Ciberseguridad para periodistas: habilidades y herramientas para proteger las comunicaciones

Los periodistas se enfrentan a un reto creciente para proteger sus comunicaciones en el marco del ejercicio de la profesión. Así, la protección de las fuentes puede verse fácilmente comprometida en un mundo donde la vigilancia da la sociedad es cada vez más omnipresente y cada vez menos perceptible. Pero sacrificando un poco su tiempo, los periodistas pueden igualmente aprovechar estos mismos avances tecnológicos para hacer más seguras sus comunicaciones y para protegerse mejor y reforzar la relación de confianza con sus fuentes.

Para reforzar la ciberseguridad de los periodistas, la Federación Europea de Periodistas (FEP) y el Instituto Sindical Europeo (ETUI) han organizado del 19 al 22 de enero de 2015, con el apoyo financiero de la Comisión Europea, una formación de cuatro días en Bruselas reuniendo a 23 periodistas procedentes de 19 países europeos.

Dirigida por el experto en seguridad informática Dmitri Vitaliev, esta formación ha permitido a los 23 participantes –en representación de organizaciones sindicales o asociaciones profesionales de periodistas de Europa aprender de manera rápida y práctica el uso de las nuevas herramientas en este campo. Los periodistas han podido también conocer medios técnicos para evitar la censura en Internet, examinar casos prácticos de pirateo y de violaciones de los derechos humanos mientras han ido descubriendo nuevas herramientas para encriptar comunicaciones o reforzar contraseñas.

Consejos y herramientas

Esta es una una lista no exhaustiva de los consejos y de los recursos útiles compartido por el experto durante los cuatro días de formación. *(Este artículo ha sido redactado en el transcurso de las sesiones por participantes no expertos en cuestiones informáticas)*.

Los principios de base

1.– Es imprescindible instalar un **software antivirus** en el ordenador (inexcusablemente en el caso de Windows). Si se adquiere un nuevo ordenador, este antivirus debe instalarse antes de cualquier conexión a internet con el fin de minimizar los riesgos de infección informática.

2.– Cortafuegos. La instalación de un software antivirus no es suficiente para proteger el ordenador. El cortafuegos viene a ser como una segunda capa de pintura más robusta que debe instalarse para reforzar el antivirus.

3.– No deben utilizarse softwares pirateados. Si no se puede instalar un software bajo licencia para evitar que el ordenador se infecte per haberle implementado aplicaciones sin control, ni garantía o con posibles *regalos escondidos*, hay r**ecursos alternativos de programario libre** que se pueden descargar y utilizar con plena seguridad y con mayor transparencia.

4.– Si se utiliza un ordenador público o que no se puede garantizar que esté exento de virus, se debe trabajar con **una simple llave USB**. Así, no se deja ningún rastro del trabajo en el ordenador de un cibercafé.

5.– Se deber utilizar una **contraseña segura**. Es preferible que sea larga antes que complicada. Así será más difícil para los piratas romper el código. Releyendo a Edward Snowden, se constata que es mejor utilizar una combinación mínima de más de 12 carácteresp ara una contraseña con una combinación de letras, cifras y símbolos

diferentes. No sólo hace falta generar una contraseña larga y compleja, además también es muy desaconsejable utilizar la misma contraseña para todo. No tener una memoria de elefante para retener estos secretos no supone ningún problema. Se puede recurrir a la mnemotécnica (primera letra de una larga frase), o utilizar un software como *KeePass* para almacenar las múltiples contraseñas de que uno puede disponer irrompibles con total seguridad.

6.– Amnistía Internacional propone ***DETEKT,*** un software que permite saber si las agencias de información controlan el ordenador, sea en casa o no. La herramienta escanea la máquina y el sistema operativo Windows para buscar rastros de softwares malignos como *FinFisher* y *Hacking Team RCS*, un tipo de aplicaciones espías de vigilancia comercial que son utilizados regularmente para vigilar y seguir a defensores de los derechos humanos o a los periodistas en cualquier parte del mundo.

La gestión de los datos: ¿cómo suprimir, recuperar y encriptar los datos?

1.– Pérdida de datos ¿Poner un fichero secreto en la papelera, garantiza que este será suprimido para siempre? Si obligan a borrar unas fotos durante una manifestación, ¿hay que temer que se han perdido para siempre? La respuesta es no, cosa que es mala o buena, según el caso. El fichero que se ha suprimido siempre puede ser recuperado, incluso cuando ya no es visible para el usuario. En realidad, los ordenadores mienten, cosa que es particularmente cierta en cuestión de gestión de ficheros borrados. Cuando se suprime un fichero, el ordenador *olvida* el sitio donde este se guarda aunque siempre permanecerá en el disco duro. Para suprimirlo definitivamente se puede descargar gratuitamente un software de supresión permanente (como *CC-Cleaner*) que permitirá la supresión definitiva del fichero. Pero es importante tener en cuenta que no basta con eliminar el fichero en cuestión, es necesario suprimir igualmente las múltiples copias que se han ido haciendo cuando se ha ido modificando y que generalmente se encuentran en una carpeta que reúne los ficheros temporales.

2.– Recuperación de datos. Los periodistas pueden utilizar en su favor las falsas eliminaciones. Si cualquier autoridad obliga a suprimir unas fotos, se pueden recuperar técnicamente con posterioridad. Solo hace falta un software específico (como *Recuva*) para hacerlo.

3.– Gestionar, modificar o suprimir los metadatos: **los metadatos** son informaciones técnicas sobre las propiedades de un archivo (documento o foto) y proporcionan indicaciones precisas sobre el tipo de aparato utilizado, la fecha y el lugar de las visualizaciones,… Proporcionan mucha información sobre el usuario y de cómo se ha creado el archivo. Si no se desea permanecer en el anonimato o proteger las fuentes, guarda los metadatos por sí mismo.

4.– Crear una **protección segura de los datos**. Se debería disponer siempre de un sistema de protección de las informaciones importantes pero es preferible almacenarlos en un servidor seguro y encriptado (como *Mega.co.nz*). Si no se quieren llevar encima los datos sensibles durante los desplazamientos, se pueden almacenar sobre este tipo de servidores que los encriptan automáticamente.

5.– Encriptar datos y comunicaciones. Se puede descargar gratuitamente el software (como *TrueCrypt* o *BoxCryptor*) para cifrar los datos antes de enviarlos o almacenarlos en un servidor. Estos softwares permiten crear una *caja de caudales secreta* que solo es visible para la persona que conoce la contraseña y la localización de un archivo en el ordenador. Así, no hay ninguna necesidad de tener conocimientos técnicos sobre la encriptación de datos para proteger los archivos más sensibles.

6.– ¿Qué hacer si se es obligado por la fuerza, sea por la autoridad o por otra persona, a revelar la contraseña que permite abrir el dossier encriptado? El software *TrueCrypt* permite crear *un agujero escondido* dentro de *la caja de caudales secreta*, una especie de doble fondo donde guardar los datos que se considere. En este caso, la *caja de caudales*

secreta se convierte en un ardid para engañar al atacante en caso de ser forzado a revelar la contraseña.

Ciertas verdades difíciles a aceptar a propósito de las comunicaciones en internet

La verdad sobre el anonimato en la red es que es muy dificil mantener las actividades totalmente privadas. Hoy, ya no es posible el anonimato en internet salvo si se toman medidas específicas extremadamente pesadas y difíciles de aplicar para esconder la identidad, su uso y las comunicaciones.Alguien, en alguna parte, siempre intentará, por diferentes razones, vigilar la actividad de cualquiera en la red.

Según el derecho comunitario europeo sobre la conservación de los datos, los proveedores de accesos a internet (ISP) y los operadores telefónicos deben conservar la totalidad de los datos para proporcionarlos, en caso de petición, a los servicios de seguridad o a las autoridades judiciales. El pasado 19 de enero, un artículo revelaba que una agencia de información británica había espiado miles de correos de periodistas que trabajan para medios de comunicación internacionales.

Aunque sea prácticamente muy difícil proteger las comunicaciones en un entorno numérico, hay algunas medidas que se pueden adoptar para proteger la confidencialidad de los correos, las conversaciones a través de mensajería instantánea o de debates por video o audioconferencia.

1.– Cifrado y encriptado del correo. Se pueden descargar módulos complementarios del navegador *Firefox* o *Chrome* (como *Mailvelope*) para encriptar los e-mails para que nadie (al margen, claro, de uno mismo y el destinatario) pueda leer los mensajes. Por ahora, *Mailvelope* solo encripta el contenido de los mensajes y no los ficheros adjuntos.

2.– Protección de las conversaciones instantáneas por audio o vídeo. Las plataformas más populares de mensajería instantánea (como *Skype*, *Facebook Chat*, *Google Hangout*, etc.) son gestionadas por grandes empresas cuya reputación es más que dudosa en materia de respeto a la privacidad de los usuarios. Para preservar la confidencialidad de las conversaciones, se deben utilizar herramientas alternativas eficaces basadas en tecnología p*unto a punto* (como *Cryptoca*t, *Jitsi*, *Talky.io*, *Whispersystems,* etc.). Para leer un resumen de las características de cada plataforma, se puede visitar la web de la **Electronic Frontier Foundation** que ha auditado todos las últimas que han aparecido.

3.– ¿Alguien ha oído a un colega decir que prefiere poner su móvil en la nevera para evitar escuchas indiscretos? No, esto no es un chiste. Los móviles pueden ser activados a distancia y utilizados como herramienta de espionaje a nuestra espalda. **Ya no podemos ser anónimos con los móviles** porque incluso apagados envían una señal para indicar su ubicación. En muchos países, hay que facilitar un documento de identidad para poder comprar una tarjeta SIM. La sociedad WhisperSystems ha desarrollado una aplicación para los usuarios de smartphones con el objetivo de garantizar la confidencialidad de los mensajes y de las localizaciones de los usuarios.

4.– ¿Qué hacer para esquivar la **censura en internet**? En los países donde la censura es una práctica habitual para oprimir a los periodistas o a las voces críticas, el acceso a la información o a los medios de comunicación puede ser un problema para los periodistas. Hoy, hay medios técnicos fáciles de utilizar para esquivar la censura. Se puede alquilar una cobertura privada virtual (*VPN*) para encriptar y redirigir la totalidad de vuestro uso sobre internet.

5.– Algunos periodistas utilizan **direcciones electrónicas temporales** para ser anónimos. Si se quiere evitar el correo basura o no se quiere dar la dirección electrónica real a desconocidos, se puede utilizar el servicio de correo electrónico temporal (como *GuerrillaMail* o *Mailinator*) para ser anónimo. El servicio proporciona una única dirección electrónica.

6.– La **privacidad de la navegación**. La limpieza de las *cookies* y del historial de navegación no es suficiente. Si se desea reducir al mínimo la vigilancia en Internet, se puede usar el navegador *Tor* donde nadie puede ver los sitios que se han visitado ni rastrear su ubicación. También permite el acceso a sitios web que no están disponibles para los navegadores normales.

Más información sobre la ciberseguridad:
https://securityinabox.org
https://www.level-up.cc
http://saferjourno.internews.org/
https://learn.equalit.ie

Softwares de almacenamiento de las contraseñas: http://keepass.info
Servidor de seguridad: http://mega.co.nz
Encriptación del correo con Firefox o Chrome; https://www.mailvelope.com/
Electronic Frontier Foundation: https://www.eff.org
Protección de las comunicaciones en el móvil: https://whispersystems.org/

FeSP
Federación de Sindicatos de Periodistas

EFJ FEP FEJ
European Federation of Journalists

etui.