PRIVACIDAD 101

UNA INTRODUCCIÓN SOBRE COMO LUCHAR CONTRA LA INTRUSIÓN ONLINE

¿POR QUÉ DEBERÍA PREOCUPARME?

"NO TENGO NADA QUE ESCONDER"

La procrastinación siempre ayuda a encontrar la perfecta excusa para evitar hacer cualquier cosa sobre lo que sea que tenemos en nuestra cabeza. Pero la frase de más arriba es una vieja excusa que fue repetida de muchas maneras distintas para personas extremadamente distintas:

"No tienes nada que temer si no tienes nada que esconder" - Joseph Goebbels

"Cualquiera que tenga miedo ahora es culpable; la inocencia jamás teme a la vigilancia pública" - Maximilian Robespierre

"Las únicas personas que no quieren revelar la verdad son aquellas personas que tienen algo que esconder" - Barack Obama[1]

La privacidad no es un fin o un objetivo, es el medio por el cual pensamos por nosotros mismos, investigamos y llegamos a conclusiones. La libertad de pensamiento sólo ocurre cuando sentimos que estamos en un ambiente privado. ¿Cuántas opiniones tontas tuviste primero sobre un tema antes de investigar o pensar un poco más al respecto? ¿Podrías haberte preguntado todas esas preguntas vergonzosas que tenías si todos los que te conocen sabrían que te las estas preguntando? Nos auto-censuramos y actuamos de manera distinta cuando creemos que estamos siendo supervisados o somos parte de un grupo.[2]

Entonces... ¿hay algo que podamos hacer al respecto? ¿Qué puede llegar a hacer un individuo para defenderse a sí mismo de la intrusión de los gobiernos y compañías más poderosas del mundo?

---

[1] En el contexto del juicio de la Corte Suprema, caso Citizens United.

[2] Experimento Solomon Asch de Conformidad: https://www.simplypsychology.org/asch-conformity.html. También llevado a cabo por el canal de YouTube, VSAUCE: https://youtu.be/fbyIYXEu-nQ

EL PODER ESTÁ EN TUS MANOS

VUELVE A TOMAR EL CONTROL

¿Y si hubieran dispositivos, herramientas, programas y servicios que fuesen hechos especialmente para poder recuperar tu privacidad? Ya existe una comunidad de personas preocupadas por la privacidad y compañías que intentan resolver el problema de la vigilancia a través de distintas soluciones de hardware y software. Estas son algunas que te podrán ayudar en luchar contra la vigilancia gubernamental y corporativa:

Cifrado	Nube Privada/Cifrado de Archivos
VPN	Hardware Enfocado en Privacidad
Tor & otros navegadores	Modelo de Negocio Pagar para Usar
DNS Pública	Software de Código Abierto

Algunas de estas soluciones son gratuitas, algunas son baratas y otras pueden ser caras. Sin embargo, hay muchas aplicaciones, servicios y productos distintos en el mercado que varían en precio y calidad. Sólo tienes que buscarlos. Mientras que debes mantener el cuidado y usar herramientas en las que puedes confiar, el hecho de que estemos tomando la privacidad en cuenta al seleccionar un producto, app o servicio, ya es un indicador de que estás tomando cartas para tener una vida más privada. Las recomendaciones hechas en este documento acerca de un producto o proveedor en especifico son sólo eso, recomendaciones. No hay una bala de plata, una pieza perfecta de software. Hay ventajas y desventajas con todo. El objetivo de este documento es informarte sobre los conceptos y opciones disponibles, para que luego puedas tomar tu propia decisión.

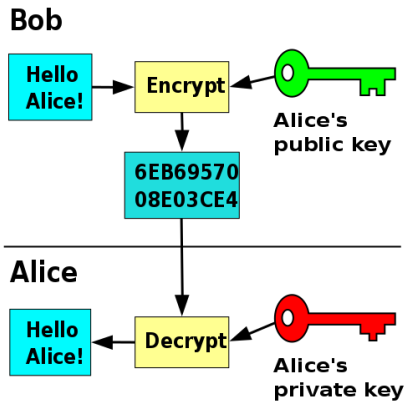
Como regla general, intenta no tener datos no cifrados guardados en servicios basados en el Reino Unido, Estados Unidos, Australia, Canada y Nueva Zelanda, dado que comparten bases de datos de inteligencia y pueden obligar a las empresas a que entreguen claves de cifrado[3]. Pero, ¿qué es el cifrado?

---

https://www.privacytools.io/providers/#ukusa

CIFRADO

El cifrado existe previo a la era de las computadoras modernas. Durante la Segunda Guerra Mundial, el ejército alemán de manera famosa se comunicaba usando un dispositivo llamado Enigma. Una máquina que codifica mensajes en texto legible o "texto plano" a un texto ilegible o "texto cifrado". Para leerlo, necesitarías la llave que descodifica el texto cifrado pasándolo a texto plano de nuevo. Aunque la tecnología lo ha hecho infinitamente más avanzado y complejo, el concepto del cifrado es prácticamente lo mismo:



¿Por qué entonces no está absolutamente todo cifrado? Bueno, el cifrado puede ser costoso en términos de recursos y desarrollo: hace que las páginas web sean más lentas y no es tan fácil de implementar.

Debería un blog sobre gatitos usar cifrado? Cuál es el beneficio de cifrar ese contenido? Puede el autor de ese blog cubrir el costo? La página va a funcionar más lento? Qué sucede con la página de tu banco?

Entidad	¿Beneficio de Cifrado?	¿Costo del cifrado?	¿Consecuencias sobre performance?
Blog sobre gatitos	Terceros no podrán saber sobre el contenido que posteas, comentas o likeas en el sitio.	Contratar a un desarrollador o servicio que pueda aplicar protocolos de cifrado al blog.	Como el sitio tiene muchas fotos de alta calidad, cifrar todo el contenido haría que la página cargue más lento.
Banco	Tus datos financieros están seguros.	Ya tiene un equipo de desarrollo que puede implementar técnicas de cifrado.	Como el sitio tiene más que nada texto y números, el cifrado no aumenta significativamente la velocidad de carga.

De todas maneras, los costos no le reducen el valor a la privacidad. Este ejemplo es un absurdo que no refleja la problemática técnica real, pero que sí muestra que no todo es tan simple como "cifremos todo y problema resuelto".

Por otro lado, el cifrado cambia el foco de la seguridad. No es necesario tener una infraestructura 100% segura (que es imposible de tener de todas maneras) cuando la información que contiene es imposible de leer.

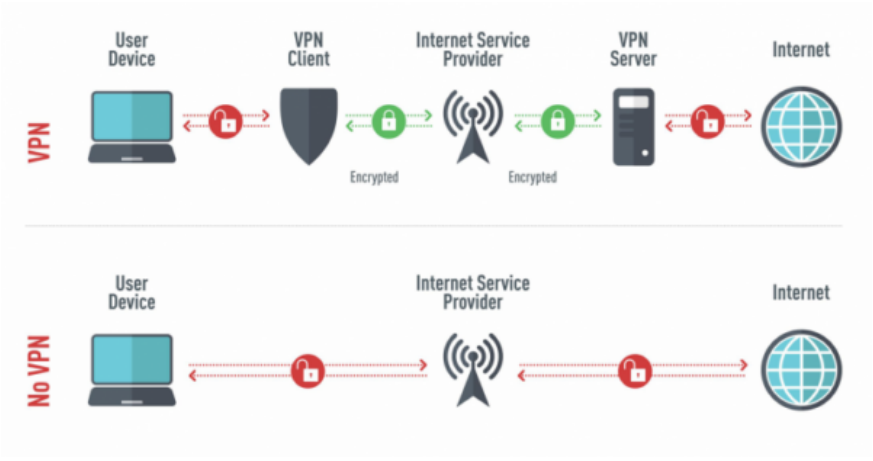
VPN[4]

Cuanto entramos a un negocio o un supermercado, nadie sabe la dirección de nuestra casa. Pero si estás navegando internet, cada sitio puede encontrar dónde estás. Esto se debe a tu dirección IP (por sus siglas en inglés para protocolo de Internet).

Cuando escribes "www.google.com", tu computadora solicita una dirección de IP. Una vez que obtienes esa dirección de IP, tu computadora envía una solicitud con *tu* dirección de IP a ese sitio web, el cual le envía su contenido a tu dirección.

Una VPN (por las siglas en inglés para red virtual privada) es un intermediario que actúa como la cara pública a los sitios de internet. Los sitios creen que tu dirección de IP es la que le pertenece al servidor de VPN al que estás conectado, por lo que mandan su contenido allí. De manera privada, la VPN envía ese contenido a tu verdadera dirección de IP, sin que nadie sepa cuál es la dirección online de tu dispositivo.

Si le haces una pregunta a alguien en la calle, te ven, te escuchan, pueden identificarte. Pero si le pides a un amigo cómo hacer una pregunta, entonces tu amigo es el que será reconocido y no tú. ¿Aún no se entiende? Mira esto:



Tu VPN se interpone ante tu proveedor de internet e internet mismo. Los servicios de VPN también cifran tus solicitudes para que sean no sólo privadas sino también seguras.

Cuando busques por una VPN, asegúrate de elegir una que tiene pocos casos o ninguno de brechas en su seguridad y ofrece las funcionalidades que quieres y

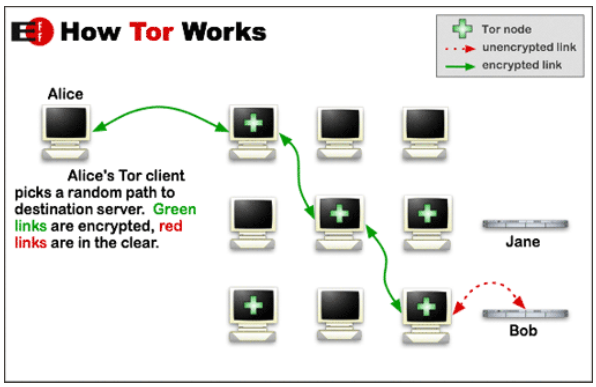
[4] https://www.privacytools.io/providers/vpn/

necesitas. ProtonVPN es una buena opción, con sede en Suiza. También provee otros servicios que serán mencionados en este documento.

¿Son las VPN la bala de plata? ¿Todo lo que necesitamos? Ni cerca, pero si pueden jugar un enorme rol en mejorar tu privacidad online.

TOR & OTROS NAVEGADORES[5]

Probablemente has escuchado de Tor en las noticias. Es el método por el cual hackers, activistas políticos y criminales usan para navegar internet y compartir información. ¡Suena súper peligroso! No quieres estar en la compañía de ese tipo de personas, solamente quieres hablar con tus amigos sobre deportes y mirar videos de bloopers. Pero todo lo que Tor hace es darte anonimidad usando una red especial:



Puedes usar Tor para acceder a los mismos sitios que visitas regularmente; si no quieres comprar o vender drogas, no vayas con el narcotraficante. Tan simple como en la vida "real". Esta explicación de Tor no le hace justicia a lo que es y cómo puede beneficiarte, ¡así que por favor investiga más al respecto! Revisa lo que es un servicio Onion. Si se *pudre todo*, Tor es tu mejor chance para mantenerte privado y anónimo online. La manera más fácil de acceder a la red Tor, es usando el navegador Tor.

¿Tor no te convence? Hay algunas opciones más "normales", más conocidas. Busca navegadores que estén enfocados en privacidad. La opción más conocida es Mozilla Firefox, por la fundación Mozilla. A diferencia de Tor, deberías instalar algunos complementos y hacer algunos ajustes (los cuales pueden ser un poco avanzados para principiantes). Pero los complementos son fáciles de instalar y de usar.[6]

Si usas Firefox o cualquier otro navegador enfocado en privacidad, recuerda usar una VPN. Esta es la diferencia con Tor: Tor usa descentralización mientras que la VPN depende de los servidores del proveedor. No necesitas confiar en Tor para usarlo, pero si necesitas confiar en el proveedor de VPN dado que posee las llaves del reino.

---

[5] https://www.privacytools.io/browsers/#browser

[6] https://www.privacytools.io/browsers/#addons

DNS PÚBLICA

Aunque ya se mencionó la DNS en este documento, aquí va un poco más de información al respecto. Imagina la DNS como la guía telefónica (o lista de contactos para quienes nunca vieron una guía telefónica) de internet. Cuando ingresas una URL en tu navegador, ¿cómo sabe a dónde ir? ¿De dónde descargar el contenido de una página web?

Cuando buscas el número de teléfono de alguien, buscas su nombre y obtienes el número. Para internet es lo mismo, pero en lugar del número de teléfono obtienes la dirección de IP. Tu proveedor de internet (ISP por sus siglas en inglés), provee este servicio usando su propio DNS, el cual normalmente:

- Está desactualizado: cuando no puede encontrar un sitio, rebota tu solicitud a otros servidores para poder encontrarlo.

- Está desprotegido: No tiene protección contra el phishing, no cifra tus solicitudes.

- No es privado: tu ISP puede grabar las solicitudes que van de tu dirección de IP a su servicio de DNS.

Entonces, ¿cómo puedes hacer para pasarte a una DNS pública? Esto se puede hacer a nivel del dispositivo (es decir, computadoras, smartphones) o a nivel del router. Busca por una guía rápida usando estas palabras clave: "cambiar DNS [insertar sistema operativo]". Puedes hacer lo mismo para tu router, pero puede ser que sea más difícil para los inexperimentados.

Espera un momento, si es público, ¡entonces todas tus solicitudes son públicas también! Es por esto que tienes que usar DNS con HTTPS (DNS cifrado).

MENSAJERÍA PRIVADA

La sugerencia para mensajería privada es simple: los datos tienen que estar cifrados y se tiene que cifrar la mayor cantidad de metadata también. Ningún producto de Facebook cifra la metadata y algunas preguntas surgen sobre si tiene cifrado para los datos. Esto incluye Facebook Messenger, WhatsApp y Instagram Messages. Facebook no es la única en no cifrar la metadata en inclusive guardarla, ¿entonces qué opciones existen?

Hay una app llamada Signal que es de código abierto y tiene cifrado en todos lados. Está disponible para cualquier plataforma así que dale una chance y consigue que todos tus amigos y familia comiencen a usarlo también. Para que sepas, Edward Snowden usa Signal.

Pero no tiene que ser Signal. Hay otras opciones, con diferentes ventajas y desventajas. La principal debilidad de Signal es que está centralizado, así que tal vez deberías investigar sobre opciones de software descentralizado para chats en tiempo real.[7]

NUBES PRIVADAS/CIFRADO DE ARCHIVOS

¿Sabías que Google puede escanear el contenido de cualquier archivo que tengas guardado en Google Drive? Claro, cuando solicitas abrir un archivo, lo haces a través de una conexión segura (HTTPS) y estás autenticado. Pero ese archivo no está cifrado en sus servidores, entonces con acceso a ellos, tus archivos se pueden leer, copiar por cualquier persona con acceso a los servidores de google (como la NSA[8]).

Entonces, ¿cuál es la solución? Puedes pagar por un proveedor privado cuyo modelo de negocio dependa en recibir pagos mensuales en lugar de acceder a tus datos y/o podrías cifrar tus datos tú mismo y subirlos cifrados. Hay muchas opciones de software de cifrado de archivos, como 7zip para Linux y Windows o VeraCrypt, disponible para Linux, Windows y MacOS.

HARDWARE ENFOCADO EN PRIVACIDAD

Una de las filtraciones de Edward Snowden mostró cómo la NSA usaba programas llamados pitufos. Estos son algunos de los pitufos y qué es lo que pueden hacer:

Pitufo Soñador: prender y apagar tu teléfono sin que te des cuenta.

Pitufo Entrometido: prende tu micrófono y graba todo lo que escucha.

Pitufo Rastreador: es una herramienta de geolocalización que es más precisa que la que usan en las películas (donde vemos cómo triangulan la señal de un teléfono usando torres).

Pitufo Paranoico: ayuda a los otros pitufos a mantenerse no detectados.

Estos programas pueden funcionar en cualquier tipo de dispositivo, smartphone o computadora (en términos prácticos, para nosotros son lo mismo). Entonces, ¿qué podemos hacer? Esta pregunta es difícil y no hay ninguna evidencia que la NSA estuviese usando estos programas de forma masiva, así que deberíamos estar a salvo. Habiendo dicho eso, no podemos confiar más en que nuestros teléfonos sean

[7] https://www.privacytools.io/software/real-time-communication/

[8] https://en.wikipedia.org/wiki/Edward_Snowden#/media/File:NSA_Muscular_Google_Cloud.jpg

completamente privados, inclusive si estamos usando un software de código abierto, enfocado en privacidad. No tengas tu teléfono contigo todo el tiempo.

Para las computadoras, hay algunas soluciones. Muchas laptops están viniendo con cobertores de webcams pero algunas también vienen con switches físicos para el micrófono, cámara, WiFi y Bluetooth. Sin que tengan electricidad, esas funcionalidades no pueden ser activadas por ningún software.

Muy probablemente, no vas a ser objeto de un ataque de spyware con pitufos o programas similares. Así que al menos toma las medidas necesarias: usa contraseñas fuertes y únicas, cifra tus discos de almacenamiento, entre otras prácticas. Internet está llena de guías que puedes seguir[9], incluyendo este documento. Edúcate y usa las herramientas a tu disposición. Es posible seguir las mejores prácticas de privacidad sin sacrificar comfort. Además, una vez que entiendes que tu privacidad está en peligro, vas a apreciar cualquier herramienta que te ayude a protegerla.

MODELO DE NEGOCIO PAGAR PARA USAR

Sugiero veas el documental "The Social Dilemma". Allí, Jaron Lanier, explica qué es lo que está mal con el modelo de negocio de la mayoría de las grandes empresas de tecnología están usando. Piensa sobre los productos de Google, Facebook y muchos otros. ¿Cómo ganan dinero? Los usuarios no pagan, no reciben donaciones. ¿Entonces de dónde viene el dinero?

Lanier no cree que las empresas sean necesariamente malvadas, pero que dependen del modelo de negocio del uso gratis. Para proveer un servicio gratis, estas empresas monetizan tus datos mientras usas sus plataformas. Estos datos incluyen: el contenido que usuarios publican (fotos, comentarios, publicaciones, audio, y datos personales que como edad y género), metadata (registros de actividad de todo lo que haces en la plataforma) y una mezcla de las dos: un perfil virtual que le venden a anunciantes. Es el modelo de negocio que fomenta a estas empresas a tener estos invasivos productos de software.

¿La solución? Comenzar a utilizar servicios de subscripción paga como Netflix o Spotify. Comienza a pasarte a software creado por fundaciones que dependen de donaciones (los que donan cubren el costo de los que no lo hacen). Pero más importante, **elimina** tus cuentas en redes sociales. Hay otros problemas relacionados a las redes sociales que no están relacionados a la privacidad, por favor mira "The Social Dilemma" para más información al respecto. Es una gran manera de arrancar a entender mejor esta temática.

[9] https://proprivacy.com/

SOFTWARE DE CÓDIGO ABIERTO

¿Cómo puede ser el software de código abierto mejor para la privacidad? ¿Mejor para la seguridad?

Contrario a la intuición, tener el código fuente a disponibilidad de la comunidad online, ayuda a que ese código sea auditado y se remuevan las vulnerabilidades y hacerlo transparente. Si la aplicación está recolectando tus datos, ese comando va a aparecer en el código fuente. Nada puede suceder detrás de escena.

Si puedes, intenta pagar por este tipo de software inclusive si es gratis. Haz una donación. Nada es gratis, alguien está cubriendo el costo por ti.

OK, ¿Y AHORA QUÉ?

ESTE DEBERÍA SER SÓLO EL COMIENZO

Cualquiera que lea esta guía y ya está interiorizado en prácticas de protección de la privacidad, va a pensar que esta guía esta sobre-simplificando y sobre-estimando muchos conceptos y es un poco inocente en pensar que todas las sugerencias aquí descriptas alcanzan para proteger la privacidad. Y tendrían razón.

El propósito de esta guía es ayudar a las personas que saben casi nada sobre privacidad y quieren comenzar a tomar cartas en el asunto para usar internet de mejor manera. Algunas personas ni siquiera saben que no están navegando internet de forma privada.

A esas personas: bienvenidos. Continúen haciendo preguntas, usando pensamiento crítico, continúen aprendiendo. ¿Es correcta toda la información de esta guía? ¿Está actualizada? ¿Es ese proveedor de servicios seguro? ¿Son todos los sistemas operativos seguros y privados? Habiendo tomado todos los pasos de la guía para navegar de manera segura en mi computadora, ¿qué tengo que hacer con mi teléfono? ¿Cuáles son los servicios onion de Tor? Si los servicios onion no están indexado en ningún motor de búsqueda (ejemplo: Google Search), ¿cómo puedo usarlos? ¿Las configuraciones de red no debería hacerlas en mi router en lugar de hacerlas en cada dispositivo?

No te frustres, aprender toma tiempo y práctica.

...

Pero cuando te frustres y la procrastinación empiece, imagina cómo sería tu vida si todos conociesen todas tus búsquedas de Google Search. Que supiesen cuánto tiempo miraste la foto de alguien y qué foto. Si tu verdulería supiese qué hiciste el último viernes a la noche o cuánto dinero ganaste el último mes. No tengas estándares de privacidad distintos para tu vida online que para tu vida “real”.