4.

REDUCE TUS RASTROS

El navegador de tu móvil almacena mucha información sobre ti –tu ubicación, qué buscas, qué sitios web utilizas– y puede entregar estos datos a otras personas y entidades.

Los móviles, tablets y ordenadores suelen venir con navegadores instalados por defecto que no tienen como prioridad resguardar nuestra privacidad. Pero, puedes **descargar y utilizar un navegador** que mantiene tu actividad web más **privada por defecto**, protegiéndote contra rastreadores.

Y para aumentar más aún tu privacidad, puedes instalar elementos adicionales llamados "addons y extensiones" (pequeños programas fáciles de instalar en tu navegador que pueden **mejorar tu privacidad en línea**).

5.

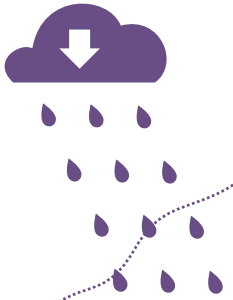
DESETIQUÉTATE A TI Y A OTRAS PERSONAS

¿Alguna vez has contribuido a la acumulación de datos sobre una persona cercana al etiquetarla en imágenes y publicaciones? Aligera su carga de datos (y tu cargo de conciencia social) **desetiquetando a tus amistades** de tantas fotos y publicaciones como puedas.

¡Pasa la voz! Anima a tu círculo cercano (amistades, familiares, personas de tu trabajo) a retomar el control sobre estos datos volátiles. Si nos unimos para gobernar nuestros rastros digitales, podemos ayudarnos mejor a desintoxicar nuestras vidas digitales.

Para bloquear anuncios espía y rastreadores invisibles, instala uBlock Origin (para Chrome, Safari, y Firefox) o Privacy Badger (para Chrome, Firefox y Opera).

Para realizar conexiones más seguras con páginas web cuando sea posible, instala HTTPS Everywhere: una extensión de navegador que asegura que la comunicación (los datos en tránsito que envías y recibes por internet) con las páginas web esté cifrada y protegida (siempre y cuando tengan certificado HTTP/SSL disponible). Si utilizas Safari y quieres optar por una funcionalidad similar, configura tu navegador para usar por defecto un buscador que no sea Google, como DuckDuckGo, que intenta incluir en sus resultados enlaces más seguros a las páginas web (las que empezian con HTTPS son conexiones cifradas).



DATA DETOX KIT

TOMA EL CONTROL DE LOS DATOS DE TU SMARTPHONE

mejora tu privacidad en línea

Si nos ponemos a pensar qué revelan tus datos sobre tu vida, puede no parecer gran cosa: ¿a quién le importa si me gusta Isabel Pantoja, si compro más zapatos de los que necesito o empiezo a planear mis vacaciones con un año de antelación?

El problema está en qué pasa con tus datos. Con el paso del tiempo, salen a la luz patrones digitales sobre nuestra intimidad: nuestros hábitos, movimientos, relaciones, preferencias, creencias y secretos se exponen ante quienes analizan y sacan provecho a nuestros datos como las empresas y las agencias de datos.

Poco a poco, siguiendo este Data Detox, vas a descubrir cómo y por qué todo ésto está pasando. Podrás dar pasos prácticos para tomar el control sobre tus rastros digitales en internet.

¡Empezamos!

Un proyecto de
TACTICAL TECH

Con el apoyo de
Firefox

datadetoxkit.org
#datadetox

1.

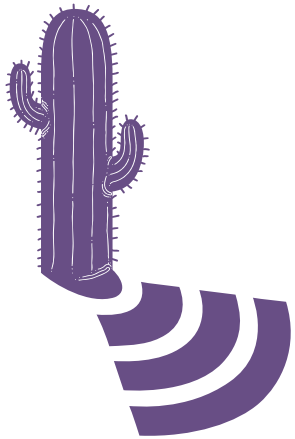
CAMBIA EL NOMBRE DE TU MÓVIL

A lo mejor, en algún momento, le "pusiste un nombre" a tu móvil para configurar el Wi-Fi y/o Bluetooth –O puede ser que se asignara automáticamente un nombre en la configuración.

Este nombre, por ejemplo "El móvil de Isabel" está visible para las personas que administran las redes Wi-Fi a las que te vas conectando y, si tienes habilitado el Bluetooth, todas las personas a tu alrededor con el Bluetooth habilitado pueden verte también.

No te pondrías a decir en voz alta tu nombre al entrar en un café, restaurante o aeropuerto. Tampoco tienes que hacerlo con tu móvil.

Puedes **cambiar el nombre de tu móvil** a algo que te identifique menos, sin perder ese toque personal . Aprende cómo hacerlo:



iPhone:
Ajustes → General → Acerca de → Cambia el nombre del dispositivo

Android:
Cambia el nombre de Wi-Fi:
Ajustes → Wi-Fi → Menú → Avanzado / Mas herramientas → Wi-Fi Directo→ Cambiar nombre de dispositivo
Cambia el nombre de Bluetooth:
Ajustes → Bluetooth → Habilita el Bluetooth si está apagado → Menú → Nombre del dispositivo → Desactivar Bluetooth

2.

ELIMINA TUS HUELLAS DE UBICACIÓN

Aunque puede parecer que tus datos de ubicación solo sean pedazos aleatorios de información, cuando se juntan y analizan, pueden revelar **detalles importantes** sobre ti, tus hábitos, dónde vives y trabajas, dónde te gusta reunirte con tu círculo social... Por eso muchas empresas y agencias de datos quieren conseguir tus datos.

Puedes **revisar tus permisos de apps y deshabilitar los servicios de localización y ubicación**. Identifica las apps que realmente no necesitan tener esta información para funcionar (¿esa app de juego tiene que saber dónde estoy?) y las que, aunque lo necesiten, no quieres que lo tengan:

Android:
Ajustes → Apps → Gestiona, para cada app, los accesos a tu ubicación.

iPhone:
Ajustes → Privacidad → Localización → Gestiona, para cada aplicativo, los accesos a tu ubicación.

3.

ORGANIZA TUS APLICACIONES

Tus apps (plataformas de redes sociales, pronóstico del tiempo, juegos, etc.) quieren tus datos... y pueden estar recolectando bastante información sobre ti.

Deshacerte de aquellas apps que ni utilizas puede ser un impulso para desintoxicar tu vida digital.

Ademas, una limpieza puede liberar espacio en tu móvil, bajar el consumo de tus datos móviles y hacer que te dure más la batería. Hasta puede mejorar el funcionamiento general de tu móvil según las aplicaciones que elimines.

Android:
Ajustes → Apps → Selecciona la aplicación que quieres desinstalar → Desinstalar

iPhone:
Deja presionado el dedo encima del icono de la aplicación hasta que empiece a moverse y aparezca una "x" en la esquina superior izquierda.
Para eliminar una aplicación, pulsa la "x".
Para regresar al modo "normal", pulsa el botón de inicio.