Privacidad Para la Persona Común: Una Guía Para Mantenerse Más Seguro en Línea

Por Astrid Floegel-Shetty

Con el generoso apoyo de la Fundación Rose para las Comunidades y el Fondo para los Derechos de Privacidad Ambiental

OAKLAND PRIVACY

Apoyo de edición de J.P. Massar y Yadi Younse

Índice

(1): Introducción

(2): Herramientas de Privacidad Digital

(3): Correo Electrónico

(4): Gestores de Contraseñas

(5): Mensajes Privados

(6): Navegadores, Motores de Búsqueda y Herramientas para Proteger tu Privacidad en Línea

(7): Videollamadas

(8): La Nube

(9): Reproductores de Vídeo en Línea

(10): Aplicaciones de Bienestar y Salud

(11): Asistentes Inteligentes y Privacidad (Por Qué Quizá Quieras Evitar Decir "Oye, Alexa")

(12): Filtración de Datos (Antes De Que Tu Información Sea Robada)

(13): IA Generativa (Qué Saber Antes de buscar por ChatGPT)

(14): CALIFORNIA – Eliminar Tus Datos en Línea

(15): Recursos

Capítulo 1: Introducción

¿VPN? ¿Cifrado? ¿Navegador Tor? ¿Geolocalización? ¿Seguro? ¿Inseguro? ¿Filtración de datos?

¿Qué significa TODO esto?

Si alguna vez has intentado entender cómo proteger tu información en línea y te has sentido completamente abrumado, no estás solo. Parece que todo el mundo habla en código: VPNs, cifrado, "de extremo a extremo", cookies, firewalls...

No necesitas ser un experto en tecnología para proteger tu privacidad en línea. Solo necesitas:

(1) una idea sobre por qué esto de la privacidad realmente importa para tu vida diaria,

(2) unas pocas herramientas, y

(3) explicaciones claras.

¿Qué significa para mí tener privacidad digital?

La privacidad significa que tú decides quién ve qué sobre ti. Es como tener cortinas en tu casa o piso, porque simplemente no quieres que extraños te vean comer cereal en pijama. La privacidad digital en línea significa mantener tus cosas personales —tus búsquedas, tus mensajes, tu información de salud, incluso tu ubicación— fuera de las manos de empresas, hackers y gobiernos a quienes no dijiste "sí".

¿Cuál es el sentido de intentar mantener mi vida en línea/digital privada?

Cada pequeño cambio en la privacidad digital que haces te ayuda a protegerte de:

1) Tu información privada accidentalmente siendo compartida o robada.
Esto incluye tu número de teléfono, ubicación o incluso fotos privadas filtradas en línea.

2) Alguien fingiendo ser tú en internet para abrir cuentas de crédito o robar dinero. *Esto se llama **robo de identidad**. Puede afectar negativamente tus finanzas y tardar años en arreglarse.*

3) Recibir mensajes basura o correos fraudulentos que intentan engañarte.
Los estafadores suelen enviar mensajes falsos a tu correo electrónico o número de teléfono para robar tu información e identidad, pidiendo datos como tu número de tarjeta de crédito.

4) Páginas web que siguen todo lo que haces en línea.
*Esto se llama **rastreo**. Es como los anuncios online "te siguen" por internet después de que buscas algo una vez. Por ejemplo, imagina que buscas en Google "ropa de bebé" porque tu amigo organiza un baby shower. Ahora todos los anuncios que ves en internet son sobre bebés y crianza.*

5) Empresas que crean un archivo sobre tus hábitos en línea sin preguntarte y venden esa información.
Cuando las empresas rastrean lo que haces en línea, recopilan información personal tuya sin permiso, como lo que buscas, compras o ves. Podrías pensar, ¿a quién le importa? ¡A tí debería! Las empresas utilizan esta información para dirigirse a ti con anuncios, cambiar los precios que ves e influir en tus decisiones sin que te des cuenta.

Pero más que todo eso, la privacidad digital trata de la libertad de existir sin vigilancia. La privacidad significa que puedas explorar, aprender, hablar y vivir tu vida sin que te vigilen todo el tiempo en persona NI en línea.

Esta guía te orientará a través de pasos sencillos que puedes seguir y herramientas que puedes utilizar para comenzar tu camino hacia la privacidad digital. Desafortunadamente, ninguna herramienta ni configuración puede garantizar al 100% la privacidad digital total.

Sin embargo, pequeños pasos (como usar contraseñas fuertes, poner cinta sobre la cámara de tu computadora, estar al día con las nuevas actualizaciones de software para tu móvil) pueden ayudar mucho a mantener tu vida digital más segura.

El objetivo no es la perfección, ¡sino la protección!

Sigue leyendo para descubrir cómo puedes implementar fácilmente herramientas de privacidad digital.

Capítulo 2: Herramientas de Privacidad Digital

¿Cómo funcionan las herramientas de privacidad digital?

Piensa en herramientas de privacidad digital de este modo.

En un barrio tranquilo, a menudo hay un tramo largo y recto de carretera. ¿Qué ocurre cuando no hay reductores de velocidad? La mayoría de los conductores aceleran de forma natural, aunque no lo hagan a propósito. Y hay gente que aprovecha que no hay reductores de velocidad para conducir muy, ¡muy rápido! Pero cuando hay reductores de velocidad, esos disminuyen la probabilidad de que la gente conduzca peligrosamente rápido o que si quiera circule por la calle.

O piensa en las cerraduras de tu puerta principal, o incluso en señales de seguridad como "Protegido por ADT" o "Cuidado con el perro". Estas medidas de seguridad no hacen que tu hogar sea completamente inmune frente a robos, pero sí lo hacen menos atractivo para quien busca un objetivo fácil.

Las herramientas de privacidad funcionan igual en línea.

Cuando sitios web, aplicaciones, empresas, gobiernos o incluso hackers saben que nadie está vigilando—o que tus datos no están protegidos—tienden a apresurarse para robar tus datos o verte como un objetivo fácil.

Pero cuando añadimos "reductores de velocidad", "cerraduras" y "señales de seguridad" a tu vida digital (como contraseñas fuertes, autenticación de dos factores (2FA) y ajustes de privacidad), ¡los retrasamos! Enviamos el mensaje de que esta información está protegida. La información protegida es menos accesible y atractiva para sitios web, aplicaciones, empresas, gobiernos y hackers.

Estos pequeños pasos (tus reductores de velocidad digitales, cerraduras y señales) quizá no detengan todas las amenazas, pero contribuyen mucho a que seas un objetivo menos atractivo y mucho más difícil.

No tienes que hacerlo todo.

¡Pero algo es mejor que nada!

Aquí tienes algunas respuestas a preguntas que puedas tener mientras lees esta guía de privacidad digital.

¿Qué significa cuando algo es "seguro" en línea?

"Seguro" en línea significa que el sitio o la aplicación hace cosas para mantener tu información protegida. Por ejemplo, un sitio web seguro (identificado por el icono de candado en la barra del navegador, mostrado en las imágenes de abajo) utiliza cifrado, actualiza sus sistemas y protocolos de seguridad regularmente, y no pide más datos de los que realmente necesita.

Es como elegir un banco con una caja fuerte y guardias de seguridad, en vez de uno con la puerta trasera completamente abierta. Solo ten en cuenta que "seguro" no significa que estés perfectamente protegido, sino que tienes algún tipo de protección.

¿Qué es el cifrado?

Imagina que estás enviando una carta a un amigo, pero antes de dejarla en el correo, la metes dentro de una caja cerrada con llave—y solo tu amigo (al que le diste la llave anteriormente) puede abrir esa caja. Eso es básicamente lo que hace el cifrado. Bloquea tus mensajes, fotos y contraseñas de una manera que los hace indescifrables para cualquiera que no tenga la llave. Así que, aunque alguien intercepte la caja con la carta, esa persona no podrá leer tu carta porque no tiene la llave para abrir la caja.

Ahora que esto ha sido explicado, ¡vamos a aprender sobre herramientas específicas de privacidad digital!

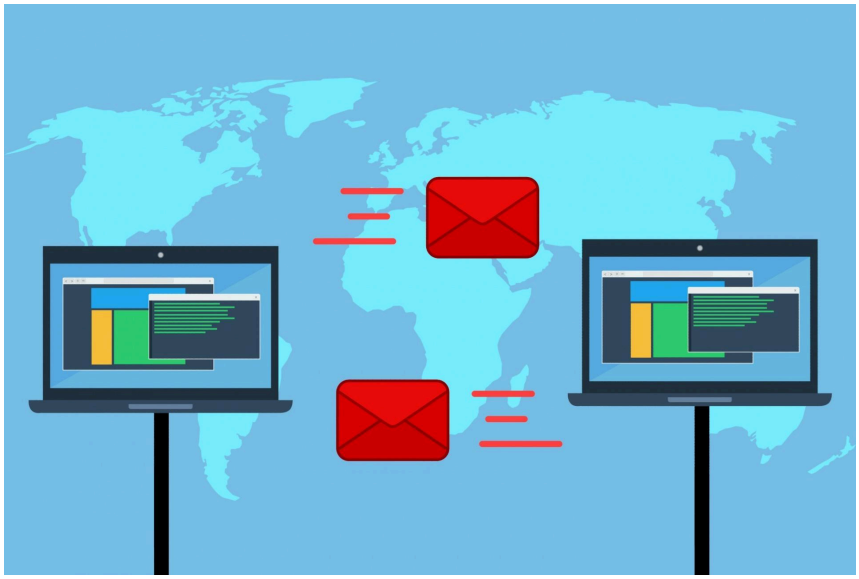
Solo recuerda: no tienes que hacerlo todo

¡Pero esperamos que esta guía te ayude a encontrar cosas fáciles que puedas hacer!

Capítulo 3: Correo electrónico

El correo electrónico es como una postal digital: fácil de enviar, fácil de leer y fácil de interceptar.

La mayoría de la gente usa el correo electrónico todos los días: para el trabajo, para comprar en línea, para comunicarse con amigos, familia, doctores, terapeutas, atención al cliente y para muchas cosas más...



Pero aquí está la realidad: el correo electrónico es una de las formas menos seguras de comunicarse. En los primeros días de el internet y las computadoras, la gente no pensaba en hackers, vigilancia o estafas. Así que el correo electrónico no fue diseñado con muchas funciones de privacidad digital.

¿Qué puede salir mal con el correo electrónico?

Spoofing y phishing: Spoofing es el disfraz. Phishing es el truco.

Spoofing es cuando alguien finge ser otra persona falsificando una dirección de correo electrónico, número de teléfono o página web para parecer fiable. Por

ejemplo, esto incluiría ocasiones en las que has recibido un mensaje de texto extraño de alguien que dice ser FedEx.

Phishing es la estafa en la que los malos actores usan esa identidad falsa para enviarte un correo electrónico pidiéndote tu contraseña o número de tarjeta de crédito. Por ejemplo, el estafador que se hace pasar por FedEx diría en un correo electrónico que para que tu paquete sea entregado, tienes que enviar tu número de seguro social. Al suplantar la identidad de FedEx, el estafador espera engañarte para que le des tu información, convirtiéndote así en víctima de un ataque de "phishing".

•

Usar tu correo electrónico para restablecer tus contraseñas

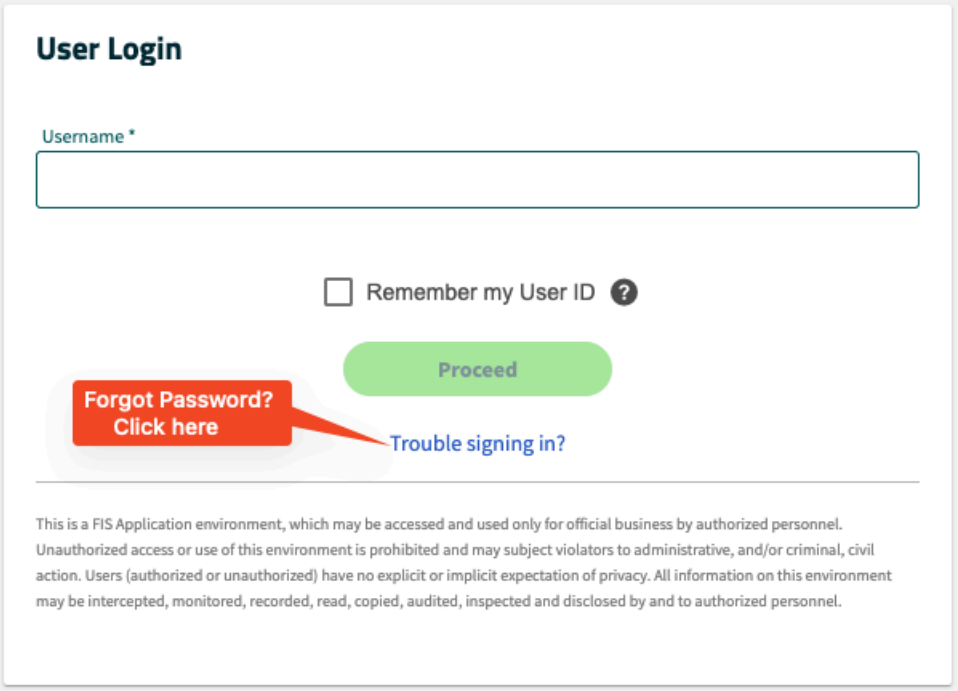
Si alguien entra en tu correo, puede restablecer tus contraseñas para otras cuentas (como tu banco, aplicaciones de compras o redes sociales) porque los enlaces de restablecimiento de contraseña que recibes para esas otras cuentas (normalmente después de hacer clic en "¿Olvidaste tu contraseña?" o "¿Problemas para iniciar sesión?") van a tu correo. Estos hackers TAMBIÉN pueden leer mensajes antiguos, encontrar información personal (como tu dirección, contactos o documentos guardados) e incluso enviar correos falsos haciéndose pasar por ti (como el spoofing que acabamos de descubrir).

El gobierno leyendo tus correos electrónicos

En muchos casos, cuerpos de seguridad o agencias de inteligencia pueden solicitar acceso a tus correos electrónicos a la empresa (como Google o Yahoo!) que los almacena.

Por eso, proteger tu correo electrónico con una contraseña fuerte y autenticación de dos factores (2FA) es uno de los pasos más importantes que puedes dar para tu privacidad general.

Lee más sobre la autenticación en dos factores en el Capítulo 4.



¿Y qué puedes hacer?

No hay una respuesta única para todo esto. Depende de cómo uses el correo electrónico, qué intentas proteger y quién te preocupa.

Consejos Básicos de Seguridad con el Correo Electrónico que Todo el Mundo Debería Conocer

1) Nunca envíes por correo electrónico información sensible como tu número de seguro social, datos bancarios o contraseñas
Utiliza una aplicación de mensajería cifrada o llama si tienes que enviar algo personal.
Consulta el capítulo 5 para más información sobre aplicaciones de mensajería recomendadas.

2) Ten cuidado al hacer clic en enlaces de mensajes de personas que no conoces o incluso de personas que sí conoces, si el mensaje te parece extraño.

Simplemente reporta el correo extraño como "spam" y luego bórralo.

Si realmente no estás seguro de si el correo es real, el siguiente paso es (¡en un correo aparte, un mensaje de texto, o una llamada!) preguntar a la persona que te envió el correo original si realmente te lo envió.

3) Siempre cierra sesión de tu correo electrónico en computadoras compartidas, ya sea en casa o en la biblioteca.

4) Actualiza la configuración de privacidad de tu cuenta de correo electrónico.

Actualizar la configuración de privacidad de tu cuenta de correo electrónico

Asegúrate de activar la configuración de privacidad de tu correo electrónico. Por ejemplo, Gmail te permite desactivar la publicidad dirigida, grabar tu historial de YouTube y Google Maps, y mucho más.

Ve a la configuración de tu cuenta de correo electrónico y normalmente encontrarás una sección de "Seguridad" que te permite hacer cambios para proteger tu privacidad. Infórmate más sobre la configuración de privacidad de tu: GMAIL; YAHOO/AOL; MICROSOFT/OUTLOOK.

Además, crea contraseñas fuertes para tu cuenta de correo electrónico y añade autenticación en dos factores (2FA) si la ofrecen.

Una contraseña fuerte es aquella larga, difícil de adivinar y que no se basa en información personal como tu nombre o fecha de nacimiento. Las mejores contraseñas usan una mezcla de letras (mayúsculas y minúsculas), números y símbolos... algo como **Purpura$Guitarra!Lluvia29**.

¿Aún mejor? Usa una **"frase de contraseña"** formada por palabras aleatorias, como **perro-arbol-baile-honesto**, especialmente si usas un gestor de contraseñas para recordarla.

Evita cualquier contraseña corta, sencilla o reutilizada en varias cuentas.

Consulta el Capítulo 4 para más información sobre gestores de contraseñas.

Sin embargo, incluso si tienes activadas todas las opciones de privacidad para tu correo, la empresa que aloja tu correo (Gmail, Yahoo, Outlook) puede seguir viendo lo que hay en tu correo.

La mayoría de los proveedores de correo electrónico (como Gmail, Yahoo o Outlook) almacenan tus mensajes en servidores.

¿Qué significa cuando un correo electrónico está "almacenado en un servidor"?

Supongamos que escribes una carta a un amigo. No se la entregas directamente. En vez de eso, la dejas en la oficina de correos y ellos la guardan hasta que tu amigo venga a recogerla. La oficina de correos es el servidor.

Básicamente eso es lo que ocurre cuando envías o recibes un correo.

En lugar de viajar directamente de tu teléfono o computadora a otra persona, tu correo electrónico se envía primero a un servidor, una potente computadora propiedad de una gran empresa tecnológica como Google (Gmail), Microsoft (Outlook), Yahoo, Apple u otro proveedor de correo electrónico.

Ese servidor almacena una copia de tu mensaje, a veces durante años. Ese correo puede quedarse ahí incluso después de que lo borres de tu bandeja de entrada. La gran empresa tecnológica puede acceder a estos correos cuando quiera. Los hackers podrían intentar entrar en el servidor para robar mensajes. Los gobiernos

o la policía pueden acceder a tus correos electrónicos usando la ley para obligar a las empresas a abrir el servidor.

Así que cuando la gente dice "tu correo electrónico está almacenado en un servidor", se refieren a que tu correo está en la computadora de otra persona, esperando a ser leído —y posiblemente copiado, escaneado, robado o filtrado.

Por eso, elegir un servicio de correo más privado, o aprender a cifrar tu propio correo, puede darte más control sobre la privacidad de tu correo.

Servicios de Correo Electrónico a Considerar

Aquí tienes algunos servicios que toman medidas adicionales para proteger tus mensajes:

Proton Mail	Based in Switzerland, where privacy laws are strong. Proton also offers a password manager, VPN, Drive, and calendar. Free & paid plans.
tuta	Based in Germany, another country with strong privacy protections. Includes encrypted calendar and contacts. Only uses renewable energy to power their service. Free & paid plans.
RISEUP	A nonprofit collective focused on secure communication for activists. Encrypts email on their own servers and avoids logging user activity. Free, but relies on donations to keep the service going.

Estos servicios no eliminarán todos los riesgos relacionados con el correo electrónico, pero harán un mejor trabajo que la mayoría de los servicios de correo electrónico (como Google, Yahoo, etc.) manteniendo tus correos privados.

¿Quieres cifrar tus propios correos electrónicos? Puedes—pero puede ser un poco complicado.

Hay una herramienta llamada PGP (Pretty Good Privacy, traducido a "Muy Buena Privacidad") o su versión gratuita GPG (GNU Privacy Guard) que te permite cifrar tus propios mensajes de correo electrónico. Es como poner tu mensaje en una caja cerrada para que solo la persona con la llave correspondiente pueda abrirla.

Esto es lo que toma para configurarlo:

1. Descarga un programa como PGP o GPG en tu computadora o teléfono.
2. Crea dos "llaves": una que puedas compartir con otros (pública), otra que solo tú conozcas (privada). Das tu llave pública a otros. Usan esta llave pública para bloquear sus mensajes hacia ti. Solo tu llave privada puede desbloquear esos mensajes. (Y puedes bloquear tus mensajes a otros con la llave privada que ellos pueden abrir con la llave pública.)
3. También necesitas usar una aplicación de correo electrónico que permita el uso de estas llaves. La mayoría de la gente usa Mozilla Thunderbird con un add-on llamado Enigmail para crear un correo electrónico que pueda utilizar el sistema de llave pública y privada.

Si esto suena un poco complicado, lo es. Pero una vez que configuras el sistema PGP o GPG, funciona de forma fiable.

Si quieres probar este método, la Electronic Frontier Foundation ofrece instrucciones paso a paso (con imágenes):

- Cómo usar PGP en Windows: https://ssd.eff.org/en/module/how-use-pgp-windows
- Cómo usar PGP en Mac: https://ssd.eff.org/en/module/how-use-pgp-mac-os-x
- Cómo usar PGP en Linux: https://ssd.eff.org/en/module/how-use-pgp-linux

Plug-Ins de Correo Electrónico

Un plug-in para correo electrónico añade funciones adicionales a tu correo. Esto incluye Grammarly para el correo electrónico, Boomerang para Gmail, SaneBox o Mailtrack.

Estos plug-ins, y los más recientes que usan IA (inteligencia artificial), hacen cosas como escribir correos electrónicos para ti, resumir hilos largos, programar correos, revisar tu gramática u organizar tus mensajes.

Aunque suena cómodo, hay una trampa: muchos plug-ins leen y almacenan tus correos electrónicos para que funcionen. Eso significa que tus mensajes privados podrían acabar en el servidor de otra persona.

Si te importa la privacidad, sé selectivo con qué plug-ins de correo usas, especialmente si provienen de grandes empresas tecnológicas o piden acceso completo a tu bandeja de entrada

¿Cuál es entonces la conclusión cuando se trata de correos electrónicos?

Si no lo escribirías en una postal, no lo envíes por un viejo correo electrónico.

Actualiza la configuración de privacidad en tu cuenta de correo electrónico, incluyendo la autenticación de dos factores (2FA).

Prueba usar servicios de correo electrónico que tengan servidores más seguros.

Potencialmente configura tu propio cifrado de correo electrónico.

Ten cuidado con los plug-ins que pones en tu correo.

Capítulo 4: Gestores de Contraseñas

¿Qué es un gestor de contraseñas y por qué debería importarme?

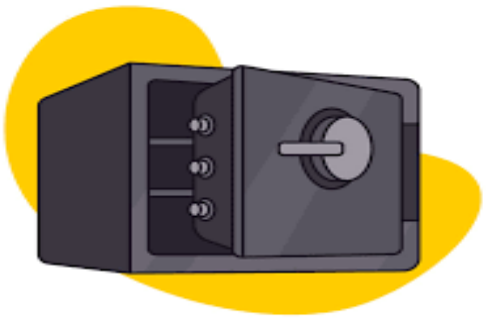
¿Alguna vez olvidas una contraseña y te quedas atascado dando click una y otra vez en "Restablecer mi contraseña"? O peor aún, ¿usas la misma contraseña para más de un sitio?

(No te avergüences. La mayoría de la gente lo hace.)

Aquí está el problema: si usas la misma contraseña en varios sitios web y solo uno de ellos es hackeado, el ladrón ahora tiene las llaves de toda tu vida online. Tu correo electrónico. Tu banco. Incluso tus servicios de streaming como Netflix o HBO.

Ahí es donde entran los gestores de contraseñas ("PMs" por su nombre en Inglés "Password Manager").

Piensa en un PM como una bóveda donde se guardan todas tus cosas preciadas. Solo necesitas recordar UNA "contraseña maestra" (como una llave o un número PIN de una bóveda) para desbloquear la bóveda. Dentro de la bóveda están todas tus otras contraseñas.



Los verdaderos beneficios de un PM son los servicios que puede ofrecer.

- Recuerda todas tus contraseñas por ti. No hay notas adhesivas. No hay hojas de cálculo. No hay intento de recordar si usaste una letra mayúscula o minúscula.
- Puede completar contraseñas automáticamente cuando visitas sitios web.
- Puede generar nuevas contraseñas largas y diferentes (como gR%8K!z7fM$32) para que las contraseñas sean más difíciles de descubrir para hackers o ladrones.
- Puede avisarte cuando hackers o ladrones descubran tu contraseña.
- Puede permitirte compartir contraseñas de forma fácil y segura con amigos y familiares.
- Te permite eliminar el acceso a tu contraseña al compartirla con amigos o familiares. ¿Rompiste con tu novia, novio o pareja? ¡Recupera tu contraseña esa misma noche!
- Ayuda a tu familia a gestionar sus contraseñas, especialmente a los padres con niños o a los adultos con sus padres mayores. Olvídate de tu mamá llamándote a las 7 de la tarde diciendo que ya no recuerda la contraseña de su correo electrónico.

Existen diferentes tipos de gestores de contraseñas:

Dashlane. A user-friendly password manager that also includes a password health checker and dark web alerts. Offers web and mobile apps.

Proton Pass. Proton also offers a VPN, encrypted email, and secure cloud storage.

Bitwarden. A free, open-source password manager that stores your passwords in a secure vault you can access on any device. You can host it yourself or use their cloud. It's one of the most trusted options in the privacy community.

NordPass. Nord also offers a VPN and secure cloud storage.

¿Deberías dejar que tu navegador web o dispositivo (como Chrome, Safari, Firefox, Apple Keychain) guarde tus contraseñas?

La mayoría hemos visto la pequeña ventana emergente: "¿Quieres guardar esta contraseña en Chrome?" O Firefox. O Safari. O en un iPhone Apple.

¡Es rápido, fácil y recuerda tus inicios de sesión por ti!

Pero, ¿es realmente seguro dejar que tu navegador web o dispositivo guarde tus contraseñas?

La respuesta corta: es mejor que nada, pero no es la mejor opción si quieres una protección de privacidad más seria.

¿Lo bueno?

Chrome, Firefox y Safari "**cifran**" tus contraseñas guardadas, es decir, que se guardan en forma de codificación para que nadie pueda leerlas. (Así que en lugar de guardar tu contraseña como "applepie27", la contraseña parece "#4kkl3@*" para cualquiera que no seas tú que intente acceder online). Chrome, Firefox y Safari también te avisarán si aparece una contraseña en una brecha de datos conocida.

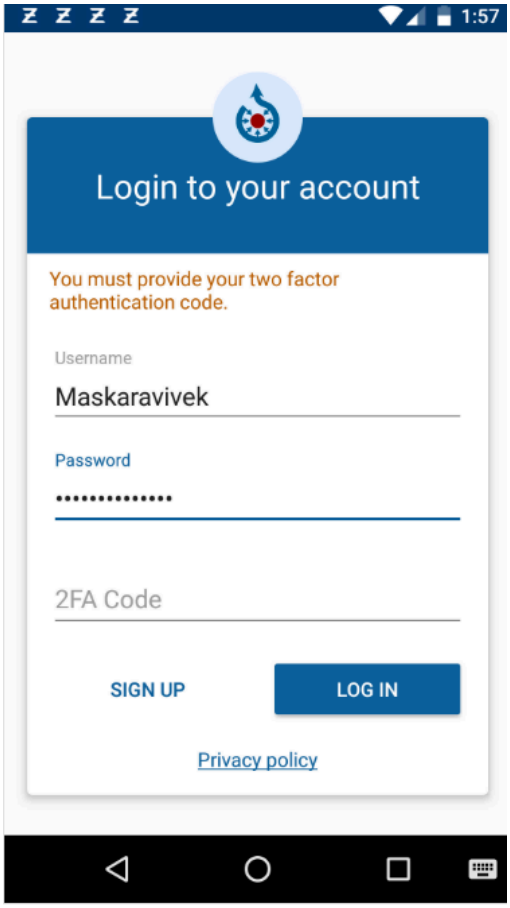
¿Lo malo?

- **Vinculado a las grandes tecnológicas:** Cuando usas un navegador como Chrome, tus contraseñas se almacenan con tu cuenta de Google. ¡Eso significa que una empresa puede tener acceso a tu historial de búsqueda, ubicación, correos electrónicos y contraseñas!
- **Funciones limitadas**: Los gestores de navegadores no te ayudan a crear contraseñas fuertes que sean tan buenas como las que crean las aplicaciones reales de gestores de contraseñas.
- **Riesgo de robo de dispositivo**: Si alguien accede a tu dispositivo desbloqueado, puede que consiga tus contraseñas directamente a través del dispositivo o navegador, especialmente si no usas una contraseña maestra para proteger el acceso a la lista de contraseñas almacenada en tu navegador.
- **No hay doble factor para la bóveda**: La mayoría de los navegadores no ofrecen una autenticación 2FA (doble factor) fuerte para la bóveda de contraseñas de tu navegador como sí lo hacen los gestores de contraseñas dedicados.

¿Qué es la Autenticación de Dos Factores (2FA) y, por qué molestarse?

Quizá te haya pasado esto antes: intentas iniciar sesión en tu correo de Gmail o correo del trabajo, y te envía un código a tu teléfono o te pide que apruebes el inicio de sesión en otra app como "Duo Mobile", "Authy", "Microsoft Authenticator", "Google Authenticator" o "1Password".

Quizá tu trabajo lo requería. O quizá tu banco envió un correo de advertencia: "Hemos añadido protección extra a tu cuenta."



Podrías haberte quejado y pensado: "Uf, ¿otro paso?"

Así que... ¿Qué es la Autenticación de Dos Factores (2FA)? ¿Por qué la usaría alguien? ¿No es que simplemente retrasa el inicio de sesión en mis cuentas?

Autenticación de Dos Factores = Doble cerradura en tu puerta digital

Imagina que tu cuenta en línea es como la puerta de tu casa. Una contraseña es tu llave. Esa es una cerradura. ¿Pero qué pasa si alguien roba o copia tu llave? Ahí es donde entra la segunda cerradura.

Supongamos que alguien roba tu contraseña de correo electrónico e intenta iniciar sesión con esa contraseña robada. Si has activado la 2FA, tu correo requerirá que esta persona proporcione una segunda llave para verificar su identidad. La mayoría de los hackers no tienen esa segunda llave, así que se rinden.

Esa segunda llave podría ser:

- Un código enviado a tu móvil
- Un código enviado a tu cuenta de correo electrónico asociada a la aplicación a la que intentas acceder
- Una app especial como Authy o Google Authenticator
- Una llave física
- Una huella dactilar o un escaneo facial

¿Cuándo deberías usar la 2FA?

Cada vez que se ofrece, especialmente para:

- Cuentas de correo electrónico
- Aplicaciones bancarias y de pago (Venmo, PayPal)
- Redes sociales (Instagram, Facebook)
- Historiales médicos (Kaiser Permanente)
- Almacenamiento en la nube (Google Drive, Dropbox)

Sí, añade un paso extra. Pero bloquea casi todas las formas sencillas en que los hackers entran en tus cosas. De hecho, Microsoft dijo en 2024 que el 99,9% de las cuentas hackeadas no tenían activada la 2FA. ¡Es un número enorme!

Así que la próxima vez que una página web diga "¿Añadir autenticación de dos factores?" simplemente di que sí. Es gratis, es fácil y puede ahorrarte un gran dolor de cabeza más adelante.

¿Hay algún inconveniente?

Una desventaja de la autenticación en dos factores es que algunos sitios solo te ofrecen una forma de obtener el código, como enviarlo a tu móvil o a un correo electrónico.

Si no puedes acceder a esa opción porque olvidaste la contraseña del correo electrónico o porque tu teléfono está perdido/roto/indisponible, puede que no puedas iniciar sesión en absoluto.

¡La 2FA requiere que tengas cuidado de tener acceso al lugar donde se envía el código de autenticación!

¿Cuál es la conclusión en cuanto a las contraseñas?

(1) Los gestores de contraseñas son una excelente forma de crear y llevar un control de contraseñas fuertes.

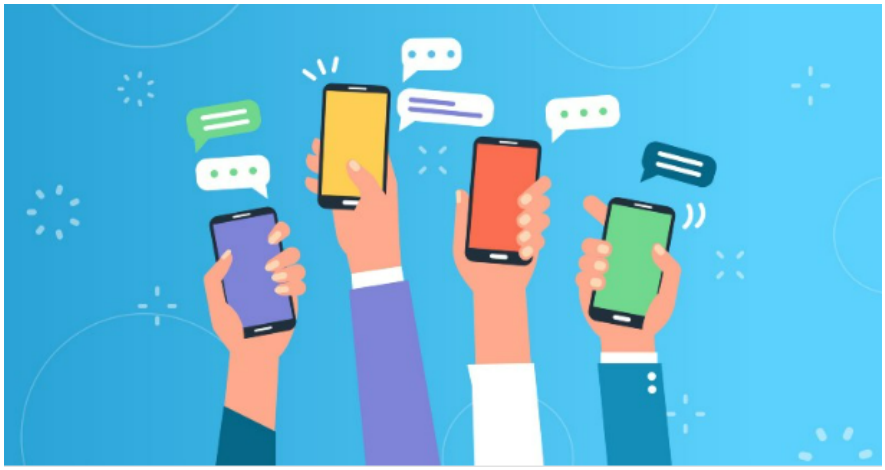
(2) Utiliza la 2FA siempre que puedas.

AQUÍ tienes un vídeo de YouTube que trata sobre los gestores de contraseñas.

Capítulo 5: Mensajes privados

Cómo enviar mensajes sin que todo el mundo lea lo que has escrito

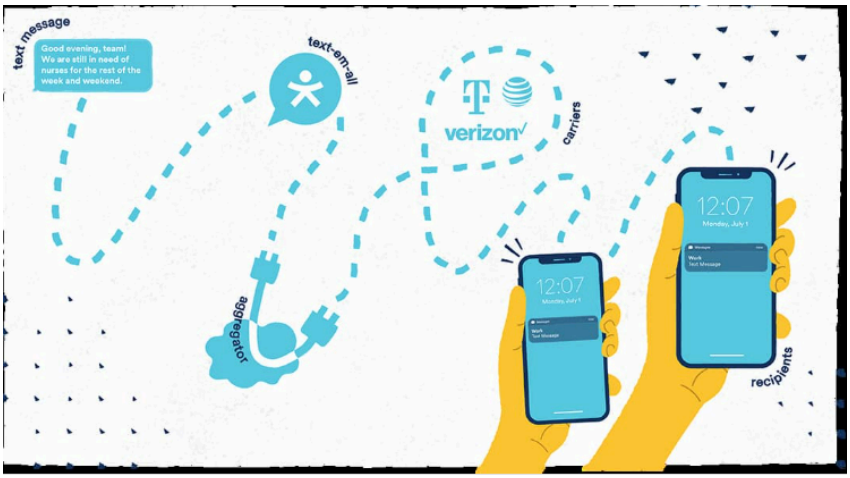
Enviar mensajes de texto con un smartphone es la forma en que la mayoría hablamos: mensajes rápidos a amigos, parejas, compañeros de trabajo o familiares. Pero hay algo que mucha gente no se da cuenta: ¡no todos los textos son privados!



Ese mensaje que enviaste la semana pasada ("¿Puedes traer leche?") puede que no parezca gran cosa. ¿Pero y si hubiera sido tu nueva dirección? ¿Un enlace bancario? ¿Una foto privada? ¿O una conversación sobre tu salud, tu hijo, tu trabajo?

La realidad es que los mensajes de texto pueden ser leídos por tu compañía telefónica, copiados mientras viajan de teléfono a teléfono, e incluso accedidos en caso de brecha de datos. Así es como funciona eso:

1. Escribes un mensaje en tu móvil: "¡Voy tarde! Estaré allí a las 7"
2. Tu teléfono envía ese mensaje a tu compañía telefónica.
3. La compañía telefónica reenvía ese mensaje a la compañía telefónica de tu amigo.
4. La compañía telefónica de tu amigo envía ese mensaje al teléfono de tu amigo.



En ningún momento de esa cadena de comunicación tu mensaje de texto está protegido digitalmente. A menos que utilices lo que se llama una aplicación de mensajes de texto "cifrada", el mensaje de texto es visible para:

- Tu compañía telefónica
- Hackers que puedan acceder a partes débiles de ese sistema de mensajería de texto
- Cualquiera que acceda a los registros de la compañía telefónica
- Agencias gubernamentales que solicitan acceso a los registros de la compañía telefónica

¡Ahí es donde entran las "aplicaciones de mensajería cifradas"! Son una de las mejoras de privacidad más fáciles que puedes hacer.

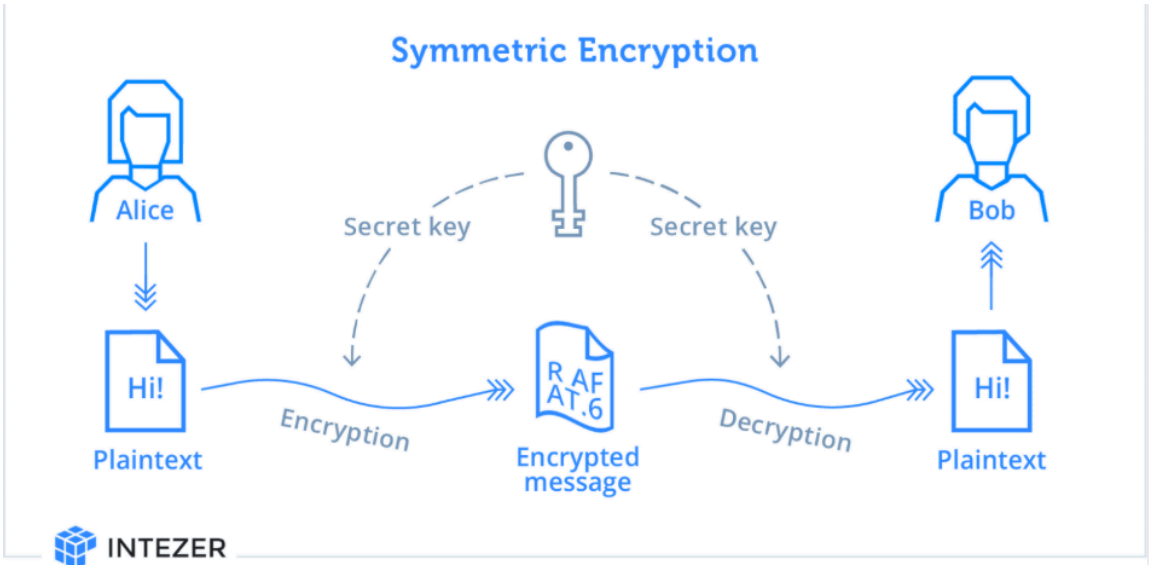
¿Entonces, qué es la mensajería cifrada?

Enviar mensajes cifrados es como meter tu mensaje en una caja cerrada con candado, y solo la persona a la que estás escribiendo tiene la llave de esa caja cerrada. ¡Aunque un hacker, una compañía telefónica o incluso un gobierno intente apropiarse de la caja con tu mensaje de texto, no pueden leer el mensaje de texto porque no tienen la llave de esa caja!

¿No paro de oír hablar de cifrado de extremo a extremo?

Cuando alguien dice que un servicio proporciona **cifrado de extremo a extremo**, quiere decir que solo tú y la persona a la que estás enviando mensajes pueden leer los textos porque:

- El mensaje de texto está bloqueado ("cifrado") dentro de tu teléfono
- El mensaje de texto permanece bloqueado mientras viaja al teléfono de la otra persona
- El mensaje de texto solo se desbloquea cuando llega al teléfono de la otra persona porque solo esa persona tiene la llave para desbloquear ("descifrar") el mensaje.



Así que, con el cifrado de extremo a extremo, incluso si un hacker, una empresa o un gobierno roba el mensaje de texto mientras viaja desde ti a tu amigo, el hacker, la empresa o el gobierno no pueden leer el mensaje porque no tienen la llave para desbloquear la protección ("cifrado") que oculta tu texto.

A veces las cosas solo están "cifradas en tránsito". ¿Qué significa eso? Significa que tu mensaje está protegido mientras se envía, pero el teléfono o la empresa tecnológica que lo envía aún pueden leerlo o almacenarlo. Esto es como si la oficina de correos pudiera leer el contenido de cada carta que envías. En

comparación, con el cifrado de extremo a extremo, solo el remitente y el receptor pueden ver lo que hay dentro de tu carta.

Por eso el cifrado de extremo a extremo es una de las herramientas más potentes para la privacidad hoy en día. Ayuda a asegurarte de que tus mensajes de texto sean leídos solo por ti y por la persona a la que envías el mensaje.

¿Entonces, cómo consigo esa mensajería cifrada del que hablas?

Vamos a repasar los servicios de mensajería cifrada más comunes:

What is Signal? Signal is a texting program that provides mostly secure end-to-end encryption. Signal doesn't sell ads, and it doesn't collect your data. It runs entirely on donations and grants.

Sounds too good to be true? The catch is that both users have to have the program to enable the encryption, so you need to use Signal and you need to make your friends use Signal too.

Who owns Signal? The Signal Foundation, a non-profit organization focused on privacy.

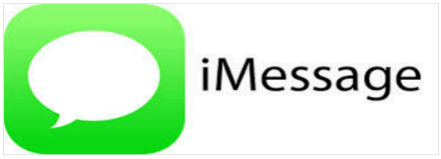
What is Whatsapp? Whatsapp is heavily used outside America and was one of the first messaging services to use end-to-end encryption. However, even though your messages are encrypted, the company who owns WhatsApp (Meta, previously called Facebook) still collects metadata.

What does metadata mean? Let's say you send your friend a letter in the mail. The message is what you wrote inside the envelope. The metadata is what's on the outside of the envelope, which includes information like: Who the message is from; Who the message is going to; The date and time the message was sent; The return address; The post office the message went through. That's still a lot of information that Meta collects about you!

Who owns WhatsApp? WhatsApp was bought by Meta, a technology company with some of the worst privacy practices on the planet.

What is Telegram? Telegram is a fairly new encrypted texting service. It offers self-destruct features similar to the program Snapchat. Regular chats on Telegram are not end-to-end encrypted unless you turn on “Secret Chat.”

Who owns Telegram? Telegram was started by Pavel Durov, a Russian tech entrepreneur who left Russia and moved the company abroad. Telegram is now based in Dubai, and it’s funded by private investors.



What is iMessage? When you send an iMessage (those blue bubble texts), Apple uses real end-to-end encryption. So, not even Apple can read what you wrote. But there’s some drawbacks: this encryption only works if both people are using Apple devices, like iPhones. Apple collects some metadata, just like Meta for WhatsApp.

Also, if you back up your text messages to iCloud without turning on something called **Advanced Data Protection**, your messages are no longer fully private. This is because your messages will still be accessible to hackers and law enforcement if they get access to the iCloud.

¿Cuál es la conclusión cuando se trata de enviar mensajes de texto?

¡Utiliza un servicio de mensajería cifrada siempre que sea posible!

AQUÍ tienes un vídeo que habla sobre las aplicaciones de mensajería.

Capítulo 6: Navegadores, Motores de Búsqueda y Herramientas para Proteger tu Privacidad en Línea

Cada vez que abres tu navegador de internet (ya sea Chrome, Safari, Firefox o Edge) dejas pequeñas migajas digitales atrás. Esas migajas indican a las empresas qué buscas, qué páginas web visitas, cuánto tiempo permaneces allí y, a veces, incluso tu ubicación.

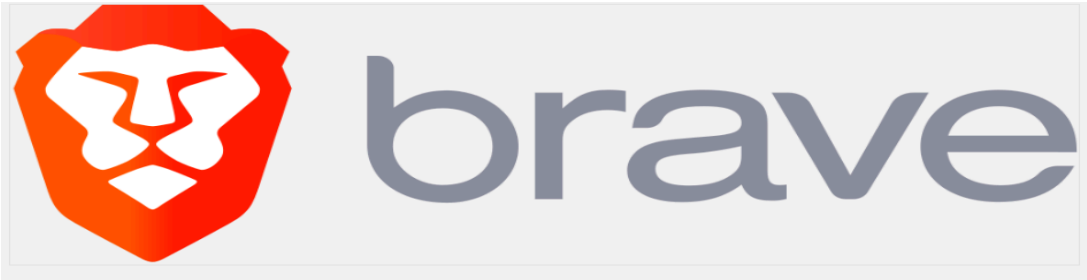
Si eso suena raro para tí, ¡no estás equivocado!

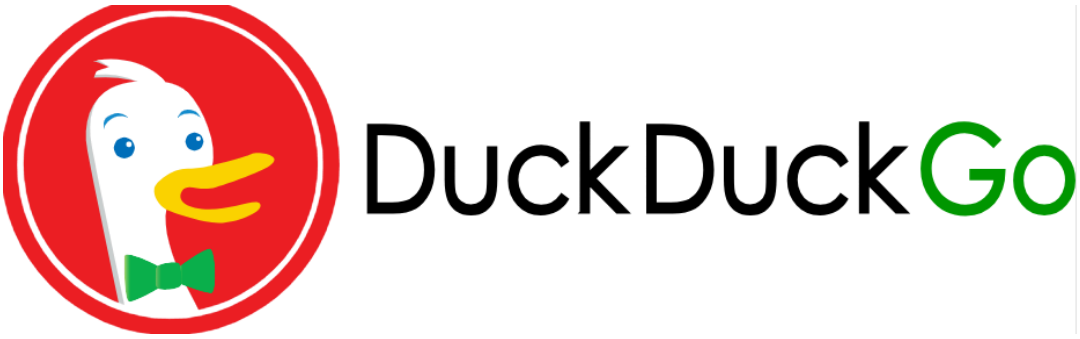
Existen herramientas que facilitan la navegación en línea de forma privada sin necesidad de convertirse en un experto tecnológico. Aquí hablaremos de algunos de ellos: navegadores que mejoran la privacidad, software de bloqueo de anuncios y Redes Privadas Virtuales (VPN).

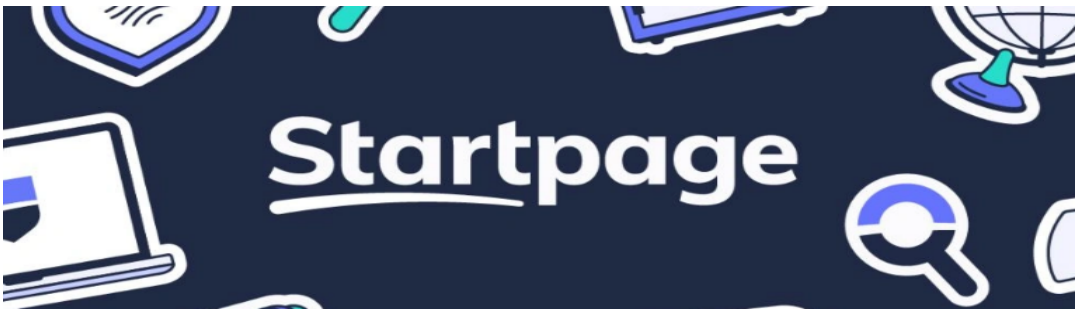
Navegadores y motores de búsqueda: Elige la puerta correcta a Internet

La mayoría de la gente usa navegadores como Chrome o Safari porque vienen preinstalados en los dispositivos. Pero estos navegadores suelen rastrear lo que haces en línea. Si quieres un navegador que te dé más control sobre tu privacidad, prueba Mozilla Firefox o Brave. Son gratis, funcionan igual que los otros navegadores y no te espían tanto.

Para los motores de búsqueda, prueba a cambiar de Google a Brave, Firefox, Startpage o DuckDuckGo. Estos motores de búsqueda no mantienen un historial de lo que buscas.





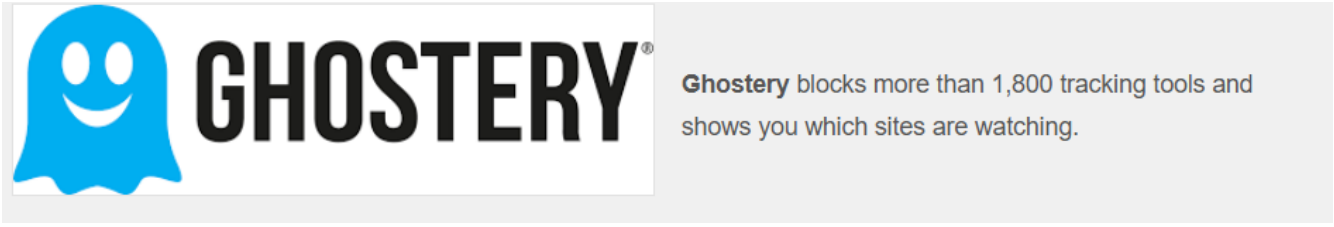


Detén los rastreadores: Software anti-rastreo

Cada vez que visitas una página web, los "rastreadores" pueden empezar a seguirte por internet. Estos rastreadores observan a lo que haces click, lo que buscas e incluso cuánto tiempo permaneces en una página.

Y como un detective privado, estos rastreadores construyen un perfil sobre ti. Este perfil se utiliza para dirigir anuncios hacia ti o el perfil se vende a otras empresas.

Las herramientas anti-rastreo bloquean esos rastreadores para que no te espien. Aquí tienes algunos buenos:



AdBlock Plus blocks pop-ups and ads.

uBlock is a free, open-source ad content blocker. Here is a blog post and video explaining how to install uBlock.

¿Qué es una VPN, y la necesitas?

Una VPN, o "Red Privada Virtual", es una herramienta que oculta lo que haces en línea a tu proveedor de internet, a tu colegio, a tu trabajo o a cualquiera que intente espiarte, ¡especialmente cuando usas Wi-Fi público!

Pero no todas las VPN son seguras. Algunos rastrean tu actividad y venden tus datos a anunciantes, lo que anula completamente el propósito de usar una VPN para la privacidad. Por eso es importante elegir una VPN en la que puedas confiar.

Las opciones más seguras incluyen:

¿Quieres aún más privacidad? Prueba con el navegador Tor

El navegador Tor es para personas que buscan privacidad seria. Tor oculta tu ubicación, bloquea los rastreadores y mantiene tu actividad en internet privada. Pero hay intercambios:

- Tor es más lento que los navegadores normales.
- Puede llamar la atención de las agencias gubernamentales, ya que vigilan el tráfico de Tor más de cerca.
- Algunas páginas web no funcionan correctamente en Tor.

Solo para tomarlo en cuenta, si vives en un pueblo pequeño y eres el único que usa Tor, tu actividad en línea podría destacar.

¿Cuál es la diferencia entre VPN y Tor?

Esto es un poco más técnico, y no es muy necesario entender si planeas usar una VPN y/o Tor. Pero si tienes curiosidad, ¡sigue leyendo!

Una **VPN** crea un túnel seguro entre tu dispositivo e internet. Oculta tu dirección IP (es un número que identifica dónde estás, similar a una dirección postal) y oculta lo que haces en línea a tu proveedor de internet, trabajo, colegio, etc. Sin embargo, tu proveedor de VPN puede llevar un registro de todo lo que haces en línea, por eso es tan importante elegir una VPN fiable y que proteja la privacidad. Por ejemplo, los que se han identificado arriba: Mullvad, ProtonVPN, NordVPN, etc. Una VPN es buena para la privacidad diaria, incluyendo el uso de Wi-Fi público o streaming en línea.

Navegador Tor envía tu tráfico de internet a través de varias computadoras aleatorias (llamadas "nodos") antes de llegar a su destino final. Esto hace que sea muy difícil rastrear cualquier cosa hasta ti, incluso para gobiernos o empresas tecnológicas. Esto hace que el navegador Tor sea muy bueno para el máximo anonimato y situaciones de alto riesgo (activismo, periodismo, investigación sensible).

Entonces, ¿cuál es la conclusión en cuanto a navegadores, rastreadores, VPN y Tor?

(1) Existen navegadores/motores de búsqueda que protegen mejor tu privacidad digital que Google.

(2) Utiliza complementos anti-rastreo para protección adicional en línea.

(3) Una VPN y Tor son tus mejores opciones para ocultar tus actividades en línea.

AQUÍ tienes un vídeo sobre la privacidad de los navegadores.

Capítulo 7: Videollamadas

¿Recuerdas cuando las videollamadas parecían algo del futuro? Ahora están por todas partes: reuniones escolares, visitas al médico, entrevistas de trabajo, visitas familiares e incluso noches de juegos. Ya sea que uses FaceTime, Zoom, Meetings

o WhatsApp, las videoconferencias son la forma en que muchos de nosotros nos mantenemos conectados.

Pero al igual que con los mensajes de texto, no todas las videollamadas son privadas. Algunas empresas de videollamadas observan lo que haces, almacenan grabaciones o rastrean "metadatos".

¿Qué son los "metadatos"?

Describimos esto en el contexto del Capítulo 5 sobre Mensajes de Texto Privados. Los metadatos son información que describe o da contexto a otros datos.

Piénsalo como la etiqueta en un paquete. La etiqueta te da información sobre el paquete, igual que los metadatos te informan sobre los datos. Por ejemplo, para una fotografía (los datos), los metadatos incluyen: la fecha y hora en que se tomó la foto, el modelo de la cámara, la ubicación (coordenadas GPS) y quizás el nombre del fotógrafo.

Los metadatos de una videollamada pueden indicar a la empresa qué tipo de dispositivo usaste (teléfono o computadora, Mac o Windows), dirección IP (que muestra tu ubicación), cuándo llamaste, quién se unió a la llamada y cuánto tiempo permaneciste en la reunión.

Ahora repasemos tus opciones para las videollamadas:

FaceTime (Apple only): If you and the other person both use Apple devices (iPhones, iPads, or Macs), FaceTime is a pretty good option. Apple uses end-to-end encryption, which means your video call is locked down, and no one can watch or listen in (not even Apple).

But FaceTime only works with other Apple users. If one person's on Android, you're out of luck.

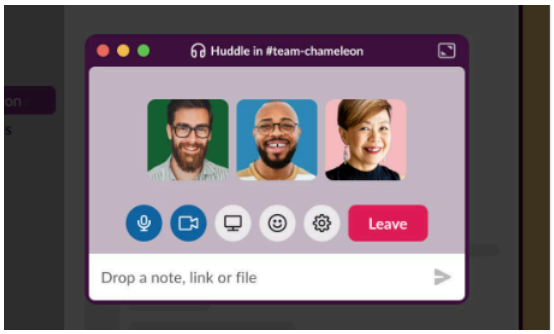
WhatsApp Video offers end-to-end encrypted video calls, so the video and audio are private. But WhatsApp is owned by Meta (the company behind Facebook), which collects lots of "metadata."

Zoom is used by schools, businesses, and families for everything from work meetings to birthday parties.

But here's what to know: Zoom does not use full end-to-end encryption by default. They do offer a feature called "end-to-end encryption", but you have to turn it on manually, and it has some limits (like you can't use all features when it's on). Also, all participants need to use the Zoom app—so yes, you'll need to download it. Zoom also collects some "metadata."

Google Meet is built into Gmail and Google Calendar. Google encrypts calls while they're are happening, but not with end-to-end encryption. That means Google could access the content of your video call if required. Google Meet also collects "metadata."

Jitsi Meet is a lesser-known but useful video service that focuses on privacy. Jitsi offers encrypted video conferencing through your browser. It doesn't collect "metadata," doesn't require registration, and you can use it on any device with a browser. You just go to the website, start a room, and send your friend or group the link.



Slack Huddle: Slack is a workplace messaging tool, and its Huddles feature lets people start quick voice or video chats. Huddles are encrypted while they happen between devices, but not with end-to-end encryption. Slack could technically access what was said or shown in the video. Slack also collects "metadata."

Microsoft Teams video calls are encrypted as they happen, but not with end-to-end encryption. The meeting organizer has to turn on end-to-end encryption before the meeting starts. Microsoft also collects "metadata."

IA (Inteligencia Artificial) y Videoconferencias

Cada vez más aplicaciones de videoconferencia (como Zoom, Microsoft Teams y Google Meet) utilizan IA para facilitar las llamadas. La IA puede hacer cosas como:

- Convierte el habla en texto (subtítulos en directo o transcripciones)
- Resumen automático de reuniones
- Identifica quién está hablando
- Filtra el ruido de fondo

Solo ten en cuenta: las funciones de IA a menudo requieren grabar o analizar tu voz, vídeo y lo que se dice en las reuniones. Esos datos pueden almacenarse, ser vistos por personas que no aprobaste, o incluso utilizada para entrenar otros modelos de IA.

¿Qué puedes hacer?

- Utiliza servicios que respeten la privacidad siempre que sea posible (como Jitsi Meet).
- Pregunta si la reunión está siendo grabada, y comenta si no te sientes cómodo.
- Desactiva funciones que no necesites, como la autotranscripción o el análisis facial.

Entonces, ¿cuál es la conclusión cuando se trata de servicios de videoconferencia?

Las videollamadas son convenientes, ¡pero no siempre son privadas! Si no lo dirías en una sala llena de desconocidos, piénsalo dos veces antes de decirlo por videollamada.

Capítulo: 8 La Nube

Probablemente hayas oído la expresión "la Nube". ¿Pero qué significa realmente eso?

La Nube es una forma de almacenar tus archivos (como fotos, documentos o copias de seguridad) en la computadora de otra persona que tiene mucha más memoria que la tuya, normalmente la computadora de alguna gran empresa (por ejemplo, Amazon, Microsoft). Luego puedes acceder a tus archivos en esa otra computadora a través de internet.

Cuando algo está en la Nube, puedes abrirlo desde cualquier sitio. No necesitas llevar una memoria USB ni preocuparte de que la computadora falle. Solo necesitas una conexión a Internet. La Nube es rápida, sencilla y utilizada por miles de millones de personas cada día.

Pero, como todo en línea, la Nube conlleva riesgos para la privacidad.

Proveedores de Nube comunes que quizá ya estés usando

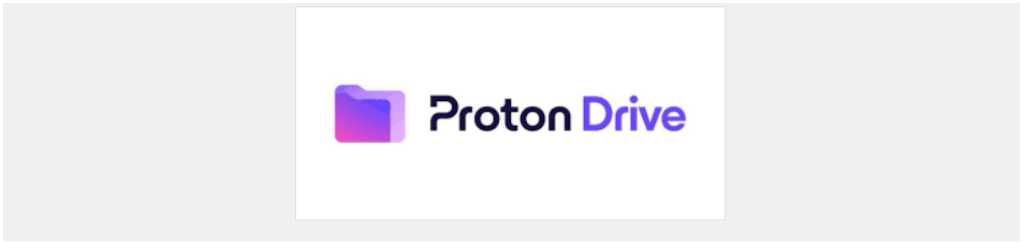
iCloud (Apple): Si tienes un iPhone, probablemente estés usando iCloud. Automáticamente hace copias de seguridad de tus fotos, mensajes, notas y más. Apple dice que **cifra*** (ver la definición más abajo) tus datos, pero Apple posee las claves de tu Nube, lo que significa que aún pueden acceder a tus datos en la Nube si la policía o la ley lo requieren. Para evitar esto, tienes que activar la Protección Avanzada de Datos.

Dropbox: Dropbox es un servicio popular de almacenamiento en la Nube para compartir archivos y hacer copias de seguridad de documentos personales o de trabajo. Es fácil de usar y funciona en cualquier dispositivo. Pero Dropbox no ofrece cifrado completo de extremo a extremo* por defecto.

OneDrive: OneDrive es el sistema de almacenamiento en la Nube de Microsoft, integrado en la mayoría de las computadoras Windows. Hace copias de seguridad de tus documentos, fotos y carpetas de escritorio en línea para que puedas acceder a ellos desde cualquier lugar. Microsoft tiene las claves de tus datos, así que pueden leer tus archivos si es necesario. Los archivos pueden ser escaneados en busca de "violaciones de políticas" y tu información podría compartirse con las fuerzas de la ley u otros terceros.

GoogleDrive: Tus archivos no están cifrados de extremo a extremo*, lo que significa que Google puede acceder al contenido si quiere. Google puede escanear tus archivos, vincular tu actividad a tu perfil personal y entregar tus datos a las autoridades si se le solicita.

> **¿Qué puedo usar?** Si quieres tener más control sobre tus datos, existen herramientas en la Nube diseñadas específicamente para la privacidad:


Proton Drive


NordLocker


Nextcloud


tresorit


SPIDEROAK

Necesito borrar un archivo de mi computadora. ¿Cómo puedo asegurarme de que realmente se ha ido?

La mayoría de la gente no se da cuenta de que cuando "eliminas" un archivo, usualmente no desaparece realmente de tu computadora. Simplemente se marca como "se puede sobrescribir". Eso significa que, hasta que ese espacio de memoria en tu computadora se reutilice para guardar otra cosa, alguien podría recuperar el archivo eliminado.

Si usas Windows, un programa gratuito llamado Eraser puede realmente deshacerse de archivos, asegurándose de que se borren completamente electrónicamente y no puedan recuperarse. Imagínalo como una trituradora digital de papel.

Si usas MacOS, deberías activar FireVault o puedes usar el programa gratuito llamado Permanent Eraser.

¿Cuál es la conclusión al usar la Nube?

(1) Ten cuidado con lo que subes a la "Nube".

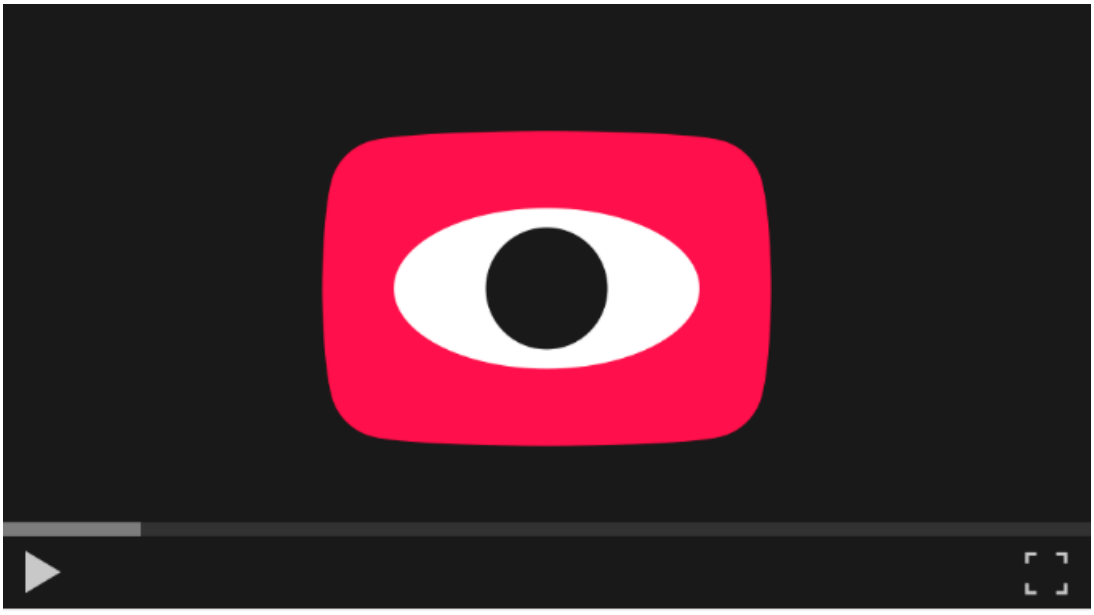
(2) Utilizar una "Nube" más segura siempre que sea posible.

*Cifrado explicado en el capítulo "Introducción" AQUÍ

Capítulo 9: Reproductores de Vídeo en Línea

Cuando te sientas a ver un vídeo, lo último que quieres es que te vean de regreso. Pero eso es exactamente lo que ocurre cuando usas YouTube, servicios de streaming y televisores inteligentes.

Estas herramientas están diseñadas para la comodidad, pero también recopilan muchos datos personales. Lo que ves, cuánto tiempo lo ves, en qué haces click, en qué pausas—lo registran todo. Esa información puede usarse para crear un perfil sobre ti, mostrarte anuncios segmentados o incluso moldear tu experiencia online.



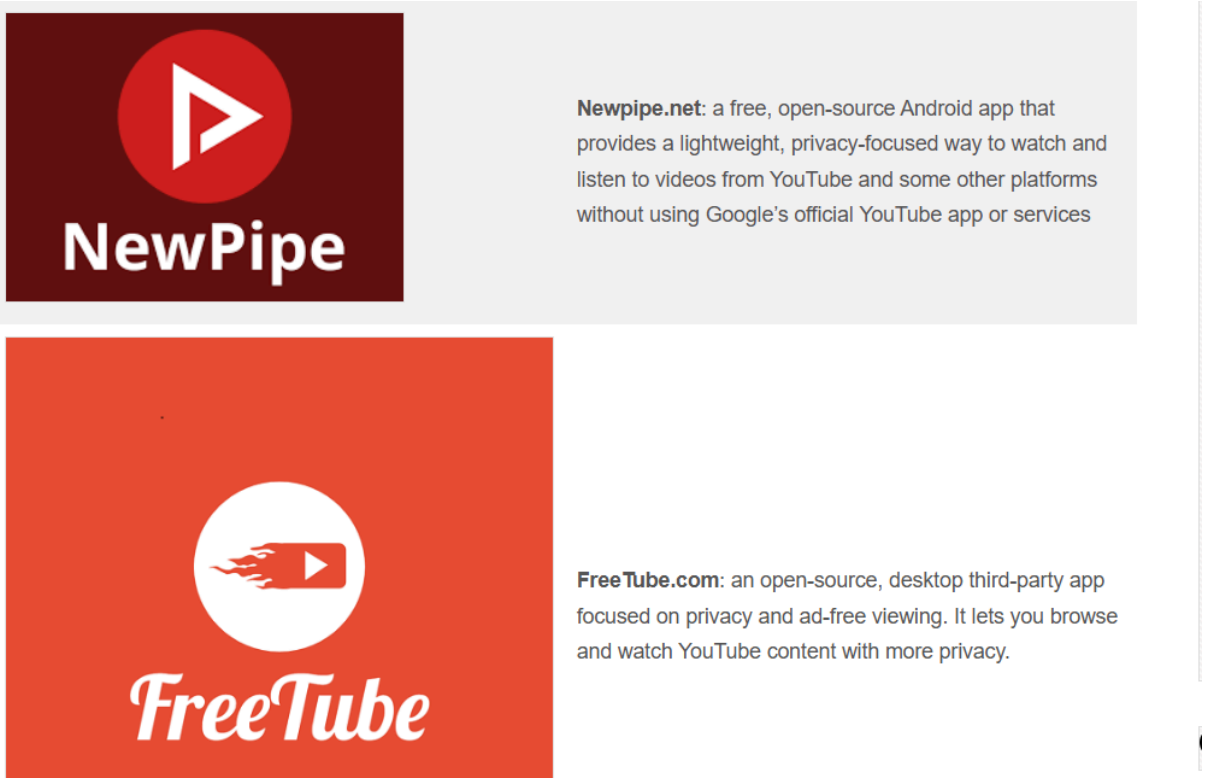
Vamos a profundizar un poco en YouTube, que es gratuito, pero no está libre de rastreo. Google (que es dueño de YouTube) utiliza tu historial de vídeos, búsquedas y le gusta:

- Utilizarte como objetivo con anuncios
- Compartir datos con anunciantes y otros socios
- Vincula tu actividad a tu cuenta de Google

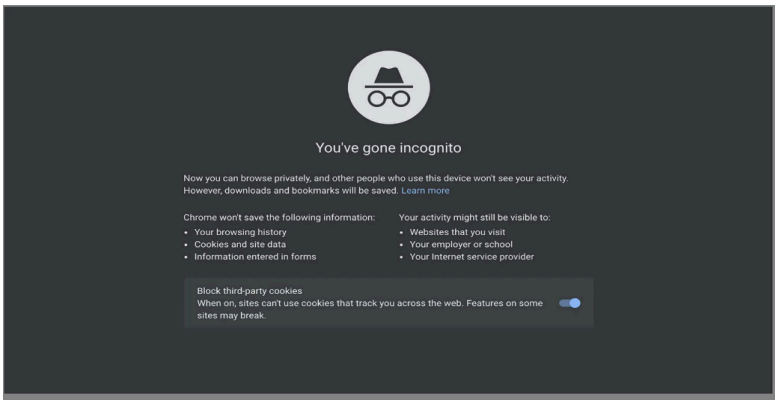
Si has iniciado sesión en tu cuenta de Gmail, el seguimiento obtiene aún más información personal tuya. Tu comportamiento en YouTube está conectado a tu Gmail, ubicación e historial de búsquedas.

Alternativas privadas a YouTube

Si te gusta ver vídeos en YouTube pero no quieres que te rastreen, prueba estas dos herramientas:



También puedes ver vídeos de YouTube en modo incógnito en tu navegador o usando una VPN.



(Hablamos anteriormente sobre las VPN y cómo pueden usarse para ocultar lo que haces en Internet AQUÍ.)

Capítulo 10: Aplicaciones de Bienestar y Salud

Las aplicaciones de salud pueden ayudarte a controlar tus pasos, entrenamientos, ritmo cardíaco, sueño o incluso tu ciclo menstrual. Están integrados en muchos teléfonos (como Apple Health, Samsung Health y Google Fit) o descargados por separado (como Strava y Flo). Estas aplicaciones son súper prácticas, ¡pero también recopilan parte de la información más privada y sensible sobre ti!

Y aquí está la cuestión: no todos los datos de salud están protegidos, especialmente si usas una aplicación normal en lugar de ir al médico. Eso significa que tu información (como la frecuencia con la que corres, cuándo ovulas o cuánto duermes) puede almacenarse, compartirse o incluso venderse por la empresa propietaria de la app.

AQUÍ tienes un resúmen de la privacidad de las aplicaciones comunes de salud reproductiva (para menstruaciones, embarazos, fertilidad, etc.)

Qué puedes hacer para proteger tus datos de salud

- Desactiva las copias de seguridad en la Nube para aplicaciones de salud y fitness si no quieres que tus datos se almacenen en línea.
    - Utiliza un código de acceso y/o contraseña fuerte para la app si se ofrece la opción.
    - Revisar permisos de la app (¿Realmente tu contador de pasos necesita acceso a tu micrófono o contactos? Probablemente no. Haz click AQUÍ para saber cómo cambiar la configuración del iPhone. AQUÍ para Android.)
    - Evita registrar datos de salud muy sensibles en las aplicaciones.

Capítulo 11: Asistentes Inteligentes y Privacidad (Por Qué Quizá Quieras Evitar Decir "Oye, Alexa")

Asistentes inteligentes como Amazon Alexa, Google Assistant y Apple Siri pueden ser muy útiles. Puedes pedirles que pongan música, pongan un temporizador o vean el clima, todo simplemente hablando. Pero la forma en que funcionan conlleva riesgos reales para la privacidad.

Estos dispositivos siempre están escuchando por su "palabra de activación" (como "Hey Siri" o "Alexa"). Eso significa que están monitorizando constantemente el sonido en tu casa, esperando a ser activados. A veces, empiezan a grabar por accidente, como cuando dices algo que suena como su nombre.

Las empresas dicen que estas grabaciones son seguras, pero en muchos casos:

- Las grabaciones se almacenan y pueden ser revisadas por los empleados
- Algunos clips de voz se conservan a menos que los borres manualmente
- Los datos pueden compartirse con otras empresas o con las fuerzas de la ley

Nuestro consejo: No utilices asistentes inteligentes activados por voz

Los dispositivos que siempre escuchan no son buenos para la privacidad. No tienes que renunciar por completo a las herramientas inteligentes, pero recomendamos saltarte los asistentes activados por voz, ¡y usar aplicaciones o dispositivos que te den el control!

Capítulo 12: Filtración de Datos (Antes De Que Tu Información Sea Robada)

Una "brecha de datos" ocurre cuando una empresa u organización que posee tu información personal es hackeada o filtra información por error. Esto puede incluir cosas como:

- Tu nombre, dirección, número de teléfono
- Correo electrónico y contraseñas
- Número de Seguro Social
- Datos de tarjeta de crédito o de cuenta bancaria
- Registros médicos o de seguros

Una vez que esta información está disponible, puede usarse (a veces meses o incluso años después) para robo de identidad o fraude de crédito.

Qué hacer si oyes sobre una brecha de datos

Puede que recibas un correo electrónico o una alerta de noticia diciendo que tus datos forman parte de una brecha. Aunque solo sea tu correo electrónico y contraseña, es inteligente tomar la alerta en serio. Dos de los pasos más importantes son:

(1) Congela tu crédito

Congelar tu crédito significa que nadie puede abrir nuevas cuentas a tu nombre (ni siquiera tú) hasta que lo descongeles. Es gratis, y puedes activarlo y desactivarlo cuando quieras.

Congelar tu crédito NO afecta a tus tarjetas de crédito o préstamos actuales. Te protege de que alguien solicite una tarjeta de crédito, un préstamo o un contrato de alquiler usando tu identidad.

Necesitas congelar tu crédito en cada una de las tres principales agencias de crédito**:** Equifax**,** Experian**,** TransUnion**.,**

Este es uno de los pasos más sólidos que puedes tomar para evitar el robo de identidad antes de que ocurra.

(2) Obtén tu informe crediticio semanal gratuito de estas tres agencias de crédito

AnnualCreditReport.com es el sitio oficial establecido por las 3 principales agencias de crédito (Equifax, Experian, TransUnion) para cumplir con la ley federal que les obliga a ofrecer al menos un informe de crédito gratuito anualmente. Estas 3 agencias de crédito ahora ofrecen voluntariamente informes semanales de crédito. ¡Solo tienes que registrarte!

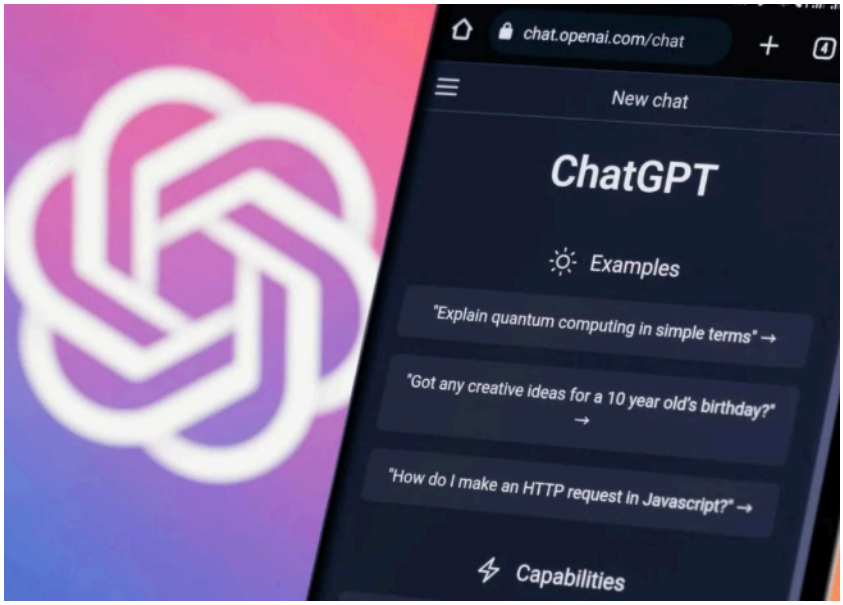
¿También tengo que pagar a una empresa para que controle si mi información personal está en línea?

Probablemente no. La mayoría de las personas pueden mantenerse seguras sin pagar por un servicio de identidad o monitorización de crédito, siempre que tomen algunos pasos básicos para proteger su seguridad y privacidad digital, incluyendo:

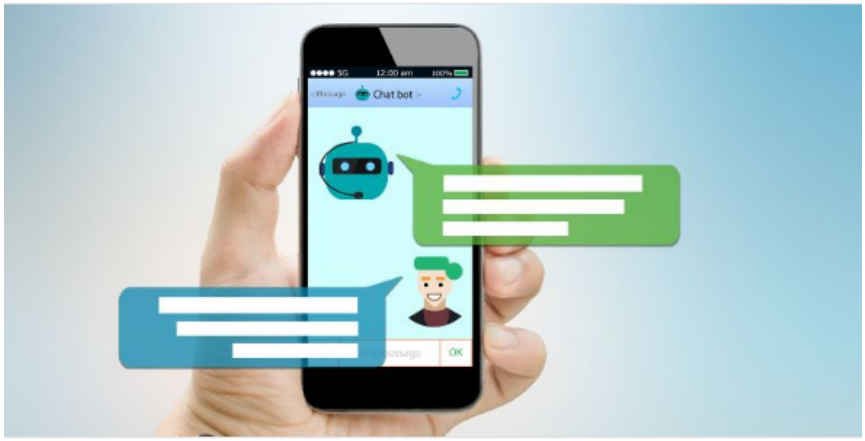
- Congelar su crédito
- Revisar sus informes de crédito desde AnnualCreditReport.com
- Configurar alertas en sus tarjetas bancarias y de crédito para recibir mensajes de texto cuando haya actividad sospechosa
- Usar contraseñas fuertes y Autorización de Dos Factores (2FA), especialmente para cuentas de correo electrónico, bancarias o de compras

Capítulo 13: IA Generativa (Qué Saber Antes de buscar por ChatGPT)

Probablemente hayas oído hablar mucho sobre herramientas de IA últimamente, como ChatGPT, Gemini o Perplexity. Quizá hayas visto a algún amigo usarlos o incluso los hayas probado tú mismo para hacer de todo, desde encontrar el mejor restaurante chino de tu vecindario hasta conseguir ideas creativas para el cumpleaños de tu hijo de 10 años.



Estas herramientas de IA son como versiones superpoderosas de Google con las que puedes conversar, casi como una persona real que puede responder casi cualquier pregunta que se te ocurra.



Sin embargo, hay un inconveniente: cuando usas estas herramientas de IA, no solo buscas una respuesta rápida. Estás dando información a un programa digital que recuerda *todo lo* que le cuentas. Por eso, ¡deberías tener cuidado con lo que compartes!

Hay tres grandes problemas al usar estas herramientas de IA:

1. El riesgo de la "memoria"

La mayoría de las herramientas de IA están configuradas para "recordar" lo que les digas. Si le cuentas a una IA tus síntomas médicos privados o un secreto sobre tu trabajo, esa información ahora se almacena con la empresa que proporciona el asistente de IA.

2. El riesgo de lo "desconocido"

A veces, personas reales (empleados de la empresa de herramientas de IA) leen los chats para asegurarse de que la IA no está siendo grosera o rota. Debes asumir que cualquier cosa que escribas podría acabar siendo vista por un ojo humano.

3. El riesgo de la "confusión"

Las herramientas de IA son geniales, pero no siempre son las correctas. Pueden "alucinar", que es una forma elegante de decir que pueden sonar muy seguros mientras dicen algo completamente falso. Nunca utilices herramientas de IA para obtener consejos importantes (médicos, legales, financieros) sin comprobar dos veces si esa información es correcta.

Aquí tienes consejos generales para mantenerte seguro:

- **No compartas datos personales o sensibles:** No compartas tu nombre completo, los nombres de tus hijos, tu dirección ni información específica de salud o finanzas.
- **Mantenlo general:** En vez de decir: "¿Por qué me duele el codo después de chocar contra la puerta del 123 de Main St?", simplemente pregunta: "¿Por qué me duele el codo después de chocar contra una puerta?"
- **Consulta la configuración:** La mayoría de estas apps tienen una sección de "Privacidad" o "Datos" en la configuración. Busca un interruptor que diga "No usar mis datos para entrenar" y actívalo. (¡O, por qué no, pregunta al Asistente de IA cómo hacerlo!)

AQUÍ tienes un vídeo más largo sobre la privacidad de las herramientas de IA.

Capítulo 14: CALIFORNIA – Eliminar Tus Datos en Línea

En California, hay una nueva ley poderosa llamada Ley de Eliminación (y una herramienta que crea llamada DROP). Si vives en California, esto es un cambio radical para tu privacidad.

¿Qué es la "Ley de Eliminación"?

Actualmente, hay cientos de empresas llamadas "Corredores de Datos". Son empresas de las que probablemente nunca hayas oído hablar, pero su trabajo es recopilar tu información personal (como tus ingresos, tus pasatiempos o tu partido político) y venderla a otros.

Incluso si tienes cuidado con lo que publicas en redes sociales, los corredores de datos siguen "absorbiendo" información sobre ti de registros públicos y otras aplicaciones, desde lo que compras, hasta dónde visitas, y a quién estás relacionado.

Antes de esta ley, si querías que borraran tus datos, tenías que encontrar cada una de esas cientos de empresas y preguntarles una a una, ¡una tarea casi imposible!

La Ley de Eliminación cambia eso. Crea una "parada única" donde puedes decirle A LA VEZ a todos los corredores de datos registrados que eliminen tu información.

¿Qué es "DROP"?

DROP significa **Plataforma de Solicitud de Eliminación y Opción de Exclusión (Delete Request and Opt-out Platform).**

Piénsalo como el registro de "No llamar", pero para tus datos personales. A partir de enero de 2026, podrás acceder a una única página web y pulsar un botón, lo que enviará un aviso de "Bórrenme" a todos los corredores de datos de California.

¿Por qué debería importarte?

- **Detiene el perfilado:** Un aviso DROP impide que las empresas construyan un archivo secreto sobre ti para decidir qué anuncios ves o si te aprueban para ciertos servicios.

- **Protección continua:** Una vez hagas la solicitud a través de DROP, los corredores de datos deben seguir eliminando tu información cada 45 días. No pueden simplemente borrarlo una vez y luego volver a comenzar la semana siguiente.
- **Sanciones severas:** Si una empresa no cumple tu solicitud, el estado puede multarlos con $200 diarios por solicitud. Este castigo económico hace que las empresas se tomen tu privacidad muy en serio.

¿Qué deberías hacer?

Usa el botón DROP, a partir de enero de 2026

La plataforma oficial (DROP), creada por la Agencia de Protección de la Privacidad de California, está AQUÍ.

Hoy en día puedes ver empresas ofreciendo "limpiar tus datos" a cambio de una cuota mensual. Aunque algunos sean útiles, recuerda que la plataforma California DROP será GRATUITA**.** No tendrás que pagar a una empresa privada para que haga lo que el estado está poniendo a disposición para todos.

RECURSOS ADICIONALES

AQUÍ tienes una explicación más detallada de la Ley de Eliminación y la herramienta DROP que crea.

AQUÍ tienes un vídeo más detallado sobre los corredores de datos.

Capítulo 15: Recursos

Vigilancia y autodefensa	Una guía de la Electronic Frontier Foundation que te enseña cómo proteger tu privacidad en línea. Incluye herramientas, estrategias y tutoriales paso a paso para defenderse de la vigilancia gubernamental y corporativa.	Asistir a una protesta Cómo conocer: Privacidad y configuración de seguridad del iPhone Privacidad para estudiantes
Defiendan nuestros movimientos	Un conjunto de herramientas para activistas, organizadores y comunidades marginadas para fortalecer la seguridad digital.	Usar Facebook en una era de deportación masiva Guía antidoxxing para activistas que sufren ataques de la alt-right
Activista tecnológico	Un centro de recursos centrado en la educación tecnológica y los derechos de privacidad para las comunidades negras y latinas. Ofrece talleres y formaciones para potenciar la libertad digital y resistir la vigilancia.	Clases virtuales continuas – Consejos de seguridad tanto presenciales como online para manifestantes y organizadores
Centro de Información de Privacidad Electrónica (EPIC)	EPIC es un centro de investigación de interés público en Washington, DC. EPIC presenta habitualmente escritos amicus curiae en tribunales federales, lleva casos abiertos de gobierno, defiende la privacidad del consumidor, organiza conferencias para ONG y habla ante el Congreso y organizaciones judiciales sobre cuestiones emergentes de privacidad y libertades civiles.	Guía de herramientas prácticas de privacidad
Centro de Defensa de las Libertades Civiles	Proporciona apoyo legal y educación a activistas y movimientos. Se centra en defender los derechos civiles en los tribunales y en ofrecer recursos para "conocer tus derechos".	Programa de Seguridad Digital
Laboratorios de Igualdad	Equality Labs es una coalición de artistas, defensores, sanadores,	Seguridad Digital

	tecnólogos y organizadores que trabajan en sistemas intratables de opresión a través de un modelo colaborativo de creación de soluciones para movimientos.	
Centro de Acceso a Derechos de Privacidad	Privacy Rights Clearinghouse es una organización sin ánimo de lucro 501(c)(3) comprometida con promover la privacidad de los datos para todos ampliando el acceso a la información, aumentando la participación en debates políticos y defendiendo derechos más sólidos.	Resumen de Derecho Aplicaciones móviles de salud y fitness
Guía de Privacidad en Línea de Wizcase	¡Una gran introducción a las Redes Privadas Virtuales con fotos y consejos prácticos!	
Guías de privacidad	Guías de Privacidad es un sitio web con motivación social que proporciona información para proteger la seguridad y privacidad de tus datos. Somos un proyecto sin ánimo de lucro con la misión de informar al público sobre el valor de la privacidad digital y sobre iniciativas gubernamentales globales que buscan monitorizar tu actividad online. Nuestro sitio web está libre de publicidad y no está afiliado a ninguno de los proveedores listados. Las Guías de Privacidad son elaboradas por voluntarios y miembros del personal de todo el mundo. Todos los cambios en nuestras recomendaciones y recursos son revisados por al menos dos personas de confianza, y trabajamos diligentemente para garantizar que nuestro contenido se actualice lo antes posible para adaptarnos al panorama de amenazas de ciberseguridad en constante cambio.	Herramientas de privacidad recomendadas
Vídeos de privacidad digital en YouTube	NBTV es un proyecto del Instituto Ludlow, un instituto de investigación y medios dedicado a ayudarte a recuperar el control	¡Encuentra vídeos AQUÍ!

	de tu vida digital. Creado y presentado por Naomi Brockwell.