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 clav
2. Usa doble factor de
3. Mejora la privacidad d
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

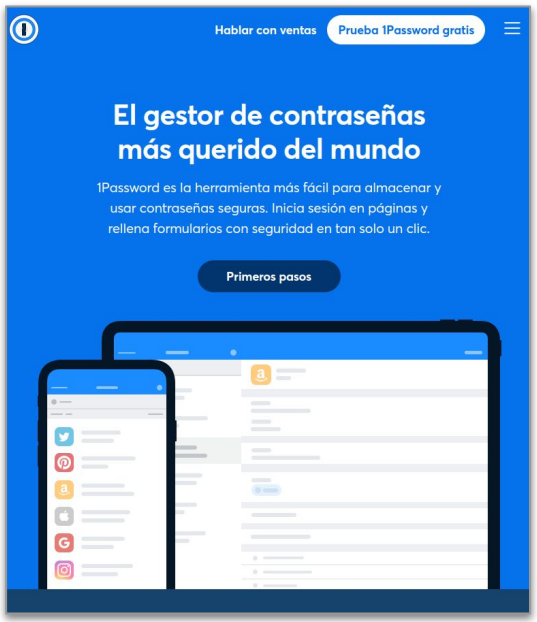
Usa un gestor de claves

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

MES DE LA CSIRT CIBERSEGURIDAD

1 Usa un gestor de claves

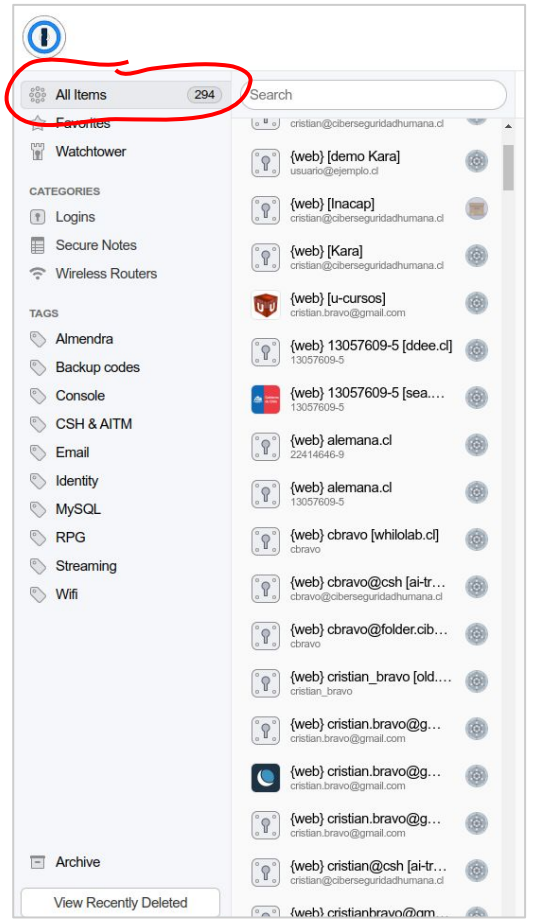
¿Por qué es importante usar un gestor de claves?

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



¿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?

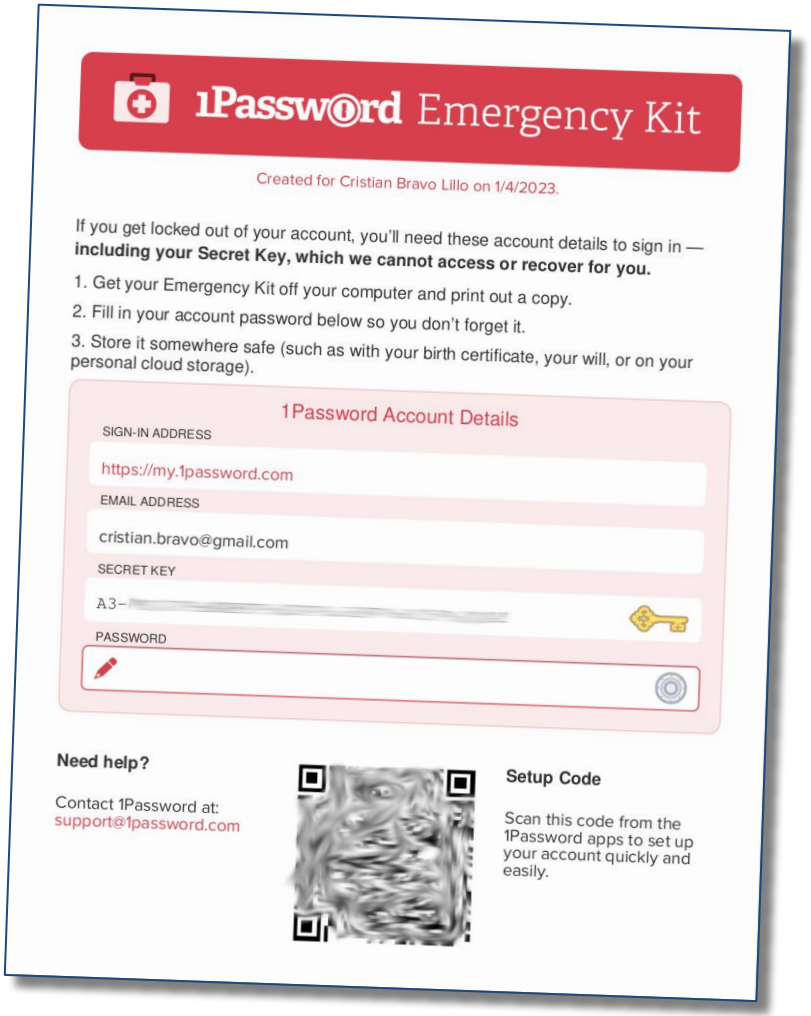
- La clave maestra tiene que ser realmente buena
- Para expertos, es molesto abrir el browser para una clave por CLI

“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!**



¿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

MES DE LA CSIRT CIBERSEGURIDAD

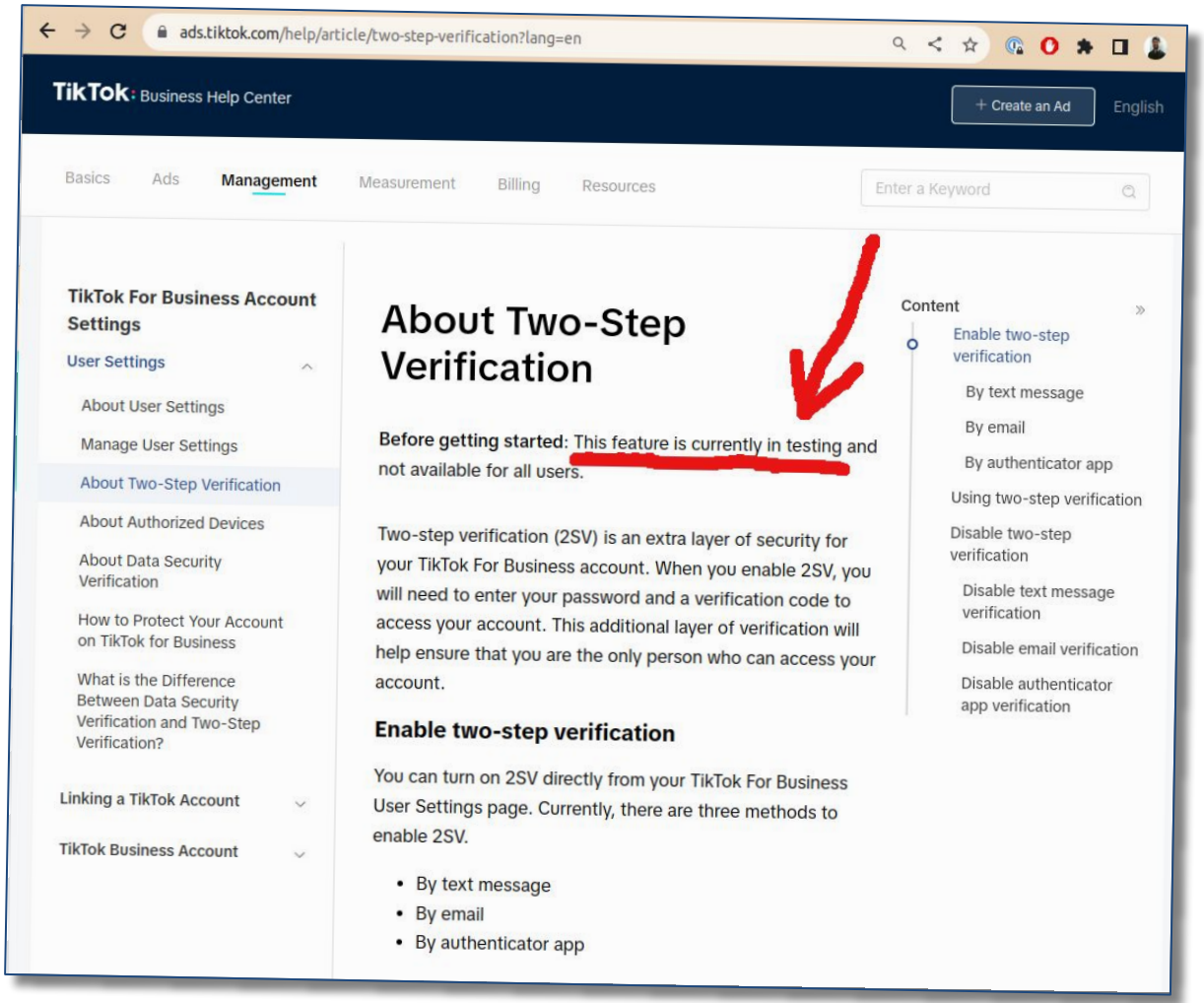
2 Usa doble factor de autenticación

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…?

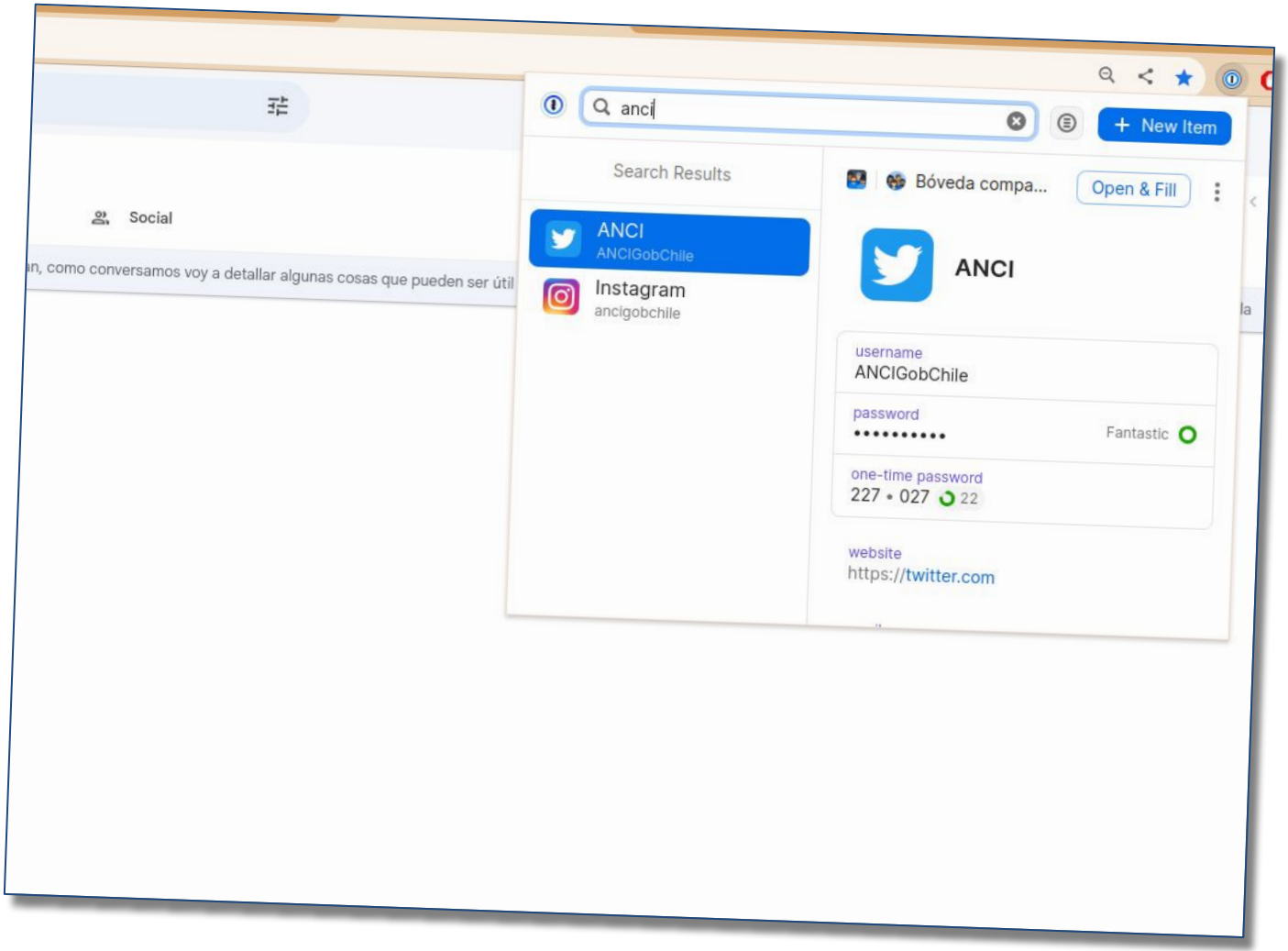


MES DE LA CIBERSEGURIDAD CSIRT

¿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.

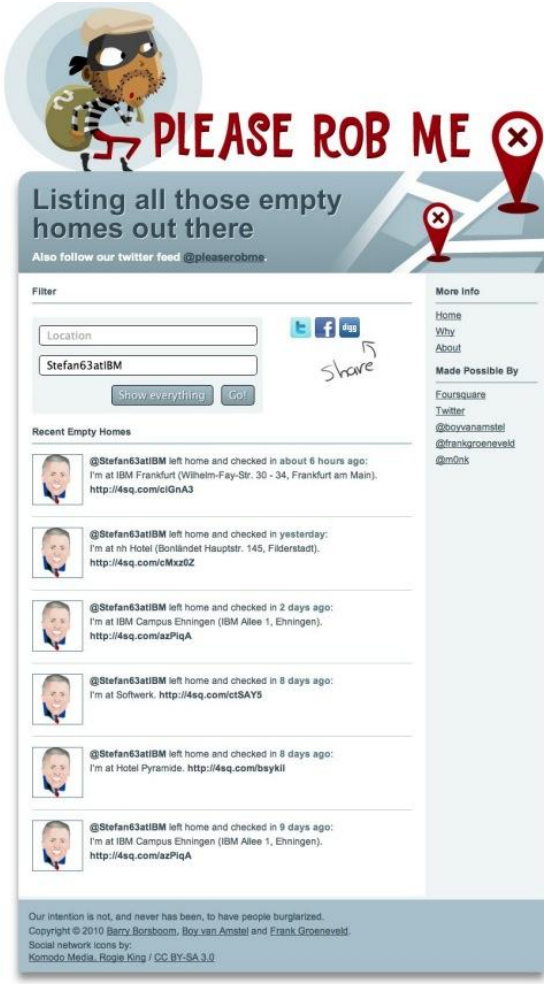
Algunos gestores de clave también guardan TOTPs

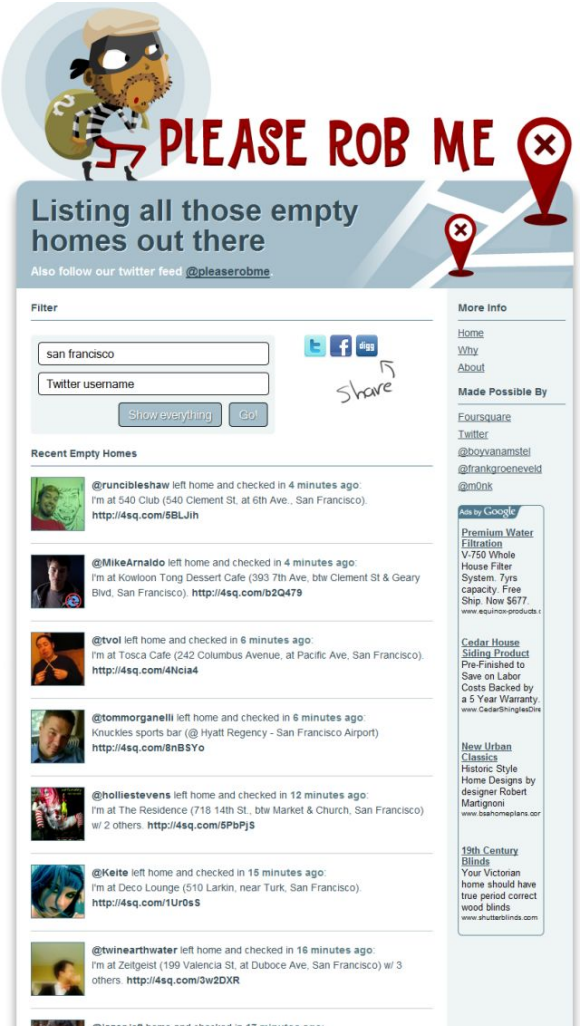


3 Mejora la privacidad de tu navegador

La privacidad también es ciberseguridad

El 2010 apareció un sitio llamado pleaserobme.com.





Instala un bloqueador de rastreo en tu navegador

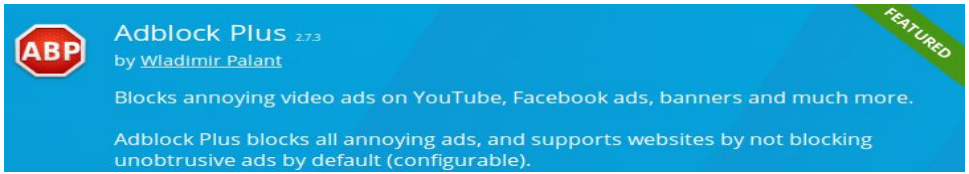
- Mientras navegas, muchos sitios recogen datos y crean perfiles tuyos para:
  - Mostrarte avisos publicitarios
  - Decidir qué venderte
  - Vender tus datos a empresas

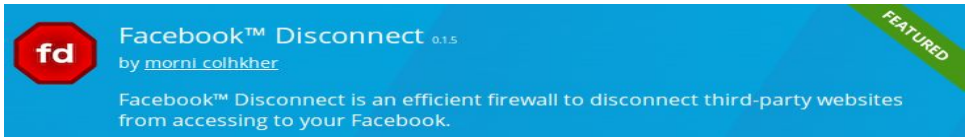
- Es posible instalar pequeñas aplicaciones sobre tu navegador para evitar que tus datos sean recogidos

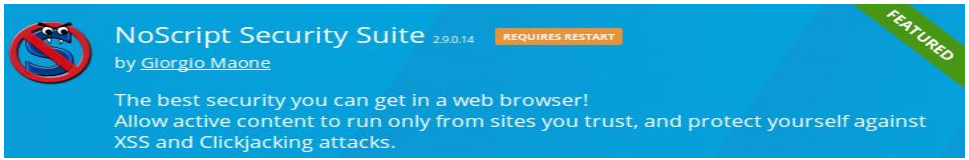
Instala un bloqueador de rastreo en tu navegador

- ¿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?

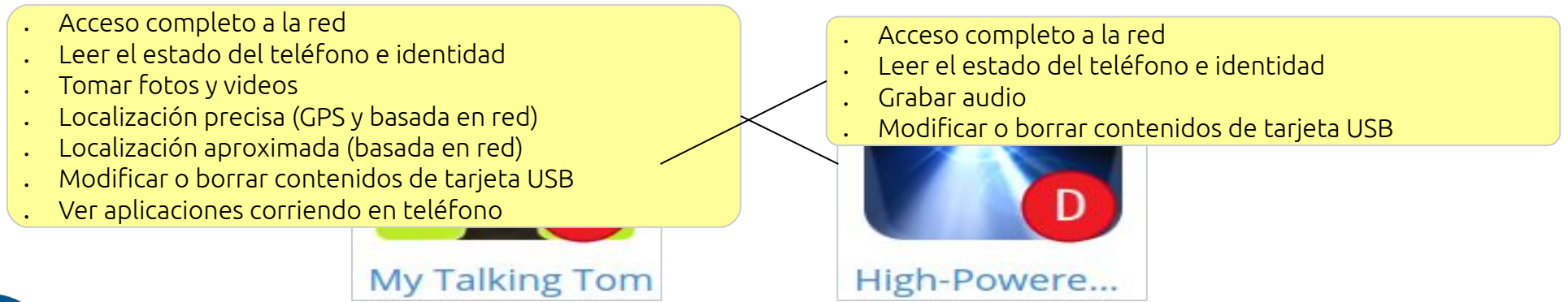
4 Instala sólo apps “oficiales”

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

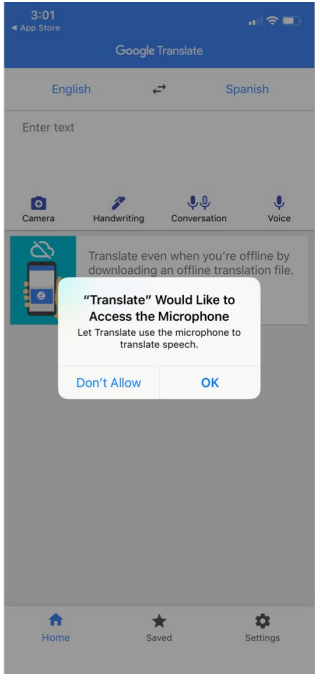
- Los teléfonos obligan a las aplicaciones a pedir permiso por cada recurso al que tienen acceso: cámara, micrófono, GPS, etc.
- Muchas aplicaciones piden mucho más de lo que realmente necesitan:
  - Algunas aplicaciones piden permisos para recoger información y venderla a empresas



Información obtenida de PrivacyGrade: http://privacygrade.org/

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

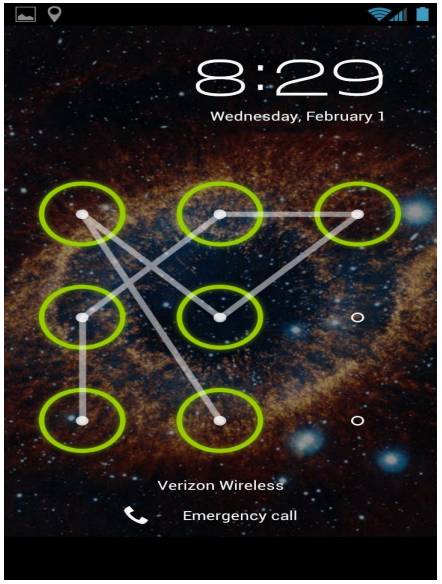
Bloquea tu computador/teléfono

- "¿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