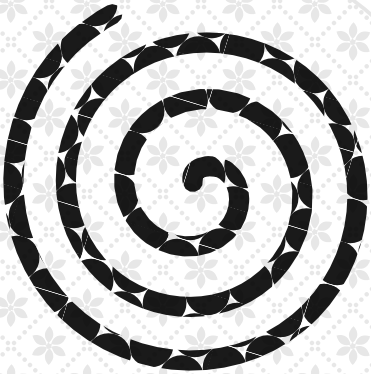
Grog & Tor



Guía de Autodefensa Digital

PARTIDO
INTERDIMENSIONAL
PIRATA

¿Qué es la autodefensa digital?

Vivimos dejando rastros de nuestra actividad en la red. Contactos, ubicaciones, fotos. Pero ¿dónde viven estos datos?, ¿quiénes tienen acceso realmente?, ¿qué riesgos tienen asociados?

La autodefensa digital es el conjunto de hábitos y herramientas que usamos para proteger nuestra información personal en internet y a nuestros dispositivos de amenazas como virus, robos de datos o accesos no autorizados. Es como ponerle una cerradura a tu casa pero en el mundo digital: cuidás tus contraseñas, evitás caer en estafas, usás conexiones seguras y controlás quién ve tus datos.

Algo a tener en cuenta es que no existe nada completamente seguro, por eso conviene adaptar las medidas que se tomen al contexto en el que se está. No serán las mismas para una periodista que necesita comunicarse con una fuente que para une amigue mensajeando a otre sobre la noche anterior o un abogado hablando con su cliente.

Desde el Partido Interdimensional Pirata venimos dando talleres de concientización en esta temática para diversos colectivos, universidades y activistas. Si vos o tu espacio comparten estas inquietudes, podés contactarnos :)

Mensajería

Marquitos

Hay muchas apps que podemos usar para comunicarnos con nuestras conocidas y no todas ofrecen lo mismo en términos de privacidad y seguridad.

Whatsapp: la de Marquitos. Si bien nos ofrece cifrado extremo a extremo (E2E) en los chats, los metadatos (a quién le hablo, cuándo, etc.) no lo están y Meta junta esta información para venderla. Además, al ser de código cerrado, no conocemos el verdadero funcionamiento de la app y es más difícil saber si posee vulnerabilidades o "puertas traseras". También tiene como desventaja que comparte nuestro número con cualquier persona a la que le hablemos. Este dato puede ser usado para doxearnos.

Si se desea seguir usándola, hay cosas que podemos hacer para estar más seguras:

- Activar la verificación en dos pasos. Esto agrega un PIN para poder ingresar a la cuenta, evitando que nos la roben clonandonos el número.

- Desactivar la copia de seguridad en Google. Si bien es cómodo que los mensajes se guarden, nos expone a que puedan leerlos si nos roban la cuenta de Google.

- Si se mantiene la copia de seguridad, activar el cifrado de la misma.

Telegram: antes se consideraba más segura, pero ya NO la recomendamos. Posee cifrado E2E únicamente en los "chats secretos", que por defecto no son usados. La empresa tiene acceso a todos los demás chats y metadatos y ya ha compartido información con fuerzas de seguridad.

Signal: está cifrada extremo a extremo, es de código mayoritariamente abierto y está enfocada en privacidad y seguridad. No recopila datos personales.
También existe Molly, una versión completamente abierta y con más opciones de seguridad. Se puede descargar en https://molly.im/fdroid/

Cómo último tip, estas apps cuentan con mensajes temporales, para que ningún mensaje con tonos sospechosos sea leído por ojos sin humor ;)

Redes (A)sociales

Recordemos que cuando habitamos las redes sociales estamos en una plataforma de empresas privadas con sus propios intereses. Centralizan el control de la información, explotan y trafican datos personales para su beneficio comercial y político. ¡Nada es privado!

Un par de consejillos si seguimos usando las redes privativas:

- Revisar las configuraciones de privacidad de la plataforma.
- Ser conscientes de lo que publicamos y compartimos.
- Podemos poner un mail/número que no sea fácilmente asociado a una misma.

Ahora, si queremos alternativas... existe lo que se llama el Fediverso. Como introducción muy básica podemos decir que son varias redes sociales que se pueden comunicar entre ellas. O sea, imagínate que desde Instagram pudieras ver un tweet. Además, los datos están en instancias manejadas por comunidades, en vez de en manos de las multinacionales. Como el software para correr estas instancias es libre, las comunidades pueden poner las reglas que elijan.

Para crearte una cuenta, tenés que elegir una instancia, la que mejor te caiga. Algunas de América Latina que recomendamos son:

rebel.ar
mastodon.uy
fedi.lat
mast.lat

Más alternativas libres

Navegadores: para navegar de manera más privada y segura, podemos usar Firefox o LibreWolf. También está Tor, con el cual podemos acceder a sitios sin revelar nuestra IP y evitando que nuestro proveedor de Internet vea a cuáles accedimos.

Buscadores: DuckDuckGo, Startpage o SearX. SearX es un metabuscador: recompila resultados de muchos motores de búsqueda y no tiene un servidor centralizado sino que está distribuido en muchas instancias. Podemos ver una lista de servidores en searx.space

Mapas: OpenStreetMap en vez de Google Maps. Si nos bajamos la app OsmAnd también podemos descargar los mapas y usarla sin conexión.

Mail: Disroot, nacida en 2015, se trata de una comunidad autogestiva que opera por fuera del paradigma monopólico y de vigilancia masiva. Además de mail, brinda alternativas para compartir documentos, excels, calendarios, etc.

Correos descartables: si necesitamos un mail para registrarnos en algún sitio podemos usar los servicios de temp-mail.org, 10minutemail.com o guerrillamail.com. Al usarlo perderemos la posibilidad de recuperar la cuenta a través de email o recibir códigos de un solo uso. También tenemos que anotar la dirección, que no suelen ser amigables. No hay garantías de privacidad en su uso: cualquier dato que recibamos o enviemos puede ser visto por terceros.

Seguridad

Limpieza de metadatos: los metadatos son etiquetas que detallan la fecha, ubicación, autor o las características de un archivo o mensaje. Tenemos que tenerlos presentes a la hora de subir cualquier cosa (como fotos) a Internet. Como herramientas para revisar y modificar metadatos tenemos ExifTool para compu y ScrambledExif para celu.

Phishing[1]: no importa cuánto sepas o creas saber de seguridad, todas podemos estar distraídas, apuradas o cansadas. Basta con una vez no dudar de un email, mensaje o link para caer. Algunas útiles son:

- VirusTotal: podemos subir archivos si sospechamos que son malware
- UrlVoid: para analizar enlaces antes de abrirlos

[1] Ataques diseñados para engañar y conseguir que la usaria facilite sus contraseñas o que instale malware.

Podés descargar nuestro recursero con muchísima data acá!

Y podés contactarnos por acá

partidopirata.com.ar

@PartidoInterdimensionalPirata

@pip@todon.nl

contacto@partidopirata.com.ar