Manual de Seguridad digital para activistas, defensoras, periodistas y organizaciones feministas

Octubre 2022

Cultivando Género A.C.

Compañeras y compañeres activistas, defensoras, periodistas y organizaciones feministas, en los últimos días a raíz de la información que se ha dado a conocer de las filtraciones de la SEDENA y Guacamaya Leaks, con relación a las revelaciones del espionaje a personas defensoras y periodistas usando Pegasus en #EjércitoEspía, es necesario tener en cuenta tu seguridad digital como una prioridad que incluya estrategias para el autocuidado.

Por lo que desde Cultivando Género hemos elaborado este Manual con el propósito de compartir información y recursos prácticos que distintas compañeras y colectivos han ido desarrollando a lo largo del tiempo frente a los embates de vulnerar su seguridad por el trabajo de disidencia que realizan.

La seguridad digital depende de la creación consciente de redes de apoyo, para hacerles saber cómo nos sentimos y las estrategias que podemos implementar, es importante que tengamos presente que la seguridad digital depende de muchos factores, no sólo de una contraseña segura o un buen antivirus.

Recuerda: En la red no navegas sola

¿Qué es la Seguridad Digital?

La seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger infraestructura computacional (activos de la organización) y todo lo relacionado con esta, así como a los propios usuarios de la misma.

Definición extraída de
https://guiasbib.upo.es/ciberseguridad/definicion#:~:text=La%20seguridad%20inform%C3%A1tica%2C%20tambi%C3%A9n%20conocida,seguros%20y%20tecnolog%C3%ADas%20que%20pueden

¿Por qué es importante?

La seguridad digital es importante porque abarca todo lo que tiene que ver con la protección de tus datos confidenciales, tu información biométrica, personal, software, compras y banca en línea, los sistemas de informática gubernamental y otros detalles de la vida moderna que dependen de las computadoras y otros dispositivos inteligentes.

La Seguridad digital no es un tema que se resuelva comprando el antivirus más caro o instalando la aplicación más sofisticada para enviar mensajes, desde Cultivando Género apostamos por trabajar la seguridad desde tres capas pensando en la seguridad desde las medidas personales y colectivas.

Imagina que la seguridad digital es un pastel, cada capa tiene un papel importante en el pastel, no solo da forma y mantiene la cobertura o el glaseado en su lugar, sino que tiene un propósito que abona a la seguridad pensada de forma integral y no solo desde el yo.

Yo

La capa de Yo hace referencia a lo que puedo hacer de forma individual para mi seguridad.

-*Como me cuido yo*, qué acciones y que herramientas puedo utilizar para cuidar mi seguridad digital: tener contraseñas seguras, verificación de dos pasos, entre muchas más.

-*Hago caso a mi instinto*, la persuasión o ese poder de convencimiento (para sonar bien profesionales se llama ingeniería social) es lo que usan las personas que quieren cometer un delito o son agresores, te van convenciendo, te hacen sentir miedo, que

dudes de ti y de lo que has hecho, se hacen pasar por amistades, alguien que conoces para que caigas en el engaño, la estafa.

- *¿Lo necesito?*, ¿cuándo descargo una nueva aplicación, aceptamos todos los permisos que nos aparecen? pero ¿en verdad necesito esa app?, ¿en verdad necesito darle permiso a la aplicación para que entre a mis fotos o a mi directorio?

Para comenzar te invitamos a responder el siguiente cuestionario de seguridad que encontrarás en *Nos acompañamos online, guía para adolescentes* que publicamos en marzo del 2022.

¿Qué onda con tu seguridad?

Antes que pase cualquier cosa, porfis contesta las siguientes preguntas. Vamos a ver qué tanta seguridad tienes:

1.- Tus contraseñas de redes sociales, correo electrónico ¿tienen letras mayúsculas, minúsculas, números y signos?

A) Sí

B) No

2.- ¿Tienes la verificación de dos pasos en WhatsApp?

A) Sí

B) No

3.- ¿Tienes respaldo de la información que tienes en tu celular?

A) Sí

B) No

4.- ¿Tienes contraseñas diferentes para cada red social, plataforma, cuenta?

A) Sí

B) No

5.- Si te mandan un link que no conoces o qué te parece sospechoso ¿lo ignoras y reportas?

A) Sí

B) No

Ahora vamos a sumar

A=2

B=1

Tu resultado: _____

Vamos a revisar:

10 y 8 puntos: Súper bien, tu seguridad digital es muy buena.

7 y 5 puntos: Vamos bien, pero debes revisar que te hace falta para tener una seguridad digital de 100%

4 puntos o menos: Aquí algo no anda bien, pero no te preocupes te invito a que sigas leyendo esta guía.

Después de contestar el cuestionario vamos a ver qué nos dice el INEGI, en el 2020 quienes usaban Internet utilizaron como medida de seguridad:

94.4% contraseña, huella, clave, patrón.

30.4% instalar o actualizar antivirus, cortafuegos y antiespías.

9.7% cambiar periódicamente las contraseñas.

7.5% bloquear ventanas emergentes del navegador.

6.8% no abrir archivos que envían personas desconocidas.

Te recomendamos:

Utiliza un cortafuegos. Los sistemas operativos como Windows y macOS tienen firewalls integrados. Se trata de software diseñado para crear barreras entre tu información y cualquiera que desee acceder a ella. Este tipo de programas evitan los accesos no autorizados a tu computadora y te avisan de cualquier intento de ingreso.

Utiliza contraseñas complejas. El uso de contraseñas seguras es la forma más importante para evitar intrusiones en tus cuentas o dispositivos. Utiliza claves que tengan más de 8 caracteres y que incluyan una combinación de letras mayúsculas, minúsculas, números y símbolos especiales (caracteres como @, #, $, entre otros). Evita palabras o datos que puedan estar relacionados contigo e intenta no repetir tus contraseñas en todos los sitios o aplicaciones.
No repitas la misma contraseña en otras aplicaciones.

Ignora el spam. Ten cuidado con los mensajes de correo electrónico de personas desconocidas, nunca hagas clic en enlaces ni abras archivos adjuntos en ellos. Si bien los filtros de spam de la bandeja de entrada se han vuelto muy buenos detectando estas amenazas, los correos de phishing también son cada vez más sofisticados.
El spam también puede venir de WhatsApp.

Haz una copia de seguridad de tu computadora. Hacer una copia de seguridad de tu información es fundamental. Si eres atacado por un ransomware, te pedirán dinero a cambio de liberar el acceso a tu información. Recuerda que los equipos de cómputo, teléfonos se pueden robar o perder.

Apaga tu computadora. Si no estás trabajando en tu computadora, apágala durante la noche o cuando no la vayas a utilizar en períodos prolongados. El que esté siempre encendida hace que tu dispositivo se encuentre disponible para los hackers. De esta manera, los cierres de sesión rompen la conexión que un pirata pudo haber establecido y así se interrumpe cualquier ataque que busque hacer daño. De igual manera con el Bluetooth.

Utiliza la autenticación de dos factores (también conocido como autentificación de dos pasos) Las contraseñas son la primera línea de defensa, pero la segunda capa aumenta la protección, este te enviará una clave al número de teléfono o correo electrónico que tengas registrado.

No uses redes Wi-Fi públicas. Las redes Wi-Fi públicas pueden ser utilizadas para acceder a tu computadora, capturar tu información o instalar software malicioso. Utilízalas lo justo y necesario (puede que requieras pedir un vehículo de plataforma), pero no ingreses a tu cuenta bancaria ni accedas a tu información personal desde ellas.

Desactiva la función de autocompletar. Autocompletar es la función que adivina lo que estás escribiendo y completa las palabras, frases u otra información en formularios. Si bien es conveniente, este tipo de herramientas prácticamente entregan tu dirección de correo electrónico, dirección postal, número de teléfono y otra información que hayas escrito alguna vez a un atacante informático.

Nosotras:

La capa de Nosotras, implica pensar a nivel colectivo, es decir como cuido-cuidamos y nos apoyamos con las compañeras y compañeres de las colectivas y organizaciones en las que colaboramos.

-*Como cuido a las demás personas*, que acciones puedo hacer para cuidar la privacidad y seguridad de las personas con quien me relaciono.

Cuidar a la otra persona significa no compartir sin su autorización su número de teléfono, correo a quien lo solicita (pregunta primero si lo puedes compartir), si veo alguna publicación que violente a una persona conocida hago captura de pantalla, reporto y aviso, no publicar información personal o sensible sin autorización.

-*Red de apoyo*, Contar con una red de apoyo formada por personas que puedan escucharte, apoyarte, ir a comer helado y darte un abrazo cuando lo necesitas es importante.

Una red de apoyo está conformada por personas que son de confianza, que quieres y que sabes que te van a escuchar y estarán para apoyarte.

Para identificar tu red de apoyo, te invitamos a realizar el siguiente ejercicio:

-Identifica quienes son las personas con las que siempre acudes cuando tienes un problema y quieres platicar.

- ¿Estas personas te escuchan y no te juzgan?

- ¿Te dan un consejo?

- ¿Apoyan la decisión que tomas?

Esas personas en las que pensaste son tu red de apoyo.

Confía en ellas y recuerda que hablar de la violencia que estás pasando también es una forma de denuncia.

Te recomendamos:

En eventos, actividades que organicen como colectiva u organización pregunta antes si pueden tomar fotografías y publicarlas, si alguna de las personas participantes no quiere que su rostro sea publicado, respeta su decisión.

No compartas información de contacto o datos sensibles, personales de las compañeras y compañeres, pregunta antes si puedes compartir su contacto.

Si almacenas información de acompañamientos no la compartas, no la almacenes en la nube, genera un respaldo de la información.

Platica con las compañeras y compañeres de la organización para el tratamiento de la información que almacenan.

Construyan un protocolo de seguridad de la organización, qué les funciona a ustedes, cuál plataforma de mensajería es más útil, qué hacer en caso de que les roben o pierdan su celular. Cada organización, colectiva o medio sabe cuáles temas trabajan y cómo quieren trabajar, apostamos más a construir acuerdos donde todas las personas se involucren.

Todas:

La última capa hace referencia a las acciones que podemos hacer como comunidad,

-*Reviso y exijo,* puede sonar aburrido, pero tenemos que leer las normas de comunidad de cada red social, plataforma o producto que descargamos y sumarnos a exigir que las empresas de las redes sociales mejoren sus procesos de denuncia, respuesta y ayuda a las personas que pasan por violencia digital.

Te recomendamos:

Revisa las fuentes de la información, no compartas noticias, imágenes que se vean muy "espectaculares" o desconoces el origen de la información. La desinformación

Si te llega información que violenta, discrimina o fomenta el odio a una persona, grupo o colectiva denuncia desde los canales disponibles, ya sea en redes sociales, plataformas, instituciones o en el grupo donde se esté compartiendo.

Comparte con las demás personas sugerencias sobre seguridad digital, compartan experiencias y buenas prácticas.

Pregunta, no tengas miedo a preguntar cuando desconoces de un tema.

Nota: El estado y las empresas también juegan un papel muy importante en la seguridad y también toca exigir que realicen las acciones y mecanismos necesarios.

Recomendaciones generales

Evita la exposición innecesaria. Reflexiona ¿qué quieres compartir en redes sociales y que momentos prefieres guardar para ti?

Utiliza contraseñas de confianza. No tengas escritas las contraseñas en papelitos junto a tu computadora o notas en tu celular, usa un gestor de contraseñas, te recomendamos LastPass.

Ten cuidado con las descargas peligrosas. Solo descarga archivos de sitios web conocidos.

Utiliza antivirus. En computadora y celular.

Crea un respaldo de la información de tu equipo de cómputo, celular.

Instala las actualizaciones. Todas.

Activa la verificación de dos pasos en todas tus redes sociales, plataformas de mensajería, correo electrónico, en todo.

Recursos que sí debes descargar

Que no quede huella, que no que no

https://derechosdigitales.org/wp-content/uploads/que-no-quede-huella.pdf

¿Hicieron un perfil de Instagram que se hace pasar por ti y una página falsa de Onlyfans?

https://cultivandogeneroac.org/2022/07/06/suplantacion-de-identidad-y-cuentas-falsas-de-onlyfans/

Guía de Resistencia Digital entre amigas No Navegas Sola
https://cultivandogeneroac.org/en-la-red-no-navegas-sola/

Hacks de Vida Cuadernillo
https://archive.org/details/DocumentoHacksdeVida_201803

8 claves prácticas de autocuidado feminista #CuídateElCoco
https://www.pikaramagazine.com/2018/09/autocuidado-feminista/

También puedes visitar los siguientes sitios web:

SocialTic y las herramientas de privacidad y seguridad

https://socialtic.org/herramientas/

La clika

https://www.libresenlinea.mx/

Red Rompe el Miedo

https://informaterompeelmiedo.mx/

Protege.la

https://protege.la/

Grítalo en la red

https://gritaloenlared.articulo19.org/

Alerta Machitroll

https://mtroll.karisma.org.co/

¿Te gustan los podcasts?, entonces no puedes perderte a:

Las hijas de Internet

https://open.spotify.com/show/4HqBnWXPVusZbh1meZr0Fk?si=14d55e7b59f140b4

Navega Segura

https://open.spotify.com/show/2VmuKR9PmpZY2bsOocHPe9?si=9d1a6f36f9b544bc

Señoras de Internet

https://open.spotify.com/show/4dN3QG3K2kAbgB81R3T8QJ?si=3ff76241f9aa4572

Organizaciones que debes seguir, puedes seguir a todas estas colectivas, asociaciones que trabajan por los derechos digitales en México (las encuentras en todas las redes sociales)

Acoso Online

https://acoso.online/mx/

Artículo19

https://articulo19.org/

Ciberseguras

https://ciberseguras.org/

Cultivando Género AC

https://cultivandogeneroac.org/

Luchadoras

https://luchadoras.mx/

Red por los Derechos Digitales

https://r3d.mx/

Social TIC

https://socialtic.org/

Sursiendo

https://sursiendo.org/

Vita Activa

https://vita-activa.o