AUTODEFENSA DIGITAL para ACTIVISTES y comunicadorxs POPULARES

PARTIDO
INTERDIMENSIONAL
PIRATA

Utopía Pirata

https://utopia.partidopirata.com.ar contacto@partidopirata.com.ar

Autodefensa Digital para activistas y comunicadorxs populares

Introducción

Esta publicación es una guía rápida y no exhaustiva que recoge los artículos disponibles en la Wiki del Partido Interdimensional Pirata[1]. Si bien la dirigimos específicamente a comunicadoras y activistas, no todos los artículos fueron concebidos con ese objetivo, por lo que notarán que varios son breves y a veces hasta insuficientes…

Los talleres de autodefensa digital que venimos coordinando/facilitando desde hace un tiempo y que dimos en llamar **Grog & Tor**, se piensan desde las prácticas comunicacionales de diferentes comunidades, territorialidades y organizaciones con las que venimos interactuando y hacia las cuales nos sentimos afines. Por eso, esta selección de herramientas tiene incorporada una mirada sobre las problemáticas comunes con las que nos encontramos en la práctica de nuestros activismos. Sin embargo, se trata de una mirada que no está cerrada sobre si misma, ya que como Partido Interdimensional Pirata todavía estamos construyendo (y fortaleciendo) ese diálogo entre activistas digitales y otras activistas y comunicadoras, para repensar nuestras prácticas, para cuidarnos entre nosotras, de forma de prevenir abusos estatales y paraestatales. Por eso, en el marco de nuestras comunidades, de nuestras organizaciones, grupas y/o movimientos, vamos haciendo y rehaciendo el compromiso de asumir ese desafío. Se trata de un trabajo colectivo que queremos ir circulando y mutando, para que pueda contribuir a experiencias que generen poder popular en el contexto de luchas concretas. Este material constituye una manera de dejar abierta la invitación a ensayar el uso de

[1] https://wiki.partidopirata.com.ar

tecnologías libres que nos sirvan para comunicar desde nuestras experiencias y especificidades reivindicativas, así como para intercambiar ideas sobre los usos de las tecnologías en el hecho comunicativo; si sirven o si no sirven en los contextos comunicacionales de nuestras colectivas, territorios y movimientos; qué pasa cuando las necesitamos usar de urgencia; cómo son tomadas por las colectivas y con qué dificultades se encuentran; si son necesarias otras herramientas y si hace falta ponernos a imaginar y desarrollar tecnologías nuevas…

F-Droid

F-Droid es un instalador de aplicaciones libres para Android, que reemplaza a Google Play. Si te preocupa que Google obtenga y utilice datos privados tuyos y/o querés asegurarte de que todo el software que usás en tu Android sea libre, F-Droid es lo que necesitás P) Lo bueno de F-Droid es que las personas detrás del proyecto también se preocupan por la auto-defensa digital, con lo que eliminan cualquier tipo de extracción de datos que utilice una aplicación o si no es posible, lo avisan en la descripción para que podamos decidir si la queremos instalar o no. Por ejemplo, ninguna aplicación muestra publicidad.

Se instala descargando la aplicación desde el sitio https://f-droid.org.

Se va a descargar un archivo.apk. Al abrirlo, da la opción de instalarlo. A veces, Android dice que necesitamos permitir instalar aplicaciones “de orígenes desconocidos” o “fuentes desconocidas” (es decir, que no sean de Google Play). Para habilitarlo, hay que ir a los Ajustes del celular y en la sección “Seguridad”, activar la opción.

Ya instalado vamos a tener acceso a ~1500 aplicaciones libres. Para obtener acceso a todas las aplicaciones tal vez sea necesario agregar o habilitar otros repositorios desde Ajustes > Repositorios.

Los repositorios son bases de datos de aplicaciones disponibles para instalar. F-Droid viene con su propio repositorio activado y algunos proyectos tienen sus propios repositorios.

Guardian Project[2] tiene un repositorio donde publica todas las aplicaciones de autodefensa digital que desarrollan.

[2] https://guardianproject.info/

Buscar aplicaciones

Al ingresar a F-Droid va a mostrar un listado de todas las aplicaciones disponibles en orden de actualización. También se pueden navegar por categorías, usando los botones al pie.

Con el botón verde con ícono de lupa se puede buscar. Al momento, F-Droid solo sube las descripciones en inglés :(

Instalar aplicaciones

Al tocar cualquier aplicación, vamos a ver su perfil, con información como ícono, descripción, enlaces al sitio y código fuente y versiones disponibles. Desde ahí podemos instalar la aplicación. F-Droid la descarga y luego nos muestra los permisos necesarios para instalarla.

Actualizar aplicaciones

F-Droid actualiza regularmente los repositorios y cuando detecta que hay una actualización disponible, muestra una notificación. Podemos elegir cuáles actualizar y el momento en que lo queremos hacer.

Agregar repositorios

Los repositorios son bases de datos de aplicaciones disponibles en un sitio web. Para agregar un repositorio hay que copiar el enlace y agregarlo en el gestor de repositorios de F-Droid.

Pero como es un proceso con varios pasos, encontramos una más simple que es copiar el enlace, compartirlo en un chat y abrirlo. Android va a detectar que es un repositorio y preguntarnos si lo queremos abrir con F-Droid. No se puede hacer esto desde el navegador porque lo va a abrir directamente en lugar de preguntarnos con qué aplicación lo queremos abrir.

Repositorio pirata

Para probar agregar un repositorio, podés probar compartiendo esta dirección: https://fdroid.partidopirata.com.ar/fdroid/repo

Orbot

Orbot es la versión de Tor para Android. Permite hacer anónima nuestra ubicación física y dependiendo del uso que le demos, es capaz de hacernos anónimas también. Si nos estamos identificando con un servicio que tiene algún dato personal nuestro, no somos anónimas, solo dejan de saber dónde estamos.

Está disponible en F-Droid, habilitando el repositorio de Guardian Project.

Navegación

Orbot viene acompañada de otra aplicación que se llama Orfox, una versión de Firefox ya preconfigurada para conectarse solo a través de Tor. Recomendamos usar este navegador en lugar de otros, como el de fábrica (¡al que no recomendamos para nada!) o Firefox Klar.

Modo VPN

Orbot también tiene un modo VPN, que permite hacer pasar todas las conexiones de Internet que hacen las aplicaciones del celular a través de Tor.

Para eso habilitamos el “Modo VPN” deslizando la opción y luego al pie, donde dice “Torenabled apps”, seleccionamos las que queremos anonimizar.

Signal

Signal[3] es una app libre3 para enviar mensajería cifrada, desarrollada por Open Whisper Systems[4].

Normalmente, Signal se encuentra en Google Play y las que apostatamos de Google nos quedamos sin poder instalarla. Por eso creamos un repositorio de F-Droid P)

[3] https://signal.org/

[4] https://whispersystems.org/

Ya que Signal requiere compartir números de teléfono para poder comunicarse recomendamos usarlo como herramienta de comunicación interna con nuestras colectivas de confianza.

Ventajas

- Ostenta las características de cifrado más modernas
- Cifra todos los mensajes por defecto
- ¡Los grupos también están cifrados!
- ¡Tiene video llamadas!
- Permite enviar SMS (ver desventajas)
- ¡Permite enviar audio, imagen, video y GIFs!
- Si le ponemos contraseña, los mensajes se almacenan cifrados en el celular
- Tiene cliente de escritorio y sincroniza los mensajes
- Tiene mensajes autodestructibles, se eliminan pasado un tiempo de leídos
- No permite hacer capturas de pantalla de los mensajes

Desventajas

- La identidad es nuestro número de teléfono, no vamos a poder hablar con gente a la que no se lo queramos compartir.
- Hay que agendar el número de teléfono tal cual se registró la compañera.
- Antes se podían cifrar los SMS, pero lo desactivaron. Ahora sale un mensaje “Enviar un mensaje SMS inseguro” cuando la otra persona no tiene Signal. Hay una app que se llama Silence. que mantiene la característica de enviar SMS cifrado.

¿Cómo lo instalo?

Si no tenemos o queremos usar Google Play (recomendamos que no), Signal se puede instalar desde F-Droid, agregando el repositorio pirata P)

Configurar Signal

- Abrir la aplicación y registrar el número de teléfono. Para los números de Argentina, recomendamos registrarse con el número internacional: +54 9 NUMERO_DE_AREA TELEFONO_SIN_15. Por ejemplo, para los números de CABA y conurbano, sería: +54 9 11 1234 4567.
- Con el botón redondo del lápiz podemos abrir una conversación nueva.
- Van a salir todos los números de la libreta de contactos, pero no quiere decir que todos sean capaces de recibir mensajes cifrados.
- Al abrir una conversación, el espacio para escribir va a decir "Enviar un mensaje seguro con Signal" o "Enviar un mensaje inseguro con SMS". Así vamos a poder distinguir con quién podemos hablar de forma segura.

Versión de escritorio

Para no tener que estar pendientes del celular, Signal tiene una versión para computadoras de escritorio (o de faldas:)

- Visitá el sitio de Signal para escritorio[5]
- Descargá la versión para tu sistema operativo (las piratas recomendamos GNU/Linux donde es posible que ya esté disponible en sus repositorios específicos, buscando el paquete signal o signal-desktop).
- Seguí los pasos de instalación
- Al abrirla, pide sincronizar con el celular, mostrando un código QR
- En el celular, ir al menú (los tres puntos verticales arriba a la derecha), abrir las Preferencias y buscar Dispositivos enlazados
- Agregar uno nuevo con el botón (+)
- Apuntar al código QR de la pantalla
- Los dos Signal se van a reconocer y sincronizar mensajes, esto puede tomar un rato.

Controversia

Estas son algunas de las contras que le encontramos al uso de Signal. Ninguna app es una panacea que resuelve todos los problemas, sino que tenemos que usarlas sabiendo sus carencias.

- Durante muchos años Signal solo podía instalarse a través de Google Play, lo que nos obligaba a muchas que queremos apostatar de Google a

[5] https://signal.org/download/

dar vueltas para instalarlo. Aun así, requería un servicio de Google llamado Google Cloud Messaging, con lo que tampoco podíamos usarlo. Ahora esto es opcional.

- Si bien Signal es software libre, Open Whisper Systems o al menos algunxs de sus miembrxs han sido abiertamente hostiles con la comunidad del Software Libre, impidiendo que Signal se distribuya por canales comunitarios como F-Droid. Esto sigue sucediendo y nos impidió recomendar Signal por muchos años, ya que teníamos que pedir a las personas que dependan de Google. Por esto hicimos un repositorio de FDroid.
- Signal es un servicio centralizado, es decir que los mensajes se envían a través de servidores bajo control de OWS. Esto no quiere decir que los puedan leer, pero sí implica que si OWS sufre una caída o deja de existir, Signal va a dejar de funcionar. Existen sistemas de mensajería decentralizados, como XMPP, el correo electrónico incluso y hasta P2P que mitigan o superan estos problemas.
- El cliente de escritorio está basado en una plataforma que se llama Electron, a su vez basada en Chrome, que no solo ha demostrado ser pesada sino también bastante insegura, lo que es motivo para desconfiar, aunque no para descartar su uso.
- Se han descubierto problemas de seguridad[6] . Sin embargo, esto es así para cualquier aplicación/software. Lo importante es que el equipo de desarrollo responda rápido y en este caso lo fue. Tenemos que tomar con pinzas cuando alguien nos dice que un programa es totalmente inseguro y que no tenemos que usarlo solo porque se han encontrado problemas de seguridad en el pasado.
- El diseño de las notificaciones de recepción de mensajes[7] (las dos marcas de visto en cada mensaje) permite saber desde qué dispositivo se está leyendo un mensaje que nos enviaron. No nos parece un gran problema en sí, pero hay que tenerlo en cuenta en nuestras prácticas de seguridad, si no queremos que se sepa cuándo estamos en el celular y cuándo en la computadora.

Guía de seguridad y privacidad en Facebook

Ya sabemos que Facebook monetiza todo el contenido que creamos en su plataforma, por eso las piratas decimos que trabajamos para Facebook P),

[6] https://ivan.barreraoro.com.ar/signal-desktop-html-tag-injection/

[7] https://anarc.at/blog/2018-07-27-signal-metadata/

pero además, por la cantidad de datos que le proporcionamos y porque Facebook no los cuida, esta plataforma también puede usarse para que tercerxs y las fuerzas represivas puedan hostigarnos o vigilarnos. No te vamos a decir que cierres tu cuenta (…o sí), pero te vamos a compartir una guía para que tu cuenta sea más segura y puedas mantener un poco mejor la privacidad.

Esto no implica que no se pueda tener acceso a las cosas que publicamos en Facebook, solo dificulta el trabajo.

Primero que nada, entrá a tu cuenta de Facebook y andá a las opciones de configuración.

En la sección **Privacidad**, ajustá las siguientes opciones:

- ¿Quién puede ver las publicaciones que hagas a partir de ahora? -> Amigxs
- ¿Quieres limitar los destinatarios de las publicaciones que compartiste con los amigxs de tus amigxs o que hiciste públicas? -> Sí
- ¿Quién puede enviarte solicitudes de amistad? -> Amigxs de amigxs
- ¿Quién puede ver tu lista de amigxs? -> Solo yo
- ¿Quién puede buscarte con la dirección de correo electrónico que proporcionaste? -> Amigxs
- ¿Quién puede buscarte con el número de teléfono que proporcionaste? -> Amigxs
- ¿Quieres que los motores de búsqueda fuera de Facebook enlacen a tu perfil? -> No
- Desactivá el reconocimiento facial

En la sección **Ubicación**, si tenés activado el historial de ubicaciones y lo usas en tu celular o tablet, hacé lo siguiente:

- Ver historial -> … (son tres puntitos verticales) -> Eliminar todo el historial de ubicaciones
- Configuración -> Desactivar historial -> Desactivar servicios de ubicación En la sección Biografía y etiquetado, ajustá las siguientes opciones:
- ¿Quién puede publicar en tu biografía? -> Amigxs/Yo
- ¿Quién puede ver lo que otros publican en tu biografía? -> Amigxs/Yo
- ¿Quién puede ver las publicaciones en las que te etiquetan en tu biografía? -> Amigxs/Yo
- ¿Quieres revisar las publicaciones en las que te etiquetan antes de que aparezcan en tu biografía? -> Activado

- ¿Quieres revisar las etiquetas que las personas agregan antes de que aparezcan en tu biografía? -> Activado En la sección Seguridad e inicio de sesión, ajustá las siguientes opciones:
- Dónde iniciaste sesión -> Borrá todos los que no conozcas o hayas dejado de usar
- Contraseñas -> Es recomendable usar una frase que sepamos de memoria, pero no le digamos a nadie. 3 o 4 palabras al azar o, mejor, usá un Gestor de contraseñas.
- Desactivá el inicio de sesión con foto
- Activá la Autenticación en dos pasos (es como la tarjeta y el pin, algo que tenemos y algo que sabemos). Podemos usar el celular y contraseña, pero sería un problema si perdemos el celular.
- Contraseñas para aplicaciones -> Si activamos esta opción podemos generar contraseñas específicas para otras Apps en las que nos registramos, en vez de usar el inicio de sesión automático con Facebook. Estas contraseñas luego se pueden revocar, limitando el acceso que tienen las apps a nuestra cuenta.
- Recibir alertas sobre inicios de sesión no reconocidos -> Activar
- Elegir de 3 a 5 amigxs para contactar en caso de que pierdas el acceso a tu cuenta > Depende de si queremos que FB sepa quiénes son, quizás lo mejor sería darles la contraseña en persona.

En la sección **Aplicaciones y sitios web**, hacé lo siguiente:

- Eliminá las que hayas dejado de usar
- Ver y editar las que usemos
- Desactivá los accesos opcionales
- Quién puede verlas -> Solo yo

En la sección **Publicaciones públicas**:

- Cambiá la opción Quién puede seguirme a Amigxs, para que solo ellxs vean tus publicaciones en la sección de Noticias.

Cuando hayas terminado de ajustar estas opciones, podés probar cómo ve otra gente tu perfil, para ver qué queda público, si todavía salen publicaciones en la sección de Noticias, etc.

Tinfoil for Facebook

Tinfoil for Facebook es una aplicación que podemos usar en el celular para navegar en el sitio web móvil de Facebook. Esta aplicación no tiene

acceso a los contactos y otros datos del celular, con lo que minimizamos los datos que nos pueden extraer. Podés descargar la aplicación desde F-Droid.

New Pipe

Dentro de F-Droid, buscar e instalar New Pipe, para conectarse a YouTube sin compartir información y sin ver publicidades.

Escuchar audio

Cuando se abre un video con New Pipe, nos pregunta si lo queremos ver o lo queremos abrir “en segundo plano” o “de fondo”. Esta opción abre el audio como si fuera el reproductor de música del celular, con lo que se puede estar haciendo otra cosa (dentro y fuera del celular) sin dejar de escuchar.

Firefox Klar

Firefox Klar es una versión de Firefox minimalista que desactiva publicidades y otras técnicas de rastreo. No nos hace anónimas, como usar una VPN como Bitmask o Tor, pero reduce los datos que nos extraen y hace más liviana la navegación.

Además, al cerrarlo elimina el historial de navegación para que no quede rastro de lo que hacemos en el celular.

Características

Privacidad automática: Bloquea un amplio rango de rastreadores web comunes sin tener que activar ninguna opción y permite borrar con facilidad el historial (sin contraseñas, sin cookies, sin rastreadores).

Navegación más rápida: Al eliminar los rastreadores y anuncios, las páginas web pueden requerir menos datos y cargarse más rápido.

Desarrollado por Mozilla: Mozilla es el proyecto detrás del navegador Firefox.

¡Tampoco permite sacar capturas de pantalla!

Instalar

Firefox Klar está disponible en F-Droid.

Grabar audio

Audio Recorder es una aplicación instalable desde F-Droid que permite grabar audio:P

Tiene un cálculo de cuánto tiempo podemos grabar en relación al espacio disponible, gráfico de ondas y además convierte a MP3 u otros formatos al terminar de grabar.

Ajustes (Settings)

La opción más interesante es Encoding. Por defecto viene en OGG, un formato libre similar a MP3. Hay varios para elegir, incluyendo MP3.

Bitmask

Bitmask es un cliente de VPN que permite asegurar las conexiones. Las VPN ocultan nuestro uso de Internet a los proveedores de Internet inmediatos, de forma que no pueden saber qué estamos haciendo, solo que estamos usando una VPN.

Ventajas

- Es de confianza, los proveedores como RiseUp[8] tiene un amplio historial de apoyar a activistas de todo el mundo
- Es gratuita
- No permite conexiones a Internet cuando está reconectándose. Si tenemos Bitmask abierta todo el tiempo, solo vamos a acceder a Internet a través de Bitmask. Esto impide que al reconectarnos, una app le gane de mano a Bitmask y se deschave nuestra navegación.

[8] https://riseup.net/

Desventajas

- Puede usar mucha batería
- Puede ser lenta, aunque no mucho más de lo lenta que puede ser una conexión 3G. La lentitud se debe a que al ser gratuita mucha gente la usa y los servidores se saturan, aunque son bastante estables. No nos ha sucedido que Bitmask deje de estar disponible o sea inestable.

Usos recomendados

Recomendamos Bitmask como alternativa a VPNs pagas como IPredator[9], para usos cotidianos de Internet (mensajería, navegación, etc.)

Instalar

Se la puede instalar desde F-Droid.

Al abrirla, nos pide que seleccionemos el proveedor, nosotras recomendamos RiseUp.

Nos podemos registrar, aunque si tenemos una cuenta de RiseUp no la va a aceptar (todavía). También la podemos usar anónimamente.

Cifrar el celular

Aunque el celular esté apagado es posible recuperar lo que tengamos guardado. Para proteger nuestra información es importante que cifremos el celular.

Al cifrarlo, todos los datos ya guardados y los por venir se almacenan en la memoria del celular (tanto la interna como la tarjeta miniSD) de forma que son ilegibles sin tener la contraseña. Cuando el celular esté apagado no se puede acceder a los datos. Esto es importante porque un análisis forense es capaz de recuperar información de la memoria del celular aunque esté bloqueado con contraseña o patrón.

Lo que no impide es que un malware como Pegasus acceda a las datos mientras el celular está encendido.

[9] https://ipredator.se/

Para cifrar el celular, hay que ir a Ajustes > Seguridad > Cifrar dispositivo y seguir los pasos.

Pegasus

Pegasus es el nombre de un malware para dispositivos Android e iOS, desarrollado por una empresa israelí llamada NSO Group y que se rumorea ha sido comprado por el gobierno argentino.

Es utilizado por las agencias de vigilancia para espiar y perseguir activistas políticxs, con uso comprobado en México y otros países. Una vez instalado, es capaz de obtener toda la información del celular y comunicarla inmediatamente, incluso si estamos usando apps de mensajería cifrada, ya que obtiene la información a medida que la tipeamos.

¿Qué puede hacer?

- Keylogging. Esto es, registrar todo lo que escribimos (mensajes, contraseñas, etc.)
- Capturas de pantalla
- Captura de audio en vivo
- Extraer mensajes de aplicaciones de mensajería como Facebook y Whatsapp
- Obtener historial de navegación de navegadores
- Obtener correos electrónicos del cliente nativo de Android
- Extraer contactos y SMS
- Recibir órdenes por SMS

¿Cómo prevenimos la infección?

Según los reportes iniciales del 2016, los intentos de infección comienzan cuando recibimos uno o varios mensajes de texto con un link, que al abrir habilita la descarga. Una vez descargado, es capaz de obtener acceso total al celular (técnica conocida como rooteo) o si falla, de todas formas obtiene acceso a algunos datos y es capaz de "ex-filtrarlos", la jerga de la cibervigilancia para vigilarnos.

Las técnicas pueden variar y todavía no hemos presenciado esto, por lo que la primera recomendación es no abrir links que nos lleguen de números que

no conozcamos o que parezcan sospechosos, especialmente si están acortados con servicios como bit.ly. Van a tratar de hacernos creer que se trata de algo urgente, como el fallecimiento de alguien, o una noticia con título sensacionalista o una amenaza. Cualquier cosa que nos transmita ansiedad y nos haga abrir links sin pensarlo. Estas técnicas se llaman phishing e ingeniería social, seguro que ya la conocés porque nos llegan un montón de mails con links falsos, todo el tiempo.

La única prevención es no abrir los links. Ante la duda, preguntale a alguien más y recordale que no tiene que abrir el link.

Al parecer, los ataques son dirigidos. Si el malware detecta que se instaló en un celular al que no iba dirigido, se auto-destruye después de un tiempo. No se trata de un virus, cuyo objetivo es auto-replicarse. Se trata de un ataque dirigido a personas específicas.

Otras recomendaciones:

- Utilizar una app de SMS libre y segura en lugar de la que viene en el celular. Signal es capaz de recibir los mensajes de texto y guardarlos cifrados en el celular. Silence hace lo mismo que Signal y además permite enviar mensajes cifrados si las otras personas también usan Silence.
- Si revisamos mail en el celular, no usemos el cliente de correo por defecto. K-9 es la alternativa libre.

¿Cómo saber si está instalado? ¿Cómo lo elimino?

Por el momento no hay forma de detectarlo ni eliminarlo, ni siquiera volviendo el dispositivo a la configuración de fábrica.

Referencias

- Pegasus for Android[10]
- Gobierno Espía[11]
- Destapa la vigilancia[12]

[10] https://blog.lookout.com/pegasus-android

[11] http://r3d.mx/2017/06/19/gobierno-espia/

[12] http://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-conmalware-gubernamental/

Gestor de contraseñas

Un gestor de contraseñas es una herramienta que nos permite generar y guardar contraseñas en una base de datos cifrada. De esta forma, no tendremos que recordar infinidad de contraseñas y evitaremos usar la misma para más de un servicio, que es una práctica desaconsejada. La base de datos se cifra con una contraseña maestra que sí tendremos que memorizar.

Hay varias opciones, pero las piratas recomendamos estas:

KeePassXC

KeePassXC es una herramienta libre con la que podemos crear una base de datos cifrada donde guardaremos las contraseñas. Está disponible para todos los sistemas operativos y tiene la opción de autotipado, para no tener que andar copipegando las contraseñas todo el tiempo. Se puede descargar desde su sitio web https://keepassxc.org.

KeePassXD

KeePassXD es una implementación libre para Android del gestor de contraseñas KeePass. Se puede descargar desde F-Droid.

Recomendaciones para crear la contraseña maestra

En general, se recomienda que para crear esta contraseña (que cifra la base de datos) elijamos una serie de palabras al azar que sea fácil de recordar. Lo importante es no elegir una frase famosa de algún libro, poema o canción, ni palabras relacionadas con datos personales. Por ejemplo, no sería recomendable tener una frase que sea: fulanitoOctubre1992, donde 1992 y octubre sean nuestro año y mes de nacimiento.

Para que la contraseña maestra sea más segura, se recomienda utilizar mayúsculas y minúsculas, números y signos de puntuación.

Remoción de Metadatos de Imágenes con Scrambled EXIF

Ejemplos de usos

Muchas veces queremos o necesitamos compartir imágenes rápidamente, por ejemplo para que circule por redes sociales para denunciar represión, en cuyo caso la opción preferida sería tomar una foto con la cámara del celular para luego compartirla por chat. Aunque también puede pasar que estemos conociendo a alguien por chat y querramos mandar una foto privada sin que se sepa nuestra ubicación… En cualquiera de los casos, si no sacamos los metadatos antes, estaremos enviando también información acerca de la ubicación, hora, fecha, dispositivo desde el que tomamos la imágen, etc… Esto podría volvernos vulnerables en caso de rastreo.

Qué es

Scrambled Exif es una aplicación para celulares (Android, Lineage u otras versiones libres…) que nos permite quitar de manera rápida los metadatos de nuestras imágenes e inmediatamente compartirlos mediante cualquier otra aplicación del teléfono (Telegram, mensaje multimedia, etc.)

Dónde descargarla

Podés descargarla del repositorio de F-Droid.

Cómo usarla

Elegís la foto que querés compartir y esta función (compartir). Entre las opciones para hacerlo, tiene que aparecer la de Scrambled EXIF. Al seleccionarla, verás la leyenda avisándote que la aplicación está removiendo los metadatos. Luego te llevará a la opción de compartir la nueva imagen sin metadatos entre tus aplicaciones disponibles. Seleccionás una y ya estarás compartiendo la imagen sin metadata.

Bienvenidxs al fediverso

Como parte de una estrategia para empezar a habitar redes sociales libres a la que venimos llamando Apostasía de Redes Sociales, nos planteamos empezar a difundir noticias de medios alternativos, de forma que a medida que vayamos emigrando, podamos encontrarnos con información que de otra forma quedaría acallada por el alcance que pueden comprar los medios hegemónicos en las redes hegemónicas.

Desarrollamos una herramienta para publicar automáticamente lo que estén publicando en sus sitios, es decir que no habría esfuerzos duplicados P) ¡Por el momento es capaz de publicar en Mastodon y Telegram!

Algunos canales que ya están funcionando:

- https://todon.nl/@anred
- https://todon.nl/@rnma
- https://todon.nl/@radiolanegra
- https://todon.nl/@radiodelaazotea
- https://t.me/CanalDeNoticiasDeANFenEspanol

FACEBOOK

Parte hombre. Parte máquina. Policía del todo. El futuro de las fuerzas de seguridad.