

Un acercamiento a la seguridad digital

Savant, la periodista.

Savana es una periodista que trabaja en una investigación acerca de criaderos de animales. Las fuentes de Savant tienen información secreta acerca de un criadero que podría ayudar a cerrarlo. Sujetos sospechosos ya han intentado averiguar qué información es, así que ahora Savant se encarga de proteger sus comunicaciones, cifrándolas y cuando colabora en un artículo, usa herramientas que permitan el envío de documentos de manera cifrados.

Los pronombres elegidos por Savant son: Ella

¿Qué se necesita proteger?

1. Fuentes: nombres, comunicaciones y contactos.
2. Comunicaciones con editores.
3. Investigaciones de información sensible al tiempo.
4. Documentos y artículos en borrador, que algunas veces involucran colaboradores.

Savant usa constantemente su celular para comunicarse mientras se desplaza. Constantemente colabora con otras personas en documentos y artículos futuros. Savant es reconocida por trabajar en historias que desafían el status quo, y tiene todo tipo de personas poderosas interesadas en su trabajo.

Para mitigar sus riesgos:

Savan cifra sus correos, especialmente los dirigidos a sus fuentes desde su computador para asegurarse de la confidencialidad de sus mensajes.

Para conversar en su computador de mesa o portátil, Savant usa un servicio de mensajería cifrada con cliente de voz.

Ella usa servicios de mensajería y voz cifrados para contactarse con sus fuentes en su celular.

Su trabajo colaborativo se realiza a través de servicios para compartir documentos cifrados.

Cuando usa señales de wifi compartidas o no seguras (como en un café) Savant usa una VPN virtual para conectarse de manera segura al internet.

Cuando se mueve por puntos de seguridad, como paso de fronteras, ella apaga por completo todos sus equipos para asegurarse que el cifrado funcione correctamente.

Maya, la activista.

Maya es una activista y bloguera que llama la atención sobre los efectos de las alzas en temperaturas de costas habitadas por pingüinos. No todo el mundo está de acuerdo con el trabajo de Maya, así que sus cuentas en línea están en constante amenaza de ser atacadas, hackeadas o “desfiguradas”.

Recientemente, las tensiones han aumentado y Maya está preocupada por la posibilidad de que alguien pueda robar sus equipos. Han decidido cifrar todos su equipos y disco duros para asegurarse de la protección de la información.

¿Qué necesita proteger?

1. Investigación y datos contenidos en discos duros.
2. Cuentas en línea
3. Comunicaciones con otros activistas

Cuidadosamente cultivado a través de años de trabajo, las cuentas en línea de Maya y blog son su vida. Su integridad es de suma importancia para ellos, para sus lectores y sus contactos. Investigaciones importantes, datos y planes se mantienen en sus discos duros y teme que puedan caer en manos enemigas.

Para mitigar estos riesgos:

Todos sus cuentas en línea están aseguradas por autenticación de dos pasos.

Maya mantiene un registro de cuales computadores han accedido a sus cuentas, y desde dónde, con las verificaciones de acceso y seguridad ofrecidas por Gmail y Facebook.

Usan extensiones de navegadores que potencian la protección de la privacidad para evitar rastreadores en las páginas web que puedan revelar sus intereses.

Maya expande enlaces cortos encontrados en cuentas de redes sociales para saber de antemano a qué página la van a dirigir.

Usa Contraseñas fuertes en todas sus cuentas: más de 20 caracteres, todas únicas, con números y caracteres especiales. Para recordar todas las contraseñas usa un administrador de contraseñas al que accede a través de una contraseña generada por el método del dado.

Maya se asegura de que todos sus equipos tengan el cifrado de disco completo activo.

Ellos cifran todos los archivos sensibles, también en medios externos, memorias y discos duros.

Maya usa servicios de mensajería cifrados para organizar eventos y reuniones.

Jaha, el estudiante

Jaha es una estudiante en su último año de escuela. Ella se interesa en hacer parte de movimientos que acepten un estilo de vida libre de moscas, un tabú en la comunidad de las ranas. Muchos recursos sobre el tema están bloqueados por la universidad, y ella enfrenta estigma y sospecha si se conociera que este es uno de sus intereses. Jaha necesita permanecer anónima y mantener sus búsquedas en línea de manera privada.

¿Qué se necesita proteger?

1. Vida privada
2. Control personal sobre su identidad
3. Acceso a la libre circulación de información
4. Separación de su persona en línea frente a su persona fuera de ella.

Jaha no quiere que su familia o varias personas en su círculo cercano sepan de sus intereses aún. Quiere libertad para explorar esta posible nueva faceta suya sin sentirse vigilada por otras personas. Jaha ha creado una persona en línea separada y no quiere arriesgarse a ser expuesta públicamente hasta que esté lista, pero quiere acceder a material que la universidad ha censurado.

Jaha emplea herramientas de elusión y para el anonimato; para enmascarar su identidad y evitar la censura.

Usa una extensión de navegador que asegura la conexión con los sitios web que visita.

Jaha configura sus servicios de mensajería y en línea para que no registren sus historial. Si esto no es posible, limpia su historial de conversación para evitar acceso malicioso a conversaciones previas.

La mensajería cifrada permite que Jaha pueda conversar con personas como ella.

Ella mantiene sus identidades en línea separadas, para dividir su vida personal de la académica, tomando especial precaución de ser identificada.

Julio, el abogado de derechos civiles

Julio trabaja en una ONG en defensa de los derechos civiles. Aunque no trabaja directamente con clientes, sabe que sus hábitos personales protegen a sus colegas y por ende, a los clientes. Julio trabaja muy duro para asegurarse que su higiene en materia de seguridad es muy buena para cuidar responsablemente de su organización.

¿Qué se necesita proteger?

1. Información legal y financiera cerca de su organización, donantes y empleados.
2. Lista de contactos: clientes y aliados.
3. La integridad y confianza que la organización ha construido
4. Documentos privados, como declaraciones de clientes y estrategias de incidencia.

Julio es vulnerable durante sus continuos viajes por el wifi sin protección, conexiones, paso de fronteras y múltiples estadías en los hoteles. Él tiene una naturaleza abierta y hospitalaria, lo cual lo hace confiar en la gente demasiado rápido. Su organización es vastamente conocida por su trabajo, y él es la cara pública de la misma, muchas veces siendo contactado por extraños en busca de ayuda, acompañamiento y consejos.

Para mitigar estos riesgos:

Julio mantiene su software actualizado.

El tiene un gestor de contraseñas, donde genera contraseñas fuertes y únicas. Para asegurar su gestor, ha creado frases que son fuertes y fáciles de recordar usando el método de los dados.

Cuando usa señales de wifi compartidas o no seguras (como en un café) Julio usa una VPN de confianza para cifrar su conexión inicial a internet.

Cuando lee sus correos, Julio es precavido al abrir enlaces o archivos inesperados, a menos que haya verificado la identidad del remitente llamándolos o enviando un mensaje.

Cuando atraviesa una frontera, Julio apaga por completo sus equipos para asegurar que el cifrado funcione correctamente para prevenir el acceso a información de manera no autorizada.

Él recuerda que lo que se publica por fuera del trabajo puede impactar el trabajo de la organización también. Se asegura entonces de que lo que publica en su cuenta personal no puede ser usado para atacarlo a él o a la organización (no publica ubicación, imágenes de eventos privados, direcciones, etc.)

¿Y tú, qué necesitas proteger?

Responde la pregunta para mapear tus preocupaciones y prioridades para mantenerte seguro y protegido en línea.

Escribe tu historia...

- ¿Qué haces?
- ¿Con quién trabajas?
- ¿Alguien quisiera detener tus actividades? Si la respuesta es positiva, ¿quién?
- ¿Alguien quisiera saber qué estás haciendo? Si la respuesta es positiva, ¿quién?
- ¿Haz tenido alguna razón para preocuparte por tu actividad en línea o por tus equipos?

¿Qué necesitas proteger?

Enlista tu información y actividades más importante. ¿Necesitas ideas? Mira las páginas anteriores para inspirarte

Ahora considera los riesgos en tus actividades, comunicaciones e información.

- ¿Quién tiene acceso a ellas?
- ¿Quién no debería tener acceso a ellas?
- ¿ Consideraste alguno de tus riesgos después de leer este folleto? ¿Qué riesgos, en qué sentido?

Plan de acción:

Lista de estrategias y soluciones que has hallado en este folleto o en otros materiales que quisieras explorar más.