. <http://4sq.com/bsykl>
- @Stefan63atIBM left home and checked in 9 days ago: I'm at IBM Campus Ehingen (IBM Allee 1, Ehingen). <http://4sq.com/cmiz2PIqA>

At the bottom, a note states: "Our intention is not, and never has been, to have people burglarized." Copyright information and social network icons are also present.



The screenshot shows the same "Please Rob Me" website, but with a different search result. The "Location" input field now contains "san francisco", and the "Share" button is visible on the right. The "Recent Empty Homes" section lists entries for users in San Francisco:

- @runcibleshaw left home and checked in 4 minutes ago: I'm at 540 Club (540 Clement St, at 6th Ave., San Francisco). <http://4sq.com/5BLJh>
- @MikeArnaldo left home and checked in 4 minutes ago: I'm at Kowloon Tong Dessert Cafe (393 7th Ave, btw Clement St & Geary Blvd, San Francisco). <http://4sq.com/b2Q479>
- @tvol left home and checked in 6 minutes ago: I'm at Tosca Cafe (242 Columbus Avenue, at Pacific Ave, San Francisco). <http://4sq.com/4Ncia4>
- @tommorganeelli left home and checked in 6 minutes ago: Knuckles sports bar (@ Hyatt Regency - San Francisco Airport) <http://4sq.com/6nBSYo>
- @holliestevens left home and checked in 12 minutes ago: I'm at The Residence (718 14th St., blw Market & Church, San Francisco) w/ 2 others. <http://4sq.com/5PbPjS>
- @Keite left home and checked in 15 minutes ago: I'm at Deco Lounge (510 Larkin, near Turk, San Francisco). <http://4sq.com/1Uro5s>
- @twinearthwater left home and checked in 16 minutes ago: I'm at Zeitgeist (199 Valencia St, at Duboce Ave, San Francisco) w/ 3 others. <http://4sq.com/3w2DXR>

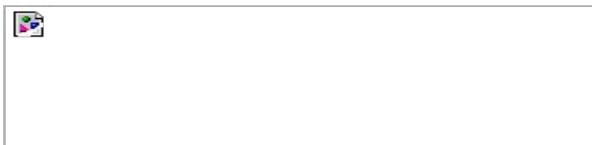
On the right side of the page, there are several sidebar sections: "More Info" (Home, Why, About, Made Possible By), "Foursquare" (Twitter, @boyvanamstel, @frankgroeneveld, @m0nk), "Recent Empty Homes" (with a list of users and their locations), "Ads by Google" (Premium Water Filtration, V-750 Whole House Filter System, Cedar House Siding Product), and "New Urban Classics" (Historic Style Home Designs by designer Robert Martignon).

Instala un bloqueador de rastreo en tu navegador

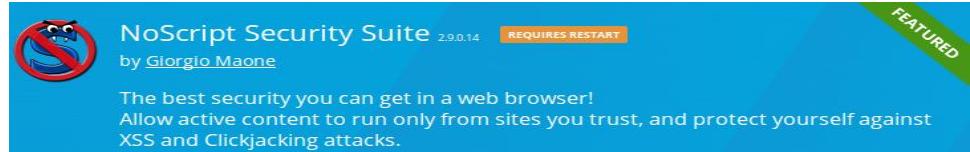
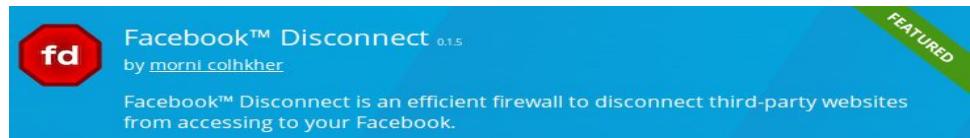
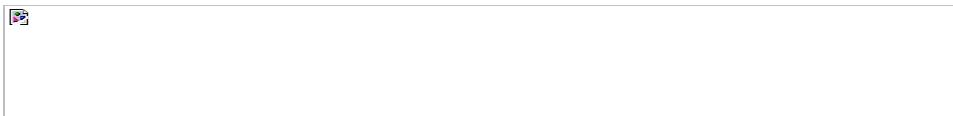
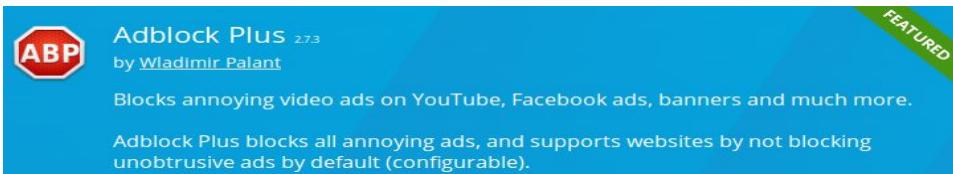
- Mientras navegas, muchos sitios recogen datos y crean perfiles tuyos para:
 - Mostrarte avisos publicitarios
 - Decidir qué venderte
 - Vender tus datos a empresas
- Es posible instalar pequeñas aplicaciones sobre tu navegador para evitar que tus datos sean recogidos

Instala un bloqueador de rastreo en tu navegador

- ¿Chrome?



- ¿Firefox?



No entregues datos que no te pidan

- Muchos sitios/organizaciones piden mucho más de lo que necesitan
- Mientras más información hay de ti afuera, más fácil es construir un perfil de ti y/o tu familia y:
 - Acosarte
 - Extorsionarte por teléfono
 - Enviarte emails de phishing dirigido (spear phishing)
 - Pedirle dinero a familiares/amigos a tu nombre
 - Etc.
- “Pero, ¿no es todo esto exagerado, considerando que estos son consejos para el usuario común?”



Una historia real...

- En 2003, en Minneapolis, EE.UU., una persona entró a una tienda Target con cupones y pidió ver al gerente:
 - “¡Mi hija recibió esto por correo! ¡Ella está todavía en [enseñanza media], y ustedes le envían cupones para ropa de bebé y cunas! ¿Están tratando de motivarla para que quede embarazada?”
- El gerente revisó los cupones y estaban dirigidos a la hija de la persona. Se disculpó y llamó algunos días después para disculparse de nuevo...



Fuente: [“How companies learn your secrets”, New York Times, 2012](#)

¿Qué fue lo que ocurrió?

- Las personas tenemos hábitos de compra muy arraigados:
 - Heredados de padres/tutores
 - Sigues comprando lo que compraste por primera vez
- Hábitos cambian sólo en momentos de grandes cambios personales:
 - **Nacimientos**, matrimonios, divorcios
 - Cambios de casa, de trabajo

Un año antes...

- Un año antes Target contrató a un estadístico llamado Andrew Pole
 - *“¿Podemos saber si una clienta está embarazada, incluso si ella no quiere que sepamos?”*
- Pole investigó listas de regalos para bebé:
 - Descubrió 25 productos que comprados en combinación predicen con gran certeza un embarazo
- Target comenzó a enviar cupones de ofertas con artículos para embarazos a un gran número de clientas en segundo trimestre de embarazo

La moraleja de la historia

- Las empresas quieren conocer tus datos porque quieren saber qué venderte:
 - *"Si usas una tarjeta de crédito, o un cupón, o llenas una encuesta, o nos envías una petición de devolución [refund], o si llamas al teléfono de ayuda de clientes, o si abres un email que te enviamos o visitas nuestro sitio web, lo registramos todo y lo asociamos a tu número de ID de cliente. Queremos saber todo lo que podamos."* [Andrew Pole, Target]
- Nada impide hoy que las empresas vendan tus datos al mejor postor:
 - ¿AFPs? ¿Isapres? ¿Empresas de seguro? ¿Hospitales y clínicas?

4

Instala sólo
apps “oficiales”

Instala sólo aplicaciones dentro de las App Stores

- Las grandes marcas tienen grupos de aplicaciones seleccionadas y revisadas:
 - Android → Google Play Store, Google Play Music
 - Iphone → iTunes Store
 - Samsung → Samsung Galaxy Apps
- **Usar aplicaciones fuera de las App Stores es un riesgo de seguridad:**
 - Aplicaciones externas son frecuentemente fuente de malware
 - Aplicaciones roban datos personales o espían al usuario

Revisa permisos y comentarios negativos de las apps en tu teléfono

- Los teléfonos obligan a las aplicaciones a pedir permiso por cada recurso al que tienen acceso: cámara, micrófono, GPS, etc.
- Muchas aplicaciones piden mucho más de lo que realmente necesitan:
 - Algunas aplicaciones piden permisos para recoger información y venderla a empresas

- Acceso completo a la red
- Leer el estado del teléfono e identidad
- Tomar fotos y videos
- Localización precisa (GPS y basada en red)
- Localización aproximada (basada en red)
- Modificar o borrar contenidos de tarjeta USB
- Ver aplicaciones corriendo en teléfono

My Talking Tom

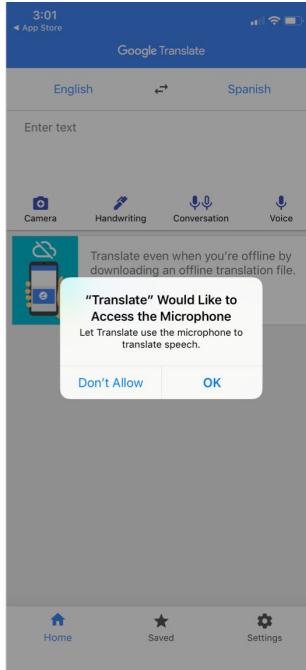
- Acceso completo a la red
- Leer el estado del teléfono e identidad
- Grabar audio
- Modificar o borrar contenidos de tarjeta USB



High-Powere...

Revisa permisos y comentarios negativos de las apps en tu teléfono

- “Pero Cristian, ¡son demasiados permisos! ¡no puedo mirarlos todos!”
 - Las aplicaciones piden permisos cuando hacen uso de ellos. Cada vez que el teléfono pide permiso para algo, **chequea si el permiso tiene sentido o no para ti en tu contexto.**



5

Bloquea tu
computador
y teléfono

Bloquea tu computador/teléfono

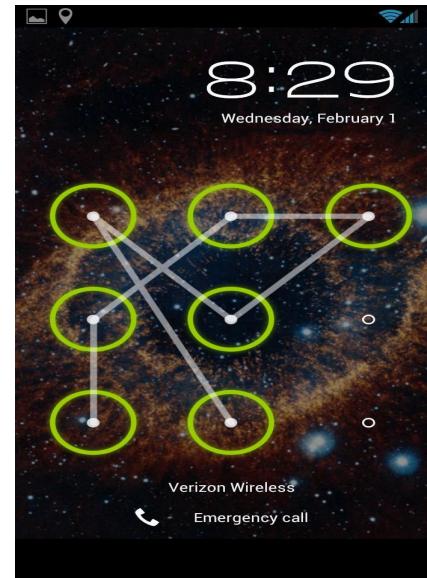
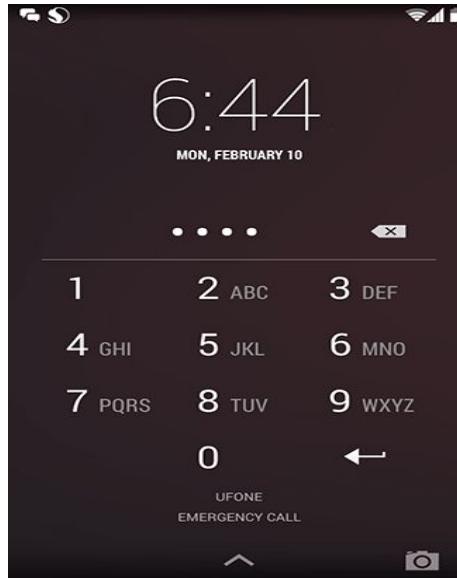
- “¿Qué significa *bloquear mi computador*?”
 - Configurarlo para que pida password cada vez que me ausento
 - Configurarlo para que se bloquee automáticamente luego de 2/3 minutos de inactividad

En Mac:



Bloquea tu computador/teléfono

- “¿Qué significa *bloquear mi teléfono*?”
 - Configurarlo para que pida pin/password/patrón cada vez que ocupo el teléfono
 - Configurarlo para que se bloquee automáticamente



Preguntas usuales

- “¿Porqué debo bloquear mi computador en la oficina?”
 - Para evitar que otros vean mi información, mis emails, documentos, etc.
 - Para evitar que alguien se haga pasar por mí
 - Para evitar que alguien instale un malware
 - Para evitar que alguien envíe un email a mi familia pidiendo dinero
 - Etc.



Las cinco recomendaciones

1. Usa un gestor de claves
2. Usa doble factor de autenticación
3. Mejora la privacidad de tu navegador
4. Instala sólo Apps “oficiales” en tu teléfono
5. Bloquea tu computador/teléfono



¡Muchas gracias!

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

