HERRAMIENTAS Y TIPS PARA ESTAR MÁS SEGURAS

La lucha de las mujeres para encontrar espacios seguros en línea sigue vigente, debido al actual abordaje fallido por parte de los gobiernos, empresas y otros proveedores de servicios web. ¿Cómo podemos, como mujeres, desarrollar niveles de confianza y una mayor sensación de seguridad cuando habitamos espacios digitales, a través de la creación de contenido, relacionamiento con los demás y expresión de nuestras opiniones?

Como TEDIC creamos una serie de ***recomendaciones*** para una navegación y apropiación de las tecnologías más segura y ágil. Aquí van.

Cubre tus pasos

¿Sabías que al habitar espacios en línea, a medida de que realizamos una búsqueda, damos un like, navegamos de una página a otra, enviamos un mensaje o una foto, se crean huellas digitales y rastros de tu comportamiento? Estos rastros dan lugar a la compilación de información que permite contar una historia detallada de tu perfil y actividades en línea.

Esta información también se conoce como sombra digital, la cual contiene datos que generamos de manera consciente (contenido que creamos y compartimos), así como también datos que se crean sin nuestro consentimiento como resultado de las acciones que realizamos en línea. A estos datos invisibles los llamados metadatos. Los metadatos son conocidos como los datos de los datos y son generados de manera pasiva, como por ejemplo, nuestro historial de navegación y nuestra dirección IP (identificador específico y único de nuestros dispositivos).

Ejemplos de los metadatos que creamos son nuestro nombre, ubicación, marca de dispositivo, duración de llamadas, información sobre los sitios visitados y otros. Con esa información, muchas compañías de servicios en línea pueden determinar tus patrones y hábitos de navegación de manera no consentida, con el fin de determinar qué clase de información poner a tu vista, en especial propaganda y anuncios de productos determinados para promover la compra de los mismos.

Por ende, los datos que vamos generando a través de nuestras interacciones en línea pueden ser vendidos a estas compañías, e incluso al gobierno, para así potencialmente usarlos para fines de control, opresión y daño.

Es difícil saber cómo nuestros datos están siendo usados, y por quiénes, pero existen varias estrategias recomendadas para lograr una navegación que proteja nuestros datos y privacidad, y te mencionamos algunas a continuación:

Auto-doxeo

Una estrategia para entender e identificar qué clase de datos e información se puede determinar desde nuestros hábitos y acciones en línea es el auto-doxeo. El auto-doxeo nos ayuda a entender mejor lo que está disponible sobre nuestra identidad, para así poder tomar medidas de prevención, remover e incluso dificultar la disponibilidad de esos datos.

Para realizar el auto-doxeo, podemos ver cómo nuestros datos están siendo rastreados a través de herramientas para ellos. Por ejemplo, están los de ***Me and My Shadow*** (Yo y mi sombra), quienes proveen una plataforma específica para entender cómo nuestros datos están siendo rastreados por ***geolocalización*** y por tus hábitos de ***navegación***.

Medidas para empoderarnos sobre los metadatos

Es importante preguntarnos lo siguiente a la hora de estar conectados y compartir o generar contenido:

Lo que comparto en las redes ¿es algo muy personal o trata de algo más bien público?

Cuando comparto contenido, en especial fotos etiquetando a otras personas, ¿quién tiene acceso a ello? Muchas veces esto significa exponer información o datos sobre otras personas, no solamente sobre tu identidad y tu vida.

Tener una respuesta realista a estas cuestiones nos ayuda a dimensionar qué tan disponible dejamos a terceros la información que pueda ayudar a vulnerar nuestra identidad y a exponerla sin nuestro consentimiento, así como también a entender qué tan fácil o difícil sería que estemos siendo víctimas de vigilancia, robo de identidad, y otras situaciones de ataque.

Para reducir el grado de acceso que terceros puedan tener a tus contenidos, datos y metadatos, puedes utilizar las siguientes medidas y herramientas para disminuir tu sombra digital:

● Asegurate de que, al visitar sitios, estos estén encriptados. Esto quiere decir que el enlace del sitio que visitas tiene que empezar con https://(fijate que no sea sólo http://). La “s” dentro de https significa: seguro.

● Para ofuscar tu dirección de IP (el identificador único de tu dispositivo), puedes utilizar el navegador de TOR, el cual facilita que puedas navegar de manera más anónima y que tu navegación sea más difícil de rastrear.

● Usar contraseñas distintas y fuertes para cada perfil que tenemos, o servicio que usamos (más detalles en la sección sobre Contraseñas en esta guía).

● Al compartir contenido con detalles personales acerca de tu vida e identidad, apunta a hacerlo a través de perfiles privados, con la configuración de seguridad y privacidad apropiada para que solamente tus contactos seleccionados puedan acceder a ese contenido.

● A la hora de compartir contenido, en especial imágenes sobre eventos públicos, es importante no examinar si pone en riesgo la identidad de las personas que aparecen en esas imágenes. Para evitar el riesgo de exposición de terceras personas, puedes utilizar algunas apps tales como ***Signal*** y ***ObscuraCam***, la cual están disponible en el PlayStore y en F-Droid.

● Apaga el rastreador GPS del celular o cámara, así como también limita el acceso a tu ubicación a otras aplicaciones dentro de tu dispositivo.

● Para quitar metadatos antes de compartir archivos, puedes utilizar aplicaciones como SendReduced, la cual está disponible en el PlayStore y en F-Droid.

● Para compartir ***archivos de forma segura*** te recomendamos que utilices share risep.

Mantente anónima

Muchos tipos de ataques se basan en vulnerar nuestras identidades a través de la difusión de nuestros datos personales. ***El anonimato es una manera de acceder a sitios y espacios***, manteniendo nuestra identidad y cualquier otro dato que nos pueda identificar oculto.

En muchos contextos y espacios, el anonimato se presenta como una buena opción, en especial si se visitan espacios o plataformas digitales en las cuales las otras personas con las que se interactúan no son de confianza. Además, el anonimato evita que nos expongamos a mayores riesgos de ataques o violencia que vulneren nuestra identidad. Cuando realizamos acciones en línea que son de índole privado o sensible, es conveniente hacerlo de una manera anónima para no tener nuestra identidad expuesta y para evitar que esas acciones se sumen a los datos que existen sobre nuestros hábitos de navegación.

Aunque Internet es abierta, como habíamos mencionado anteriormente, no es neutral. Esto quiere decir que, aunque reconozca la información dentro de ella de una manera similar, existen actores cuyo interés es controlar el tráfico y la manera en la cual recibimos información y habitamos estos espacios.

El anonimato hace posible que nuestros derechos a la privacidad, libertad de expresión y acceso a la información sean ejercidos de mayor manera en Internet y que no seamos víctimas del control que otros quieren ejercer sobre cómo quieren que recibamos información. Necesitamos muchas veces del anonimato para poder expresarnos sin temer a los ataques o situaciones de violencia y vulnerabilidad, o que estos actores nos identifiquen para luego ejercer vigilancia y uso de datos sin consentimiento.

Algunas medidas para navegar de manera anónima son:

● Utiliza el navegador Tor para hacer que la detección de tu IP y el rastreo de tu navegación sea más difícil.

● Puedes también utilizar los otros navegadores como Mozilla, Opera y Google Chrome en modo privado. Este tipo de navegación también es una medida de protección contra rastreos, ya que no guarda las búsquedas realizadas, páginas visitadas, archivos temporales y cookies (datos que almacenan los sitios web en tu navegador con la finalidad de facilitar la navegación a la par de identificar tu visita al sitio). A pesar de esto, es importante notar que esto no nos hace completamente anónimas en Internet, ya que el proveedor de servicios de Internet aún puede tener acceso a las páginas visitadas.

Comunicándonos a través de canales seguros y encriptados

Contar con espacios de comunicación segura, en los que la información que pasamos de un punto a otro no sea interceptada ni apropiada por terceros, es sumamente importante a la hora de construir entornos de comunicación digitales que no nos vulneren ni expongan sin consentimiento. Una medida recomendada para una comunicación segura es el uso de aplicaciones y canales encriptados. La encriptación es un mecanismo de código que utiliza las matemáticas para así cifrar el contenido de un mensaje, con el fin de esconderlo de terceros y de que sea solamente descifrado o visible por el destinatario del mensaje, a través de una contraseña o clave de encriptación.

El tipo específico de encriptado que utilizan los canales de comunicación es conocido como de extremo a extremo, o E2E. Esto crea un cifrado que dificulta la intercepción y vista del contenido del mensaje por intermediarios y/o terceros, asegurando que la comunicación efectivamente se realice entre el emisor y el receptor de manera más segura.

Plataformas de comunicación como WhatsApp poseen este tipo de cifrado de extremo a extremo, pero por cuestiones de otras mecánicas, es muy fácil que la privacidad y seguridad se vean en riesgo.

En cuestiones de comunicación segura, la aplicación de ***Signal*** se presenta como una de las más completas. Signal es una plataforma de mensajería que permite configurar la duración de los mensajes una vez que fueron leídos para autodestruirse después, pueden bloquear la opción de guardar una captura de pantalla, entre otros. Esto ayuda a limitar la cantidad de información que puede quedar expuesta en caso de que el dispositivo en donde esté alojada la aplicación sea robado o perdido.

También cifra tu disco duro y computadora: Tu información privada u organizacional es muy importante y si cae en manos no deseadas pueden ocurrir muchas cosas feas: filtrado de información personal o íntima, exposición de datos de tu organización, chantajes, campañas de desprestigio, etc.. Para todas esas situaciones es que existe la técnica criptográfica de cifrado de la información: puedes cifrar todo el disco duro de tu dispositivo (o almacenamiento), o parte de él (una carpeta), también puedes cifrar un disco externo, un pendrive o incluso una carpeta «en la nube». Desde TEDIC hemos elaborado esta guía (***https://www.tedic.org/como-proteger-la-privacidad-de-tu-informacion/***).

Creando contraseñas fuertes y seguras

Muchos servicios, plataformas y aplicaciones requieren una contraseña para ser utilizadas. Las contraseñas tienen el rol de servir de obstáculo a terceros a la hora de tener acceso a perfiles o a información y nos permiten realizar acciones únicas como: inicio de sesión, comprobación de cambios y actualizaciones, y otros que son claves para la seguridad digital. En TEDIC hemos elaborado una guía básica y preguntas frecuentes para crear contraseñas seguras y difíciles de adivinar o interceptar por terceros, te recomendamos que crees y tengas contraseñas que:

- **Sean largas:** Cuanto más corta es una contraseña, es más fácil para una computadora u otra persona adivinarla. Te recomendamos utilizar una contraseña larga para justamente dificultar el acceso a terceros, ya que se volvería mucho más compleja de adivinarla. Puedes usar una frase que contenga varias palabras, por ejemplo.

- **Sean complicadas:** Aparte de ser larga, la complejidad de las contraseñas también dificulta que se puedan descifrar con facilidad. Te recomendamos incluir mayúsculas, minúsculas, números y símbolos en tu contraseña, como por ejemplo: m3gUst4L4p1Zz4siN4nch0AsYc0ny0gHurt (me gusta la pizza sin anchoas y con yoghurt).

- **Sean impersonales:** Recomendamos que elijas algo que no se relacione contigo de manera personal. Por ejemplo, evita proveer información como nombres, fechas de nacimiento, números telefónicos, ni nada similar que alguien pueda llegar a encontrar sobre vos. Además, en plataformas que proveen preguntas de seguridad a la hora de olvidar tu contraseña, puedes también dar respuestas falsas. Así evitas que otros busquen tu información en línea y te roben la identidad.

- **Sean secretas:** Nunca compartas tu contraseña a otras personas, a no ser que lo consideres extremadamente necesario. En caso de tener que compartir una contraseña, te recomendamos cambiarla a una temporal y compartir esa, y luego cambiarla de vuelta a la que tenías anteriormente una vez que ya otras personas no deban tener acceso a tu cuenta. Aparte de cuestiones técnicas, también estate atenta a tu alrededor: presta atención a que nadie esté leyendo detrás tuyo cuando la estés tipeando.

- **Sean prácticas:** Ya que escribir contraseñas largas y complejas hace difícil que recordemos cada

contraseña que tengamos, te recomendamos utilizar un gestor de contraseña para guardarlas en un lugar seguro, a diferencia de guardarlas solamente en un archivo para ayuda memoria. Gestores seguros de contraseña como KeePassXC ayudan a que guardes tus contraseñas en un mismo lugar de manera segura.

- **Sean únicas:** Para una mayor seguridad, es recomendable no usar la misma contraseña para más de una cuenta o servicio que estés utilizando. Esto es porque, en caso de utilizar la misma contraseña en otros espacios y que sea adivinada por terceros, el acceso a otras cuentas o dispositivos será mucho más fácil.

- **Sean nuevas:** Es recomendable también realizar un cambio y actualización de contraseñas periódicamente. Esto se debe a que, cuanto más tiempo mantenemos las mismas contraseñas, más oportunidades tendrán terceros para adivinarla. Recomendamos que realices estos cambios cada 3 meses aproximadamente, o cada un año a más tardar. Puedes luego guardar estos cambios en el gestor de contraseñas para evitar el olvido de la nueva contraseña.

Muchas veces, incluso, si hay una brecha de seguridad y terceros consiguen el acceso a tu contraseña, seguirán utilizándola hasta que la llegues a cambiar. Te recomendamos visitar el sitio del investigador de seguridad ***Troy Hunt Have I Been Pwned?*** (Have I Been Password Owned?) para identificar si algunas de tus contraseñas han sido vulneradas o filtradas.

Lecturas para profundizar

- Manual de seguridad holística por Tactical Tech.
- Proyecto Security in a Box
- Checklist de seguridad por Protege.la y SocialTic.
- Cyberwomen.

BIO.

TEDIC

Es una organización sin fines de lucro creada en Paraguay por personas con trayectorias en diferentes disciplinas, que promociona y defiende los derechos digitales en América Latina. Buscamos el cumplimiento pleno de los derechos civiles en Internet. Investigamos, difundimos información y capacitamos en temas de privacidad, datos personales, ciberseguridad: cuidados digitales, libertad de expresión y manifestación, neutralidad en la red, derechos de autor, inteligencia artificial, biometría, entre otros, con un enfoque transversal de género.