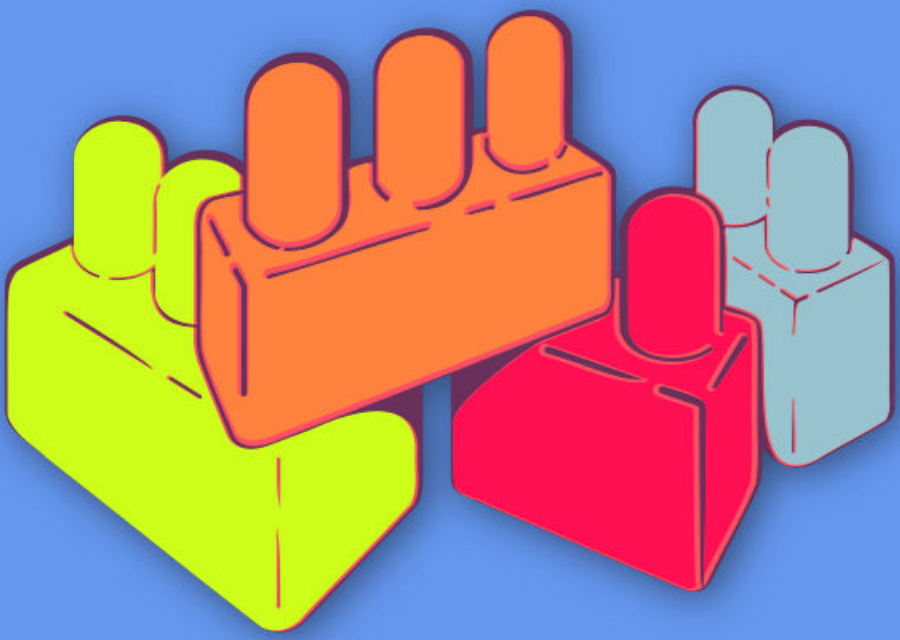
CIBERMUJERES



Principios básicos de seguridad digital 1

Principios básicos de seguridad digital 1

https://iwpr.net/

Índice general

¿Cómo funciona Internet?

- **Objetivos:** Compartir una comprensión de los flujos de información de internet, las distintas vulnerabilidades que emergen y buenas prácticas de seguridad relacionadas a cada componente y tramo de la cadena.
- **Duración:** 60 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - ¿En quién confías?[1]
  - Impresiones personales sobre la seguridad[2]
  - Nuestros derechos, nuestra tecnología[3]
- **Materiales requeridos:**
  - ¿Cómo funciona Internet? Tarjetas de representaciones icónicas

[1] https://cyber-women.com/es/ejercicios-para-fortalecer-la-confianza/en-quién-confías/

[2] https://cyber-women.com/es/repensar-nuestra-relación-con-las-tecnologías/impresiones-personales-sobre-la-seguridad/

[3] https://cyber-women.com/es/repensar-nuestra-relación-con-las-tecnologías/nuestros-derechos-nuestra-tecnología/

de los distintos componentes de la ruta que sigue un correo electrónico desde que se envía hasta que es recibido: dispositivos (computadora/celular) (x 2) (nota: representa la computadora y el celular en la misma tarjeta para evitar confusiones), módem (x2), poste telefónico/fibra óptica subterránea (x 2), proveedor de servicio de Internet (x 2), servidores Google (x 1), simulacro de email (x 2, o más)
  - Documentos con sugerencias sobre prácticas de seguridad digital
  - Papel para utilizar a modo de pizarrón: un trozo de 4 metros y dos trozos de 1 metro cada uno.
  - Marcadores de colores
  - Cinta adhesiva
  - Diapositivas (con puntos clave comentados a continuación)
  - Computadora y proyector ya configurados
  - Altavoces/bocinas
- **Recomendaciones:** Procura cubrir todas las preguntas que puedan surgir. es importante cerrar la sesión cubriendo las inquietudes que puedan surgir en torno a las vulnerabilidades comentadas en la sesión y que sientan que tienen la información necesaria para tomar medidas. evita crear un entorno de miedo, estrés o ansiedad - brinda suficiente información y recursos, además de señalar otras oportunidades para formación (si es posible).

Esta sesión fue desarrollado conjuntamente con Mariel García (SocialTIC) y Spyros Monastiriotis (Tactical Technology Collective)

Conducir la sesión:

Parte 1 - Cómo funciona Internet – Flujos de información y puntos de vulnerabilidad.

1. Esta parte del taller comenzará a modo de juego. Cada participante recibe tarjetas representando diferentes componentes de una cadena de flujo de información (módem, computadora, edificio de proveedor de servicio de internet, etc.). Pide a las participantes que las ordenen correctamente para mostrar cómo se envía un correo a través de Internet.
2. Haz observaciones del orden de las tarjetas y repasa el proceso con el grupo. Pide a una persona voluntaria que explique el proceso de nuevo en sus propias palabras. Recomendamos pedir que tres personas en total cuenten el proceso de vuelta. Puedes cambiar las ilustraciones de referencia y en qué orden se explica para darle más variedad al ejercicio. Procura un tiempo para resolver dudas también.
3. Puedes apoyarte en un recurso audiovisual como https://www.youtube.com/watch?v=7_LPdttKXPc para ayudar a las participantes a identificar si están ordenadas correctamente las tarjetas.

   Opcional: para grupos más grandes, en vez de una tarjeta por persona, reparte una por pareja; para grupos más pequeños, coloca todas las tarjetas en el suelo y debate en grupo el orden.

Parte 2 - Vulnerabilidades

4. Una vez completado el paso anterior, las participantes colocan cada tarjeta en un papel grande en el suelo. Repasa de nuevo la cadena, esta vez señalando y explicando las vulnerabilidades en cada etapa (comparte brevemente algunas buenas prácticas relevantes para generar una sensación de calma y confianza entre las participantes)

Comentaremos algunas vulnerabilidades a continuación. Puedes agregar otras prácticas o vulnerabilidades que consideres relevantes a tu propio contexto o los contextos de las participantes. También puedes compartir algunos ejemplos de prácticas de otros colectivos con los que trabajas, con el fin de ayudar a las participantes pensar cuáles podrían ser prácticas buenas o malas en su caso.

Dispositivo 1 (computadora/celular): inseguridad física; pérdida de información

Módem 1: sniffing de WiFi; información sin cifrar

Poste telefónico/fibra óptica subterránea: no aplica

Proveedor de servicio de internet: solicitudes de datos y metadatos de instancias gubernamentales locales/nacionales

Servidores de Google: vigilancia internacional; contraseñas inseguras y phishing, solicitudes de instancias gubernamentales nacionales

Poste telefónico/fibra óptica subterránea 2: N/A

Módem 2: problemas de seguridad al utilizar las conexiones de terceros (ej. cibercafé)

Dispositivo 2: software malicioso; borrado inseguro de datos

Parte 3 - Buenas prácticas de seguridad digital

5. Una vez que se hayan centrado en las vulnerabilidades, para que no sea demasiada información para las participantes que tienen menos experiencia en estos temas, cada grupo tomará un papel que describa una posible solución. Este papel será el detonante para discutir en grupo.

   Al final, los grupos tendrán entre 30 segundos y un minuto para presentar sus ideas (una de las facilitadoras tomará notas y aportará retroalimentación). Las facilitadoras se moverán por el espacio dando explicaciones cortas y respondiendo preguntas y, sobre todo, alentando la discusión entre las participantes.

Es importante que, conforme avance esta actividad, las facilitadoras expliquen los conceptos básicos de cada solución. También, según el nivel de interacción y ritmo del taller, quizás no dé para cubrir todas las propuestas.

Algunas de las más importantes para tomar en consideración son:

Inseguridad física: reduce la exposición de los dispositivos de tu organización a personas desconocidas.

Inseguridad física: utiliza bloqueos de dispositivos en tu oficina y casa.

Pérdida de información: guarda tu respaldo en un lugar que no sea tu oficina o casa.

Pérdida de información: escoge una persona para encargarse de los respaldos en tu organización.

Intevención de redes (WiFi sniffing): retira todas las indicaciones que muestren la contraseña de WiFi.

Intervención de redes (WiFi sniffing): cambia la contraseña de tu WiFi frecuentemente.

Datos sin cifrar: asómate a una criptofiesta en tu ciudad o participa en un taller.

Datos sin cifrar: lee la sección sobre cifrado del manual "Security in a Box".

Solicitudes de datos y metadatos por parte de entidades gubernamentales locales/nacionales: trabaja con organizaciones de derechos digitales para encontrar maneras para protegerte legalmente.

Solicitudes de datos y metadatos por parte de entidades gubernamentales locales/nacionales: investiga qué dicen las leyes en tu país sobre la intervención de comunicaciones.

Vigilancia internacional: cámbiate a servicios seguros para realizar búsquedas, administrar tu correo, alojar tus datos y comunicaciones en general.

Contraseñas inseguras: utiliza contraseñas largas y complejas.

Contraseñas inseguras: utiliza KeePass para recordar todas las contraseñas que tienes.

Phishing: piensa antes de hacer clic (presta atención donde introduces tus datos de acceso a una cuenta).

Utilizar el WiFi de otras personas: siempre cierra adecuadamente tu sesión.

Utilizar el WiFi de otras personas: cuéntanos -¿qué no deberías estar revisando cuando estás en el WiFi de otra persona?

Software malicioso: instala un programa de antivirus y ejecútalo manualmente cada semana.

Borrar datos de manera segura: usa Cmd+derecha para vaciar la papelera en Mac.

Borrar datos de manera segura: utiliza programas como Eraser o CCleaner.

Parte 4 - Asuntos y recursos pendientes

6. Este momento de la sesión es para sondear preguntas relacionadas con seguridad digital que no hayan surgido en el taller hasta ahora, además de discutir temas relevantes en las comunidades de las participantes. Aprovecha para compartir materiales para seguir aprendiendo y mantenerse al día. La facilitadora hará ronda de preguntas, dará unas pistas de posibles respuestas y mencionará referencias que pueden servir para responderlas más en profundidad.

Referencias

- https://securityinabox.org/es
- https://ssd.eff.org/es

- https://myshadow.org/es
- http://www.sinmiedo.com.co
- https://cuidatuinfo.org
- https://temboinalinha.org
- https://prism-break.org/es

Creando contraseñas más seguras

- **Objetivos:** Revisar vulneración de contraseñas - cómo son comprometidas, cuáles son las implicaciones-, cómo crear contraseñas más robustas y desarrollar mejores hábitos en relación con nuestras contraseñas.
- **Duración:** 45 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - ¿Cómo funciona Internet?[1]
  - Cómo hacer más segura tu computadora[2]
- **Materiales requeridos:**
  - Proyector
  - Diapositivas

[1] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-funciona-internet/

[2] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-hacer-más-segura-tu-computadora/

- Papel
- Conexión a Internet/WiFi para descargar KeePass

Esta sesión está basada en el módulo "Prácticas de contraseñas más seguras", desarrollado por Cheekay Cinco, Carol Waters y Megan DeBolis para LevelUp.

Conducir la sesión:

Parte 1 - Introducción

1. Comienza preguntando a las participantes:
    - ¿Cuándo fue la última vez que cambiaste alguna de tus contraseñas?
    - ¿Tienes contraseñas diferentes para cada cuenta?
    - ¿Anotaste tu contraseña en alguna parte como un post-it?
    - ¿Almacenas todas tus contraseñas en un documento sin cifrar?
    - ¿Tus contraseñas están en tu celular?

Parte 2 - Por qué las contraseñas son importantes

2. Antes de empezar a hablar de la importancia de las contraseñas, pide a las participantes enumerar toda la información que es asegurada con una contraseña. ¿Qué información tienen en sus cuentas de correo, cuentas de redes sociales y celulares? ¿Qué pasaría si otra persona pudiera acceder a esta información?
3. Ahora, comparte algunas razones por las que las contraseñas son importantes:

    Las contraseñas brindan acceso a un abanico de cuentas importantes como tu correo, cuentas bancarias, redes sociales, etc.

Estas cuentas suelen contener información muy sensible y nos permiten ser "nosotras mismas" en interacción orgánica con las demás a través de diferentes servicios digitales: enviar un mensaje a través de una plataforma de red social, enviar un correo, realizar una compra online, etc. También pueden darnos la oportunidad de asumir otras identidades - cualquier persona que accede a una contraseña de una cuenta puede, en efecto, simular ser la propietaria de la cuenta. Las contraseñas también dan acceso a otras cosas - puntos de acceso Wi-Fi, desbloquear celulares, iniciar sesión en computadoras, descifrar dispositivos, archivos y mucho más.

Parte 3 - ¿Qué pasa si comprometen tu contraseña?

4. Comparte papeles con las participantes y pídeles hacer una lista de todas las plataformas donde se acuerden que tienen cuentas. Después, que anoten qué pasaría si alguien tuviera su contraseña y pudiera acceder a sus cuentas o dispositivos.

    - Pueden robar (copiar) o borrar información importante o archivos; si esto sucede, quizás no te des cuenta de ello inmediatamente. Podría ser desde documentos y archivos con información confidencial, hasta contactos del directorio y correos electrónicos.
    - Podrían robar o malversar fondos a través del acceso de tarjetas de crédito o cuentas bancarias.
    - Pueden usar cuentas de correo o plataformas de redes sociales para enviar spam o hacerse pasar por ti o tus amigo/as, familiares y compañero/as.
    - O secuestrar tu cuenta a cambio de un "rescate" que podría ser dinero, acceso a contactos.
    - Alguien indebido con una contraseña podría acceder y revisar tus comunicaciones y actividades sin tu conocimiento.
    - A través del acceso de una cuenta de correo, se podría desencadenar un "efecto dominó" y restablecer las contraseñas de otras cuentas a través de links de solicitud, hasta dejar a la persona

legítima fuera de todas de sus cuentas.

Parte 4- ¿Cómo son las maneras más comunes de comprometer una contraseña?

5. Comparte algunas prácticas que pueden resultar en que otras personas tengan acceso a tus contraseñas:
    - Cuando las compartes con otras personas o las almacenas en lugares fáciles de descubrir, por ejemplo, en un post-it pegado cerca de la computadora.
    - Cuando alguien te ve escribiendo una contraseña en tu pantalla y lo anota o se acuerda de ella.
    - Si estás usando un cliente de correo que no utiliza SSL (https) durante toda la sesión (y no sólo en el login), las contraseñas y demás información queda potencialmente expuesta a cualquiera que tenga acceso a tu conexión.
    - Al acceder físicamente a un dispositivo, se puede obtener las contraseñas a través de la configuración "Save My Password" ("Guarda mi contraseña") o "Remember Me" ("Recuérdame") de tu navegador. Esto es aún más probable si el disco de tu dispositivo no está cifrado.
    - Malware, como los keylogger (registrador de teclas), puede registrar cada golpe de tecla de un dispositivo y enviarlo a un tercero, revelando no sólo contraseñas sino potencialmente una cantidad mucho más amplia de información confidencial.
    - Las brechas de seguridad de una plataforma también pueden exponer información sobre sus usuarias.

Parte 5 - ¿Cómo podemos crear contraseñas más robustas?

6. Explica que si utilizan la misma contraseña para todo y esa contraseña es comprometida, todas las cuentas podrán ser vulneradas. Comenta algunas características para contraseñas más seguras y robustas:

Duración: en pocas palabras, ¡cuanto más larga, mejor! 12 caracteres es el mínimo recomendable para contraseñas robustas y 20 es mejor todavía.

Complejidad: utiliza una contraseña alfanumérica, con mayúsculas y minúsculas, una mezcla generosa de números y caracteres especiales.

Cambios frecuentes: cambia a menudo tus contraseñas, particularmente las de tus cuentas más confidenciales y, sobre todo, cámbialas si recibes un correo legítimo y verificado (no phishing) diciéndote que la cuenta de determinado servicio ha sido comprometida.

Utilizar frases enteras: imagina varias contraseñas juntas en una misma "frase"- es un ejemplo de práctica segura de contraseñas. Aquí van unos ejemplos:

NoALaMineriaEnAmericaLatina

AbortoSiAbortoNoEsoLoDecidoYo

NosotrxsNoCruzamosFronterasEllasNosCruzanANosotrxs

7. Propón a las participantes dedicar varios minutos a crear algunos ejemplos de contraseñas robustas. Recuérdales que tengan en cuenta la importancia de la confidencialidad de la información que están resguardando a la hora de escoger la longitud y complejidad de sus contraseñas - quizás quieran utilizar contraseñas más robustas para sus cuentas más importantes y unas menos complejas (pero aún seguras) para sus cuentas sin tanta relevancia.

Referencias

- https://ssd.eff.org/es/module/creando-contrase%C3%B1as-seguras
- https://securityinabox.org/es/guide/passwords

Malware y virus

- **Objetivos:** Abordar, en un contexto de riesgos cercano a las realidades de las defensoras, conceptos básicos de malware y la exposición de nuestros dispositivos a distintos tipos de malware y software malicioso.
- **Duración:** 30 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - ¿Cómo funciona Internet?[1]
  - Cómo hacer más segura tu computadora[2]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)
  - Computadora y proyector configurados
- **Recomendaciones:** Idealmente, después de esta sesión, sigan con la de

[1] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-funciona-internet/

[2] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-hacer-más-segura-tu-computadora/

"cómo hacer más segura tu computadora", también incluida en este módulo.

Conducir la sesión

Parte 1 - Introducción al Malware

1. Explica a las participantes qué es el malware, un repaso de algunos tipos - como mínimo, recomendamos cubrir los siguientes:

    - Troyanos
    - Spyware
    - Ransomware
    - Keylogger (registrador de teclas)
    - Virus

    El ransomware y los registradores de teclado (keyloggers) son tipos de malware cada vez más comunes en el contexto de las defensoras en Latinoamérica; si estás trabajando con un grupo de mujeres en esta región, será especialmente importante abordarlas. En general, asegúrate de incluir estudios de caso y ejemplos de malware que sean comunes en las realidades de las participantes de tu taller.

Parte 2 - ¿Cómo te puedes infectar?

2. Explica algunas de las maneras más comunes de infección de malware. También es importante explicar los distintos propósitos o motivaciones que puede tener el uso de malware:

    - Algunos se viralizan a una escala amplia sin ningún objetivo concreto.
    - Otros van dirigidos específicamente a activistas, periodistas o disidentes para obtener acceso a sus datos y comunicaciones.

- O a personas que están en contacto con una red de activistas y defensoras y que, a través de infectar su equipo, alcancen el resto de su red.

Parte 3 - Comparte ejemplos que afecten a mujeres y defensoras de derechos humanos

3. Concluye la sesión compartiendo ejemplos de casos de infección de malware comunes en el contexto de mujeres y defensoras; puedes basarte en estudios de caso (de blogs, portales de noticias o desde la experiencia personal de cada una). Recuerda anonimizar las fuentes al menos que tengas permiso explícito de la(s) persona(s) afectada(s). Aquí mostramos algunos ejemplos de casos. Quizás conozcas casos similares más relevantes a tu contexto.

   > Una mujer que recibió un correo que oferta boletos gratuitos a un concierto; el enlace que contenía el correo infectó su smartphone (celular inteligente) con malware.
   >
   > Una activista recibió un correo de quien era, aparentemente, un/a compañero/a; al hacer clic en el enlace del correo, un mensaje aparece diciendo que su disco duro está cifrado y que necesita pagar para obtener acceso de vuelta a sus datos.

Referencias

- https://securityinabox.org/es/guide/malware/
- https://ssd.eff.org/es/module/protegi%C3%A9ndote-contra-el-malware

Navegación más segura

- **Objetivos:** Brindar una introducción sobre prácticas de navegación web segura, incluyendo un repaso a plugins y otros servicios que pueden utilizarse para crear un entorno de navegación más seguro.
- **Duración:** 45 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - ¿Cómo funciona Internet?[1]
  - Cómo hacer más segura tu computadora[2]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)
  - Computadora y proyector configurados
  - Conexión WiFi

[1] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-funciona-internet/

[2] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-hacer-más-segura-tu-computadora/

Conducir la sesión

Parte 1 - Escoger un navegador

1. Arranca la sesión preguntando a las participantes qué navegadores web utilizan y qué otras conocen. Presenta Firefox - explica los beneficios de utilizarlo y comenta brevemente las diferencias que existen con otros navegadores conocidos como Google Chrome o Internet Explorer.

   Opcional: si estás trabajando con un grupo que habla español, puedes echar mano a este vídeo de Ella para detonar una discusión: https://vimeo.com/109258771

Parte 2- Prácticas más seguras de navegación

2. Existen bastantes prácticas de navegación más segura que puedan ser compartidas y discutidas con las participantes. No tienes que repasarlas todas, pero recomendamos dar a conocer suficientes para que el grupo pueda barajar opciones (toma en cuenta el contexto de las participantes a la hora de hacer recomendaciones).
3. Subraya que aún están revisando algunas prácticas y no específicamente herramientas más allá de navegadores web. Algunas participantes estarán ya dispuestas a cambiar de navegador, mientras otras no, así que antes de discutir herramientas más específicas como complementos y plugins, es importante que aterricen la discusión.

   Aquí van algunos ejemplos de prácticas que pueden discutir:

   - Estar atenta a intentos de phishing;
   - Bloquear anuncios integrados en sitios y anuncios emergentes;
   - Cómo funcionan los cookies - asegúrate de comentar que pueden ser necesarios para que un sitio/plataforma funcione, pero que también tienen desventajas;

- Deshabilitar y borrar cookies de los navegadores,
- Eliminar historial de navegación;
- No guardar las contraseñas en la configuración de tu navegador;
- Comprobar las extensiones que instalas en tu navegador;
- Habilitar la opción "No rastrear" (Do Not Track) en tu navegador;
- Alternativas de buscadores a Google (como Duck Duck Go);
- ¿Quién implementa el rastreo online y por qué? (Tanto https://trackography.org/ como https://www.mozilla.org/es-MX/lightbeam/ son buenos recursos);
- Discutir HTTP vs HTTPS;
- ¿Qué es una VPN (Virtual Private Network/Red Privada Virtual) y cuándo la deberías usar?
- ¿Qué hace exactamente el modo incógnito y cuándo la deberías usar?

Parte 3 – Herramientas y extensiones para una navegación más segura

4. Presenta, ahora que abordaste algunas prácticas para una navegación más segura, determinadas herramientas - específicamente plugins para el navegador - puedan ayudar a automatizar o facilitar la adopción de algunas de las prácticas comentadas anteriormente.
5. Dé a conocer las siguientes herramientas, explicando cómo funciona cada una. Recuerda compartir los links de descarga. Es esencial que las participantes comprendan por qué cada una de las herramientas es útil y relevante; si no son explicadas de manera clara, puede dar lugar a que las participantes tomen decisiones sin fundamento sobre su privacidad y anonimato en línea.

Herramientas de navegación para computadoras

- No Script[3]
- Adblock Plus[4]
- Privacy Badger[5]
- HTTPS Everywhere[6]
- Click & Clean[7]
- Tor browser[8]
- Disconnect[9]
- uMatrix[10]

Herramientas de navegación para celulares

- HTTPS Everywhere[11]
- Recursos de My Shadow[12]
- Orfox[13]
- Orbot[14]
- Tor for iPhone[15]

[3] https://noscript.net
[4] https://adblockplus.org/es
[5] https://www.eff.org/privacybadger
[6] https://www.eff.org/https-everywhere
[7] https://www.hotcleaner.com
[8] https://www.torproject.org/download/download-easy.html.en
[9] https://disconnect.me
[10] https://addons.mozilla.org/es/firefox/addon/umatrix
[11] https://www.eff.org/https-everywhere
[12] https://mike.tig.as/onionbrowser
[13] https://mike.tig.as/onionbrowser
[14] https://mike.tig.as/onionbrowser
[15] https://mike.tig.as/onionbrowser

Otras prácticas & funcionalidades

Modo incógnito (Modo privado)

Esta funcionalidad suele generar confusiones ya que muchas personas usuarias no la comprenden - quizás las participantes no tengan una comprensión clara de cómo funciona el modo incógnito en el navegador y cuándo puede ser útil. Explica cómo funciona el modo incógnito (y otros parecidos) y ofrece algunos ejemplos de cuándo podrían ser útiles.

Prácticas Wi-Fi seguras

En último lugar, dedica un tiempo a discutir y, si es posible, demostrar, unas cuantas prácticas básicas de seguridad cuando te conectas a una conexión Wi-Fi - esto incluye cambiar la contraseña por defecto del modem, revisar qué dispositivos se conectan a tu red.

Referencias

- https://myshadow.org/es/trace-my-shadow
- https://securityinabox.org/es/guide/firefox/windows
- https://securityinabox.org/es/guide/firefox/linux
- https://myshadow.org/es/tracking-data-traces
- https://cuidatuinfo.org/article/firefox-y-complementos-de-seguridad

Cómo hacer más segura tu computadora

- **Objetivos:** Identificar buenas prácticas para mantener nuestras computadoras seguras.
- **Duración:** 50 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - ¿Cómo funciona Internet?[1]
  - Navegación más segura[2]
  - Malware y virus[3]
  - Almacenamiento y cifrado[4]

[1] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-funciona-internet/

[2] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/navegación-más-segura/

[3] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/malware-y-virus/

[4] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-2/almacenamiento-

- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)
  - Computadora y proyector configurados
  - Copias impresas de la plantilla “Respaldo” (ver a continuación)
- **Recomendaciones:** Recomendamos enfáticamente que documentes en vivo - utilizando un proyector conectado a la computadora - cualquier herramienta que vayas a cubrir en la sesión. así, las participantes pueden seguir los pasos y replicarlos en sus computadoras con archivos “simulados” creados expresamente para la sesión (no archivos y datos importantes reales).

Conducir la sesión

Parte 1 - Introducción

1. Pregunta a las participantes: qué valor tienen para ellas sus computadoras - ¿Qué tan útiles o esenciales son en su vida profesional y personal? ¿Cuánta información almacenan en ellas?
2. Ahora, pregunta: ¿Cuánto tiempo invierten en mantener su equipo? La diferencia entre el grado de valor que otorgan a sus dispositivos contra la cantidad de tiempo que dedican a cuidarlos y darles mantenimiento suele ser bastante amplia. Explica al grupo que la sesión se va a enfocar en prácticas básicas para proteger sus dispositivos.

Parte 2- Entornos físicos y mantenimiento

3. Comenta al grupo que muchas prácticas relacionadas con seguridad tienen, de hecho, más que ver con seguridad física que seguridad digital (esta aclaración es una buena manera de reforzar el enfoque holístico de esta currícula). Un buen ejemplo de ello es la importancia

y-cifrado/

de limpiar los dispositivos (sacar polvo y otros residuos que quedan adentro) y realizar inspecciones físicas regulares del equipo para identificar si hay alteraciones o ha habido intentos físicos de acceso sin consentimiento. En este sentido, puedes recomendar prácticas digitales básicas como usar una contraseña para bloquear un dispositivo remotamente y también protección física como utilizar un protector de teclado o una cadena anti-robo para prevenir acceso sin consentimiento o hurto. Subraya el aspecto más crítico de la seguridad física de los dispositivos: tomar conciencia. Estar atenta a dónde está un dispositivo en cada momento - ya sea que lo traigas encima, en otro cuarto o en otro lugar seguro - es fundamental.

4. Pídeles a las participantes recordar los detalles de su espacio de trabajo. ¿Qué riesgos físicos pueden presentarse? ¿Está su computadora expuesta a ser robada? ¿Hay cables mal colocados? ¿Su computadora está bajo condiciones de calor o frío extremo o humedad? Estas consideraciones son importantes a la hora de estar conscientes

    - estar atenta a aspectos físicos de nuestros dispositivos no sólo es prevenir el acceso sin consentimiento sino también los daños potenciales que puede sufrir por el entorno.

Parte 3 – La seguridad de nuestro software

5. Explica a las participantes los riesgos de usar software pirata (alta probabilidad de descargar malware, más problemas para realizar actualizaciones que el software oficial, etc.); sin embargo, pagar software propietario generalmente sale caro. Puedes compartir varias referencias para abordar esta cuestión:

    Osalt[5]

    Abre un navegador y entra en Osalt, un sitio web que presenta alternativas gratuitas y open source a la mayoría de las plataformas y suites de

[5] http://www.osalt.com

software propietarios (por ej. Ubuntu vs. Windows; LibreOffice vs. Microsoft Office; Inkscape vs. Adobe Illustrator)

TechSoup[6]

A través de TechSoup, activistas de derechos humanos y organizaciones sociales pueden solicitar (a proveedores de servicios locales de TIC que son distribuidoras oficiales) versiones gratuitas o con descuento (para el sector público/sin ánimo de lucro) de software comercial. TechSoup coordina una red grande de distribución de donaciones de software - el enlace de arriba contiene una lista de socios y los países donde operan.

6. Explica la importancia de mantener el software actualizado - ante todo, les protege contra brechas de seguridad. Todo el software y actualizaciones deberán realizarse desde fuentes de confianza; por ejemplo, cuando actualices Adobe Acrobat Reader, sólo hazlo directamente desde Adobe y no sitios web de terceros.

7. Siguiente, explica la importancia de tener un programa de antivirus en la computadora. Brinda un poco de contexto para romper mitos comunes en torno a los antivirus como:

    - Utilizar dos o más me protege más.
    - Mac y Linux no necesita antivirus porque no se infectan.
    - Es totalmente seguro utilizar una versión pirata de software antivirus.
    - Los programas antivirus gratuitos no son seguros o confiables como los de pago.

8. Pueden comentar otros ejemplos que propongan las participantes. Después, discute algunas prácticas básicas de seguridad a la hora de utilizar software antivirus y protección contra malware (véase la sesión Malware & Virus de este módulo). Algunas prácticas útiles a subrayar aquí, en caso de no haberlas repasado en la sesión de Malware & Virus son:

[6] http://www.techsoupglobal.org/network

- Utilizar el complemento uBlock Origin para evitar hacer clic en anuncios emergentes que pueden conducir a descargar archivos maliciosos en la computadora.
- Tomar conciencia sobre intentos de phishing, enlaces y adjuntos sospechosos contenidos en correos enviados a través de cuentas desconocidas o parecidas (pero no iguales) a las de nuestros contactos.
- Ahora es una buena oportunidad para comentar sobre cortafuegos (firewalls): ofrecen una capa de protección automática en nuestras computadoras. Comenta herramientas como "Comodo Firewall", "ZoneAlarm" y "Glasswire". Versiones más nuevas (con licencia) de Windows y Mac OS ya vienen con cortafuegos robustos pre-instalados.

Parte 4 – Protección de datos y respaldos

9. Pregunta a las participantes - ¿Con qué frecuencia realizan respaldos? Comparte experiencias de buenas prácticas relacionadas con el respaldo de datos, tomando en cuenta el tipo de información, como guardarlo en un lugar seguro, separado de la computadora, realizarlo con frecuencia, cifrar los datos y/o el disco entero.
10. Comparte la siguiente plantilla y pide a las participantes rellenarla. Explica que es un método útil para crear una política personal de respaldo de datos y volver a ella después del taller como un recurso de apoyo para seguir la pista a dónde almacenan sus datos y con qué frecuencia respaldar.

    Plantilla para realizar respaldos

    Tipo de información
    Importancia/Valor
    ¿Con qué frecuencia se genera/actualiza?
    ¿Cada cuánto se debería respaldar?

11. Comenta, a continuación, que aunque existan herramientas para realizar respaldos automáticamente (como Duplicati.com o Cobian), puede ser más fácil para ellas empezar haciéndolo de manera manual arrastrando los archivos a respaldar al disco extraíble. Dependerá, en última instancia, de la complejidad y la cantidad de información que tengan que gestionar. Para la usuaria promedio, será suficiente con respaldar a mano.
12. A modo de seguimiento, repasa el concepto de cifrado para discos extraíbles. Explica qué implica y por qué es útil cifrar discos duros y discos extraíbles. VeraCrypt y MacKeeper, dos herramientas relativamente conocidas para cifrar archivos y discos, pueden ser opciones a explorar entre las participantes. En Linux pueden utilizar Duplicity para realizar respaldos cifrados automáticos.

Parte 5 - Borrado y recuperación de archivos

13. Lee en voz alta la siguiente afirmación:

    > Desde un punto de vista meramente técnico, no se puede borrar algo en tu computadora.

    Pregúntale al grupo qué opina: ¿les hace sentido este enunciado? ¿Cómo puede ser que no exista una función de "borrado" real? Señala que puedes arrastrar un archivo a la papelera y después vaciarla, pero lo que hace eso realmente es borrar el icono y el nombre del archivo de un inventario escondido de todo lo que hay en tu computadora; y decirle a tu sistema operativo que puede ocupar ese espacio con otra cosa.
14. Pregúntales: ¿Qué crees que pasa con esos datos cuando se "elimina"? Hasta que el sistema operativo vuelve a ocupar este nuevo espacio liberado, seguirá siendo utilizado por los contenidos eliminados, un poco como un archivador al que se le quitan las etiquetas, pero que mantiene los archivos originales.
15. Ahora explica que, debido a cómo una computadora administra el almacenamiento de datos, si tiene el software adecuado y ejecuta lo su-

ficientemente rápido, puede restaurar la información eliminada de la misma manera. Existen herramientas parar eliminar de manera permanente (no sólo retirarlos del índice de archivos hasta que se ocupe el espacio). Aprovecha para presentar las herramientas CCleaner, Eraser y Bleachbit que sirven para eliminar de manera permanente archivos y el software Recuva para recuperarlos.

Referencias

- https://securityinabox.org/es/guide/malware
- https://level-up.cc/curriculum/malware-protection/using-antivirus-tools
- https://securityinabox.org/es/guide/avast/windows
- https://securityinabox.org/es/guide/ccleaner/windows
- https://securityinabox.org/es/guide/backup
- https://securityinabox.org/es/guide/destroy-sensitive-information
- https://chayn.gitbooks.io/Avanzado-diy-Privacidad-for-every-woman/content/Avanzado-pclaptop-security.html