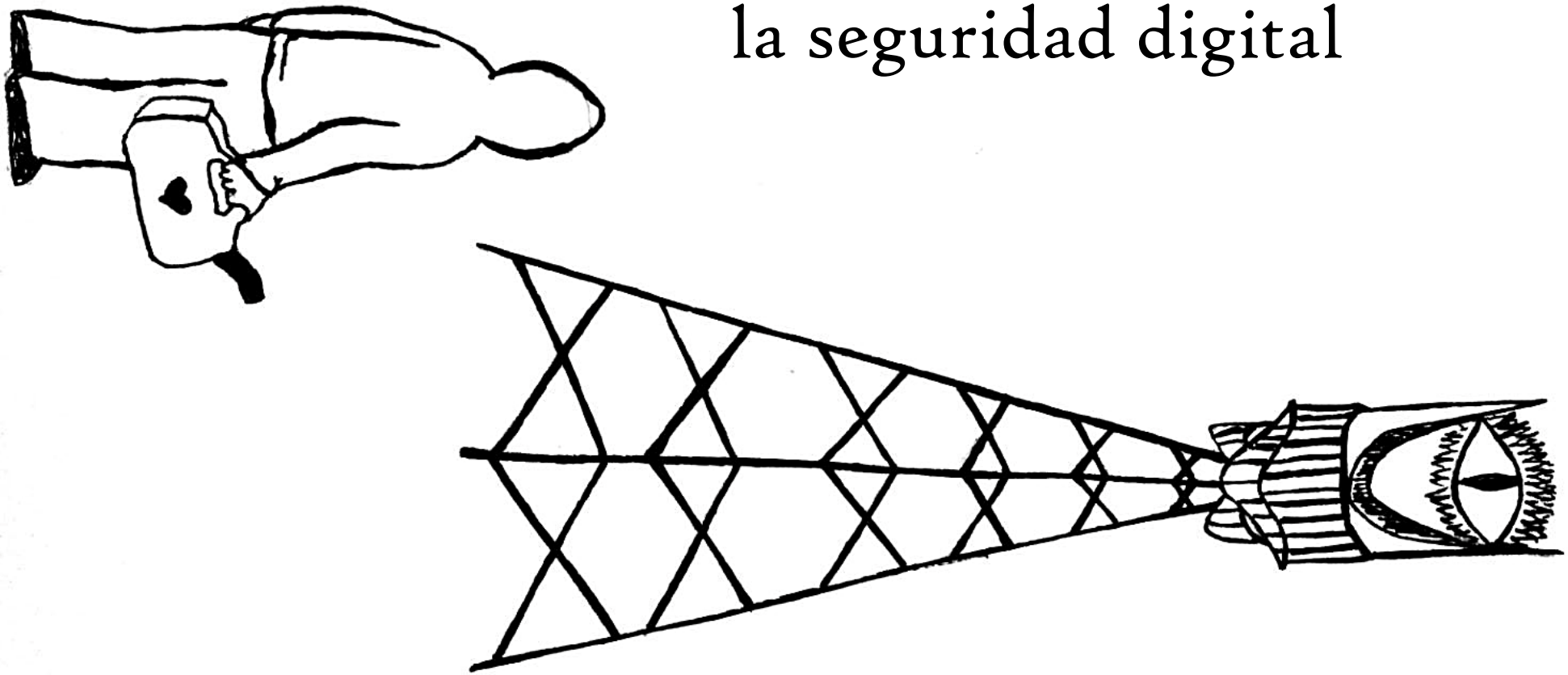
3NCRiPT4DX5

Herramientas para la seguridad digital



3NCR1PT4DX5
Herramientas para la seguridad digital

"Decir que no te importa la privacidad porque no tienes nada que ocultar no es diferente a decir que no te importa la libertad de expresión porque no tienes nada que decir." - Edward Snowden

NOTA: ¡ESTO NO ES UN MANUAL!

- PRIMERA PARTE

Registro etnográfico del colectivo intergaláctico contra la tecnovigilancia. Notas de campo.

Planeta Tierra, año 2022 del calendario gregoriano (calendario local predominante). Año 582345 del calendario Hauatzil-Londd.

1.
En las grandes ciudades del planeta Tierra, cada persona carga voluntariamente un dispositivo que en todo momento está registrando datos sobre sus decisiones, ubicación, gustos, miedos y deseos. Les llaman "teléfonos inteligentes". Un paisaje terrícola urbano típico incluye humanxs que caminan cabizbajxs, mirando ensimismadxs a las pantallas de sus dispositivos de rastreo.

2.
Estos aparatos ejecutan continuamente algortimos de aprendizaje de máquinas para influir sobre las decisiones de las personas en base a la información que recopilan, principalmente con el objetivo de inducir conductas de consumo específicas.

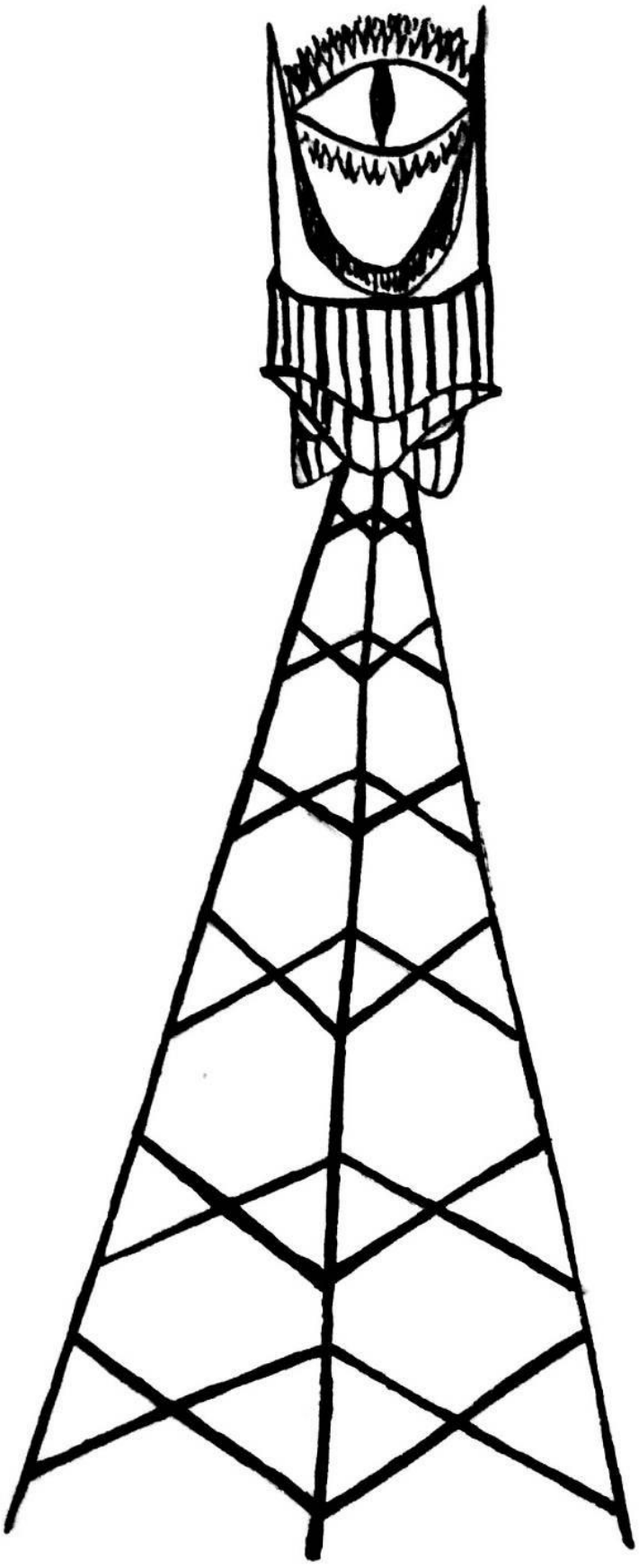
3.
Los algoritmos aprenden y evolucionan rápidamente en base a un ciclo de estímulo-respuesta donde la liberación de dopamina (hormona del placer) juega un rol preponderante. Ante ciertos estímulos del aparato, el sistema nervioso de lxs seres humanxs libera dopamina, lo cual les produce el deseo de seguir recibiendo dichos estímulos. En muchos casos el

uso de los dispositivos reúne las características de la adicción a una droga.

4.
Las personas humanas consienten en que se recopile información sobre ellas porque existe la percepción generalizada de que la vida sería más difícil sin un teléfono inteligente, y de que interferir en los mecanismos de recopilación de información es demasiado complicado.

5.
En base a la información levantada por lxs miembrxs del colectivo intergaláctico contra la tecnovigilancia, la situación de la sociedad terrícola se encuentra en la categoría "extremadamente grave".

6.
Siguiendo los principios de la intervención estética y la propaganda por el hecho, se han enviado mensajes a la Tierra en formato musical y en la forma de incidentes espontáneos de destrucción de la infraestructura de vigilancia.

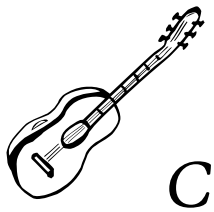


Herramientas prácticas para la seguridad digital

El texto a continuación es una interpretación libre, aunque detallada, de la canción "3ncr1pt4d4" de Annarresti. Su propósito es proveer herramientas prácticas para un uso más seguro del internet y la tecnología en el contexto de la quinta revolución industrial.

Pueden escuchar la canción en el siguiente link:

Cada una de las secciones se corresponde con algún verso (o conjunto de versos) de la canción que lxs autorxs consideraron significativo, a partir del cual se desarrollaron recomendaciones en base a la práctica cotidiana de la seguridad digital. Con el objetivo de hacer más fácil la adopción de estas recomendaciones hemos compartido un listado de herramientas digitales. Sin embargo, somos conscientes de que en el mundo de la tecnología todo es susceptible de quedar obsoleto, y lo más probable es que así sea eventualmente. Por lo mismo, la idea no es que sigas todo al pie de la letra. Antes de decidirte a usar una herramienta, investígala un poco, averigua si sigue siendo una alternativa segura o si hay mejores. Esto no es manual, sino una guía.



Cada palabra, cada pisada, cada página web visitada; cada mensaje, cada correo, una carta sin sobre al voleo.

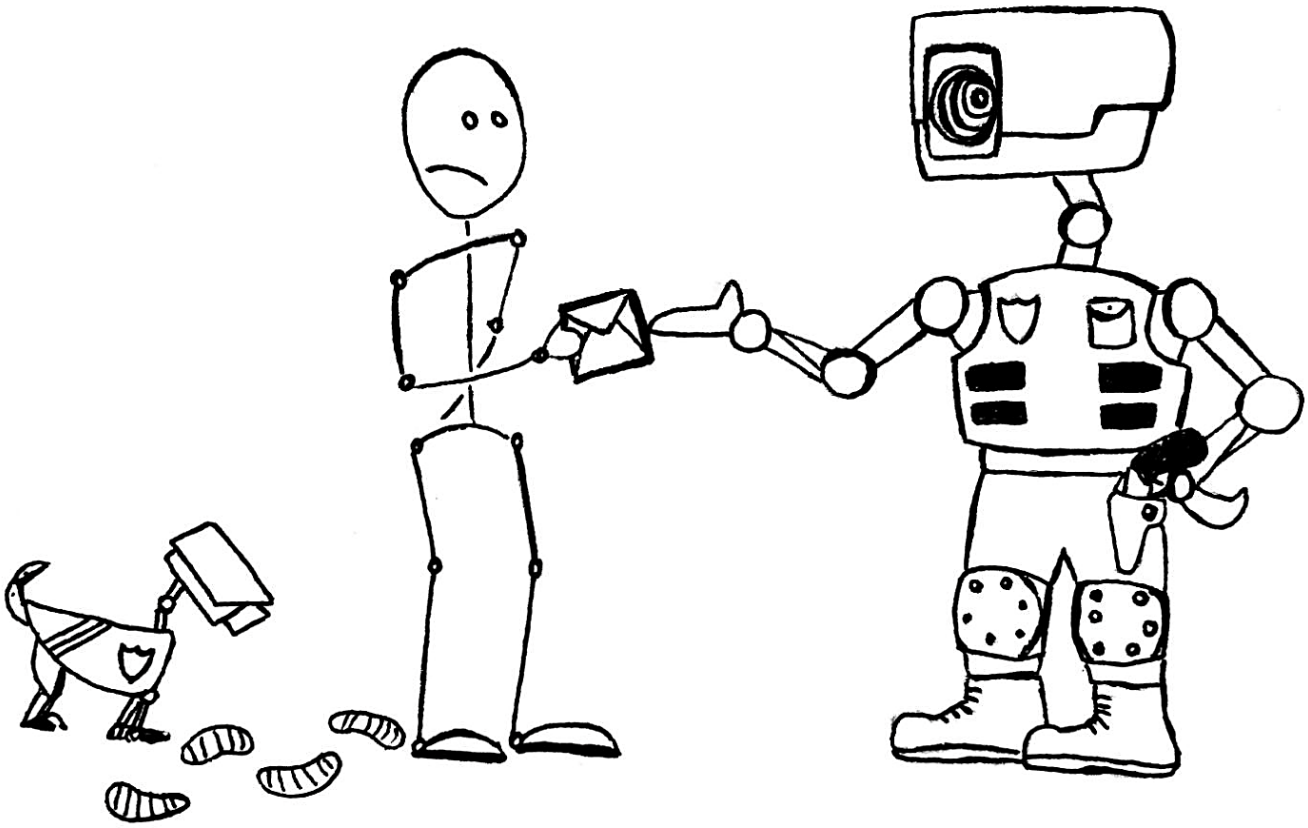
Al atravesar la web, nuestros mensajes son almacenados y leídos por máquinas que a través de ellos aprenden de nosotrxs.

Para correspondencia sensible, utiliza servicios de correo independientes, encriptados y seguros. Riseup e Inventati son alternativas decentes y gratuitas. Si tienes algo de presupuesto y la seguridad de tu correspondencia es importante para ti, Protonmail es muy buena opción.

Para mensajería instantánea sensible utiliza servicios que sean encriptados y no pertenezcan a los gigantes Meta (Facebook), Google, Amazon.

Si eres de lxs computinxs nostalgicxs, IRC sigue existiendo y es un universo paralelo en resistencia. IRC es seguro, encriptado y libre. Para lxs entusiastas, puedes instalar un emulador de terminal en tu celular y usarlo ahí.

Como recomendación general para cualquier aplicación de mensajería, configura la desaparición de mensajes o borra tus historiales sensibles regularmente, y desactiva los respaldos en la nube, a menos que quieras que todos tus mensajes sean cartas sin sobre al voleo.



¿QUÉ SIGNIFICA QUE UNA INFORMACIÓN ESTÉ "ENCRIPTADA"?

Significa que la representación original de la información, conocida como texto plano, ha sido convertida en una forma alternativa conocida como encriptado, mediante un proceso conocido como encriptación. En el mejor de los casos, sólo las partes autorizadas pueden descifrar un texto encriptado para convertirlo en texto plano y así acceder la información original. La encriptación no impide por sí misma que la información sea interceptada, pero vuelve ilegable el contenido para un posible interceptor. Por ejemplo, si tú envías un mensaje como texto plano a otra persona, y un tercero intercepta ese mensaje, este interceptor podrá leer el contenido sin problema. Si en cambio usamos encriptación, quien intercepta el mensaje no podrá leerlo.

Yo no me inclino ante San Google

Antes de 2015, Google tenía un famoso slogan: "don't be evil" (no seas malvado). A partir de 2015, la corporación comenzó silenciosamente a quitarlo de su imagen corporativa hasta prácticamente remover toda referencia a él en 2018, probablemente para protegerse de los problemas legales que la frase ya le había generado.

En 2021 Google admitió públicamente que su asistente (el equivalente de Siri en los iPhones) a veces graba por el micrófono sin ser activado por lxs usuarixs.

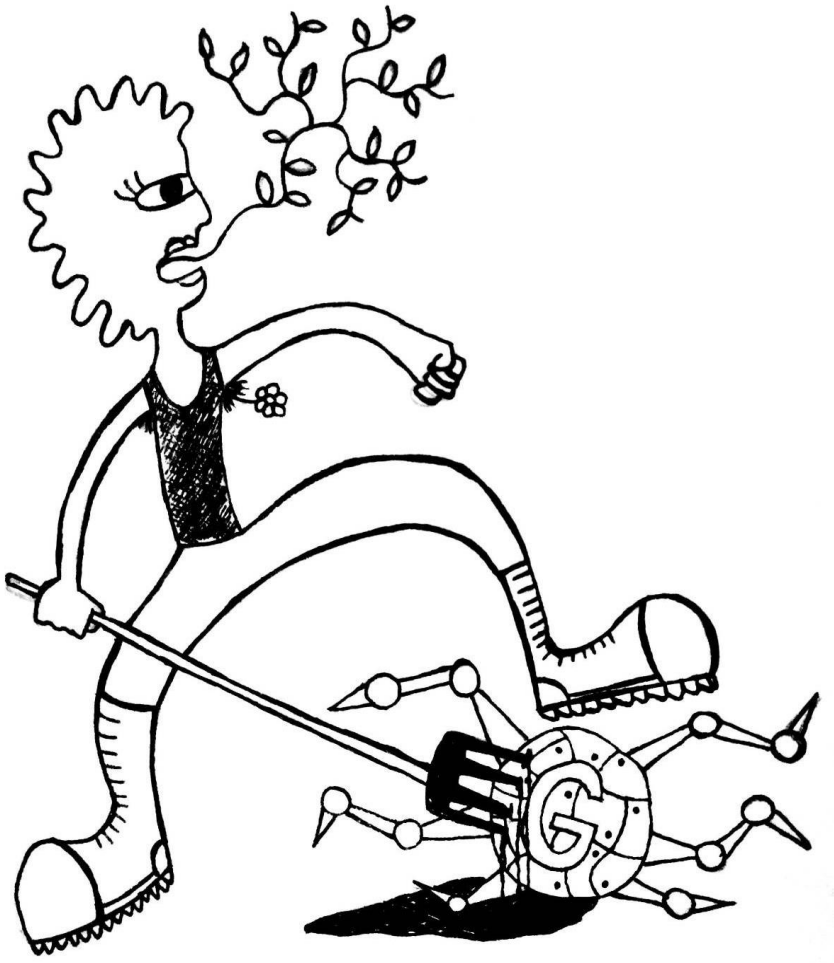
Mucho más que un motor de búsqueda, Google es una máquina compleja de múltiples brazos y engranajes. Sin mucho escándalo, esta corporación se las ha arreglado para ocupar un lugar en prácticamente todos los aspectos de la vida digital de una persona: correo electrónico, videollamadas, mensajería instantánea, almacenamiento privado y compartido de archivos, visualización de videos, mapas, publicidad, entre otros. Además de estos servicios más visibles, Google tiene un historial de colaboración con la inteligencia militar de Estados Unidos y con programas de censura en diversos territorios, incluida la guerra en curso entre Rusia y Ucrania.

¿Cómo dejar entonces de inclinarnos ante su inmenso poder? En esta publicación encontrarás recomendaciones para poco a poco liberarte de sus tentáculos (distribuidas en diferentes

secciones, ya que, repetimos, es un monstruo de muchos brazos).

Primero, utiliza motores de búsqueda alternativos a Google. Una buena opción es Duckduckgo. Es muy poderoso y no tiene trackers (rastreadores). No registra tus búsquedas para bombardearte con publicidad.

Duckduckgo también tiene un navegador para celular que funciona bastante bien, como alternativa a Chrome. Bloquea trackers y prácticamente toda la publicidad. Tiene un botón de fuego con el que elimina toda la caché (los famosos cookies) e historial, así que siempre tendrás una experiencia limpia de avisos personalizados y trackers.



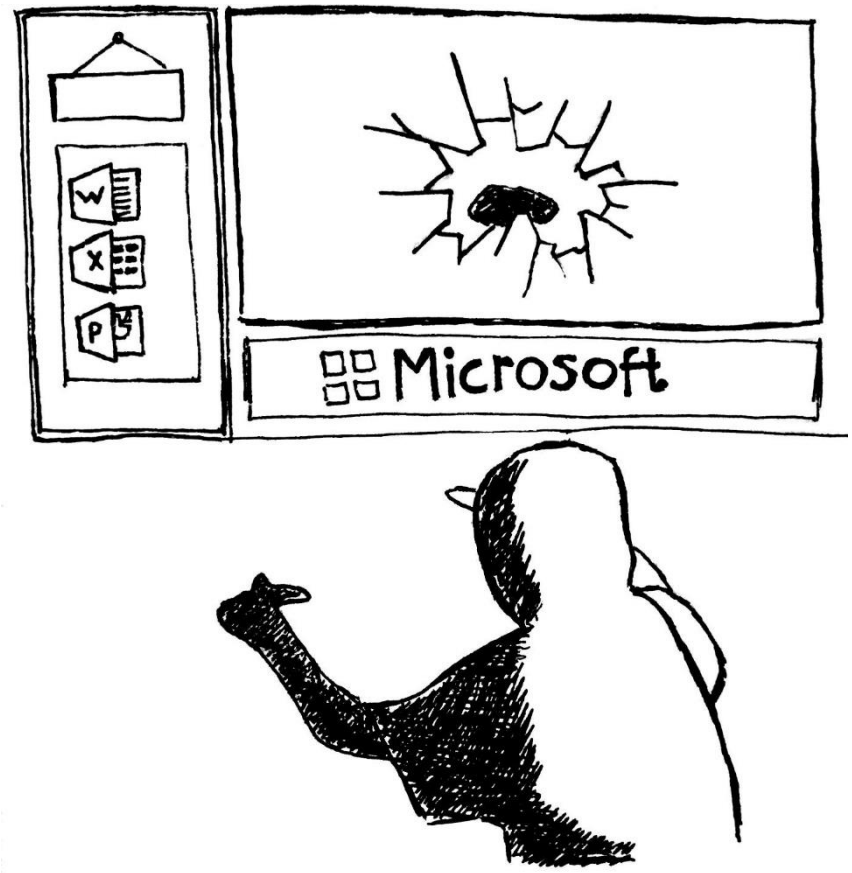
Otra buena opción en esa línea es Brave.

Si practicas la escritura colaborativa, hay alternativas a Google Docs. Dos opciones decentes, gratuitas y seguras son Riseup Pad y Crypt Pad. El primero tiene la opción de utilizarse a través de la red Tor (ver sección "Aprende a esconder tu IP").

Y no le compro a Bill Gates

Bill Gates es el dueño de Micorsoft, lo que lo convierte uno de los señores feudales del tecno-feudalismo en el que vivimos. El software propietario que produce Microsoft genera cientos o miles de millones de dólares (la cantidad no importa) a costa de la privacidad y autonomía de las personas que lo utilizan, y por supuesto a costa de la destrucción del medioambiente para obtener la energía fósil y materias primas que mantienen sus intalaciones funcionando. Al igual que Google, Microsoft recolecta información de tu actividad en sus "servicios" y la usa para mejorar sus productos y vendérsela a otras empresas.

Si la privacidad y la autonomía son importantes para ti, desecha Windows y sus derivados ~~lácteos~~ cuanto antes. Cambiarse a Linux no es tan difícil como parece. Solo necesitas un pendrive y un poco de paciencia. Busca tutoriales o acude a tu amigx computinx más cercanx.



¿USAS UNA APP PARA REGISTRAR TU CICLO MENSTRUAL? CONSIDERA BORRARLA AHORA.

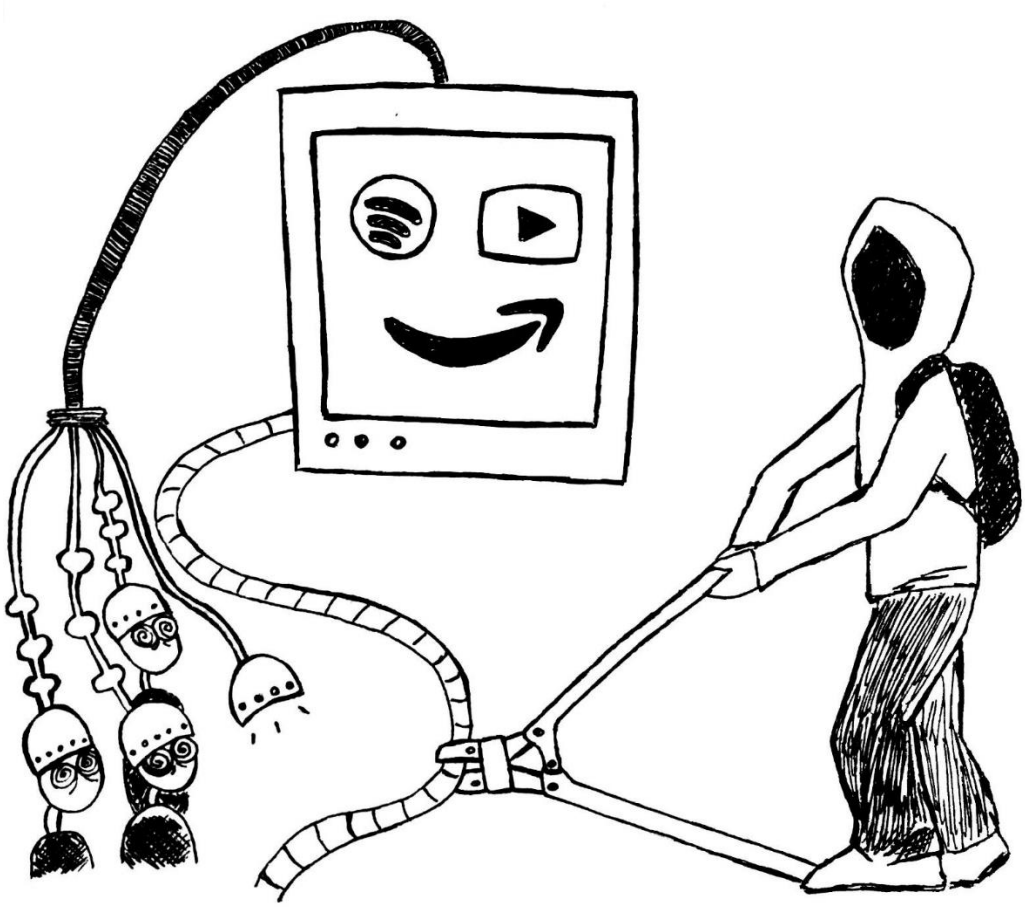
A pesar de su gran utilidad, la mayoría de estas aplicaciones no tienen ningún reparo en compartir o vender esta valiosa información sobre ti. Un ejemplo: si una aplicación tiene acceso a tu ciclo menstrual, puede predecir si estás embarazadx. En territorios donde rigen leyes contra del aborto, esta información podría ser utilizada para acosarte o vigilarte. Incluso si esto no te preocupa, una aplicación que hace seguimiento de tus estados emocionales, cambios físicos, problemas de salud, y donde además puedes escribir notas personales, es más que una simple aplicación. Es tu diario. Es tu historial de salud. Es un registro de tu vida. ¿Le darías estos objetos personales a cualquier extrañx en la calle? ¿O a una empresa de publicidad? ¿Se los darías a investigadorxs que podrían utilizarlos para manipular tu estado de ánimo?. Si alguien dice que eliminará tu nombre y otros datos que permitan vincular la información con tu identidad, ¿simplemente confiarías en que lo hará?. O si esa persona te dijera que nunca perderá esos datos y que nunca se los robarán mientras estén a su cargo, ¿le creerías?. Si la respuesta es no a cualquiera de estas preguntas, entonces entiendes que la privacidad importa.

Puedes elegir cambiarte a una aplicación "segura", pero incluso si sus términos de privacidad protegen tus datos hoy, nada les impide modificarlos mañana, así que debemos permanecer atentxs. La verdad es que la única forma de llevar un registro menstrual 100% privado es hacerlo en papel, y aún así debemos ser cuidadosxs.

Registrar nuestro ciclo menstrual para conocernos es muy importante. No renunciar a nuestra privacidad al hacerlo es igual de importante.

Yo crackeo y pirateo y ojalá que tú también

Sí, yo también crackeo y evado licencias de software propietario pero sólo cuando me lo piden, por el placer de transgredir el copyright y ayudar a unx amigx.
La verdad es que no necesitamos el software propietario. Hay un universo de software de libre acceso para todas las tareas que se te ocurran, desde procesar texto hasta producir música y editar fotografías. Es software de buena calidad, mantenido por comunidades internacionales y el código está disponible para que quien se interese pueda verlo y modificarlo. Nada de copyright ni código oculto que nadie sabe lo que hace ni cómo.



Practica la alegre piratería de forma expansiva y generosa. Piratea música, libros, películas. No le des un peso más a los servicios de streaming de video (Netflix, HBO, Prime, Disney), ni de música (Spotify, Apple Music). Te cobran por recopilar información sobre tus gustos, para luego ofrecerte más y mejor refinados dispositivos de sometimiento: series y películas más adictivas, música que "te gusta más", en suma: la preciada dopamina.
Tampoco les des tu dinero a las editoriales corporativas o a las revistas científicas.

Aquí algunas herramientas para la piratería:

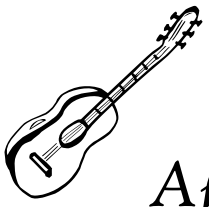
- **Sci-Hub:** Piratería de artículos científicos. Es poco probable que alguien que lea papers científicos con regularidad no lo conozca, pero no está demás pasar el dato.

- **Z-Libros y Library Genesis:** piratería de libros, como dicen los nombres. Lo que quieras, en cualquier idioma.

- **Stremio:** Todo lo maravilloso de la descarga por torrent, con todo lo maravilloso del streaming. Todas las series y películas que podías descargar por torrent, ahora servidas por streaming para verlas en el momento y/o guardarlas para después. Funciona con add-ons (extensiones) así que si instalas sólo la aplicación no sirve. Algunas extensiones recomendadas: Torrentio, TorrentioLite, The Pirate Bay, RARBG, Open Subtitles.

- **MuseScore downloader** (por Xmader): Piratería de partituras de música. Hasta hace no mucho tiempo descargar

partituras de MuseScore era gratis, pero ahora hay que pagar una suscripción. Con esta herramienta se puede evadir la suscripción y descargarlas gratis.



Apaga el GPS

Apaga el GPS en realidad significa apaga todo. Pero vamos por parte:

En la sección de configuración de tu teléfono inteligente puedes restringir el acceso a GPS de parte de las aplicaciones. El lugar de esta configuración puede variar entre sistemas operativos y sus versiones, pero un camino genérico sería:

Configuración->
Privacidad ->
Administrador de permisos ->
Localización

Asegúrate de que ninguna aplicación tenga acceso permanente a tu ubicación (a menos que quieras, por supuesto). En general es buena práctica mantener el GPS apagado y solo encenderlo cuando lo necesites.

También puedes restringir otros permisos de las aplicaciones que usas. Normalmente las aplicaciones solicitan acceso a funciones de nuestro celular y nosotrxs se los damos sin pensarlo mucho. ¿Por qué Instagram o Google necesitan

acceso permanente a tu micrófono y cámara? Después nos sorprendemos porque "pareciera que el celular nos escucha". No parece, lo hace.

Si usas Android y Google, es posible apagar la actividad web de tu cuenta. La "actividad web" es un nombre inofensivo para algo que no lo es: Google registra todo lo que haces en la web (tus búsquedas, tus clicks, cuánto tiempo te quedas viendo un aviso en youtube, etc.) y genera publicidad y "experiencias" personalizadas en base a estos datos. Si apagas la actividad web, siguen recopilando información pero ya no es utilizada para "personalizar" tu experiencia.

Si usas Google Maps, puedes hacer lo mismo con el historial de ubicaciones (apagarlo).

Si usas Youtube, puedes hacer lo mismo con el historial (apagarlo).

Aprende a esconder tu IP.

Si estamos conectadxs a una red de internet, tenemos una dirección IP que le dice al resto del mundo de internet dónde estamos. Nuestra actividad en la web puede ser rastreada hasta nosotrxs y asociada con nuestra identidad en base a esta dirección IP. Una forma común y no demasiado complicada de protegernos es conectándonos a una red privada virtual (VPN, por sus siglas en inglés). Funciona así:

nos conectamos a la VPN, y esta a su vez está conectada a internet. Si alguien quisiera ver nuestra dirección IP, va ver la de la red privada, que puede estar en cualquier parte del mundo. Otra forma son las cadenas de Proxys. Funciona así: nos conectamos a un proxy, el que a su vez está conectado a otro proxy, y este a otro y así sucesivamente. Así, si alguien quisiera rastrear nuestra ubicación, tendría que ir por cada proxy, cada uno de los cuales puede tener miles, millones de conexiones, lo cual incrementa ostensiblemente el esfuerzo de rastreo. (Ver imagen página 19)

Para actividades en la red donde la privacidad o el anonimato son críticos, utiliza Tor. Tor es un navegador que se conecta a una red "anonimizadora" (te vuelve anónimx en la red). Por lo mismo es un poco más lento, pero muy seguro. Algunas recomendaciones para su uso efectivo:
- No uses Tor con VPN, pues esta última interfiere con la anonimización de Tor. Si vas a navegar en Tor, apaga tu VPN.
- Si estás usando Tor, cierra otros navegadores, pues ellos te delatarán.

Finalmente, si necesitas realizar actividades digitales sin dejar rastro alguno, tanto en la red como de forma local, existen sistemas operativos enfocados en la seguridad. Tails es uno de ellos. Debes correrlo desde una unidad extraíble (pendrive USB), porque si lo instalas en tu disco duro pierde sus poderes. Otra vez, busca tutoriales o acércate a tus afinidades computinas para informarte sobre esta práctica.

Otras formas de proteger tu identidad en la web:
- No uses tu correo electrónico real o uno que contenga tu nombre para suscribirte a "redes sociales" u otros servicios web. Existen herramientas que permiten encontrar todas las cuentas de redes sociales asociadas a un correo electrónico. Para eludir esta exposición, puedes utilizar servicios de anonimización, como AnonAddy, el cual genera alias de correos electrónicos. Así, en vez de dar tu correo electrónico real, das un alias que por lo general será una combinación ilegible de caracteres.

- Si se trata de cuentas provisorias, utiliza correos electrónicos temporales, por ejemplo, TempEmail. Y si te piden confirmar un número telefónico en una cuenta provisoria, utiliza servicios como smsreceivefree o similares.

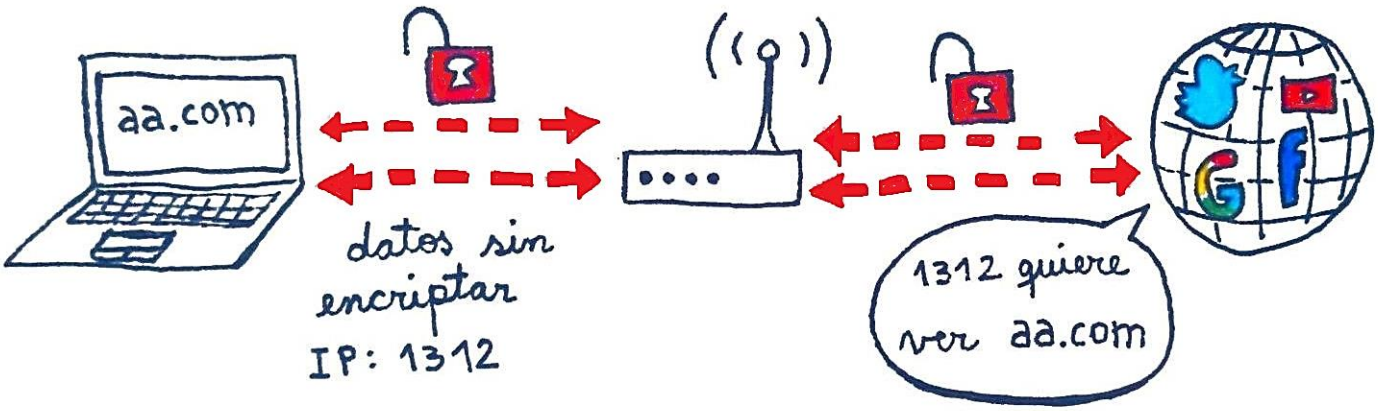
- La mayoría de los celulares inteligentes tienen un escáner de Wi-Fi activado por defecto, de manera que cuando detectan una red conocida, se conectan automáticamente. El escáner de Wi-Fi también ayuda a mejorar la precisión de la geolocalización. El problema es que, aunque tengas tu Wi-Fi apagado, el escáner está siempre encendido y emitiendo señales que permiten identificar tu dispositivo. En otras palabras, es como si tu celular fuera gritando por todas partes y en todo momento "¡aquí estoy! ¡soy yo!". La forma de apagarlo varía entre sistemas operativos (es diferente para Android que para iOS) y versiones, pero una búsqueda en DuckDuckGo te puede ayudar: "cómo apagar el WiFi scanning en [INSERTA TU SISTEMA OPERATIVO Y VERSIÓN]".

sin VPN

Tu dispositivo

Router/provedor de internet

Internet

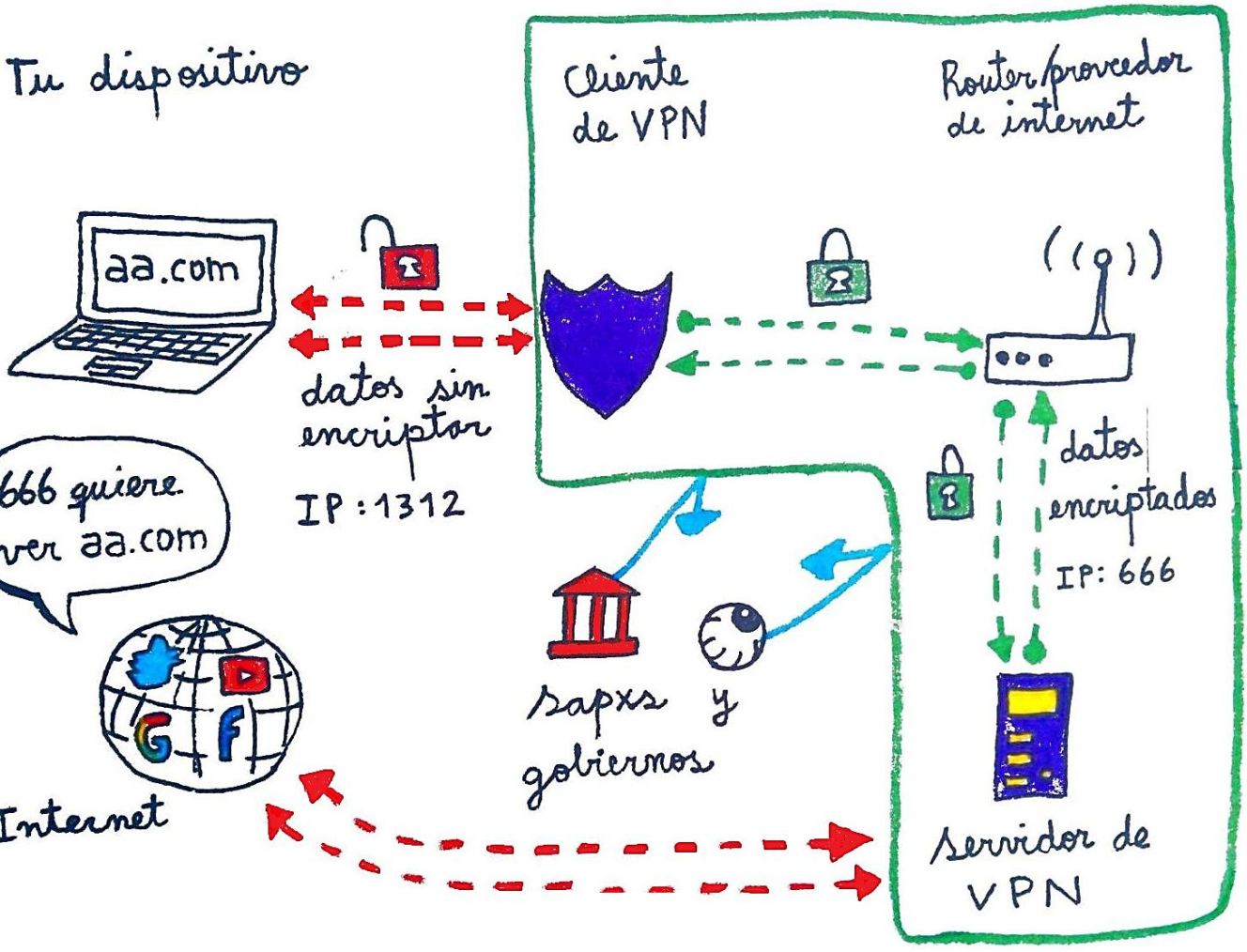


con VPN

Tu dispositivo

Cliente de VPN

Router/provedor de internet



Cambia tu clave cada vez

Piénsalo así: ¿usarías la misma llave para tu casa, tu lugar de trabajo y el candado de tu bici? ¿Qué pasaría si alguien encuentra esa llave o es extremadamente fácil de falsificar?

Los algoritmos de descifrado de contraseñas son cada vez más rápidos. Aunque da la impresión contraria, reemplazar letras por números también es fácilmente descifrable por un algoritmo.
Si queremos tener contraseñas seguras y diferentes para cada cuenta, no podemos confiar en nuestra memoria para almacenarlas. Por eso es buena práctica utilizar administradores de contraseñas (password managers) para generar contraseñas seguras y almacenarlas encriptadas en un solo lugar, protegidas por una "contraseña maestra". Así sólo tienes que recordar una gran contraseña que sea buena y no incluya el nombre de tu mascota...puedes utilizar una combinación no lógica de palabras. Por ejemplo: CalambreReliquiaJorobadoEclipse, y agregarle símbolos y números que tampoco sean lógicos para hacerla más segura.

Cámaras, drones van a arder

Dejo la interpretación de este verso a discreción de lxs lectorxs.

Interpretaciones literales son más que bienvenidas, y la inclusión de antenas de telefonía e internet -especialmente de 5G- es alentada.

LISTADO / DIRECTORIO DE HERRAMIENTAS

Correo electrónico:
Inventati.org, Riseup.net, Protonmail, TempEmail (correos temporales)

Mensajería:
IRC, Signal, Threema

Motor de búsqueda:
DuckDuckGo

Navegadores (alternativos a Chrome):
Brave, Tor, DuckDuckGo

Escritura colaborativa:
RiseupPad, CryptPad

Libros:
z-libros, library genesis

Administrador de contraseñas:
KeePass

Sabemos que si bien esta guía no es exhaustiva -ni pretende serlo-, hemos compartido una cantidad considerable de información. Sabemos que poner en práctica todas estas recomendaciones puede resultar abrumador. Sin embargo, no hay que olvidar que la tecnología de esta época está hecha para la pasividad y la adicción. Si la usamos tal cual viene configurada, en la mayoría de los casos la relación se invierte y ella nos usa a nosotrxs.

Recuperar nuestras vidas es urgente y posible, y podemos hacerlo sin irnos a vivir a la montaña como ermitañxs (aunque es una opción válida también). Podemos hacer un uso seguro de la tecnología para comunicar(nos), contrainformar(nos), autoeducarnos, sabotear, jugar, regocijarnos y todo lo que se nos ocurra, sin exponernos ni perder nuestra autonomía.

El propósito de esta guía no es que te conviertas en expertx en seguridad de la noche a la mañana. Si todavía te parece demasiado complicado, parte escogiendo una o dos prácticas sencillas e incorporándolas a tu cotidiano. Conversa de estos temas con tus amigxs y grupos de afinidad. Cuando vayas a salir, pregúntate: ¿necesito salir con celular?

"Quien quiera ser libre debe hacerse libre. La libertad no es un regalo de hadas que caiga en el regazo de alguien. ¿Qué es la libertad? Tener la voluntad de ser responsable de unx mismx." - Max Stirner

Salud y anarquía.