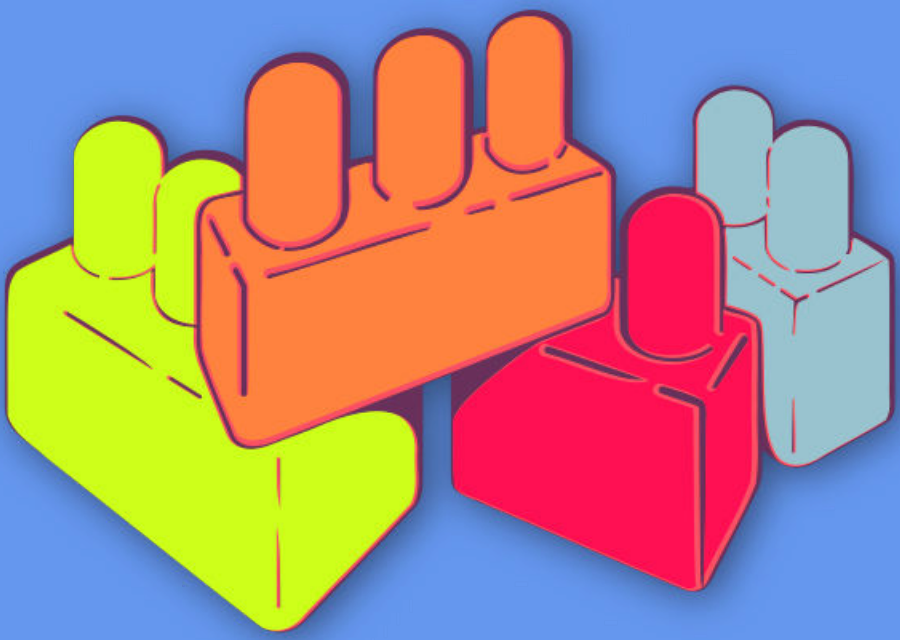
CIBERMUJERES



Principios básicos de seguridad digital 2

Principios básicos de seguridad digital 2

https://iwpr.net/

Índice general

Almacenamiento y cifrado

- **Objetivos:** Reforzar la importancia de realizar respaldos regulares de nuestros datos y discutir cómo prevenir la manipulación y acceso sin consentimiento a nuestra información.
- **Duración:** 90 minutos
- **Formato:** Sesión
- **Habilidades:** Intermedio
- **Conocimientos requeridos:**
  - Conceptos básicos de seguridad digital y/o capacitación previa.
  - Introducción al cifrado[1]
  - Cómo hacer más segura tu computadora[2]
- **Sesiones y ejercicios relacionados:**
  - Privacidad[3]
  - Campañas online más seguras[4]
  - Introducción al cifrado[5]

[1] https://cyber-women.com/es/cifrado/introducción-al-cifrado/

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

[3] https://cyber-women.com/es/privacidad/privacidad/

[4] https://cyber-women.com/es/activismo-online-más-seguro/campañas-online-más-seguras/

[5] https://cyber-women.com/es/cifrado/introducción-al-cifrado/

  - Cómo hacer más segura tu computadora[6]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)
  - Computadora y proyector configurados
  - Copias impresas de la plantilla "Respaldo" (ver a continuación)
  - USB's u otro tipo de unidades extraíbles (para cada participante)
- **Recomendaciones:** En esta sesión, usaremos veracrypt o luks (según el sistema operativo) para practicar el cifrado de respaldos y unidades extraíbles. para ahorrar tiempo, descarga los instaladores antes de la sesión. en general, y especialmente en el caso de las principiantes, no recomendamos cifrar todo el disco de la computadora aún. mejor prueben veracrypt o luks con unidades extraíbles (como una usb) utilizando archivos de prueba, preparados especialmente para esta sesión. no quieres correr el riesgo de que una participante pierda acceso a todos sus datos durante el taller sin querer. puedes preparar usb's de antemano con archivos de prueba y descargar instaladores de 32 y 64 bits de veracrypt.

Conducir la sesión

Parte 1 – Respaldo de datos y planeación

1. Pregunta a las participantes: ¿Con qué frecuencia realizan respaldos? Comparte ejemplos de buenas prácticas de respaldo de datos como guardar el respaldo en un lugar seguro alejado de la computadora, hacerlo con cierta frecuencia y -según el tipo de información que quieren respaldar- considerar cifrar su disco duro o disco extraíble donde se va a almacenar los datos.
2. Comparte la siguiente plantilla y pide a las participantes rellenarla: Explica que es un método útil para crear una política personal de respaldo

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

de datos y volver a ella después del taller como referencia que nos ayude a seguir la pista a dónde almacenamos nuestros datos y con qué frecuencia respaldamos.

Plantilla para realizar respaldos

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

Parte 2 – Almacenamiento y cifrado de respaldos

3. Una vez que hayan rellenado las plantillas, invítalas a repasar de nuevo los diferentes tipos de información (y su respectiva relevancia/valor) en las listas que crearon, tomando en cuenta qué pasaría si esa información cayera en las manos de nuestros adversario/as o si se perdiera por completo. ¿Qué tipo de impacto tendría a nivel personal o a nivel de nuestra organización?
4. Introduce el concepto de cifrado y lo cotidiano que es en realidad: es utilizado en las diferentes herramientas y plataformas con las que interactuamos cada día. HTTPS, por ejemplo, es una forma de cifrado de datos "en tránsito" (los datos viajan de un punto A a un punto B). En esta sesión revisaremos el cifrado de datos "en reposo" (información que se almacena en un lugar).
5. Recuerda a las participantes que se les indicó desde antes descargar Veracrypt o MacKeeper en sus computadoras. Dé tiempo a que lo instalen y prueben con datos de prueba (creados expresamente para la sesión). Sobre todo para principiantes, no es recomendable que cifren todo el disco duro interno de su computadora aún. No queremos correr el riesgo de que una participante pierda acceso a todos sus datos durante el taller sin querer.

Referencias

- https://securityinabox.org/es/guide/veracrypt/windows
- https://securityinabox.org/en/guide/veracrypt/mac
- https://securityinabox.org/es/guide/veracrypt/linux

¡Empecemos de nuevo!

- **Objetivos:** Reforzar la idea que las herramientas y tecnologías no tienen poderes sobrenaturales sobre nosotras! acompañarás a las participantes por un proceso de empoderamiento: aprenderán a resetear sus dispositivos desde cero.
- **Duración:** 90 minutos
- **Formato:** Sesión
- **Habilidades:** Intermedio
- **Conocimientos requeridos:**
  - Conceptos básicos de seguridad digital y/o capacitación previa.
  - Introducción al cifrado[1]
  - Almacenamiento y cifrado[2]
- **Sesiones y ejercicios relacionados:**
  - Impresiones personales sobre la seguridad[3]
  - Malware y virus[4]

[1] https://cyber-women.com/es/cifrado/introducción-al-cifrado/

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

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

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

  - Privacidad[5]
  - ¡Más identidades en línea![6]
  - Almacenamiento y cifrado[7]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)
  - USBs vivos configurados con sistemas operativos Tails y Ubuntu
- **Recomendaciones:** Considera entregar una usb a cada participante para que se quede con ella; si no hubiera usb's para todas, prepara varias computadoras, tanto con tails como con ubuntu para que puedan probarlas porque, aunque sea sólo para probar desde la usb, algunas participantes puedan sentirse incómodas probándola en su propia máquina. esta ejercicio puede adaptarse y ser una sesión por si misma si hay interés por parte del grupo en migrar de sistema operativo completamente (de windows o mac os a una distribución de linux como ubuntu).

Conducir la sesión

Parte 1 – Disipando el mito

1. Arranca explicando el objetivo de esta sesión: reafirmar el poder que tienen las personas sobre las tecnologías, disipando la noción que los dispositivos digitales tienen "poderes mágicos" sobre sus usuarias. Si ya llevaste a cabo la sesión "Impresiones personales sobre la seguridad", puedes recordar varios puntos clave:

   ¡Las herramientas y la tecnología no tienen poderes mágicos sobre nosotras! Nosotras somos quienes decidimos cuándo accedemos a ellas, sin embargo, es muy difícil tener control al 100% de los dispositivos que utilizamos y debemos tener mucho cuidado.

[5] https://cyber-women.com/es/privacidad/privacidad/

[6] https://cyber-women.com/es/anonimato/más-identidades-online/

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

Parte 2 – ¿Qué significa empezar de vuelta (resetear)?

2. Repite la afirmación anterior y enfatiza la última frase "siempre podemos empezar de vuelta, aprendiendo de las experiencias anteriores". ¿Qué significa eso? Explica ofreciendo el siguiente escenario:

   Quizás, en algún momento de tu experiencia con la seguridad digital, has sentido que lo estabas haciendo todo mal.

   - Tu computadora está llena de programas, películas, series pirata y un montón de otros archivos que ni recuerdas haber descargado.
   - Has conectado un sinfín de USB's sin ningún criterio en tu computadora y otras computadoras, incluyendo en espacios públicos como cibercafés. A veces hasta sacas la USB sin extraerla de manera segura.
   - Quizás acabas de terminar una relación con alguien que sabes, a ciencia cierta, estaba mirando tu computadora cuando tú no estabas. Probablemente adivinaron tu contraseña o puede ser que se lo diste.
   - Ahora te sientes fuera de control. ¿Quién sabe los tipos de virus están viviendo en tu disco duro o quién tiene acceso a tu información?
   - Pero sabes qué: todo está bien. No es demasiado tarde para empezar de nuevo. ¿Vamos? Esta sesión es para ti.

3. Explica qué significa "resetear" en este contexto: significa empezar de cero haciendo un "reset" de tu dispositivo o computadora para volver a su estado y configuración inicial por defecto.

   Es muy importante que consideres esto: "resetear" los dispositivos restaura la configuración original, pero no restaura información perdida ni recupera datos que fueron expuestos a personas no autorizadas. Pedagógicamente, esto te brinda una "hoja en blanco" para tu proceso de seguridad digital.

Asegúrate de recordar a las participantes que en esta sesión explicarás cómo realizar un "reset". No van a tener que hacerlo ellas mismas durante la sesión ni en el resto del taller.

Hacer un reset puede salir mal si las participantes no están preparadas o no han hecho un respaldo de sus datos recientemente. Seguramente querrán también utilizar sus laptops tal como están ahora para mantener el acceso a sus datos mientras se preparan mejor.

Sin embargo, durante esta sesión, las participantes tendrán la oportunidad de practicar utilizando sistemas operativos alternativos en sus computadoras, punto importante para prepararse para el momento que decidan hacer un reseteo.

Parte 3 – Check-in:¿Necesito hacer un respaldo?

4. Idealmente, ya habrán realizado la sesión "Almacenamiento & Cifrado" ya que aborda puntos clave con respecto a respaldo de datos. De cualquier manera, antes de empezar la parte práctica de esta sesión, haz un breve repaso con el grupo sobre cómo respaldar sus datos.

   Opcional: pregúntales a las participantes con qué frecuencia respaldar sus archivos. Comparte ejemplos de buenas prácticas de respaldo de datos como guardar el respaldo en un lugar seguro alejado de la computadora, hacerlo con cierta frecuencia y -según el tipo de información que quieren respaldar- considerar cifrar su disco duro o disco extraíble donde se va a almacenar los datos.

Parte 4 – Resetear& Reiniciar

5. Antes de comenzar con la parte práctica de la sesión, otro punto clave a abordar es la relación entre reiniciar y resetear, dos términos que pueden usarse como si fueran la misma cosa.

   Se refieren a procesos muy parecidos en un sentido más general, pero recuerda que "resetear" se utiliza para ilustrar el concepto de "empezar

de nuevo" en el contexto de esta sesión.

Reiniciar es una operación técnica que realizarán con sus computadoras durante el reseteo. Es importante que comprendan cómo funciona.

6. Profundizando en esta idea, presenta Tails y Ubuntu como sistemas operativos alternativos a Mac OS y Windows. En esta sesión, aprenderemos a utilizarlas a través de una usb.

Parte 5 – Sistema operativo vivo

7. Quizás te pregunten: ¿Cómo vamos a utilizar un nuevo sistema operativo en nuestras computadoras sin desinstalar la que tenemos ahora? ¿Qué pasará con nuestros datos? Aprovecha para explicar algunos términos que puedan ayudarlas a entender mejor cómo funciona Tails y Ubuntu.

Sistema vivo

Sistema operativo que corre directamente desde un disco extraíble como una USB o una tarjeta SD. Tails (Sistema Vivo Amnésico Incógnito // Amnesic Incognito Live System) es un ejemplo de sistema vivo; Ubuntu, otra variación de Linux, también puede ser configurado como sistema vivo.

Linux

Sistema operativo similar a Windows o Mac. La diferencia principal es que su código está abierto (opensource) y se distribuye de manera gratuita. Por ello, existen muchos tipos de adaptaciones de Linux disponibles. Debian, una de las distribuciones más conocidas es la base del desarrollo de Tails.

Dispositivo de arranque o "booteable"

Dispositivo o disco desde el cual una computadora carga archivos para poder arrancar. En la mayoría de los casos, el dispositivo booteable de una computadora es su disco duro interno. Desde aquí se carga el sistema operativo cuando prendes tu computadora. Aparte de los discos duros, los CDs, DVDs, tarjetas SD y USBs pueden ser también dispositivos de arranque.

BIOS

El Sistema Básico de Entrada-Salida (Basic Input/Output System) es el primer software que la mayoría de las computadoras corren cuando las prendes. Realizan pruebas en la máquina para asegurarse de que el sistema y el hardware esté funcionando correctamente y después inicia la secuencia de carga para el software (como el sistema operativo) disponible en el dispositivo booteable. El BIOS tiene una interfase, pero las usuarias no tienen acceso a ella al menos que sigan una serie de pasos determinados durante el arranque del sistema.

Secuencia de arranque

Puedes accederla a través del BIOS (o UEFI) durante el arranque de la computadora. Se trata de una lista de dispositivos booteables de la computadora y sirve para determinar el orden en que la computadora intentará cargar información. Generalmente, el disco duro interno es el primer dispositivo en la secuencia a cargar el sistema operativo. Sin embargo, se puede cambiar esta secuencia para cargar primero información de un disco externo/extraíble como un DVD o un USB.

Parte 6 – Sesión Práctica

8. Divide las participantes en al menos dos grupos. Dale a cada grupo una computadora para que intenten correr Ubuntu o Tails desde un usb vi-

vo. Si tienes suficientes USBs preconfigurados para entregar a cada participante, pueden practicar estos pasos por su cuenta.

9. Repasa cada paso desde tu computadora, proyectando la pantalla en la pared. Muéstrales el proceso de reiniciar sus computadoras y arrancar desde el sistema vivo Tails o Ubuntu durante la secuencia de arranque BIOS. Conforme vayas mostrando, asegúrate de explicar las diferencias entre Tails y Ubuntu para que el grupo pueda entender mejor cómo pueden ser utilizados para "empezar de vuelta".
10. Cierra la sesión conversando sobre cómo el hecho de resetear usando Tails o Ubuntu puede ser una opción para "pasar de hoja" cuando hayamos vivido un ataque de malware o perdido control. También procura comentar otros tipos de ataque donde ésto no es una solución, como tal, por ejemplo, en caso del acoso en línea.

Referencias

- https://tails.boum.org/ (Sin referencia en español)
- http://www.ubuntu-es.org