Colaboradores y visitantes

Desde que comenzamos con Weiba recibimos muchos colaboradores que compartieron su conocimiento, su tiempo y su energía con nosotros. Nos han ayudado con la gran carga administrativa que implica llevar adelante nuestra misión.

Aquí presentamos un breve resumen de todos estos colaboradores y visitantes

---

Bethan Gee

Viajera de Denver, Colorado (Estados Unidos).

Intereses: Promover una mirada internacional de la justicia social y conocer el mundo social y académico de manera bilingüe, en español e inglés. LinkedIn

---

César González

Investigador independiente y abogado (UBA).

Intereses: Cine de culto, regulación de telecomunicaciones, derecho informático y gobernanza de internet.

Catalina González

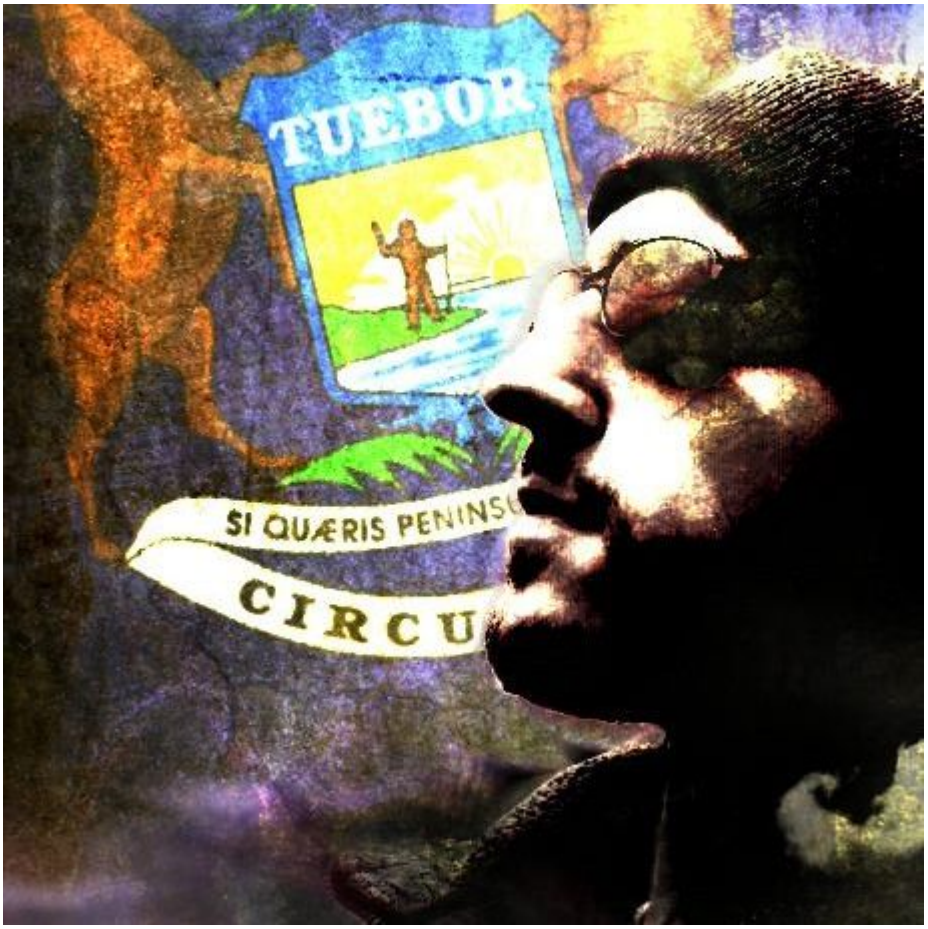
Estudiante avanzada de Relaciones Internacionales e investigadora en el IDICSO (Universidad del Salvador).

Intereses: Análisis de política pública y comparada, la gobernanza de internet, gestión de riesgos y la asistencia humanitaria.

Christine Wilson

Graduada en lengua y literatura rusa. Especialista en estudios de cultura rusa, con conocimiento de turco y español.

Intereses: Acceso a la tecnología, prevención de acciones censura y propaganda.



Noah Corradin

Más de 8 años de experiencia en el campo laboral de la seguridad informática en Silicon Valley.

Intereses: Ayudar a organizaciones sin fin de lucro con la esperanza de influir y realizar un impacto positivo en la sociedad a través de la tecnología.

Encuesta sobre seguridad y protección en línea de usuarios argentinos

Para conocer mejor como se protegen y cuidan los usuarios argentinos, te pedimos que nos ayudes con esta encuesta sobre seguridad y protección en linea!

Conocer más sobre la campaña ProtegerTE es ProtegerME

Lanzamiento de la campaña Protegete Protegeme

¿Por qué lanzamos la campaña Protegete Protegeme? Cuando somos chicos, nuestros padres nos han advertido “no hagas esto porque puede pasar tal cosa”, “no hables con extraños”, “no recibas regalos de desconocidos” y otras tantas enseñanzas que se presentaban como medidas para cuidar nuestra integridad.

Sin embargo en ese entonces, y en la actualidad, nadie nos ha enseñado otro tipo de precauciones que también tienen que ver con nuestra integridad en relación a la tecnología. Poco se dice sobre los riesgos que implica nuestra interacción con

ella, las consecuencias que podemos sufrir o el impacto negativo que pueden causar en nosotros y en nuestro entorno.

¿Por qué sabemos tan poco acerca de nuestra propia seguridad?

Existen varias explicaciones para entender porqué no sabemos protegernos. Una de ella tiene que ver la falta de educación familiar y escolar respecto de nuestra relación con la tecnología. Internet, sus aplicaciones y los diferentes dispositivos que usamos en nuestro uso diario llegaron sin aviso. Simplemente nos adaptamos al uso cotidiano, desconociendo por completo qué riesgos vienen de la mano con ellos.

Al mismo tiempo se encuentra la sobremotivación del uso de la tecnología solamente para cuestiones de entretenimiento y comunicación en línea, impulsando el uso de herramientas que se facilitan “gratuitamente”.

Por último, muchas veces desconocer implica nunca hacerse una pregunta inicial, ya que no podemos reflexionar sobre aquello que no conocemos.

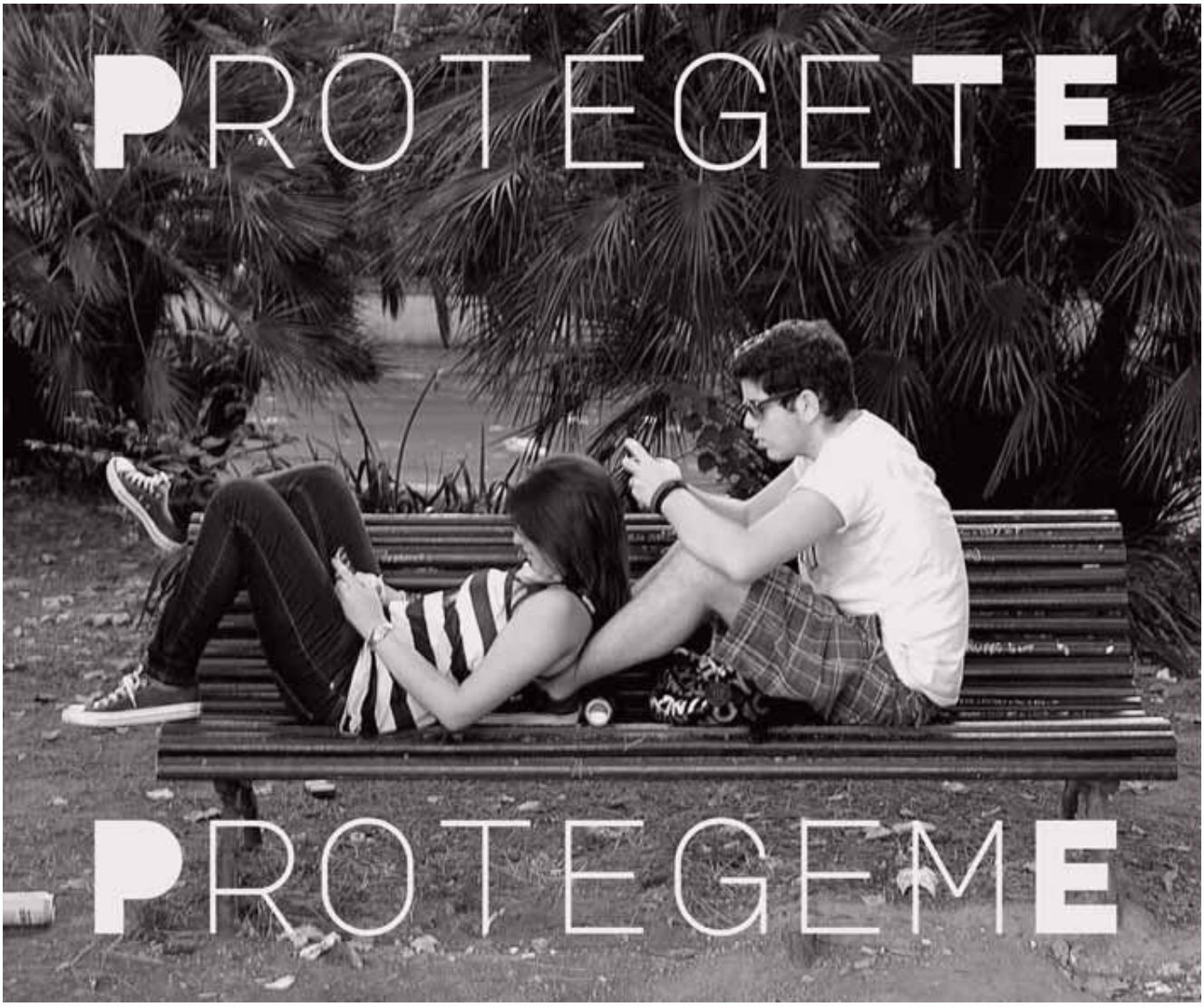
Podemos pensar que ya estamos seguros con lo que hacemos, que nuestra actividad en línea es sólo nuestra y que no se encuentra relacionada con los demás o bien que no tenemos “nada que esconder”.

Estas posturas eliminan la posibilidad de reflexión sobre otras realidades que sí se encuentran disponibles para

afectarnos por aquellos que saben que hacer y cómo beneficiarse de la ignorancia o el desconocimiento de quienes usan la tecnología de manera cotidiana.

- ¿Alguna vez pensaste para que son utilizados tus datos por quienes son dueños de una aplicación o red?
- ¿Sabías que la falta de seguridad en tus contraseñas puede permitir a terceras personas hacerse pasar por vos e interactuar con otros en tu nombre?
- ¿Tenías idea que la falta de cuidado mínimo de tus equipos puede impactar negativamente en tus relaciones más cercanas?
- ¿Pensaste alguna vez que quizás sea beneficioso para alguien que no tengas conocimiento de información fácil y sencilla para protegerte y proteger a los demás?

Si no lo habías pensado o quizás lo habías pensado pero nunca tomaste una acción, hay una buena noticia! **Weiba lanza la campaña #ProtegeteProtegeme que tiene por fin compartir con la gente esa información que generalmente sólo saben los técnicos o un círculo pequeño.** Creemos que es algo esencial para comenzar con la concientización sobre la importancia del uso de la tecnología para el desarrollo social.



Creemos que #ProtegeteProtegeme es una oportunidad para que cada persona comienza a tomar acciones efectivas para no sólo mejorar sus prácticas de seguridad informática pero por sobretodo para entender la importancia de la toma de dichas acciones. Esto implica tomar **medidas concretas -y sobre todo fáciles!- para comenzar a proteger tu seguridad en línea.**

En una sociedad que pretende avanzar, **ya no podemos movernos individualmente ignorando lo que le pase al otro.** Hoy estamos interconectados, y esta interconexión hace que cada acción mía esté conectada con algún otro, y por ende, cada omisión mía, está conectada también con los demás.

Esta manera diferente de comenzar a hacernos cargo del uso individual que cada uno de nosotros hace de la tecnología que utiliza diariamente, es un paso que parece chiquito pero tiene una fuerza enorme en el entorno que nos rodea.

Por eso, te invitamos a que seas parte de Protegete Proteme y seas parte del cambio que estamos impulsando a construir.

Bloquear programas peligrosos fácilmente

Tomar medidas para bloquear programas peligrosos (existen muchos!) en tus equipos es una de las prácticas más responsables. Estos programas generalmente se mantienen ocultos

Paradójicamente, hay muchos programas falsos que afirman ejecutar escaneos pero en realidad comienzan a registrar la actividad de los usuarios. Puede ser con fines de ofrecer publicidad, o directamente para comprometer la seguridad de datos bancarios, contraseñas, etc. Por eso, a continuación te recomendamos algunas opciones seguras.

Anti-Malware: Malware Bytes

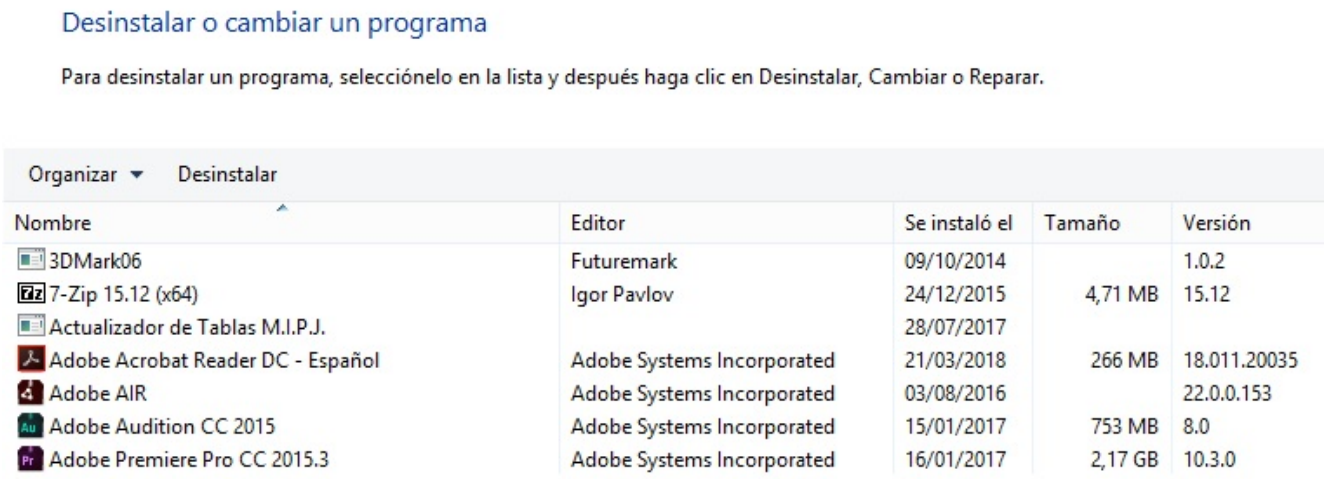
Para ayudarte en ese proceso, hay un tipo de programa que se denomina “anti-malware”. Estos programas ejecutan un análisis y permiten identificar programas maliciosos, falsos y peligrosos. Este programa es el líder de la categoría. Ofrece una versión gratuita, que es recomendable utilizar una vez por mes.

Link para la descarga

Si tenés celular, podes descargarlo desde la Play Store (Android) o desde la App Store (Apple).

Control de tus programas actuales en Windows (PC/Notebook)

Con paciencia, podés ir a Panel de Control, y buscar la sección en donde se listan los programas que tenés. Esa sección se puede llamar “Programas y características”, aunque depende de tu versión de Windows.



Ejemplo de una lista de programas actuales en una PC

Si bien es para expertos, podés revisar tu propia lista y eliminar cualquier elemento que te parezca muy extraño. En ese caso, te recomiendo hacer previamente una búsqueda online para corroborar si un programa es peligroso o si tiene algún tipo de utilidad.

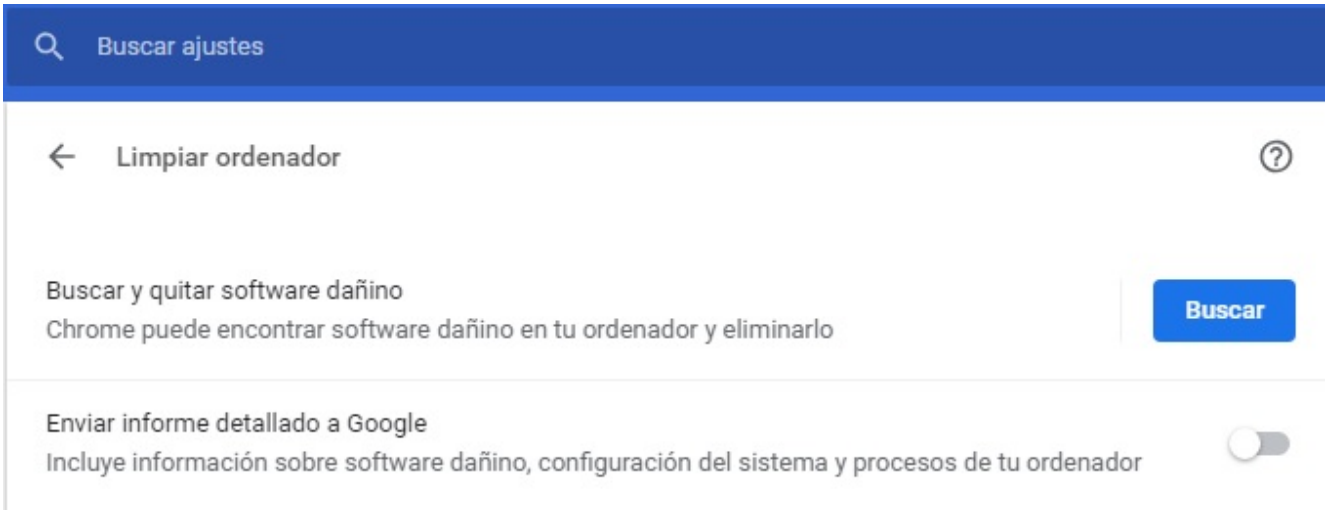
Buscar utilizando el navegador Chrome

En el 2017, una investigadora twitteo su descubrimiento: Chrome estaba escaneando sus documentos sin saberlo. Eso derivó en que todos conocieran que Chrome había integrado la funcionalidad de escanear nuestros dispositivos para detectar software peligrosos

Para utilizar esta función siguiendo las instrucciones oficiales de Chrome:

1. Abre el navegador Chrome.
2. En la parte superior derecha, haz clic en los 3 puntos, y luego en **Configuración**.

3. En la parte inferior, haz clic en **Configuración avanzada**.
4. En la sección “Recuperar ajustes y borrar”, haz clic en **Limpiar ordenador**.
5. Haz clic en **Buscar**.



Así se ve el analizador integrado de Chrome para búsqueda de software malicioso

Si se te pide que desinstales software no deseado, haz clic en **Eliminar**.

De que se trata la doble autenticación, o ¿porque pedir algo más que un usuario

y contraseña?

Doble autenticación, o autenticación de 2 factores (2FA) son **términos muy técnicos.** Lo que se esconde detrás de esto es básicamente **pedir algo más que un usuario y una contraseña**.

A diferencia de los VPNs y los programas de encriptación, este tipo de aplicaciones siempre **son gratuitas para incentivar su utilización**. De esta manera, todo el mundo gana: los comercios reciben menos quejas y reclamos, y las personas son menos vulneradas/hackeadas.

Nota: Al momento de implementar esta barrera de seguridad, se generará un **código de emergencia**. Es muy importante **siempre guardarlo emergencia que se genera, para el caso de que se pierda el celular o la PC en donde se genera este mecanismo.** De lo contrario, se perderá acceso definitivamente a las cuentas protegidas.

Cuatro maneras rápidas de implementar la doble autenticación (2FA)

Te presentamos las cuatro opciones más comunes para activar este mecanismo, vamos de la menos segura a la más segura:

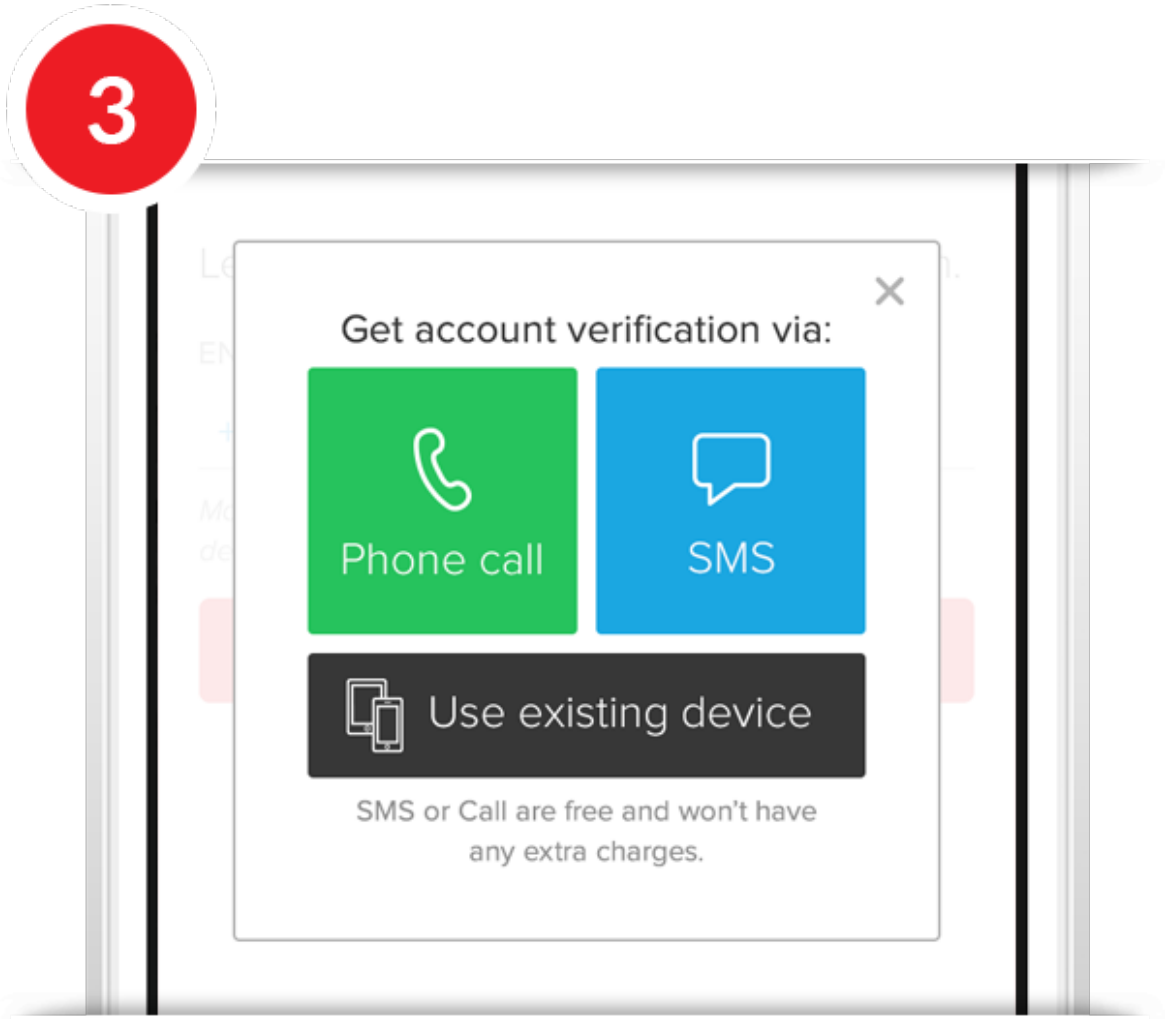
4. Código SMS

Con esta opción, cuando intentas entrar a una cuenta, simplemente se te envía a tu celular un código por SMS, generalmente de 4 a 6 dígitos. No es muy segura, porque podrían clonar tu celular, o interceptar ese código mediante antenas de telefonía ilegales.

3. Aplicación que se instala en tu PC o notebook

Con esta opción, instalas un programa que generará un código. El software más común en esta categoría es Authy. Este software fue creado en el 2011 por Daniel Palacio, y comprado

por Twilio en febrero del 2014.



Así se ve la interfaz de Authy, cuando lo estás configurando

Esta opción no es la más segura, ya que en el caso de que te roben el dispositivo, podrían generar el código fácilmente.

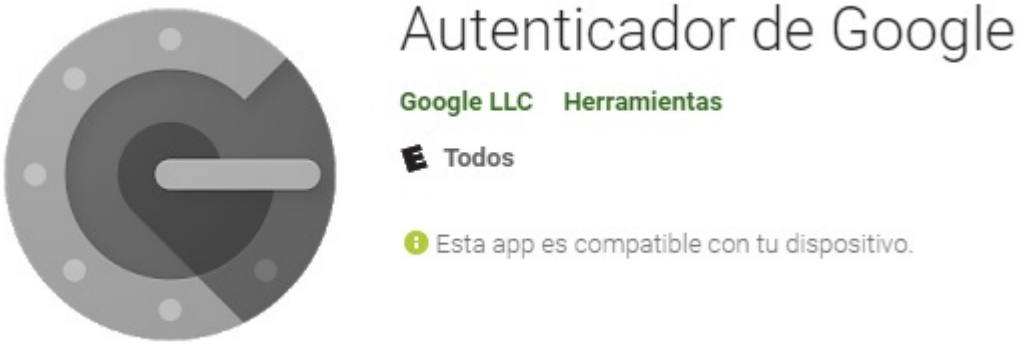
2. Aplicación que se instala en tu celular

Esta opción es más segura, si el celular tiene clave de bloqueo y además hay un código que protege esta aplicación. Básicamente hay dos opciones muy populares que existen dentro de esta categoría, además de Authy:

Por un lado, esta Duo Mobile. Desarrollado por Duo Security Inc, una empresa actualmente adquirida por Cisco.

Este es el link para descargarlo desde Google Play (para celulares con Android), y este es el link para descargarlo desde la App Store de Apple.

Por otro lado, esta la app más masiva de Google.



Este es el link para descargarlo desde Google Play (para celulares con Android), y este es el link para descargarlo desde la App Store de Apple.

1. Tokens físicos

Definitivamente, la opción más segura es tener una llave física (“token”) que se transporta. Hay muchas variantes en cuanto a los mecanismos de funcionamiento.

Por ejemplo, en el caso de los tokens de Yubico, hay versiones que se conectan inalambricamente para validar el ingreso a una cuenta, y otras versiones se conectan vía algún puerto USB, para dar un código específico que solo esta dentro.

Los cuatro VPN más utilizados. Incluye comparación de precios (diciembre 2018)

Si queres tomar un paso hacía la verdadera privacidad en relación a tu actividad digital, estas son las cuatro opciones de VPN más populares. Veamos uno por uno:

(1) VyprVPN

Desarrollado por Ron and Carolyn Yokubaitis, quienes fundaron la compania que lo desarrolla: Golden Frog GmbH (radicada en Suiza). Tiene una filial en EEUU.

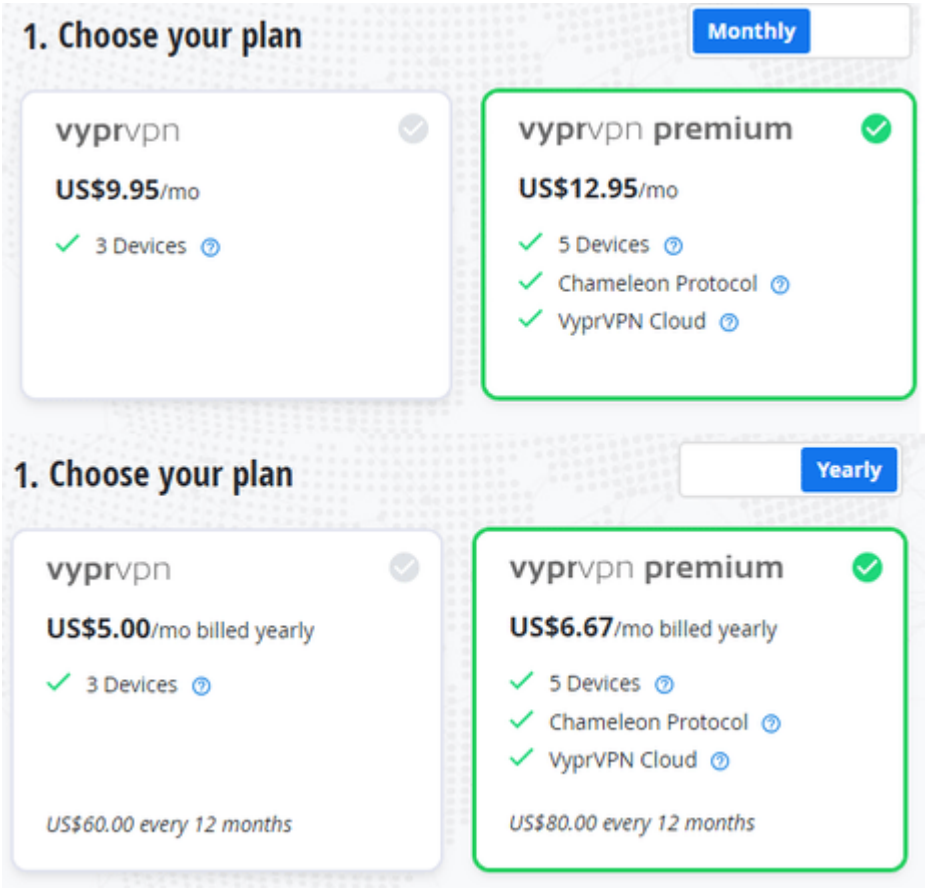


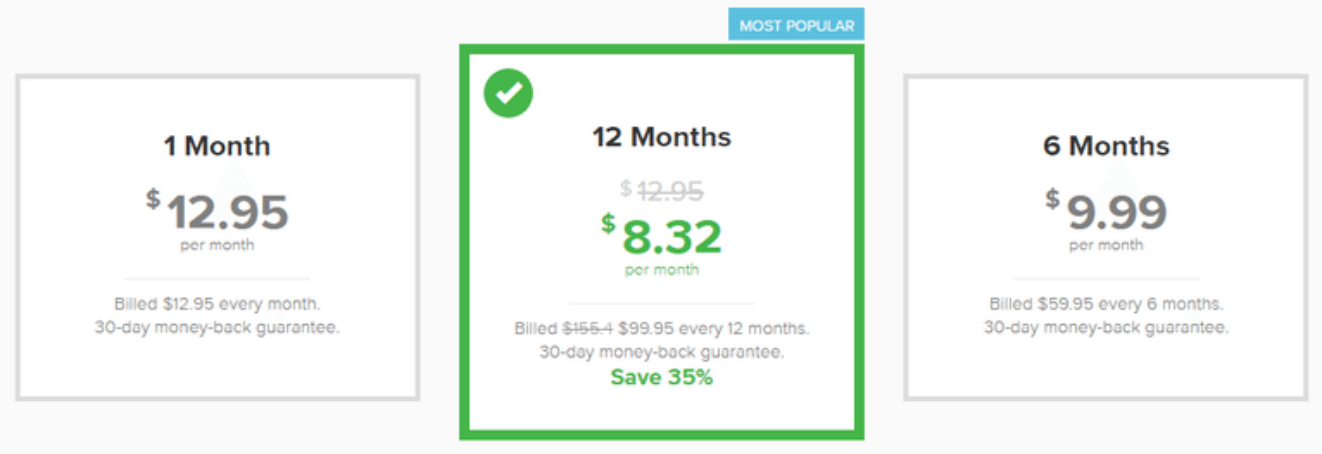
Tabla de precios VyprVPN (diciembre 2018)

Afirman ser un servicio con “cero registros” (zero logs) auditado de manera independiente, y con una infraestructura administrada por empleados propios.

[Web oficial de VyprVPN]

(2) ExpressVPN

Existe desde el 2009. Su dueño es *Express VPN International Ltd*, una empresa constituida legalmente en las islas vírgenes británicas, un paraíso fiscal. Afirman que por eso, prácticamente no tienen que respetar ninguna ley de retención de datos, como la de EUU o la europea.



Precios de ExpressVPN (datos de diciembre 2018)

Lo hemos probado varias veces, y sabemos que funciona muy bien en China. El punto en contra es que no hemos hallado información sobre quien es su fundador, ni quien es propietario de la compania.

[Web oficial de ExpressVPN]

(3) ProtonVPN

Es de los mismos desarrolladores del famoso sistema de correo electrónico encriptado y seguro (según estándares suizos). Lo comercializan como un servicio separado, o como un complemento a aquel sistema de correo electrónico.

ProtonVPN

[Precios mensuales]

Free	Basic	Plus	Visionary
$0 /mo	$5 /mo	$10 /mo	$30 /mo
	Charging $5 monthly	Charging $10 monthly	Charging $30 monthly
3 Countries	All Countries	All Countries	All Countries
1 Device	2 Devices	5 Devices	10 Devices
Speed: Low	Speed: High	Speed: High	Speed: High
P2P	P2P	P2P	P2P
Plus Servers	Plus Servers	Plus Servers	Plus Servers
Secure Core	Secure Core	Secure Core	Secure Core
Tor Servers	Tor Servers	Tor Servers	Tor Servers
Secure Streaming	Secure Streaming	Secure Streaming	Secure Streaming
ProtonMail Visionary included	ProtonMail Visionary included	ProtonMail Visionary included	ProtonMail Visionary included

[precios anuales]

Free	Basic	Plus	Visionary
$0 /mo	$4 /mo	$8 /mo	$24 /mo
	Charging $48 yearly SAVE $12	Charging $96 yearly SAVE $24	Charging $288 yearly SAVE $72
3 Countries	All Countries	All Countries	All Countries
1 Device	2 Devices	5 Devices	10 Devices
Speed: Low	Speed: High	Speed: High	Speed: High
P2P	P2P	P2P	P2P
Plus Servers	Plus Servers	Plus Servers	Plus Servers
Secure Core	Secure Core	Secure Core	Secure Core
Tor Servers	Tor Servers	Tor Servers	Tor Servers
Secure Streaming	Secure Streaming	Secure Streaming	Secure Streaming
ProtonMail Visionary included	ProtonMail Visionary included	ProtonMail Visionary included	ProtonMail Visionary included

Precios de ProtonVPN (datos de diciembre 2018)

[Sitio web oficial de ProtonVPN]

(4) NordVPN

Desarrollado por Tefinkom & Co., una empresa radicada en Panama y fundada en el 2010. Se diferencian porque ofrecen una doble encriptación, y aseguran que son la única compania en aplicar este estándar.

Precios de NordVPN (datos de diciembre 2018)

Sitio web oficial de NordVPN

Comparación de precios de diferentes VPNs (diciembre 2018)

Servicio	Precio por 1 mes	Precio por 6 meses	Precio por 12 meses
VyprVPN	9.95 a 12.95 usd	s/d	60 a 80 usd (5 a 6.66/mes)
ExpressVPN	12.95 usd	59.95 usd (8.32/mes)	99.95 usd (8.33/mes)
ProtonVPN	5 a 10 usd	s/d	48 a 96 usd (4 a 8/mes)
NordVPN	11.95 usd	s/d	83.88 usd (6.99/mes)

Tener contraseñas indescifrables ahora es fácil y gratis! Conoce los tres administradores de contraseñas más utilizados

Vamos a admitirlo: al principio puede ser que se nos haya ocurrido tener una contraseña fuerte para tener acceso a nuestras cosas. Pero con el tiempo, y al tener que hacer más de 10 logins diferentes por día en diferentes sitios, hemos optado por la rapidez en vez de la seguridad, y la repetición en vez de la dificultad. ¿O no es verdad que muchas veces usas la misma contraseña para tener acceso a diferentes páginas de internet, o quizás simplemente le cambias un número o una letra mayúscula?

El nombre de tu mascota, tu hijo, tu grupo favorito o tu número de documento son ejemplos de una mala elección al momento de proteger tu identidad digital y datos. Llevar todo anotado en un papel tampoco es muy seguro, porque quien lo tenga tendrá el absoluto control de tu vida.

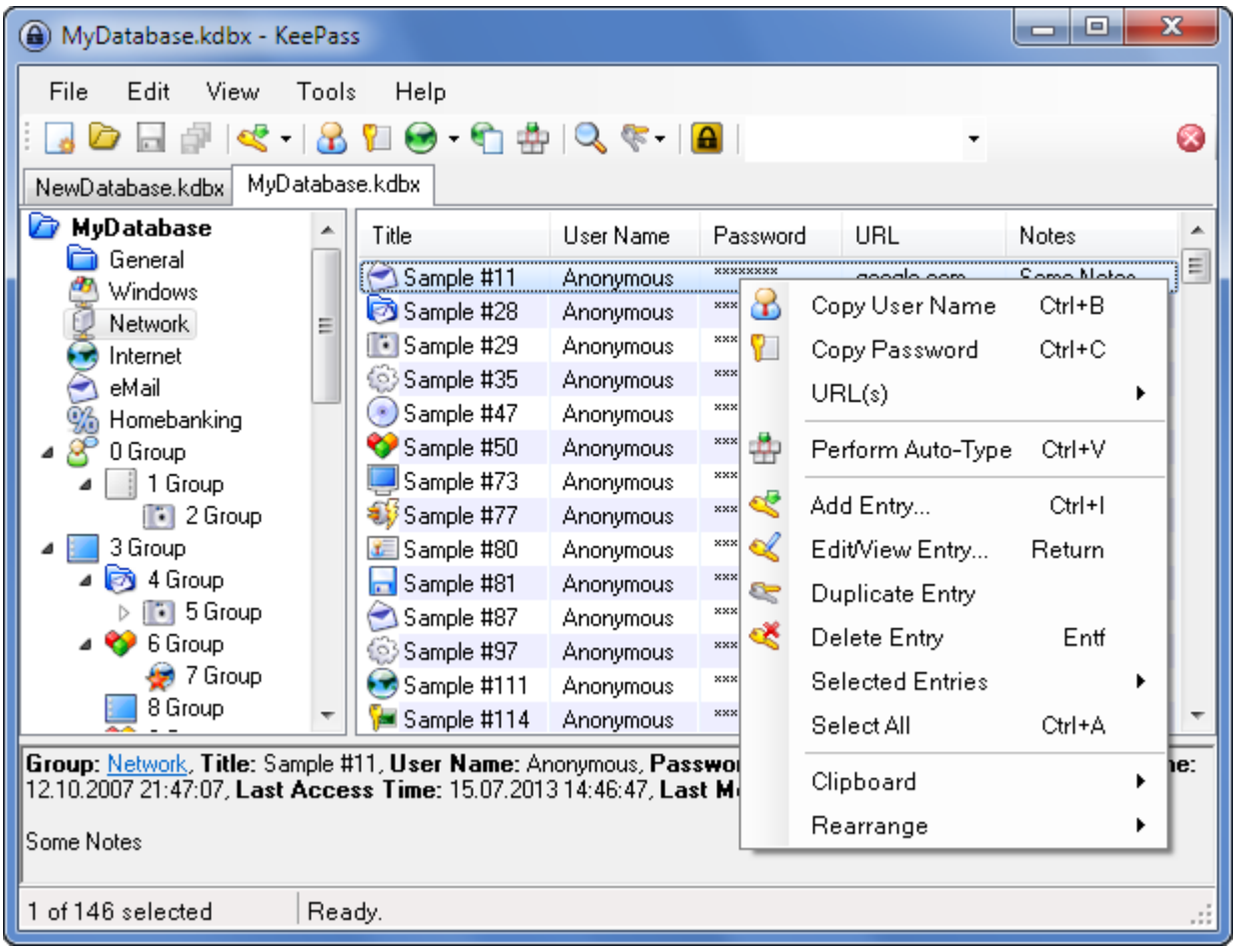
Y me dirás, **“es que es imposible acordarme de diferentes contraseñas”,** “**no tengo tiempo**” o “**no tengo nada que perder**“. Si bien estas pueden ser respuestas válidas, lo cierto es que las personas interesadas en acceder a tu información sí creen que es muy útil, y sabrán aprovecharla.

Hay millones de personas que ya lo usan como una agenda de tus contraseñas. Además, el administrador de contraseñas te permite generar contraseñas fuertes y seguras mientras que al mismo tiempo te brinda el servicio de agendarlas. No tenes que preocuparte por la instalación, es muy sencilla y rápida y estamos seguros que te van a ahorrar un dolor de cabeza en el futuro.

Existen muchísimas opciones, pero ya hicimos el trabajo preguntándole a los especialistas qué nos recomendaban y llegaron a la conclusión de que estas son **las tres mejores opciones gratuitas de administradores de contraseñas:**

3. KeePass

Este software tiene más de 15 años de evolución y desarrollo, siempre ha sido completamente gratuito gracias a las donaciones. Como se puede ver, su punto fuerte no es la estética, pero es uno de los más utilizados por los expertos.

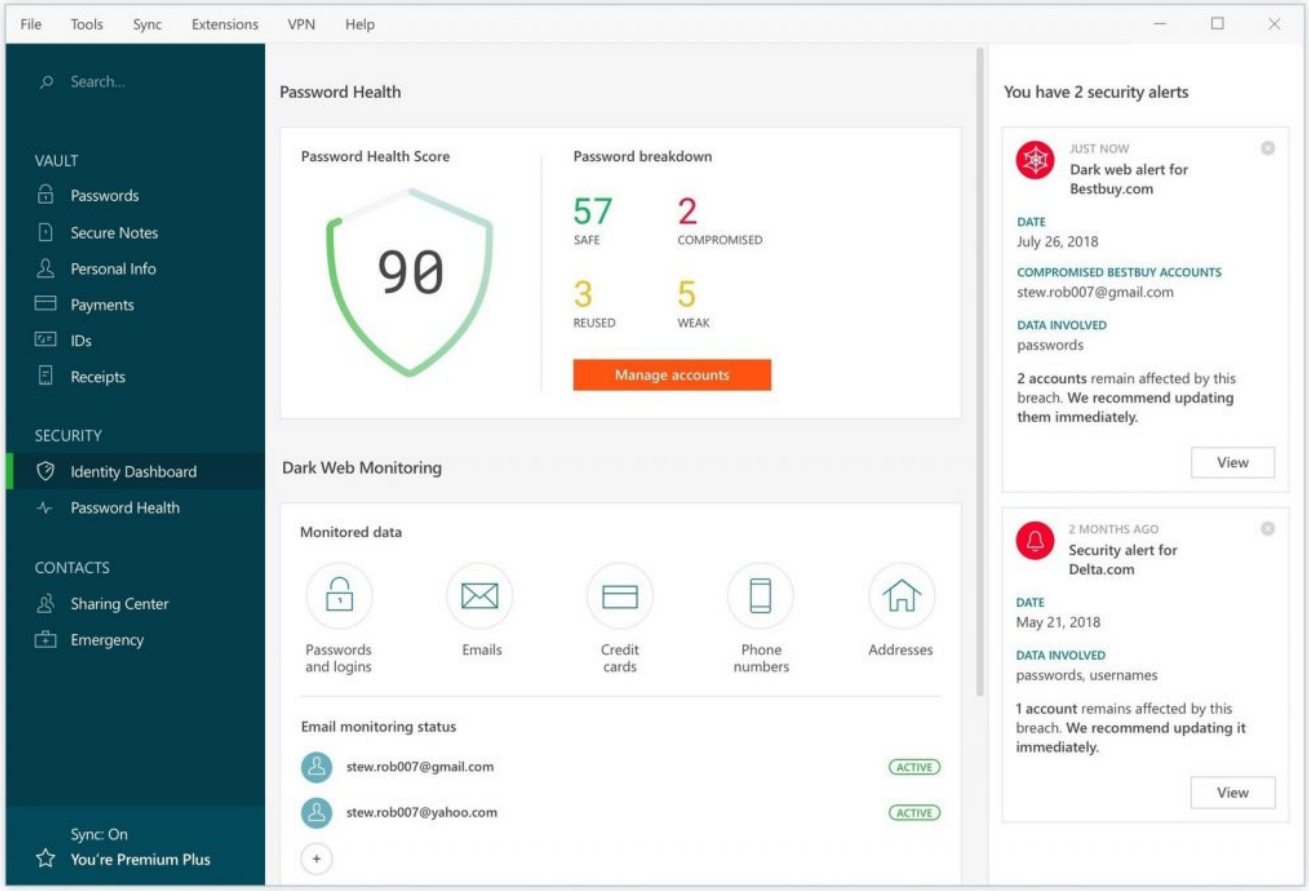


Así se ve la interfaz gráfica de KeePass, uno de los administradores más usados por los técnicos.

[Web oficial para descargarlo]

2. Dashlane

La empresa que lo desarrolla es Dashlane Inc, esta constituída en Delaware (EEUU). Tiene 10 millones de usuarios en todo el mundo. Es el segundo administrador de contraseñas con la mayor cantidad de usuarios en el mundo.

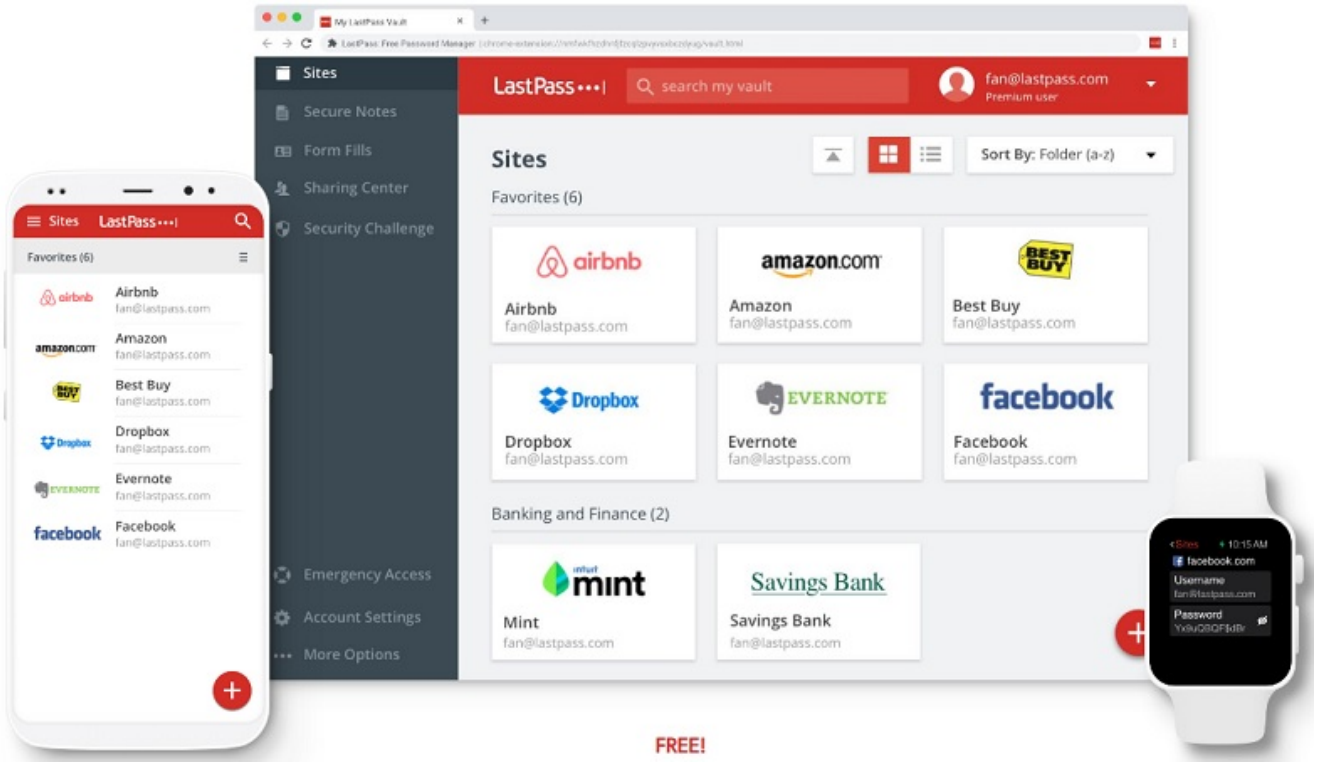


Su originalidad radica en que escanea la deep web en busca de la publicación de datos de cuentas, para alertarnos en caso de encontrar que alguien esta vendiendo nuestras contraseñas.

Web oficial para descargarlo

1. LastPass

Tiene una base de 13 millones de usuarios en todo el mundo. Este programa se basa principalmente en sumarse a los navegadores de internet, lo cual es muy práctico. Desde Octubre del 2015, la empresa propietaria del software es LogMeIn Inc (pagaron 110-125 millones de USD), un gran grupo que cotiza en la bolsa de valores (NASDAQ).



LastPass se integra a los navegadores de Internet, volviendo la administración de las contraseñas algo muy práctico

Cada vez que se han reportado fallas de seguridad, la empresa tiene una política de informar a sus usuarios públicamente, lo cual prueba que son un poco más honestos que los demás en cuanto ese tipo de información.

[Web oficial para descargarlo]

Como ya sabés, creemos que la tecnología tiene que ser usada para el desarrollo social. Parte de este desarrollo tiene que ver como poder estar tranquilos en nuestra relación con las redes y cuidados de acciones maliciosas de terceros. Seguí este #Weibatip y si tenés alguna consulta, escribimos!

Proteger tus contraseñas es proteger a los demás. Los especialistas en seguridad informática nos explican la importancia del uso de los administradores de contraseñas.

Por falta de tiempo, multiplicidad de opciones o desconocimiento, muchas personas no los utilizan. **¿Qué es específicamente un administrador de contraseñas?**

Es un programa que permite guardar de forma muy segura todas las contraseñas, y permite dejar atrás formas menos seguras de guardado.

Es una realidad que los especialistas y las grandes empresas siempre los han utilizado, porque los problemas que se solucionan son muchos:

- Recordar la enorme cantidad de diferentes usuarios y contraseñas
- Saber exactamente cuando fue la última vez que cambiaste tus contraseñas
- Poder entrar a las mismas cuentas desde una PC, celulares o tablets, de manera fácil y rápida
- Se facilita el uso de diferentes contraseñas, lo que mejora la posibilidad de estar más seguros aún en caso de tener problemas de seguridad.

Para facilitar la adopción de estas soluciones, aquí te

presentamos las tres mejores opciones de gestores de contraseñas

Cuidados colectivos: tu protección protege a los demás

Uno de los principales argumentos para utilizar un administrador de contraseñas, es proteger conversaciones y archivos de los demás miembros de un grupo (amigos, familia, compañeros de trabajo, etc).

Si dentro de una conversación hay alguien que es espiado o hackeado, pone en riesgo a todos los demás integrantes de esa conversación. Entonces, no tomar medidas se vuelve una actitud peligrosa para todos las personas que interactúan con nosotros, genera efectos indeseados colectivos que impactan en toda la sociedad.

La opinión de dos especialistas en seguridad informática

Cuando empezamos a pensar en el uso de administradores de contraseñas como acción específica para el desarrollo social, nos interesó conocer la opinión de dos especialistas en seguridad informática. Para saber que opinan, les preguntamos a dos especialistas:

Noah Corradin es Investigador en Seguridad de la Información. Trabaja hace mas de 8 años protegiendo grandes y pequeñas empresas, y **utilizó la mayoría de los administradores de contraseñas que existen en el mercado**. El nos comentó que "*desde siempre, las empresas más grandes han utilizado estos programas. Pero últimamente, prácticamente todas lo están utilizando*". Continuo diciendo que "*Todo grupo de personas, ya sea una escuela, una pequeña empresa e incluso cualquier*

persona particular que utiliza Internet como principal medio de sus comunicaciones en comunidad debiera usar uno. Al final de cuentas, de lo que estamos hablando es de conciencia colectiva, protección de aquellos que interactúan con nosotros y prevención de situaciones indeseadas". (Actualmente Noah utiliza LastPass, una de las tres opciones gratuitas que recomendamos)

Cristian Amicelli, es consultor en seguridad informática y hacker ético. Trabaja hace más de 20 años ayudando a fuerzas de seguridad, empresas internacionales y organizaciones sociales. Nos comentó que hay gente a favor y gente en contra, y que "*en el caso de las soluciones gratuitas la seguridad es menor, lo ideal es controlar que nivel de seguridad se ofrece para los datos en tránsito y para los datos almacenados, las contramedidas, el monitoreo y las auditorias existentes.* ***Hay muchísimas opciones en el mercado y eso da la pauta de que es algo que se utiliza, pero identificar la mejor solución es imprescindible****".*

Como cuidar tu dinero en internet y evitar estafas #WeibaTips

Cada vez es más común – y a veces resulta el único medio – de utilizar internet para **pagar cuentas, enviar dinero, acceder a tu banco o comprar productos o servicios**. Seguramente ya te hayas preguntado **¿como puedo cuidar mi dinero cuando estoy en internet para evitar ser estafado?**

Veamos algunos casos de la vida real:

- Un chico de Estados Unidos conoce a una chica en un bar en Argentina. Le presta su celular unos minutos para que ella le pase su número. Al otro día, él descubre que le faltan 2 mil dolares de su cuenta de PayPal. El número que ella le dio era obviamente falso.
- Una chica corta con su novio. Él tiene acceso a todas sus cuentas, por lo que cambia todas sus claves para molestarla. Ella pierde mucho tiempo en la recuperación de sus usuarios, y aunque no perdió dinero, sí perdió mucho tiempo y gano mucha preocupación durante todo el proceso.

Malas prácticas a evitar

Las 5 malas prácticas que generalmente te ponen en riesgo, si no tenes los programas adecuados instalados, son las siguientes:

- Usar contraseñas fáciles
- Usar la misma contraseña para más de un sitio
- No tener doble autentificación activada
- Pasar el tiempo navegando en páginas de apuestas, citas de todo tipo, o productos o servicios “gratis”
- Utilizar computadoras públicas o redes de internet abiertas -esas que no requieren contraseña (de locutorios, hoteles, conferencias, cafeterías)

Veamos ahora cuales son las **medidas esenciales para evitar problemas y malos tragos al manejar dinero en internet**

Cuatro medidas esenciales para cuidar tu dinero en Internet #Weibatips

(1) Utilizar un administrador de contraseñas

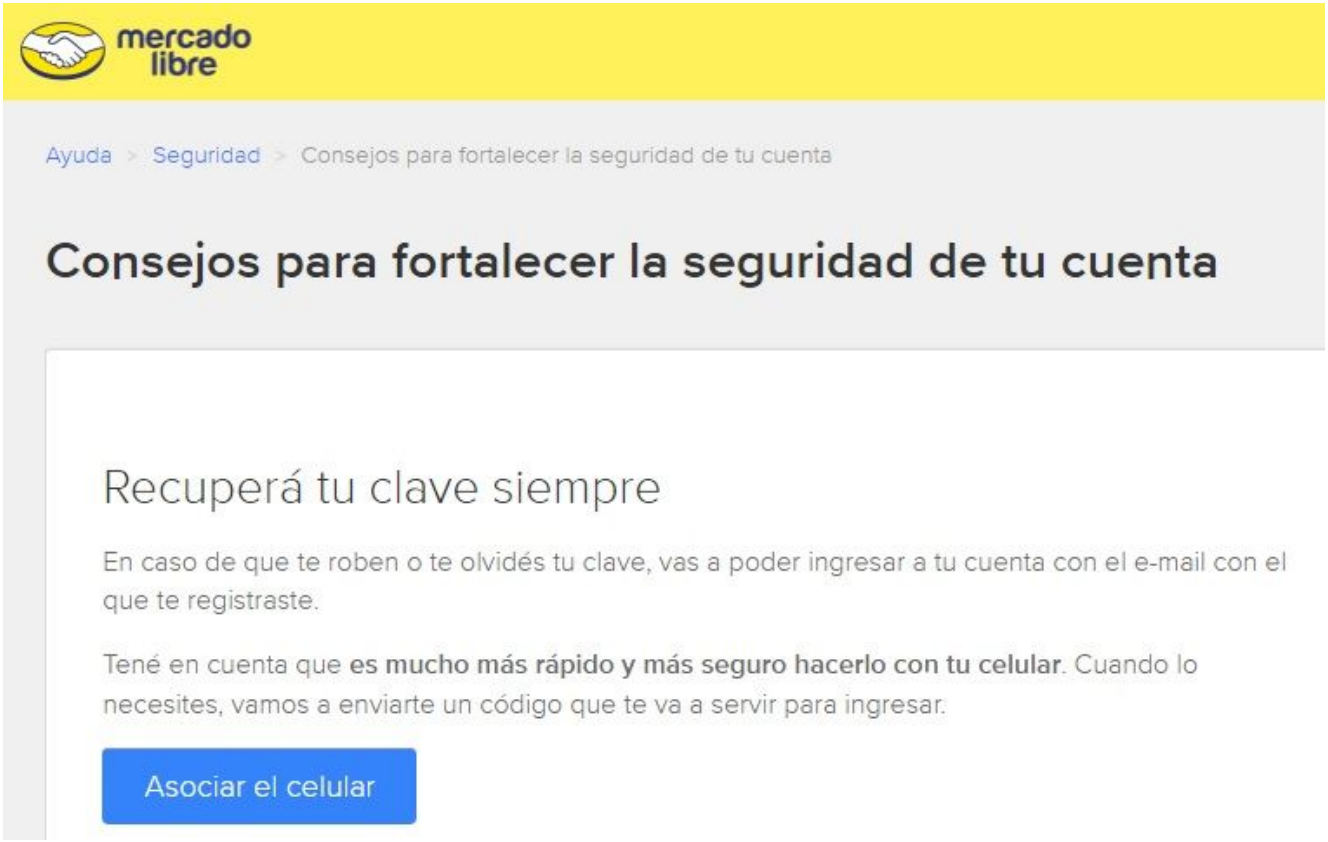
Con tantas plataformas, usuarios y claves, es imposible acordarse de todo lo que necesitamos saber. Los especialistas hace mucho tiempo que resolvieron este problema, de una manera muy sencilla y con un grado de seguridad muy alto: utilizan un programa que funciona como administrador de contraseñas.

Acá te mostramos las 3 mejores opciones gratis.

(2) Utilizar un elemento adicional además del usuario y la contraseña (factor de doble autentificación)

Las plataformas de venta por internet ya están haciendo esto por defecto, y muchas plataformas de email también, al pedirte un número de celular y enviarte allí un código o "pin".

Con esto, te aseguras de que en caso de que alguien tenga tu usuario y contraseña, eso no sea suficiente para entrar en tu cuenta bancaria o cuenta digital, o que pueda entrar con tu identidad a realizar compras por internet.



Ejemplo de como Mercado Libre explica las ventajas de la doble autenticación. A partir del 2018, la plataforma obliga a los usuarios a utilizar esta medida de seguridad.

Para conocer las mejores apps gratis para doble autenticación, escribimos este breve artículo.

(3) Protegerte al realizar compras o entrar a tu banco mediante wifi público (con un VPN)

Podes presumir que todo lo que hagas en un wifi público, como el de una cafetería, el gobierno, un local de comida, etc, esta siendo registrado. Si necesitas usar este tipo de internet de todas maneras y no lo podes evitar, la solución es usar algún “Virtual Private Network (VPN)”.

Este tipo de servicios generalmente es pago, pero te asegura que quien este escuchando tus acciones no entienda absolutamente nada, ya que toda tu actividad estará oculta por encriptación.

Aquí te dejamos un listado con las 4 VPNs más confiables.

(4) Vigilar que no existan programas maliciosos en tu PC o celular

Hay muchos programas que se ocultan, para monitorear tu actvidad y también enviarte publicidad. Son la puerta de entrada a peligros mayores, por eso es esencial tener algunos mínimos cuidados.

Eso es todo! **Con estas cuatro medidas esenciales, podrás cuidar tu dinero en internet, y estar mucho más seguro que la mayoría de los usuarios.** Esperamos que este artículo te haya resultado útil!

Si queres, podes ayudarnos con una pequeña encuesta para entender mejor como manejan su seguridad los usuarios. Esperamos tus consultas, dudas y comentarios!

Lo invisible de la tecnología. Charla abierta en el Museo del Libro y de la Lengua

El 29 de Noviembre brindamos una charla abierta a la comunidad con la consigna “Lo invisible de la tecnología”.

Muchas gracias al equipo del Museo del Libro y de la Lengua por el espacio y la buena onda! También queremos agradecer la cobertura y difusión espontanea del equipo de DiarioVivo.com