Guía de Facilitación de Ejercicios de Mesa (TTX) para Capacitación en Seguridad Digital

Propósito e Introducción

Esta guía está destinada a acompañar un conjunto de 11 escenarios de ejercicios de mesa (TTX), que pueden usarse para mejorar la capacitación en seguridad digital. Esta guía está destinada a ser usada por cualquier persona que desee diseñar y facilitar TTXs como método de capacitación en seguridad digital. En esta guía, encontrarás breves explicaciones sobre qué es un TTX, por qué los TTXs pueden ser suplementos valiosos para la capacitación en seguridad digital, y cómo se pueden desarrollar, planificar, y facilitar los TTXs.

Los 11 escenarios incluidos con esta guía fueron co-desarrollados por periodistas en Europa Central y Sudoriental como parte del proyecto Internews Journalist Security Fellowship (JSF) y fueron usados en capacitaciones realizadas por becaria(o)s de JSF en la región. Estos TTXs de ejemplo, incluyendo algunos con versiones traducidas a idiomas de Europa Central y Sudoriental y traducidos al Árabe y Español pueden ser accedidos en el enlace aquí.

Esta guía fue desarrollada específicamente con la seguridad digital para periodistas y salas de redacción en mente, pero también puede ser útil para planificar TTXs para otras audiencias objetivo.

¿Qué es un TTX? ¿Por qué son los TTX valiosos?

Un TTX es un método de capacitación basado en escenarios que a menudo toman la forma de discusión interactiva. Los TTX proveen una oportunidad para que quienes participan en la capacitación apliquen los nuevos conocimientos y habilidades adquiridos participando en una situación ficticia (denominada escenario o escena TTX) que se aproxima a una de la vida real. Los escenarios TTX pueden examinar un largo rango de situaciones de seguridad, como una redada a una oficina, una fuga de datos, un caso de doxxing, o una investigación sensible. Mientras que los métodos de capacitación más tradicionales pueden enfocarse en transferir ciertos conocimientos y habilidades técnicas, un TTX puede ayudar a::

- Proveer un espacio de bajo riesgo para que quienes participan en la capacitación **practiquen** preparándose y respondiendo a problemas de seguridad que puedan encontrar.
- Estimular el **debate** crítico sobre asuntos de seguridad digital y cómo abordarlos mejor en diferentes contextos y situaciones. Esto podría ser especialmente útil para participantes de la capacitación que trabajen en equipo regularmente para considerar su enfoque conjunto u organizacional sobre la seguridad
- **Evaluar** qué tan bien equipado está un individuo u organización para lidiar con problemas de seguridad que encuentren.

El objetivo de un TTX es identificar brechas individuales, organizacionales y comunitarias en conocimientos, fortalezas y limitaciones. Un TTX exitoso va más allá de herramientas y prácticas básicas, también destaca qué políticas o procedimientos pueden faltar o necesitar ser mejoradas.

Los TTX son más efectivos cuando se utilizan como suplemento para mejorar otros métodos de capacitación. Esto es porque el objetivo de los TTXs no es principalmente transferir nuevas habilidades y conocimiento sino inculcar y solidificar aún más el aprendizaje vía la práctica basada en escenario, la discusión y la evaluación.

Componentes de los documentos de escenario TTX

Cada una de las 11 escenas del TTX está basada libremente en la personalidad de Sara, que hemos descrito en esta guía. Cada escena incluye además los siguientes componentes:

- **Meta** - La meta general del escenario TTX.
- **Objetivos de Aprendizaje** - Opciones para objetivos generales de aprendizaje en los que enfocarse durante el TTX. Quienes facilitan probablemente se benefician al seleccionar solo unos pocos objetivos de aprendizaje en los que enfocarse.
- **Habilidades/Comportamientos para Entrenar Antes o Después del TTX** - Opciones para habilidades y cambios de comportamiento concretos y específicos para que el TTX se enfoque en inculcar en quienes participan de la capacitación. Quienes facilitan se beneficiarán al seleccionar solo unas pocas habilidades y comportamientos en los que enfocarse, y estos deben alinearse con la meta y objetivos de aprendizaje seleccionados.
- **Escenario** - Este es el escenario TTX real. Incluye lo siguiente:
    - **Antecedentes Introductorios e información contextual** al principio.
    - **Piezas adicionales de contexto** proporcionadas durante el escenario
    - **Preguntas e indicaciones** para que quienes participan debatan y respondan. Estas están marcadas con la letra P seguida de un número (p. Ej., P1, P2, P3, etc.).
    - Debajo de las preguntas e indicaciones hay algunas respuestas posibles. Estas no deben compartirse con quienes participan durante el TTX. Su objetivo es ayudar a quien facilita.
- Algunos escenarios incluyen **aportes** (se etiquetara como “Aportar”). Un aporte es una pieza nueva de información o un nuevo desarrollo insertado por quien facilita en el escenario TTX en tiempos específicos para avanzar o añadir complejidad. Un aporte podría

cambiar la narrativa del TTX y podría llamar a la acción o respuestas por parte de quienes participan.
- **Anexos** - Algunos escenarios (p. Ej., Escenario 3: Acoso y Doxxing) también incluyen anexos, que a menudo son usados para los aportes durante el escenario.

Desarrollar un escenario TTX

Once escenarios TTX fueron desarrollados bajo el proyecto JSF (enlazado aquí). Cualquiera puede modificarlos, para que se ajusten mejor a las necesidades de capacitación de su comunidad. Una(o) también puede crear propios desde cero. Si estás considerando revisar uno de los escenarios TTX o crear el tuyo propio, considera lo siguiente.

Los objetivos de aprendizaje deben establecerse al inicio de la fase de diseño, complementarse entre sí, seguir un orden lógico en términos de aprendizaje, priorizarse en base a su importancia, y conectarse con el objetivo general del TTX. Para simplificar el proceso de capacitación y facilitar la medición de éxito, conecta tus objetivos de aprendizaje a habilidades o conductas concretas en las que quienes participan deberán enfocarse durante el TTX. Idealmente, establecerás estos objetivos de aprendizaje y habilidades concretas basándose en las necesidades y nivel de habilidad de tus participantes. Puede que ya sepas esto si trabajas con una comunidad con la que tienes familiaridad. Alternativamente, puedes necesitar llevar a cabo una evaluación de necesidades inicial (quizás a través de entrevistas con informantes clave o una encuesta previa) para obtener esta información si tienes menor familiaridad con quienes participan.

Los escenarios deben asemejarse lo mejor posible a la vida real, pero en general no debes nombrar personas u organizaciones reales. Enfócate en situaciones reales, desafíos y experiencias. En casos excepcionales, puede ser apropiado usar ubicaciones reales, pero debes considerar los riesgos de seguridad y limitaciones potenciales al hacerlo. Listar ubicaciones reales podría, por ejemplo, significar que la gente pase demasiado tiempo investigando y recordando detalles sobre estos, y enfocarse menos en el escenario.

En términos de complejidad, el escenario no debe eclipsar o distraer del aprendizaje. Las opciones pueden ayudar a quienes participan a entender el impacto que tendrán sus decisiones, pero recuerda que añadir complejidad y opciones hace que sea más difícil construir un TTX y también hará todo el ejercicio mucho más largo.

También puedes usar el tiempo como un elemento de diseño durante tu escenario añadiendo tiempos a eventos que ocurren durante el TTX, hacer preguntas con temporalidad o utilizando flashbacks (retrospectivas) o flashforwards (proyecciones al futuro). En cualquier caso, debes tener claridad sobre el uso del tiempo al inicio del escenario y mantener la claridad durante la escena.

Dependiendo del nivel de habilidad de quien facilite y participantes, puedes considerar la inclusión de elementos técnicos dentro del TTX. Esto podría significar que quienes participan requieran usar una herramienta, software o proceso específicos para avanzar por el escenario. Si incluyes un elemento técnico, permite tiempo extra para completar estas tareas, y siempre ten un plan de respaldo en caso de problemas técnicos o haz que el componente técnico sea opcional para acomodar diferentes niveles de habilidad.

También puedes usar aportes en tu TTX. Los aportes pueden ser grandes o pequeños y pueden depender de quienes participan o ser independientes de ella(o)s. Generalmente, los aportes son usados en escenarios más largos, dada la cantidad de tiempo requerida. Los aportes son entregados por el facilitador y el momento es clave. Para integrar con éxito un aporte en una escena, se requieren recursos de quien facilita tanto antes como durante la facilitación del TTX. Tu uso de aportes debe coincidir con las necesidades para lograr los objetivos de aprendizaje predeterminados.

Planificar un TTX

Antes de empezar a planificar tu TTX, toma un momento para **pensar sobre tu público objetivo** y en cómo esto afectará los objetivos de aprendizaje. ¿Estás contactando a periodistas, gerentes de salas de prensa, personas en seguridad? Cada una(o) estará trabajando con información muy diferente y serán responsables de diferentes decisiones. Alternativamente, algunos TTX trabajan deliberadamente con una entidad más amplia - por ejemplo, una sala de redacción completa - para entender mejor cómo la gente se comunica y toma decisiones allí dentro. Podría ser que trabajes con participantes que tengan niveles de habilidad, conocimiento y experiencia en seguridad digital muy diferentes. Toma algo de tiempo para modificar el TTX para que aborde mejor sus necesidades específicas.

Una vez que tengas tu público destinatario, **planifica tus objetivos de aprendizaje y considera niveles de habilidad o comportamientos específicos en que les capacitarás**. Seleccionar habilidades concretas antes de tu capacitación es esencial para ayudarte a enfocar cómo capacitador(a), establecer metas de aprendizaje tangibles para quienes participan, y ayudar a establecer un punto de referencia para medir si la capacitación fue efectiva. Ve una lista de ejemplos de habilidades en la subsección de cada documento del TTX titulada “Habilidades/Comportamientos Para Entrenar Antes o Después del TTX.” Puede ser tentador cubrir tantos objetivos de aprendizaje como sea posible en un solo TTX, pero es más eficaz llevar a cabo una capacitación más limitada que cubra objetivos de aprendizaje específicos. Recuerda que tu público tiene un tiempo y capacidad de atención limitados.

Calcula cuánto tiempo necesitas para el TTX. Si bien las agencias gubernamentales o corporaciones crean TTX que duran varios días, tu público puede que tenga más presiones de tiempos. Se debe tomar en cuenta el trabajo, el cuidado de familiares y otros compromisos de vida de tus participantes. Por lo general, un TTX que tenga 4-6 preguntas o aportes puede tomar alrededor de 1 a 1.5 horas en completarse. Esto también depende mucho del tamaño de tu grupo. Los grupos más grandes, por lo general, toman más tiempo en completar un TTX. También necesitarás tomar en cuenta el tiempo para repasar y revisar los objetivos de aprendizaje y las habilidades y comportamientos concretos que te gustaría que quienes participan implementen después de la escena. Es posible que quienes participan necesiten un futuro entrenamiento o seguimiento para implementar habilidades y comportamientos de manera exitosa.

Toma en cuenta el espacio que tienes disponible para la actividad. Si se realiza en persona, es ideal facilitar el TTX en un espacio que permita la colaboración. Un cuarto con mesas y sillas cómodas probablemente sea más conducente para un TTX que una sala de conferencias. Es

posible que también necesites garantizar que haya Wi-Fi de calidad u otras comodidades tecnológicas, como un proyector. La accesibilidad del espacio también debe priorizarse, si es posible (p. Ej., acceso para sillas de ruedas, baños para la inclusión de género, opciones de transporte convenientes, etc).

Decide si habrá múltiples roles de facilitación y cuáles serán estos. Podría tener más sentido que quien facilita lidere el TTX, con otra(o)s ayudando en salas específicas o subtareas. Quienes facilitan también podrían desear ensayar cómo facilitar algunos elementos previamente.

Determina qué recursos necesitarás para el TTX. Es posible que desees crear una presentación de diapositivas, folletos, u otro tipo de materiales para mostrar el fondo de la escena, preguntas/indicaciones, y/o aportes. También es importante considerar los materiales que quienes participan puedan necesitar para tomar notas.

Facilitar un TTX

Facilitar un TTX difiere de liderar una capacitación tradicional en seguridad digital o una sesión de mejora de habilidades. En la capacitación tradicional en seguridad digital, quienes facilitan tienden a hablar mucho y se espera que compartan su conocimiento con quienes participan. Sin embargo, en una capacitación TTX la mayor parte de la conversación y trabajo sucede entre quienes participan, mientras debaten el escenario y toman decisiones. Quien facilita el TTX juega el papel de *responsable del proceso*, asegurando que el TTX se dé sin problemas y cumpla con sus metas. Quien facilita el TTX presenta los ejercicios, el contexto y los antecedentes; responde algunas preguntas básicas; y añade los aportes. Otras recomendaciones para la facilitación de un TTX incluyen:

- Asegura familiarizarte en profundidad con el TTX.
- Recordar cuál es la meta y los objetivos de aprendizaje del TTX y dirigir los debates para que quienes participan alcancen esos objetivos.
- Comunicar los roles y las expectativas claramente al principio y durante el TTX.
- Presta especial atención al reloj y asegúrate de respetar y maximizar el tiempo que tienes con quienes participan.
- Ten certeza de que el espacio es seguro y acogedor y que muchas personas puedan sentir que sus perspectivas son escuchadas y tomadas en cuenta.
- Cuando un(a) participante mencione una buena práctica, ¡destácala! Esto puede aumentar su confianza y fomentar una mayor participación.
- Si no sabes la respuesta a una pregunta, no tengas miedo de decirlo y comprométete a darle seguimiento después del TTX. Utiliza espacios comunitarios como la instancia Mattermost de Team CommUNITY para obtener respuestas a preguntas que quizás no puedas resolver por tu cuenta.
- Si es posible, recopila comentarios durante la participación y está lista(o) para hacer microajustes. Si planeas ser anfitrión(a) de múltiples iteraciones de un TTX, también puedes obtener comentarios al final de la sesión para comprender mejor cómo puedes seguir mejorando.

- Si el TTX empieza a ir en una dirección diferente a la originalmente esperada, ¡eso está ok! Sé flexible pero asegurate de que, en última instancia, se aborde los resultados del aprendizaje

Si deseas orientación más detallada, a continuación están las instrucciones paso por paso sugeridas para ayudarte con la facilitación.

1. Preséntate a ti misma(o) (y a cualquier co-facilitador(a)), explica tu(s) rol(es) y describe la meta general del TTX (p. Ej: hoy, veremos cómo una sala de redacción podría responder a un incidente de seguridad). Este es el tiempo ideal para también establecer reglas básicas como grupo.
2. Luego, describe en más detalle qué pasará durante el TTX. Explica que tiene como objetivo simular una situación ficticia que se aproxima a la vida real para comprender mejor nuestras respuestas y aquellas de nuestra comunidad más amplia.
3. Dependiendo del tamaño del grupo y su composición, podrías desear dividir a quienes participan en grupos de trabajo.
4. Presenta una introducción de la escena a quienes participan, incluyendo cualquier historia de trasfondo que sea necesaria.
5. Narra la escena, línea por línea, a medida que los participantes avanzan por el TTX. Está disponible para preguntas y para ayudar a quienes participan a resolver si se estancan.
6. Proporciona aportes como sea necesario.
7. Anima a quienes participan a relacionarse y responder a las indicaciones. Pídeles que tomen notas cuando sea relevante o de ayuda. Usa tus respuestas pre preparadas para ayudar si quienes participan están teniendo inconvenientes para comenzar.
8. Después que quienes participan completan el TTX, invítalos a discutir sus principales conclusiones sobre la experiencia y sus pensamientos sobre los TTX como método de capacitación. Este es un buen momento para grabar comentarios y considerar incorporar mejoras para futuras capacitaciones.
9. Una vez haya concluido el TTX, revisa si hay algún material final, seguimientos o resúmenes que deban compartirse con quienes participaron.

Apéndice 1: Antecedentes sobre Sara (una persona TTX)

Creamos una sola persona, Sara, para basar las experiencias en los escenarios TTX de ejemplo. Esto nos ayudó a añadir un sentido de consistencia a los TTX y dar un buen punto de partida para que la(o)s periodistas piensen sobre las amenazas y el contexto más amplio. Hemos incluido nuestra presentación de Sara a continuación la cual pueden usar quienes facilitan para preparar la escena y proveer antecedentes antes de lanzar uno de nuestros escenarios TTX de ejemplo.

Sara es una periodista de 41 años. Ha trabajado para varias organizaciones de noticia local e internacional por varios años en su país natal y países vecinos.

El año pasado, Sara empezó a trabajar con una organización de noticias de investigación llamada "Free Press Now" en su país de origen que informa frecuentemente sobre una variedad de asuntos políticos. Estos incluyen, presuntos abusos de los derechos humanos por parte del gobierno en curso, oficiales del gobierno corruptos, y políticas del gobierno que hacen la vida más difícil para minorías étnicas en el país.

Por sus informes veraces y confiables, Free Press Now se ha convertido en una fuente de información popular y confiable para la población local.

Luego de las elecciones nacionales hace 5 meses, el nuevo gobierno en poder ha empezado a limitar la libertad de prensa y la semana pasada las autoridades allanaron los hogares de tres periodistas prominentes en la capital. Recientemente, la casa de Sara también fue allanada, aunque quienes llevaron a cabo el allanamiento sólo se llevaron varios cuadernos.

Escenario 1: Dispositivo Perdido

Creado por becarios del JSF

Meta

Ayudar a la(o)s participantes a planificar y responder a una situación en la que uno o más de sus dispositivos, que pueden contener información confidencial, se pierdan.

Objetivos de Aprendizaje

- Identificar enfoques para garantizar la comunicación segura entre periodistas y sus fuentes humanas.
- Generar conciencia sobre los riesgos de perder un dispositivo como un teléfono o una computadora.
- Entender las mejores prácticas sobre la protección y seguridad de dispositivos.
- Compartir buenos métodos para la incorporación y desvinculación de personal de la organización, especialmente en lo relacionado a la seguridad de los dispositivos.

Habilidades/Comportamientos a Entrenar Antes o Después del TTX

- Instalar, configurar y usar Signal (u otra aplicación de mensajería segura)
- Configurar y usar un servicio de mensajería con cifrado de extremo a extremo alternativo (como WhatsApp o el Chat Secreto de Facebook Messenger)
- Instalar, configurar y usar Mailvelope (u otra alternativa para cifrar email)
- Cifrar un dispositivo móvil (configurar una contraseña)
- Configurar contraseñas para aplicaciones individuales en un dispositivo móvil
- Hacer y cifrar copias de seguridad de los datos en un dispositivo móvil (usando servicios en la nube o disco duro externo).

Escenario

Una fuente desconocida contacta a Sara por Facebook Messenger, declarando que tiene información sensible que quiere compartir con ella. El archivo que quiere compartir contiene información sobre las finanzas del actual Ministro de Defensa.

Queriendo mantener segura a la fuente, a Sara le gustaría persuadirlo para que transfiera la información a través de un servicio de mensajería que esté cifrado de extremo a extremo.

1 - ¿Cómo puede Sara explicar el concepto de cifrado de extremo a extremo para convencer a la fuente de su importancia?

- Nadie – ni siquiera la compañía que opera el servicio de mensajería – tendrá acceso a los contenidos del mensaje. El contenido del mensaje no será almacenado sin cifrar en los servidores de la compañía tampoco.
- Las fuerzas del orden no pueden acceder a él desde el proveedor de chat
- Si un(a) atacante logra hackear la cuenta que fue usada para enviar el mensaje, no podrán acceder al contenido del mensaje tampoco (a menos que hubieran copias de seguridad sin cifrar)

Para garantizar que su comunicación sea segura en lo adelante, ¿qué formas de comunicación digital debe considerar Sara para usar con esta fuente?

- Los servicios de mensajería con cifrados de extremo a extremo y mensajes temporales
- Correo electrónico cifrado

La fuente está satisfecha con que Sara se enfoque en asegurar que su comunicación sea segura, pero la fuente aún no está segura de qué método priorizar. Él le pide a Sara consejos sobre aplicaciones de mensajería como Signal, Telegram y Facebook Messenger, como también sobre su correo electrónico.

3 - (Elección) - Desde una perspectiva de seguridad digital, ¿qué factores se deben considerar al seleccionar y usar diferentes aplicaciones de mensajería?

- Números de teléfono: la mayoría de los servicios de mensajería con cifrado de extremo a extremo requieren números de teléfono, y en muchos lugares los números de teléfono deben estar registrados, para que el gobierno sepa cual persona está detrás de qué número. Esto significa que, si el gobierno alguna vez revisara el teléfono de Sara o el de la fuente, podrían darse cuenta de que se enviaban mensajes, incluso si usaban seudónimos o mensajes temporales (la única mitigación sería eliminar los nombres de los contactos, servicios de mensajería, e idealmente limpiar el teléfono)
- Conversaciones secretas: Facebook Messenger y Telegram ofrecen dos modos, de los cuales solo uno es cifrado de extremo a extremo. Este método suele llamarse chat secreto o algo similar, aunque con frecuencia está oculto en las configuraciones.
- Mensajes temporales: casi todos los servicios de mensajería modernos tienen una función de mensajes que desaparecen, aunque solo en algunos está disponible en el modo chat secreto.
- Eliminar chats: esto es muy simple, pero es importante reconocer que algunos servicios de mensajería solo archivan, en lugar de eliminar, chats.
- Conciencia sobre las capturas de pantalla: cualquier parte malintencionada en la conversación podría simplemente hacer una captura de pantalla o – si las funciones del

servicio de mensajería no lo permiten – simplemente tomar una foto de la pantalla del teléfono
- Verificación en dos pasos (2FV): un atacante podría apoderarse de una cuenta de mensajería tomando el número de teléfono que se utilizó para registrar la cuenta y reenviar el SMS de verificación a este. Esto les permite hacerse pasar por quien es dueña(o) de la cuenta, aunque normalmente no les da acceso al historial de mensajes. La mayoría de los servicios de mensajes ahora tienen la opción de requerir una contraseña adicional al código SMS: esto significa que, aunque un(a) atacante lograse hacerse con el número de teléfono, no podría acceder fácilmente a la cuenta.
- Códigos de acceso o frase de contraseña seguras para loguearse en el dispositivo (teléfono) mismo

4 - (Elección) Desde una perspectiva de seguridad digital, ¿qué factores se deben considerar al comunicarse por correo electrónico?

- La fuente debe crear una nueva dirección de correo electrónico solo para comunicarse con Sara
- El nuevo email debe tener una contraseña única y segura y una sólida autenticación de dos factores
- La fuente también debe estar pendiente a los ataques de phishing y usar tecnologías que ayuden a mitigarlos, como llaves de seguridad físicas o gestores de contraseña con autorelleno.
- Idealmente, la fuente y Sara deben comunicarse por PGP, por ejemplo, usando Mailvelope. Esto significa que, incluso si las cuentas fueran comprometidas de alguna manera, un atacante aún no podría leer el contenido de los mensajes sin su llave de PGP

La fuente le envía el archivo de forma segura a Sara y ella lo ve en su celular. Está contenta de tener esa información y sale con sus amistades a celebrar. Mientras está en la fiesta, pierde su teléfono y se da cuenta de que olvidó proteger su teléfono con contraseña.

Sursa îi trimite fișierul în siguranță Sarei, iar aceasta îl vizualizează pe telefonul mobil. Ea este fericită că are această informație și iese cu prietenii ei pentru a sărbători. În timp ce se afla la o petrecere, Sara își pierde telefonul și își dă seama că are o parolă foarte simplă (1111) pe el.

5 - ¿Qué le podría pasar al teléfono de Sara y la información que contiene?

- Cualquiera que encuentre el teléfono puede acceder a información sensible si descubren dónde está.
- Cualquiera que encuentre el telefono podria enviar mensajes a los contactos de Sara y pretender ser ella
- Cualquiera que vea la información en el telefono podria poner en peligro la identidad y seguridad de los contactos de Sara o recopilar información que pueda ser útil para ingeniería social
- Seriamente Sara podría perder su credibilidad como periodista

6 - ¿Qué puede hacer Sara para limitar el impacto en su seguridad digital?

- Ella puede limpiar su teléfono remotamente, si ha configurado esta función.
- Ella puede iniciar sesión en su email y cuentas de redes sociales en sus otros dispositivos, cambiar la contraseña, y, si es posible, hacer clic en el enlace “cerrar sesion en todos los dispositivos logueados”

7 - ¿Cuáles son los pros y los contras de decirle a la fuente que perdió el teléfono?

- Discusión sin una respuesta correcta exacta.

¡Buenas noticias! Un amigo de Sara que estuvo con ella en la fiesta encontró el teléfono en su abrigo. La llamó y le devolvió el teléfono al día siguiente.

8 - Ahora que Sara tiene su teléfono de vuelta, ¿qué pasos puede tomar para proteger digitalmente su dispositivo en caso de que lo pierda otra vez en el futuro?

- Considerar usar desbloqueo biométrico en ocasiones. Tiene ventajas (nadie puede mirar por encima del hombro de Sara mientras pone su contraseña, y tampoco será captada por cámaras CCTV) y desventajas (es más fácil coaccionar a Sara a desbloquear su dispositivo).
- Usar contraseñas más largas para desbloquear el teléfono. Evita los patrones (como esos que conectan puntos), ya que estos pueden ser fácilmente identificados por una persona que esté mirando, una cámara, o marcas en la pantalla
- Bloquear aplicaciones (como los servicios de mensajería) con una contraseña adicional también, si Sara está preocupada de que su teléfono pueda ser compartido/ pasado de mano en mano a veces.
- Configurar apps que puedan rastrear, localizar, y limpiar dispositivos de manera remota.

9 - Desde una perspectiva organizacional, ¿Cómo se ve un buen proceso de incorporación para un(a) nueva(o) miembro del personal para proteger sus dispositivos, como celulares y computadoras?

- Asegurarse de que todo el personal, sin importar su cargo, pase por un proceso de incorporación y comprenda su importancia.
- Las organizaciones deben enumerar claramente las expectativas del personal respecto a seguir las prácticas de seguridad digital de la organización.
- Identificar los pasos a seguir cuando la seguridad pueda estar comprometida (como si un teléfono es robado o una contraseña es hackeada).
- Debe brindarse soporte de TI a todo el personal que lo necesite.

Escenario 2: Seguridad Organizacional y Conciencia sobre los Enlaces

Creado por becarios del JSF

Meta

Ayudar a la(o)s participantes a garantizar que exista un alto nivel de conciencia y buenas prácticas de seguridad digital entre su organización, colegas de trabajo y/o periodistas independientes.

Objetivos de Aprendizaje

- En teoría, comprender el concepto de seguridad digital como un proceso continuo, no como un objetivo final.
- Hablar, enseñar y persuadir a otra(o)s sobre la importancia de la seguridad digital
- En práctica, debatir opciones para comunicarte de manera segura con tu teléfono
- Garantizar las mejores prácticas en el manejo seguro de archivos.
- Conciencia sobre la configuración de cuentas para computadoras en red.
- Comprender la importancia del modelado de amenazas.

Habilidades/Comportamientos A Entrenar Antes o Después del TTX

- Configurar y mantener permisos en plataformas colaborativas (p. Ej., Google Drive)
- (Si es posible, ya que algunas de estas funcionalidades solo están disponibles en plataformas empresariales)
- Ver los registros de acceso en plataformas como Google Drive
- Configurar y usar autenticación de dos factores, idealmente con llave de seguridad física o con mecanismos similares resistentes al phishing
- Políticas de buena contraseña (usar contraseñas únicas, usar contraseñas largas, usar frases de contraseña)
- Cifrar documentos (usando Mailvelope, etc.)
- Instalar, configurar y usar Signal (u otra aplicacion de mensajeria segura)
- Usar funciones avanzadas dentro de la aplicación de mensajería (p. Ej., eliminación programada de mensajes)
- Instalar, configurar y usar Mailvelope (u otra opción para cifrar email)
- Trabajar de manera segura con archivos y documentos de fuentes sensibles

Escenario

Sara está reuniendo a un equipo de periodistas para investigar la corrupción concerniente a la contratación pública durante el Covid-19 realizada por el Ministerio de Salud. No todos la(o)s periodistas en el equipo tienen el mismo nivel de habilidades digitales/conocimientos y prácticas de seguridad. Sara sabe que uno de los miembros de su equipo es muy malo con la protección de archivos.

Sara sabe que algún miembro de su equipo tiene prácticas descuidadas relacionadas a la protección de archivos.

P1 - ¿Cómo puede Sara alentar a sus colegas a mejorar sus enfoques para la seguridad digital? ¿Qué debe hacer Sara para garantizar las prácticas de seguridad digital al organizar un equipo colaborativo?

- Explicar por qué es importante tener buena seguridad digital: esto puede incluir hablar sobre cómo una seguridad digital pobre podría obstaculizar la carrera de un(a) periodista, cómo las fuentes y colegas podrían confiar más en ti si tienes buena seguridad digital, y la necesidad de proteger a la gente a nuestro alrededor.
- Debatir cuáles dispositivos están usando, cómo están protegiendo sus cuentas, cómo almacenan e intercambian archivos, cómo acceden a su red de trabajo (están usando sus propios dispositivos o trabajan en las computadoras de la compañía), si usan autenticación de dos factores para asegurar cuentas de usuaria(o)s y su disciplina en contraseñas (están reutilizando contraseñas, usan administradores de contraseña).
- Decidir cómo debe comunicarse el equipo, almacenar y acceder a los archivos. El segundo paso es para garantizar que toda(o)s sigan el mismo protocolo relacionado a las actividades mencionadas previamente.
- Considerar capacitar al equipo usando los protocolos recién establecidos. Después de establecer reglas, el equipo debe realizar un ensayo, probando realmente las nuevas formas de comunicación y ver si hay peculiaridades en el proceso que deban alisarse

P2 - ¿Cómo Sara y su equipo almacenarán y compartirán archivos de audio y documentos de las fuentes?

- Limitar quién accede a varios archivos y carpetas, usar con cuidado las configuraciones de compartido en lugares como Google Drive
- Disuadir a las personas de llevar archivos y documentos fuera de su entorno de trabajo (memorias USB, adjuntos de email…) que podrían expandir la plataforma de ataque e incrementar el riesgo de fugas/hackeos.
- Pedirle al equipo que solo usen las computadoras del trabajo para acceder a archivos del trabajo
- Limitar qué se puede instalar en las computadoras del trabajo, garantizar que siempre tengan contraseñas fuertes y software actualizado.

P3 - ¿Cómo Sara y su equipo garantizarán que se comuniquen de forma segura?

Al incorporar el equipo completo en la misma plataforma y asegurarse de que toda(o)s están cómoda(o)s con su uso, Sara puede ayudar a su equipo a establecer una forma de comunicación segura y protegida entre sí.

Considera:

- Mover la mayoría de las conversaciones a Signal, con mensajes que desaparecen y copiar mensajes que necesiten ser archivados
- Usar PGP en email
- Crear reglas de seguridad de cuentas fuertes (contraseñas únicas, 2FA) para email

Dos semanas antes de la publicación de su informe, Sara recibe una llamada de la principal fuente gubernamental en esta investigación. Sara conoce bien y confía en la fuente. En la llamada, la fuente simplemente dice "El Gobierno lo sabe, hubo una fuga" y cuelga.

P4 - Desde una perspectiva de seguridad digital ¿cuáles son algunos de los primeros pasos que Sara debería tomar para responder a una posible fuga de información?

- Pedir a toda(o)s en su equipo cambiar contraseñas, solo en caso de que un(a) atacante obtenga la contraseña a una de sus cuentas.
- Considerar el hecho de que el gobierno, no necesariamente necesita entrar en su sala de redacción; es posible que se hayan enterado sobre la fuga al, por ejemplo, investigar qué empleada(o)s del gobierno estaban imprimiendo qué.
- Hacer una pequeña investigación en la sala de redacción: revisar si toda(o)s seguían los protocolos, quién tenía acceso a los archivos y a la pieza de información que se filtró y qué exactamente se filtró en primer lugar. A través del uso de control de acceso y control de versiones puedes tener una forma más fácil de rastrear el acceso a piezas de datos individuales en las que estás trabajando.
- Pensar si necesitarás acelerar la publicación.

Sara se da cuenta que la filtración vino desde dentro de su organización. Una diseñadora tuvo acceso al Google Drive compartido de la organización. Sara se enteró de esto al revisar el control de acceso de Google Drive, dándose cuenta que por la naturaleza de su trabajo, el equipo de diseño tenía acceso a todo en la red, y vio que una diseñadora había compartido accidentalmente un documento con una de sus clientes freelance que trabaja para el gobierno, en lugar de una amiga que tenía el mismo apellido.

P5 - ¿Qué podría haber hecho diferente el equipo de Sara en esta situación?

- Sara debería establecer protocolos seguros que apliquen solo a su equipo de investigación. Ella debe garantizar que haya un sistema de permisos claro y que sea seguido en práctica.

- El equipo debería trabajar con diseñadora(e)s de una manera que solo tengan información cuando sea necesario: no se le debería dar ningún detalle secreto o sensible a menos que sea estrictamente necesario para la publicación.
- Sara debería considerar también la seguridad y la privacidad como un proceso y no un estado; es algo que se debe iterar constantemente.

Escenario 3: Acoso y Doxing

Creado por becarios del JSF

Meta

Ayudar a la(o)s participantes a conceptualizar cómo prepararse y responder mejor al doxing y el acoso en línea.

Objetivos de Aprendizaje

- Identificar métodos y medidas de mitigación para periodistas que lidian con acoso y doxing en las redes sociales.
- Entender como la información en redes sociales puede recopilarse y usarse contra periodistas y personal de redacción.
- Explorar la relación entre el género y el acoso, y sus implicaciones de seguridad.
- Discutir las consideraciones sobre cómo una organización de medios puede establecer procedimientos y prácticas para proteger el personal y contratistas que son objetivo de acoso y doxing.
- Considerar planes de contingencia para periodistas que no tienen apoyo de una sala de redacción (ej. Independientes, personal externo).
- Contar historias sobre seguridad y persuadir a otras personas, cómo podemos hablarle a las personas que tradicionalmente no enfrentan acoso de que es un problema importante que requiere acción y apoyo organizacional coordinado.
- Seguridad organizacional: establecer políticas dentro de las organizaciones, entender las maneras en que cada organización puede apoyar mejor a periodistas que estén enfrentando ataques de acoso[1]

Habilidades/Comportamientos A Entrenar Antes o Después del TTX

- Administrar y actualizar las configuraciones de privacidad en las principales plataformas de redes sociales
- Usar herramientas de seguridad en las principales plataformas de redes sociales, tales como reportar y bloquear. Esto incluye entender cómo usar tales mecanismos y qué hacen exactamente
- Establecer y usar autenticación de dos factores, idealmente con claves de seguridad física o mecanismos similares resistentes al phishing

[1]En la mayoría de las capacitaciones, esto sería un objetivo de aprendizaje. Si estás liderando una sesión con quienes gestionan medios u otras personas en toma de decisión y es posible medir los resultados organizacionales, también podrías ejecutar esto como una habilidad.

Escenario

Sara está trabajando en una nueva pieza sobre minorías étnicas en su país y como las políticas del gobierno están llevando a un aumento en la marginalización de estos grupos. En las últimas semanas, Sara ha visto un aumento en los comentarios en sus cuentas de redes sociales donde también comparte su trabajo. También está empezando a recibir comentarios de odio y denigrantes, hechos por diferentes Trolls en línea que la atacan directamente a ella.

P1 - ¿Qué pasos puede tomar Sara para bloquear y reportar a las personas que hacen estos comentarios?

- Ella puede contactar a grandes empresas de redes sociales (directamente o tal vez a través de su organización) para reportar el acoso a gran escala.
- Deshabilitar las publicaciones y respuestas en su perfil
- Ser más selectiva con quién puede encontrarla en las redes sociales
- Elegir no ser etiquetada en las redes sociales

Esforzándose por bloquear y reportar a algunos de los principales instigadores ha molestado al grupo de trolls, llevando a un incremento del contenido de odio contra Sara. Algunos comentarios también sugieren amenazas y violencia hacia ella, ya sea directa o indirectamente.

P2 - ¿De qué maneras Sara puede investigar esta agresión en su contra para determinar si es parte de una campaña más grande, más coordinada o algo más orgánico?

- Puede investigar la situación por sí misma, como también pedir apoyo a colegas en la investigación
- Puede revisar si los trolls usan el mismo lenguaje, palabras clave, o hashtags. Si lo hacen, es más probable que sea una campaña coordinada.
- Depende de la plataforma. En Instagram, hay variedad de opciones para ver información sobre cuentas específicas - cuándo fue creada, cómo la gente la usa, cuán frecuente ha cambiado su nombre, etc.
- Revisar si está amplificada por algún medio
- Ver el horario de publicación más común

Sara le dice a sus colegas sobre las publicaciones, pero la mayoría de los miembros masculinos del equipo, incluido el editor, le dicen que no se preocupe y que el problema se irá por sí solo. Ella está estresada y siente que su equipo no escucha ni entiende el problema.

P3 - En lugar de decirle a Sara que no se preocupe, ¿De qué maneras, su equipo y organización pueden apoyar a Sara, especialmente en términos de su presencia en línea y seguridad digital?

- Ayudar a llevar a cabo una evaluación completa de la situación

- Revisar junto con Sara sus prácticas de seguridad digital y medidas de protección existentes, y ayudar a mejorar la situación si es necesario
- Obtener práctica y experiencia compartida por otra(o)s en la organización
- Permitir a las personas en quien confías administrar y revisar tu cuenta para que no esté expuesta directamente a esas palabras y amenazas pero aun así poder mantener una presencia
- La org puede ayudar a buscar patrones en los acosos
- Rastrear cómo los acosos afectan las publicaciones de la organización en lugar de solo las de Sara
- Escalar esto al equipo de seguridad y ayudar con la investigación

Un día, las fotos personales de Sara son filtradas en línea por uno de los trolls. Las fotos, que ella publicó en redes sociales años atrás, son personales y en algunos casos incluyen información sensible.

Introducir - Comparte entre 1 y 4 fotos con la(o)s participantes. (Las fotos se pueden encontrar en el anexo de este documento).

Las fotos de ejemplo incluyen:

- Sara y su perro caminando fuera de su casa
- Sara fumando un cigarrillo de marihuana
- Sara y un grupo de sus amistades más cercanas de vacaciones
- Sara trabajando en su sala de redacción

Discute con el grupo de participantes por qué cada una de estas fotos puede ser sensible.

P4 - ¿De qué maneras podría alguien haber accedido a la información en línea de Sara, como las publicaciones antiguas en las redes sociales?

- Las amistades de Sara publicaron fotos con ajustes de privacidad pobres
- Las cuentas de Sara fueron allanadas
- Una de las conexiones en la red social de Sara pudo haber guardado la foto para compartirla luego
- Las fotos de la red social de Sara pudieron haber sido indexadas por un motor de búsqueda

P5 - ¿Qué pasos puede tomar Sara para intentar prevenir que se filtre más información sobre ella en línea?

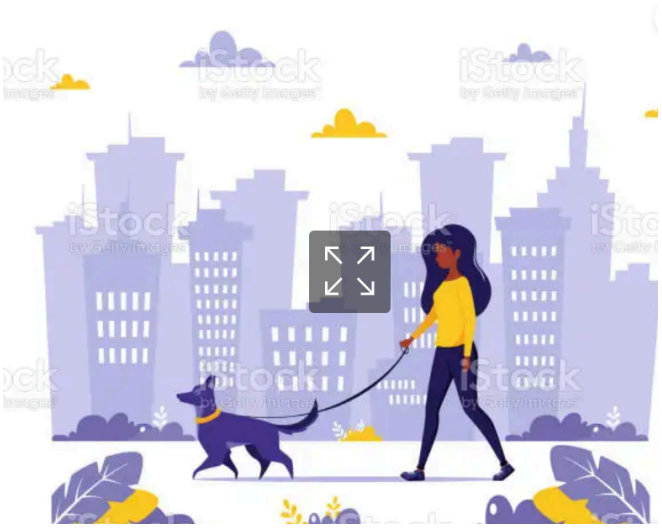
- Eliminar fotos antiguas
- Eliminar cuenta
- Bloquear cuenta
- Subir fotos nuevas pero que filtren poca información sobre ella
- Conseguir un informe de una empresa de redes sociales que resuma todos los datos que tienen sobre ella.

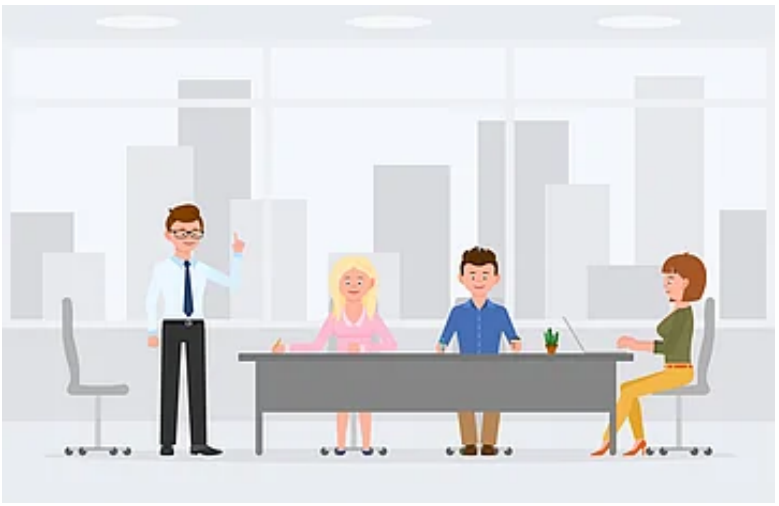
- Reportar las fotos que han sido publicadas recientemente / reportar las cuentas que las han estado publicando
- Continuar publicando contenido de trabajo, incluso si publicas menos contenido personal. Si dejas el internet, los trolls habrán ganado
- Hacer captura de pantalla de las publicaciones, documentarlas tanto como sea posible. Registrar los aliases en línea de los trolls

P6 - ¿Qué pasos podrían haber tomado Sara y su organización para prevenir que esta información sea recopilada y filtrada en línea, especialmente en términos de seguridad digital?

- Crear un grupo de amistades cercanas que sean las únicas que vean fotos y publicaciones personales en las redes sociales
- No publicar información sensible (como las fotos con el cigarrillo de marihuana)
- No publicar fotos que revelen información personal como la ubicación.
- Abrir cuentas empresariales para que así tenga una presencia en línea que no esté relacionada a su vida personal
- Políticas de contraseña segura y 2FA para las cuentas de redes sociales

Anexo 1: Introduzca las Fotos de Ejemplo





Escenario 4: Entrada de las autoridades a la sala de redacción

Creado por becarios del JSF

Meta

Ayudar a la(o)s participantes en respuestas teóricas y prácticas a la entrada de las autoridades en su sala de redacción

Objetivos de Aprendizaje

- Asegurar que existan planes de comunicación y componentes técnicos de respaldo en caso de que el acceso a una sala de redacción o dispositivo personal ya no sea posible.
- Entender las mejores prácticas en cuanto a asegurar dispositivos digitales dentro de una sala de redacción u organización.
- Identificar formas de proteger diferentes archivos en un dispositivo digital, como una computadora o un celular.
- Planificar para la información comprometida en respuesta a la entrada y allanamiento de las autoridades en una sala de redacción.
- Explorar conceptos sobre modelado de amenazas y pre planeamiento para individuos y organizaciones

Habilidades/Comportamientos a Entrenar Antes o Después del TTX

- Usar una herramienta como VeraCrypt o similar para cifrar los datos en discos duros y discos externos
- Modelado de amenaza, específicamente en términos de lidiar con las autoridades y redadas en la oficina: como evaluar riesgos, prepararse para uno e informar después de uno
- Seguridad organizacional y comunitaria, específicamente cómo trabajar con editora(e)s, gerenta(e)s, y abogada(o)s durante situaciones de alto estrés e identificar qué pregunta escalar a cual persona
- Usar las configuraciones dentro de Microsoft Office y Google Drive para ver cuáles archivos han sido accedidos y cuándo
- (Avanzado) Si la organización revisa los registros a través de una cuenta premium de Google Drive o suscripción de O365, acceder y trabajar con esos registros
- Ver los historiales de búsqueda y acceso de archivos en los principales navegadores web y sistemas operativos

Escenario

Sara trabaja en una sala de redacción de unas 20 personas. Es un lunes por la mañana atareado, con 15 periodistas y otra(o)s empleada(o)s trabajando en la sala de redacción, con otra(o)s 5 colegas trabajando remotamente.

A las 10 am, aproximadamente 50 oficiales de policía llegan a la sala de redacción. Tienen una orden judicial que le muestran al editor, y luego fuerzan la entrada mientras al mismo tiempo exigen que toda(o)s la(o)s periodistas y el personal salgan inmediatamente.

Sara y sus colegas se reúnen fuera y discuten formas de cómo mantener su organización de medios funcionando de manera segura y protegida.

P1 - ¿Cuáles son algunas prioridades en una situación como esta?

- Ponerse en contacto con un(a) abogada(o) para consultar cualquier paso a dar
- Contactar a colegas que trabajan remotamente
- Auditar quienes tienen su teléfono consigo y cuales fueron dejados atrás

P2 - ¿Cuáles son algunas de las formas en que Sara y sus colegas se pueden comunicar de forma segura durante este tiempo?

- Crear un chat grupal en WhatsApp/Signal
- Podría ser buena idea comunicarse a través de números personales, en lugar de los de trabajo. De lo contrario, el chat podría estar sincronizado a dispositivos que aún están en la oficina.

P3 - ¿Cómo deberían Sara y sus colegas administrar las cuentas en línea de la organización, como los sitios web y cuentas de redes sociales?

- Cambiar las contraseñas inmediatamente
- Si es posible cerrar sesión remotamente de los dispositivos que aún están en la oficina, hacerlo así pero consultar con abogados primero para que no se considere manipulación de evidencia (podría depender mucho de la ubicación / jurisdicción)
- Consultar con abogados antes de publicar sobre la redada policial

Sara recuerda que cuando estaba saliendo de la sala de redacción, vio a la policía empezar a poner las computadoras, dispositivos y papeles en bolsas. Sara pudo salir con su teléfono, pero su laptop se quedó en la sala de redacción. El grupo de colegas rápidamente evalúa qué información posiblemente pueda obtener la policía.

P4 - ¿Cómo deberían protegerse los dispositivos en la sala de redacción?

- Computadoras bloqueadas con contraseñas fuertes
- ¿Bloqueos de pantalla que se activan después de poco tiempo?
- Memorias USB y discos duros externos encriptados

Durante su discusión fuera de la oficina, el editor revela que olvidaron bloquear sus computadoras cuando salían de la oficina.

P5 ¿De qué maneras puede la sala de redacción evaluar inmediatamente el impacto de la redada por parte de las autoridades?

- Ver cuáles archivos en papel, si es que habían, fueron llevados o reorganizados (si los archivos fueron reorganizados, significa que la policía podría haberlos fotografiado)
- Las computadoras generalmente tienen un historial de búsqueda / archivos accedidos/ navegación, revisa estos también. Puedes ver los archivos recientes en Microsoft Word, y algún historial en navegadores si usas Google Docs. Si el historial de archivos ha sido eliminado, eso también significa que alguien ha intentado limpiar las señales
- Es poco probable que se haya instalado algún malware durante la redada pero si te preocupas por esto, consulta con un profesional que se especialice en análisis forense de malware

P6 - ¿Cómo debería la organización asegurarse de que no son puestos en mayor riesgo por esta redada policial?

- Cambiar las contraseñas, por si acaso
- Hablar con una abogada(o) sobre a qué se le permitió tener acceso y a qué no a la policía durante la redada
- Si estuvieron usando nombres clave o seudónimos para su investigación, rotar estos

Una semanas después, la/el editor(a) de la sala de redacción llama a toda(o)s la(o)s periodistas y el personal. Quieren entender cualquier amenaza similar que la sala de redacción pueda enfrentar en el futuro.

P7 - En términos de modelado de amenaza y seguridad digital, ¿a quienes identifican los individuos y organizaciones como amenazas que podrían enfrentar?

- Haz las preguntas estándar sobre modelado de amenazas: qué información tienen, a quién le interesa acceder a ella, y cuáles serían las consecuencias si las personas adversarias tuvieran éxito
- Al listar las personas adversarias, piensa tanto en el motivo (qué les gustaría hacer y por qué) como en las capacidades (¿qué son capaces de hacer realmente?¿qué medios técnicos, legales, organizacionales, y financieros tienen?

Escenario 5: Entrada de las Autoridades a la Casa de un(a) Periodista

Creado por becarios del JSF

Meta

Brindar a la(o)s periodistas las habilidades técnicas y teóricas para garantizar la mejor seguridad digital posible en su entorno doméstico

Objetivos de Aprendizaje

- Entender cómo proteger los dispositivos digitales que se encuentran en casa
- Aplicar protección en torno a las libretas de papel
- Iniciar la eliminación remota de archivos y las ventajas y desventajas de hacerlo
- Limitar el acceso a la información que ha sido comprometida
- Prepararse para la entrada de autoridades a la casa de periodistas
- Hacer que quienes participan piensen un poco sobre la seguridad organizacional y comunitaria, específicamente cómo trabajar con editora(e)s, administradora(e)s y abogada(o)s durante situaciones de alto estrés e identificar cuál pregunta escalar a qué persona

Habilidades/Comportamientos a Entrenar Antes o Después del TTX

- Usar una herramienta como VeraCrypt o similar para cifrar datos en discos duros y discos externos
- Modelado de amenaza, específicamente en términos de lidiar con autoridades y redadas en casa: cómo evaluar riesgos, prepararse para uno, e informar después de uno
- Activar herramientas como Find My de Apple o Find de Android/Samsung que pueden ser usadas para bloquear o eliminar dispositivos remotamente
- Usar las configuraciones en Microsoft Office y Google Drive para ver a qué archivos se ha accedido recientemente y cuándo
- (Avanzado) Si la organización tiene registro de accesos detallado con una cuenta premium de Google Drive o suscripción a O365, acceder y trabajar con tales registros
- Revisar los historiales de búsqueda y acceso a archivos en navegadores web y sistemas operativos populares

Escenario

Después de unas elecciones nacionales 5 meses atrás, el nuevo gobierno en poder ha empezado dirigiendo a las autoridades a limitar las libertades de prensa y las autoridades allanaron las casas de tres periodistas prominentes en la capital. En respuesta, Sara y alguna(o)s colegas se reunieron y discutieron sobre formas de protegerse a sí misma(o)s y a su información si se enfrentaran a un escenario similar.

P1 - ¿Cuáles cosas debe considerar un periodista al decidir almacenar información en su casa?

- Almacenar los dispositivos en un lugar seguro en casa
- Cifrar y proteger con contraseña todos los dispositivos
- No incluir información sensible sobre la fuente tal como nombres en documentos
- Mantener un inventario de qué información se guarda y donde (¡pero mantener esto asegurado también!)
- Información no digital: ten en cuenta las copias físicas
- Si es posible, no mantener nada sensible en casa, considera hacer esto
- Seguir las leyes locales como también las políticas de la organización
- Estar consciente de las ramificaciones legales de almacenar información sensible en casa en lugar de una oficina
- Piensa en quién tiene acceso a tu casa y dispositivos

P2 (Opcional) - ¿Cuáles son algunas de las mejores prácticas sobre almacenar libretas de papel en casa?

- Considerar destruir lo que no necesitas
- No mantener todas las notas en un mismo lugar, menos información para acceder fácilmente.
- Esconder los cuadernos
- Caja fuerte, candado y llave, ¡mantenlos seguros!
- ¿Qué nivel de información sensible debería mantenerse en casa?
- Usar acrónimos, abreviaturas, que solo tengan sentido para ti

P3 - ¿Qué medidas pueden tomarse para proteger lo mejor posible dispositivos electrónicos (computadoras, discos duros, memorias USB, etc.)?

- Cifrado
- Protección con contraseña
- Respaldar los datos fuera del sitio
- Considera deshacerte de forma segura de los dispositivos más viejos, especialmente aquellos que ya no se usan

Hoy, Sara salió de su casa a las 9am para tomar un café y comprar provisiones. Cuando regresó una hora más tarde, la puerta de su apartamento estaba abierta. Sara entró a su apartamento y encontró dos hombres revisando su escritorio y su dormitorio. Uno de los hombres estaba leyendo los cuadernos de Sara mientras el otro sostenía una bolsa con la laptop de Sara dentro. Ella ve que en su escritorio faltan las memorias USB y discos duros externos. Los dos hombres visten ropa civil, pero Sara asume que trabajan para el gobierno de alguna manera.

***Opción 1** - Sara habla brevemente con los dos hombres y puede salir de su casa a salvo. Camina a casa de un amiga(o) cerca.*

P4 (opcional) - Sabiendo que parte de su información, especialmente de su libreta de papel, ha sido comprometida, ¿a quién debe informar Sara sobre este incidente?

- Informar al editor y a la(o)s abogada(o)s de la sala de redacción
- Antes de contactar cualquier fuente que pudiera haber sido mencionada en el cuaderno, habla con el/la editor(a) y la sala de redacción en general primero, como también con profesionales de seguridad (si las fuentes fueron mencionadas solo por seudónimo pero reciben una llamada al día siguiente, esto podría permitir a los servicios de seguridad encontrar el seudónimo). Podría ser más sabio enlazar la fuente al seudónimo). Sería sabio no contactarles en primer lugar.

P5 - ¿Qué podría hacer Sara para evitar aún más el acceso a su información digital mientras los dos hombres aún están dentro de su apartamento?

- Haz todo lo que puedas para seguir las leyes locales
- Insistir que las autoridades también cumplan con las leyes locales (ej. Permitir la filmación, testigos, etc)
- Técnicas de desescalamiento
- Averiguar quiénes son y si tienen una orden
- Evaluar la situación de su propia seguridad personal
- Buscar consejo legal, llamar a la sala de redacción
- Proporcionar cuentas y documentos falsos (puede requerir algo de preparación)
- Desviación

***Opción 2** - Sara no puede salir de su apartamento. Los dos hombres le piden que se siente y le exigen que les de las contraseñas de su computadora y memorias USB. Amenazan con llevarla a la estación de policía si no provee esta información. Sara pregunta por una orden judicial, pero no le dan una.*

P6 - Sabiendo que tiene información sensible en su computadora, incluida la identificación de fuentes confidenciales, ¿Qué opciones tiene Sara en esta situación?

- Evaluar las vulnerabilidades y priorizar los problemas más importantes primero
- Cerrar sesión y eliminar las cuentas sensibles remotamente

- Identificar toda la información que se guardó en casa
- Considerar las ventajas y desventajas de informar a los miembros del equipo y las fuentes que puedan estar en peligro. Tal vez tomar esta decisión con apoyo de la sala de redacción.
- Potencial de eliminación de archivos remota

P7 - Sara tiene un programa de eliminación remota de archivos en su computadora. ¿Qué debe considerar antes de eliminar los archivos de su computadora?

- Podría ser un problema legal, obstrucción de la justicia
- Piensa sobre las repercusiones potenciales, si es posible, habla con un(a) abogada(o) primero
- Si Sara no tiene evidencia de que las personas son de las fuerzas del orden pero parecen intrusos estándar o de una fuerza de seguridad no estatal, entonces esto también cambia el panorama legal y de amenaza

P8 - (Opcional) - Sabiendo que parte de su información ha sido comprometida, ¿a quien debería Sara informar de este incidente?¿Es importante el orden en el que informa a las personas?

- El editor de la sala de redacción
- El equipo de seguridad/TI de la sala de redacción
- El equipo legal de la sala de redacción
- Considerar contactar con las fuentes
- Si es periodista independiente, considerar compartir la situación con otra(o)s independientes.

Finalmente Sara se niega a proveer las contraseñas de sus dispositivos. Después de buscar 10 minutos más en su apartamento, los dos hombres se van con la computadora de Sara, memorias USB y libreta de papel.

Ahora Sara tiene acceso a su apartamento otra vez. Ve que se han dejado una de sus dos computadoras junto con sus memorias USB. Han tomado todas sus libretas de papel del apartamento.

P9 - ¿Qué debería hacer Sara ahora para asegurar que no se continúe comprometiendo su información y seguridad por las acciones de los dos hombres mientras estuvieron en su apartamento?

- Los hombres podrían haber instalado malware en los dispositivos de Sara; puede ser buena idea enviar esos dispositivos a un especialista en análisis forense digital
- Preguntar a la organización qué tipo de ayuda ella podría recibir de esta(o)s
- Considerar que su apartamento podría estar intervenido
- Hablar con su organización y asesora(e)s legales, y de seguridad sobre si tiene más sentido desde una perspectiva de seguridad hablar públicamente sobre la redada o no

P10 (opcional) - Aparte de los aspectos de seguridad digital de este escenario, ¿Cuáles otras precauciones y respuestas podría haber tomado Sara para mantenerse segura a sí misma y a su información?

- Aprender un poco más sobre cómo operan las fuerzas de seguridad en el país, si hay grupos que intentan intimidar a periodistas que no están asociados a las fuerzas de seguridad
- Preparar con abogada(o)s y editor(a)s sobre cómo responder mejor a redadas en casa
- No mantener información sensible en casa si existen las posibilidades de redadas