Teléfonos Móviles y más

GUÍA DE PROTECCIÓN DIGITAL

Escuela Feminista

Cuerpo, territorio y tecnología

escuelafeminista.red

Taller Nacional Honduras

CódigoSur
EDICIONES

BERTA VIVE

Berta no murió, se multiplicó

Guía de Protección Digital.
CódigoSur. Julio 2018. https://codigosur.org

1ra edición.

CódigoSur 2018.
Coordinación editorial: Nikole Yanez.
Facilitación: Nikole Yanez, Mónica Monge, Angélica Cárcamo.
Agradecemos la participación de ARPAS El Salvador.
Ilustraciones: Brenda Miralda
Diseño y composición: Mez K. Lit.
Elaborado en Software Libre: Scribus, Gimp, Inkscape.

1° edición: 50 ejemplares.
Impreso en El Progreso, Yoro, Honduras.
Impresión: CódigoSur Ediciones.

Sitio web: https://codigosur.org.

ÍNDICE

Soñando una escuela feminista

La Escuela Feminista Cuerpo, Territorio y Tecnologías es un espacio dónde participamos y creamos entre colectivas, organizaciones defensoras de derechos humanos y de las mujeres, periodistas, activistas independientes, comunidad LGTBI, defensoras de la tierra y el territorio.

En una región como la centroamericana donde tenemos las tasas más altas de femicidios, donde las mujeres atraviesan constantemente múltiples tipos de violencia. Ante esta cruel y violenta realidad nosotras tenemos muchas razones por las cuales protegernos usando herramientas que estén a nuestro alcance para proteger la vida y luchar por vivir una vida libre de violencia para seguir en la defensa de los derechos de las mujeres. La protección Integral para las mujeres tiene muchos significados y áreas, para nosotras

es importante la protección en todos los espacios y ámbitos de la vida, por eso es importante conocer y elaborar nuestros propios mecanismos de protección. La violencia de genero es sistemica y generalizada y es por ello que nuestra protección es una prioridad en la agenda política.

Por lo que mencionamos anteriormente y luego de un proceso de análisis del contexto centroamericano y teniendo en cuenta el nivel creciente de riesgos y amenazas para mujeres activistas de los derechos humanos, este año la Colectiva Feminista Código Sur se ha planteado formar un Escuela Feminista para fortalecer el activismo y los derechos humanos de las mujeres, colectivas, organizaciones defensoras de derechos humanos, periodistas, activistas independientes, comunidad LGTBI, defensoras de la tierra y el territorio. Gracias a los fondos de la Cooperación Sueca (ASDI), gestionados por la Asociación para el Progreso de las Comunicaciones(APC), este proceso de formación es una realidad.

Cada activista nace cuando queremos cambiar las cosas y trabajar para crear una sociedad más justa, donde todxs seamos parte. Nuestras luchas son muy diversas pero nuestra pasión y entrega son las que nos entrelazan en cada causa. Conocernos y reconocernos nos hará más fuertes.

Preparamos la tierra y el cuerpo para la siembra.

América Latina va a ser toda Feminista.

Para quién trabaja el discurso de la seguridad digital

Una marea de información es lo que llega cuando abrimos los ojos al funcionamiento de la vigilancia ejercida desde todo tipo de dispositivos digitales y electrónicos por agencias de inteligencia y espionaje.

iferentes capas contienen a **diversos actores en esta disputa por el control de la información** y por saber lo que piensa, dice y hace la gente, para a partir de ahí crear productos de consumo y manipulación de la opinión pública a escala mundial o local dependiendo de las necesidades de turno. Vivimos en una fantasía. Los medios al servicio del poder nos cuentan historias que no coinciden con la realidad que vemos. Nos ocultan información. Nos dan información falsa. El sistema dominante del planeta es un gran circo.

En esta coyuntura trabajar temas relacionados a la tecnología da cierta desesperanza. Pues **cuando pensamos en una mayor privacidad a la hora de comunicarnos y lo compartimos con organizaciones o movimientos nos damos cuenta que también de forma indirecta estamos favoreciendo un discurso sobre seguridad** que es contrario al tipo de sociedades libres en las cuales queremos vivir.

¿Qué intereses hay detrás de la "seguridad informática"? ¿Por qué ahora cuando la cooperación internacional para proyectos de desarrollo se está extinguiendo, los Estados Unidos tienen agencias enteras dedicadas al financiamiento de proyectos de software de cifrado para garantizar la democracia?

Preocupa ciertamente el hecho de que **toda la tecnología que usamos para mejorar nuestras comunicaciones es también creada por proyectos que vienen del norte**. Hay que mirar con atención la falta de proyectos de "cifrado" o "protección digital" impulsados desde América Latina. Por ahora, quiénes tienen un poco más de conocimien-

tos de estos temas y tienen alguna sensibilidad social colaboran con organizaciones y sociedad civil para ayudar a que disminuyan los efectos de la vigilancia masiva. Otras personas o colectivos más especializados ayudan a personas defensoras en situaciones de riesgo o más expuestos a vigilancia estatal o de servicios de inteligencia. Algunas de las herramientas compartidas en estos ambientes se encuentran reseñadas en este documento. Sin embargo, no es posible garantizar de ninguna forma que alguna de estas herramientas sean "realmente" seguras.

¿Qué intereses hay detrás de la "seguridad informática"? ¿Por qué cuando la cooperación internacional para proyectos de desarrollo se está extinguiendo, los Estados Unidos tienen agencias enteras dedicadas al financiamiento de proyectos de software de cifrado para garantizar la democracia?

Es mentira que usando Signal estamos "seguros". Pues **en términos informáticos la seguridad como tal no existe**. Menos con una aplicación de mensajería que todavía se basa en el protocolo SS7[1] que está técnicamente probado que es muy vulnerable[2] incluso en dispositivos cifrados o que usen el cifrado en sus comunicaciones.

Al no poder saber con certeza sobre si algo es o no "seguro", debemos presumir que toda comunicación está comprometida. Por lo tanto, **la "seguridad digital" también es un discurso que favorece a cierto sectores de la economía informática o de inteligencia**.

Signal es un protocolo abierto para el cifrado de las comunicaciones pero no tiene soporte para federación, una tecnología que permite

[1] https://hipertextual.com/2016/06/ataque-ss7-whatsapp-telegram
[2] http://globbsecurity.com/vulnerabilidad-ss7-espionaje-masivo-38808/

Propaganda de ayer y de hoy / Imagen: https://flic.kr/p/gnmcb

descentralizar los sevicios y así ponerlo en manos de la gente. Lo cierto es que cada vez más los protocolos que representaban un camino común para seguir teniendo servicios distribuidos y descentralizados (como XMPP), han sido comprados o usados por grandes corporaciones como el caso de Google con su anterior Google Talk basado en XMPP y federado, y su implementación de Hangout que rompió la federación con XMPP.

En cuanto a los derechos de internet, algunas de las ONGs que tocan el tema en América Latina muchas veces utilizan ejemplos de países que de una u otra manera y con sus errores han emprendido un camino de independencia política y también de región. Me llama mucho la atención que esto no se hable, que esto parezca normal.

Teniendo en cuenta que las herramientas de espionaje vienen en gran medida del norte **parece a propósito el desvío de la atención hacia casos que desprestigian a gobiernos progresistas en América Latina, y no nombrar la injerencia de los Estados Unidos en cuanto a espionaje en la región**, la discusión política de fondo es a quién le hacemos el juego cuando abordamos la "seguridad digital" como estrategia para mejorar las condiciones de per-

sonas luchadoras sociales o defensoras de derechos.
Están quiénes se acomodan al discurso y las narrativas que el sistema necesita. Aquellos que usando las contradicciones del sistema se aprovechan de él para sacar una tajada. **Las neoONGs que hablan de privacidad en internet mientras hacen acuerdos de cooperación con Google**.
También está la falta de iniciativa de nuestra región de tomar mayor protagonismo. Estamos varios pasos atrás y esto nos da mucha desventaja. Ni siquiera tenemos nuestros propios foros de Internet, Gobierno y Sociedad Civil, quiénes impulsan estos foros internacionales (como IGF) son las corporaciones (Goole, AT&T y otras) con la preponderancia política y económica de los Estados Unidos como los dueños de internet.
El Internet Freedom Festival que parece una iniciativa tan linda y novedosa por nuestros derechos, está plagada de personajes corporativos y de agencias de cooperación estadounidense, vinculadas al Departamento de Estado y a Radio Free Asia (una especie de Radio Martí para Asia pero mucho más grande). Sin duda los esfuerzos de la EFF son muy valiosos. Y han realizado grandes aportes. Pero **es necesario tener nuestros propios propios referentes**. Y así entablar colaboraciones con el resto del mundo. Pero **desde nuestras autonomías, y pensando en nuestras propias agendas**. Que son muy diferentes a las agendas de resistencia en SilliconValley.
Necesitamos espacios dónde movimientos sociales de América Latina puedan construir un debate y una agenda común de trabajo en temas de tecnología. Aquí **sectores políticos con movimientos deben trazar un plan de trabajo** para poder dar pasos en una construcción regional de Protección Digital y de desarrollo de software libre. Nuestra región debe ser pionera en la constitución de verdaderos derechos humanos en el uso de una herramienta como internet.
Necesitamos seguir construyendo alternativas desde el sur, y especialmente desde América latina, porque esta lucha no es nueva, pero ahora está en **una etapa de sofisticación más compleja y es determinante el rol que juguemos** como sociedad civil, movimientos sociales y estado.

San H. M. - Revista Pillku

Por qué deberías dejar de usar WhatsApp

El servicio de mensajería de la transnacional Facebook es una de las herramientas que definitavemente tenemos que eliminar de nuestros celulares. Aunque WhatsApp dice que ahora tiene cifrado de extremo a extremo, hay razones de sobra para desconfiar de su cifrado, pero sobre todo de las intenciones de la empresa.

No es casual que posterior a todo el escándalo de privacidad a raíz de las filtraciones de Snowden y la pérdida masiva de personas usuarias a raíz de su inexistente capa de seguridad frente a Telegram o Signal, una empresa como WhatsApp haya implementando tecnología de Open Whisper System (recomendada por Snowden) para ofrecer a la gente un servicio de comunicación cifrada de extremo a extremo.

Analicemos un momento esto: ¿Podría ser posible que siendo WhastApp una aplicación insegura y la creciente demanda de mayor seguridad haya inclinado a WhatsApp a tener que tomar la decisión de cifrar sus comunicaciones sólo por amor a las personas usuarias?
Para esta pregunta no tenemos una respuesta. Podemos preguntarle a WhatsApp y probablemente la respuesta que nos de sea falsa. Pero quizás la verdadera problemática para Whatsapp se haya presentado en tener que responder a legislaciones, no sólo de Estados Unidos, sino de otros países para facilitar información. Por ejemplo en el caso de Brasil el gobierno decidió Bloquear la red de WhastApp porque la compañía se negó a facilitar información de personas vinculadas al narcotráfico.
Si WhatsApp no tuviera ahora su sistema de encriptación de los mensajes que según ellos son imposibles de leer por terceros incluso de la compañía estarían frente a un problema crececiente, la solicitud de información por parte de muchos estados por ejemplo. Al tener su sistema de comunicación cifrado de extremo a extremo se ahorran tener que dar explicaciones. Un sistema técnico que nadie sabe como funciona pero que está basado en el protocolo abierto de Signal de cifrado impide a la empresa a poder tener acceso a los mensajes. Whatsapp no puede demostrar que es seguro al no ser auditable ya que no es software libre. Pero al decir que cifran sus comunicaciones, se quitaron a todo el mundo de encima y ahora es posible que puedan ver la información sin que nadie les moleste y además pueden ofrecerla a las agencias de seguridad de su país que obviamente pueden obtener acceso con ayuda de WhatsApp o sin su ayuda. Oficialmente ya nadié podrá reclarmarle a Whatsapp que no suministra información y bloquearle el servicio por ello. Pues simplemente ahora dicen que no tienen acceso.

¿Pero por qué no usar WhatsApp si ha permitido a millones de personas en todo el mundo comunicarse?
Pues así cómo lo oyes WhatsApp se aprovecha de ti y de tus necesidades de comunicación, y brindando un pobre servicio se ha posicionado como la aplicación número uno. No es de extrañar. Recordemos que sistemas operativos que son realmente malos como los desarrollados por Microsoft han sido durante años los más usados en computadoras personales al rededor del mundo. Pareciera que las corporaciones son

expertas en vendernos simples herramientas como si fueran las más maravillosas.

WhatsApp te espía

Aunque recientemente han incorporado un protocolo de cifrado basado en OpenSignal al no ser auditable el código fuete de WhatsApp realmente no sabemos qué es lo que el programa hace y cómo recopila información. Tampoco sabemos si su cifrado puede ser leído por la compañía y si tienen puertas traseras para las agencias de seguridad.

En el caso de WhatsApp vale la pena hacer un repaso puntual de por qué no recomendamos el uso de esta herramienta por cuestiones filosóficas, políticas y de libertades individuales.

WhatsApp sabe con quién hablas y realiza estadísticas de tus conversaciones

Aunque el cifrado de WhatsApp ha mejorado un poco la seguridad de la herramienta, tanto los contactos, como las demás metadata de la información que viaja, no está cifrada. Esto quiere decir que por más que juren y re-juren que no pueden leer tus mensajes (¿quién va a creerles?) en ningún lado dicen que no se meten con tus contactos ni con la metadata generada por tus habitos de comunicación. Por lo tanto, WhatsApp recoleta muchísima información sobre ti, los lugares en los que estás, las personas con las que te comunicas y con qué frecuencia. Por otro lado, si tienes activada la opción de copia de seguridad automática en el smartphone, es posible que se guarden mensajes ya borrados que pueden ser recuperados más adelante por posibles atacantes.

WhatsApp guarda la información que tu generas

La app de mensajería no borra los chats "eliminados" por las personas usuarias, sino que los retiene y almacena en el dispositivo. Cualquier

persona con los conocimientos informáticos necesarios y acceso al teléfono podría recuperar las conversaciones borradas en WhatsApp, algo que se contradice directamente con el mensaje de protección de los datos que los responsables de la app han querido dar con la implantación del encriptado punto a punto.

Alta y en la verificación de los usuarixs

Estos procesos pueden llegar a propiciar que un atacante logre hacerse con las claves de acceso para secuestrar la cuenta de otra persona usuaria, leer los mensajes que reciba y enviar mensajes en su nombre.

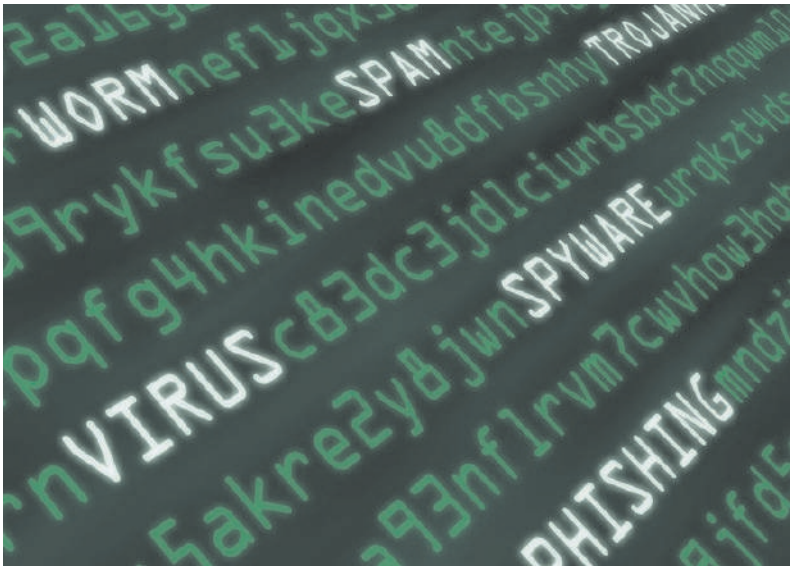
La difusión de información sensible durante la conexión inicial es otro peligro asociado al uso de WhatsApp. La aplicación intercambia en texto información privada de las personas usuarias, como su sistema operativo o el número de teléfono registrado.

Además, también se han producido robos de cuentas mediante SMS o llamadas y ataques de phishing utilizando WhatsApp Web, el almacenamiento de información en la base de datos o el intercambio de datos con la red social Facebook, propietaria de la aplicación de mensajería.

Revista Pillku

Malware o software malicioso

Malware hace referencia a cualquier tipo de software malicioso que trata de infectar una computadora o un dispositivo móvil.



Los crackers utilizan el malware con múltiples finalidades, tales como extraer información personal o contraseñas, robar dinero o evitar que los propietarios accedan a su dispositivo. Los tipos de malware incluyen spyware (software espía), adware (software publicitario), phishing, virus y ransomware etc.

Recientemente se comprobó por medio de una filtración de WikiLeaks que algunos países de América Latina contrataron una empresa de nombre Hacking Team; Brasil, Chile, Colombia, Ecuador, Honduras, México y Panamá pagaron a esta empresa para espiar a la población. Países que negociaron con Hacking Team: Argentina, Guatemala, Paraguay, Uruguay, Venezuela. Hacking Team no es la única empresa que realiza este tipo de contrataciones a empresas o gobiernos.

¿Cómo se instala?

El Malware puede instalarse en cualquier computadora ya sea Linux, Windows, Mac, en cualquier teléfono móvil inteligente o tableta con sistema operativo Android, BlackBerry, iOS (iphone), Symbian o Windows Mobile.

La primera forma en la que puede instalarse es de manera física a través de una llave USB o dispositivo de almacenamiento externo.

La segunda forma es mediante la conexión a redes Wifi, visitando y descargando archivos de sitios web, descargando archivos adjuntos del correo electrónico.

Si las autoridades (policías, oficiales, militares etc) tienen acceso directo a la computadora, teléfono ó dispositivo externo y no estabas presente, es necesario realizar análisis del equipo inmediatamente para asegurara que no contenga algún tipo de Malware o efectuado algún cambio.

¿Qué información buscan?

En el casos Hacking Team el Malware puede acceder y copiar desde el mismo equipo cualquier tipo de información contenida.

Contactos, aplicaciones utilizadas, calendario, llamadas y audios de teléfono, Skype, cámara y webcam, chat, todo lo copiado al portapapeles, archivos abiertos, disco duro, teclas apretadas, mensajes y correos electrónicos, micrófono y audio, clics del mouse, contraseñas, posición geográfica en tiempo real, impresiones, capturas de pantalla y sitios de internet visitados.

¿Cuáles pueden ser sus comportamientos?

- Si nuestra cámara web enciende la luz cuando no la estamos usando.
- También si encuentras actualizaciones con ventanas muy poco familiares.

Para protegerse del malware es importante que:

- Realizar actualizaciones regularmente del antivirus, cortafuegos, navegador de internet y el sistema operativo de la computadora, tablets y celular.
- Presta atención a los correos electrónicos desconocidos, también a los adjuntos que no estabas esperando o que te resultan sospechosos, a las aplicaciones de chat y mensajería instantánea.
- Limpiar o escanear las usb o cualquier dispositivo externo.
- Tener al menos dos respaldos de la información uno en casa u oficina y otro fuera de ella.
- Utilizar el navegador con los complementos de seguridad.
  No abrir correos ni adjuntos de personas desconocidas.
- Utiliza software libre, ya sea como sistema operativo y/o en aplicaciones o programas.

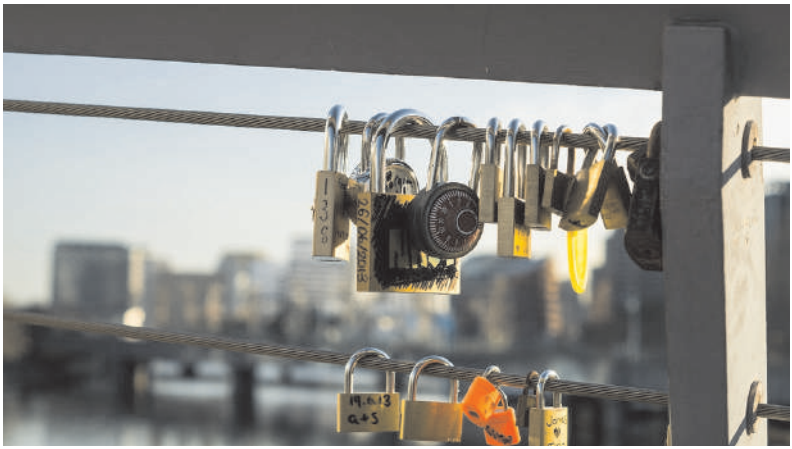
Recientemente se comprobó por medio de una filtración de WikiLeaks que algunos países de América Latina contrataron una empresa de nombre Hacking Team para espiar a la población.

Si encuentras malware:

- No se te olvide apuntar o describir ¿Qué sucedió?, en qué momento ocurrió, fecha y hora, ¿En qué lugar estabas?, una descripción de lo que pasó, datos de la computadora o celular (sistema operativo, programas, hardware etc.) estos datos ayudaran a identificar el ataque.
- Puedes tomar capturas de pantalla, y recolectar algún registro.
- Si tienes dudas de un archivo adjunto o algún documento extraño en tu computadora puedes subirlo a este sitio https://www.virustotal.com/ para hacer la verificación.

Crear contraseñas seguras

El uso de contraseñas es una de las capas más básicas de la protección digital. Por desconocimiento muchas personas usan la misma contraseña para muchos servicios, o son fáciles de adivinar por un programa informático. Aqui algunas recomendaciones básicas a la hora de crear y alacenar nuestras contraseñas.



Es importante tener una contraseña fuerte como iniciativa de autodefensa. La mayoría de los crackeos de cuentas de redes sociales, correos, banca online y otros se deben principalmente a contraseñas débiles. También es importante tener una única contraseña por cada cuenta, ya que si nos crackean y usamos la misma contraseña en varios servicios y dispositivos, toda nuestra infrmación estaría comprometida.

Para generar contraseñas seguras existen diferentes programas que nos ayudan a crearlas y también a almacenar nuestras contraseñas de forma segura. Keepass es un gestor de contraseñas que permite su almacenamiento en una base de datos dotando a nuestras claves de una mayor seguridad. La aplicación permite establecer una única contraseña a recordar que servirá como "llave maestra" al almacén del resto de

contraseñas, las cuales no tendremos que recordar nunca más.

Te recomendamos que:

- No la escriba en un papel, ni la guarde en el celular.
- No incluya información personal, (fechas de nacimiento o aniversarios, nombres, edad, etc.)
- No utilice la misma contraseña para todo, crea una contraseña para cada cuenta o servicio.
- Cree una contraseña para ingresar a la computadora, teléfono, correo, banco.
- Use el programa de administración de contraseñas keepass para almacenar las contraseñas seguras y para generar contraseñas.
- Si nunca cambió la contraseña desde que creo la cuenta, es bueno que lo haga.

Ten presente que:

- Revisar que las sesiones de tus cuentas se cierren una vez que ya no las estés usando y poner más atención de cerrar la sesión cuando estamos usando otras computadoras.
- Revisa que el navegador de internet no guarde las contraseñas. Para revisar esto ve al menú del navegador, ir a preferencias y buscar la viñeta de seguridad y desactivar recordar contraseñas.
- No reciclar contraseñas, crea una diferente cada vez, el Keepass te ayudará a crear una nueva cada vez.

¿Cómo es una contraseña segura?

- Creativa, puedes escrbir en la lengua materna, detalles que no estén en las redes o internet.
- Con muchos caracteres por ejemplo "sol reflejado en el río que baña de luz mi corazón" que contiene 51 caracteres.
- Agregandole un sasón por ejemplo números, símbolos algo especial.
- Privacidad, la contraseña no la compartimos con nadie.
- Utiliza Keepass para guardar las contraseñas de manera segura.
- Si tienes KeePassDroid que es el keepass para Android solo ten las contraseñas que necesitas para el uso en el celular.

¿Qué es la minería de datos?

Nuestros datos personales son un nuevo capital. Digamos ¡no a la minería de datos!

Así en la tierra como en la red / Cerro de Pasco, Perú.

No solo usamos internet, somos materia prima, trabajadorxs explotadxs, productores y consumidores. Evitemos utilizar servicios en Internet que lucran con la recolección de datos. No aceptemos que las grandes empresas nos vigilen, no les demos nuestros datos. Digamos NO a las Industrias Extractivas: Google, Facebook, Twitter, Whatsapp, Instagram, Apple, Microsoft, etc.
Zuboff habla sobre el capitalismo de la vigilancia, y podemos observar que el nuevo capital del mundo es de las empresas tecnológicas.
Al 06 de junio de 2018, las compañías de tecnología más valiosas del mundo, según PitchBook, son: Pinterest: 12.300 millones de dólares, Airbnb: 31.000 millones de dólares, Uber: 69.900 millones de dólares. CNNMoney en el 2017 presento que estás empresas como Alphabet (Google), Facebook, Microsoft y Apple tienen un valor

colectivo de casi 3.3 billones de dólares.
La vigilancia es la arteria principal de este capitalismo tecnológico.
Los servicios de internet que parecen gratuitos, en realidad no lo son. El costo de proporcionar a cada usuarie una cuenta de correo, un perfil en una red social o una carpeta de almacenamiento es insignificante comparado con las grandes ganancias que estas empresas perciben mediante la minería de datos. Abrir una cuenta en estos servicios requiere que aceptemos sus términos y condiciones de uso y con ello otorgamos el permiso de utilizar nuestros datos para un fin desconocido. Podría ser que hoy sólo se utilicen para vender publicidad pero lo preocupante es no saber qué uso les darán mañana, ya que efectivamente pasan a ser de su propiedad.

No aceptar que las grandes empresas de Internet nos vigilen es una medida de autodefensa y seguridad y también una postura política.

Nuestros datos personales, patrones de uso y listas de contactos son la materia prima. Somos trambién lxs trabajadores que dan forma a la información con cada laik, retuit o enlace que visitamos. Nuestros propios perfiles en las redes sociales son el atractivo principal para usar estos servicios, colocándonos como un producto. Además, soos trambién consumidores de la información de otros perfiles y de la publicada dirigiga al nuesto.
Es importante reconocer el valor de nuestros datos personales. Evitemos utilizar servicios en Internet que lucran con la recolección de nuestros datos a costa de nuestro derecho a la privacidad.
No aceptar que las grandes empresas de Internet nos vigilen es una medida de autodefensa y seguridad y también una postura política.

Fuentes: Criptotarjetas Rancho Electrónico y Ártica Online

¿Quiénes pueden espiar tus comunicaciones?

Es preciso conocer y analizar el contexto en el que realizamos nuestro pleno ejercicio de exigir respeto a nuestros derechos, teniendo claro cuales son los actores que intervienen podremos tomar acciones para resguardar nuestra información y comunicaciones. Incluso saber cuándo es mejor no decir la información por teléfono o por internet.

Proveedores de Internet

Tu proveedor de servicios es el primero que puede espiar tus comunicaciones.

Empresas

Rastrean tu navegación y el círculo de relaciones, vendiendo tus datos a Empresas y Gobiernos.

Gobiernos

Los Gobiernos pueden espiar a sus ciudadanos como se comprobó con Hacking Team.

Publicidad

Las empresas espían tu navegación y generan publicidad geolocalizada.

Crackers

Pueden espiarte para robarte información financiera o sensible para extorsionarte o por diversión.

Policía

La Policia puede infectar tus dispositivos y hacerte seguimiento.

Militares

Los militares pueden espiarte para saber tu ideología y generar estrategias de represión.

Agencias de Seguridad

Agencias de Seguridad de los Gobiernos, Privadas.
CIA, FBI, NSA, etc.

Encripta el celular

El encriptado ó cifrado es la forma de resguardar los datos para que la información sea codificada, en caso de robo del dispositivo no se podrá leer la información si no tiene la contraseña para desencriptar la información esto aplica para celulares, correos, computadoras, mensajes etc.

1

Para comenzar, ten en cuenta que algunas marcas y modelos de celular no tienen esta opción.

2

Ten cuidado con la tarjeta Sim (chip). Es un arma peligrosa, permite por medio de la vulnerabilidad ss7 clonación de tu teléfono. Usa teléfonos sin GPS ni wifi ni bluetooth para poner tu chip, hacer llamadas y validar servicios.

3

Verifica tu batería:

Asegurate que el celular tenga 80% de bateria

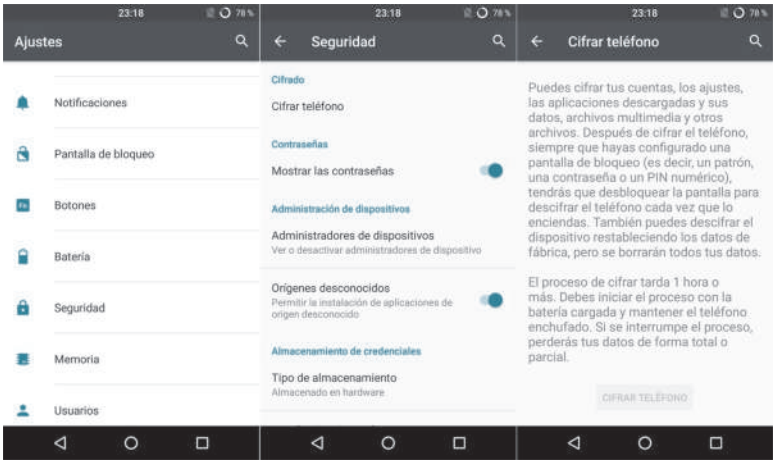
Conecta el celular a la red eléctrica

4

En primer lugar ve a Ajustes

Busca la opción Seguridad

Coloca una contraseña, no un patrón ni un pin.



Algunos consejos

Desactiva el wifi cuando no lo usas

Utiliza VPN de confianza en redes públicas

Desactiva Bluetooht cuando no lo usas

Usa Signal o Wire con autodestrucción

Desactiva el GPS cuando no lo usas

Deja los teléfonos fuera de las reuniones.

Para tener en cuenta:

- Antes de ir a una manifestación acordar un punto encuentro.
- Hacer un respaldo del celular
- Eliminar la información que no usemos.
- Ten en cuenta las leyes de ciberseguridad de tu país y los procedimientos de vaciados de información.

Lista de aplicaciones

Un listado parcial de aplicaciones que puedes utilizar para mejorar la seguridad y la privacidad de tu teléfono móvil.

Comunicaciones

Signal - Android, iOS Mensajes y llamadas encriptadas, desvanecimiento de mensajes en grupos, seguridad en grupos.
Wire - Android, iOs, Mensajería Segura
ChatSecure - Android, iOS – Mensajes instantáneos seguros (Google, Facebook, Jabber/XMPP) con OTR Off-the-Record + el uso de Orbot para Tor como integración
Conversations.im - reemplaza a ChatSecure para Android
SureSpot - Android, iOS – Mensajes instantáneos seguros
K9 Mail- Android – Cliente de correo alternativo para no usar gmail

Navegación por internet

Bitmask - Android VPN para una navegación más segura - usar la versión demo, usar para redes wifi públicas en parques, cafés u otros.
Firefox para celular y/o computadora, en el siguiente capítulo.
Orbot – Tor on Android anónimato en Internet
OrFox - Firefox configurado vía Tor (es necesario instalar OrBot) Anónimato en internet

Cámara y registro Multimedia

ObscuraCam - Android – borra los rostros de la gente en forma de pixeles u otras y también borra metadata de las fotos.
CameraV - Android - Recopila todos los datos alrededor de donde fue tomada la foto.
PixelKnot - encripatar mensajes con imagenes, ocultar mensajes en imágenes.

Protección ante malware y virus

Stagefright detector - detecta si su celular puede ser hackeado por ataques - sólo se pueden arreglar con una actualización del sistema operativo o con un nuevo celular.
AIMSICD - Android - Detector de ataque IMSI Catcher
https://secupwn.github.io/Android-IMSI-Catcher-Detector/

Privacidad y Seguridad

Encriptación del celular - Sistema Android en la opción de seguridad.
Permiso a las aplicaciones - para dar permiso a las aplicaciones se encuentra normalmente en las opciones de privacidad del celular.
F-Droid es un catálogo instalable de aplicaciones de software libre para Android descargar desde el sitio web https://f-droid.org/
Avira *, AVG, Avast – anti-virus para Android & iOS
OpenSignal - muestra la locacion de antenas GSM para localizar ataques de antenas falsas
LocationPrivacy - para hacer que compartir la ubicación sea más segura
Clueful - Información acerca de la privacidad de las aplicaciones que ofrecen las apps instaladas en el celular.
XPrivacy (lo mismo que clueful).
KeePassDroid - Android - Guardar y crear contraseñas para el celular
Keepass2Android - soporte para bases de datos con kdb2
https://keepass2android.codeplex.com/
MiniKeePass - iOS
AppLock - Android – Poner bloqueo para algunas apps
Prey - cuando el celular ha sido robado - se puede pagar para hacer un borrado remoto
Android Lost - Borrado remoto para Android http://www.androidlost.com o por msn.

Utilidades

Omni Notes FOSS - Android – tomador de Notas
OsmAnd~ - mapas libres de uso sin internet

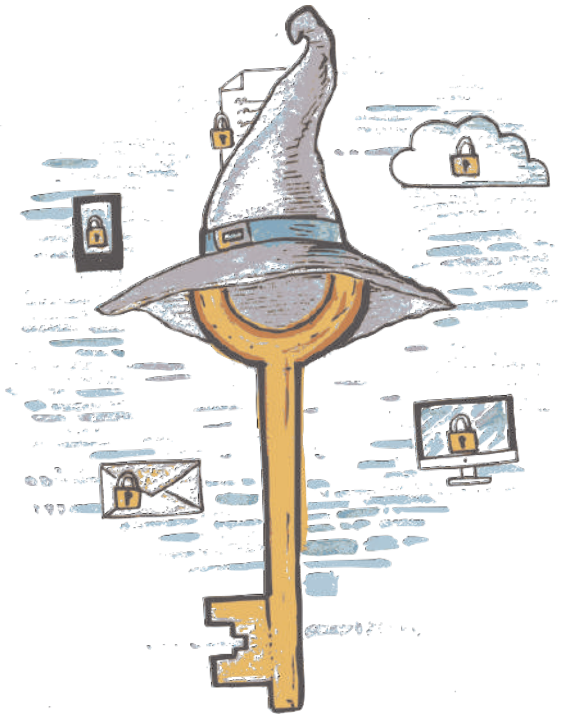
CCleaner elimina archivos basura
Martus (Android) base de datos
Google Authenticator
Open flash light
Broadcastmyself - transmisión de radio por internet desde el celular

Redes sociales

Face Slim alternativa a la aplicación de facebook y no contiene publicidad
Twitdere alternativa a Twitter y no contiene publicidad.
NewPipe alternativa a Youtube no contiene publicidad, mantiene la opción de reproducción de video en segundo plano. No se puede ver streaming en vivo.

Sistema Operativo / Software Libre

LinageOS - https://wiki.lineageos.org/devices/



MARIELLE VIVE

Firefox

Mozilla Firefox es un navegador web libre y de código abierto desarrollado para Linux, Android, IOS, OS X y Microsoft Windows. Si todavía no lo tienes instalado puedes hacerlo en este momento en tu computadora o celular.

Firefox o Panda Rojo / Imagen: https://flickr.com/photos/mathiasappel/

La privacidad es una de las principales razones por las cuales recomendamos el uso de Firefox como navegador. No tenemos que olvidarnos de que Google basa su negocio en la publicidad y que para ello debe hacer una recolección de todos nuestros datos. Si no nos gusta que Google siga haciendo más dinero con nuestros datos usemos Firefox configuremos las funciones como decirle a las webs que no nos rastreen, incluye el buscador DuckDuckGo por defecto y nos da la opción de no enviar datos de uso si no queremos y muchas más opciones, solo ve al menú y en preferencias buscas la viñeta seguridad y también en privacidad. Para finalizar solo mencionar que de los navegadores de internet que derivan de Firefox esta Tor Browser que utiliza la red TOR para tener anonimato en la red y acceder a contenidos en la Deep Web

para instalarlo entra a http://torproject.org/.

Complementos para uso básico:

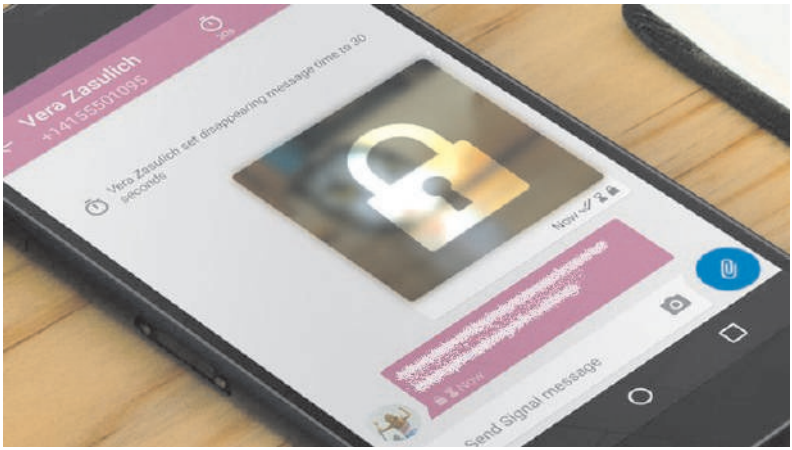
HTTPS Everywhre - Forzar las páginas seguras con https.
https://www.eff.org/https-everywhere
Privacy Badger - bloquea la publicidad que espía.
https://www.eff.org/privacybadger
Self-destructing cookies - destruye las (cookies = la información enviada por un sitio web y almacenada en el navegador, así el sitio web puede revisar tu navegación anterior).
https://addons.mozilla.org/en-US/firefox/addon/self-destructing-cookies/
Ublock Origin Bloquea la publicidad de las páginas y evita su descarga, haciendo una navegación más rápida y segura.
https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/
HTML5 - Alto performance para ver vídeos en la web.
https://addons.mozilla.org/en-US/firefox/addon/html5-video-everywhere/
DuckDuckGo - buscador alternativa a Google.
https://addons.mozilla.org/en-US/firefox/addon/duckduckgo-for-firefox/

Instala estos otros complementons cuando te acostumbres a los primeros de la lista:

NoScript - sólo permite JavaScript, Java y otros plugins en los sitios web de confianza. Para Chrome instalar Umatrix es un equivalente. https://noscript.net/getit
Canvas Blocker - bloquea JS-API https://addons.mozilla.org/en-US/firefox/addon/canvasblocker/
Open With - menús y pestañas para abrir la página en otro navegador https://addons.mozilla.org/es/firefox/addon/open-with/.
User Agent Switcher - Sustituir al agente de usuario del navegador. https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher-firefox/

Signal

Signal es una aplicación de mensajería instantánea y llamadas, con énfasis en la privacidad y la seguridad. Puede ser utilizada para enviar y recibir SMS, MMS y mensajes de datos cifrados.



Varias organizaciones, colectivos y defensores de derechos humanos alrededor del mundo están utilizando Signal para sus comunicaciones, recomendamos el uso de esta herramienta con la que pueden enviar mensajes, las conversaciones pueden ser de dos o más personas. La Electronic Frontier Foundation elaboró una tabla comparativa de los diferentes clientes de mensajería instantánea donde pueden encontrar diferencias sustantivas https://www.eff.org/node/82654.

¿Por qué Signal?

- Las llaves de cifrado están en tu poder.
- Se puede comprobar la llave de cifrado.
- Los grupos son cifrados.
- No recolecta metadatos.
- Autodestruye los mensajes.

BETY CARIÑO

Sobre CódigoSur

Somos una colectiva de personas pertenecientes a diferentes movimientos sociales, con el propósito de colaborar con el desarrollo y la socialización de la comunicación, la cultura y las tecnologías libres en América Latina.

Creemos que debe haber un nuevo modelo de producción del saber y una nueva forma de construir la cultura, por eso, como acción política y ética nos proclamamos en contra de la dominación y la privatización de la vida, el conocimiento, la comunicación y la cultura.

Nuestro trabajo se desarrolla por medio de redes de pares y de un modelo descentralizado de gestión. De esta manera, brindamos servicios tecnológicos libres y seguros a organizaciones, movimientos, colectivos y personas que promueven los derechos humanos, la ecología, la comunicación, la tecnología, las libertades individuales y colectivas y los procesos sociales de emancipación. A través de nuestro trabajo diario apoyamos a diversas instituciones y organizaciones sociales involucradas en el desarrollo de su comunidad y radio de acción.

Creemos en la construcción de un nuevo paradigma en la generación de saberes y herramientas. Transitamos por un modelo de producción y construcción horizontal y abierto. Defendemos el derecho común a la vida, al conocimiento, a la comunicación y a la cultura.

CódigoSur
codigosur.org

Con el apoyo de

APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Asdi

BARRACÓN digital_