Ciberseguretat per a periodistes: habilitats i eines per a protegir les comunicacions

Els periodistes s'enfronten a un repte creixent per protegir les seves comunicacions en el marc de l'exercici de la professió. Així, la protecció de les fonts pot veure's fàcilment compromesa en un món on la vigilància de la societat és cada vegada més omnipresent i cada vegada menys perceptible. Però sacrificant una mica el seu temps, els periodistes poden igualment aprofitar aquests mateixos avanços tecnològics per fer més segures les seves comunicacions i per protegir-se millor i reforçar la relació de confiança amb les seves fonts.

Per reforçar la ciberseguretat dels periodistes, la Federació Europea de Periodistes (FEP) i l'Institut Sindical Europeu (ETUI) van organitzar del 19 al 22 de gener de 2015, amb el suport financer de la Comissió Europea, una formació de quatre dies a Brussel·les reunint 23 periodistes procedents de 19 països europeus.

Dirigida per l'expert en seguretat informàtica Dmitri Vitaliev, aquesta formació ha permès als 23 participants –en representació d'organitzacions sindicals o associacions professionals de periodistes d'Europa– aprendre de manera ràpida i pràctica l'ús de les noves eines en aquest camp. Els periodistes han pogut també conèixer mitjans tècnics per a evitar la censura a Internet, examinar casos pràctics de pirateig i de violacions dels drets humans mentre han anat descobrint noves eines per a encriptar comunicacions o reforçar contrasenyes.

Consells i eines

Aquesta és una una llista no exhaustiva dels consells i dels recursos útils compartits per l'expert durant els quatre *dies* de formació. *(Aquest article ha estat redactat en el transcurs de les sessions per participants no experts en qüestions informàtiques.)*

Els principis de base

1.– És imprescindible instal·lar **un programari antivirus** a l'ordinador (inexcusablement en el cas de Windows). Si s'adquireix un nou ordinador, aquest antivirus s'ha d'instal·lar abans de qualsevol connexió a internet per tal de minimitzar els riscos d'infecció informàtica.
2.– Tallafocs. Amb la instal·lació d'un programari antivirus no n'hi ha prou per a protegir l'ordinador. El tallafocs ve a ser com una segona capa de pintura més robusta que cal instal·lar per reforçar l'antivirus.
3.– No s'han d'utilitzar programaris piratejats. Si no es pot instal·lar un programari sota llicència per evitar que l'ordinador s'infecti per haver-hi implementat aplicacions sense control, ni garantia o amb possibles *regals amagats,* hi ha **recursos alternatius de programari lliure** que es poden descarregar i utilitzar amb més seguretat i una major transparència.
4.– Si s'utilitza un ordinador públic o del que no es pot garantir que estigui exempt de virus, s'ha de treballar amb una **simple clau USB**. Així, no es deixa cap rastre de la feina a l'ordinador d'un cibercafé.
5.– S'ha d'utilitzar una **contrasenya segura**. És preferible que sigui llarga abans que complicada. Així serà més difícil per als pirates trencar el codi. Si es rellegeix Edward Snowden, es constata que és millor utilitzar una combinació mínima de més de 12 caràcters per a una contrasenya amb una combinació de lletres, xifres i símbols diferents. No només fa falta generar una contrasenya llarga i complexa, a més també és molt

desaconsellable utilitzar la mateixa contrasenya per a tot. No tenir una memòria d'elefant per retenir aquests secrets no suposa cap problema. Es pot recórrer a la mnemotècnica (primera lletra d'una llarga frase), o utilitzar un programari com *KeePass* per guardar les múltiples contrasenyes que un pot disposar intrencables amb total seguretat.
6.– Amnistia Internacional proposa ***DETEKT,*** un programari que permet saber si les agències d'informació controlen l'ordinador, sigui a casa o no. L'eina escaneja la màquina i el sistema operatiu Windows per buscar rastres de programaris dolents com *FinFisher* i *Hacking Team RCS*, un tipus d'aplicacions espies de vigilància comercial que s'utilitzen regularment per vigilar i seguir a defensors dels drets humans o a periodistes a qualsevol lloc del món.

La gestió de les dades: com suprimir, recuperar i encriptar les dades?
1.– Pèrdua de dades Posar un arxiu secret a la paperera, garanteix que aquest serà suprimit per sempre? Si obliguen a esborrar unes fotos durant una manifestació, cal témer que s'han perdut per sempre? La resposta és no, cosa que és dolenta o bona, segons el cas. El fitxer que s'ha suprimit sempre es pot recuperar, fins i tot quan ja no és visible per a l'usuari. En realitat, els ordinadors menteixen, cosa que és particularment certa en qüestió de gestió de fitxers esborrats. Quan se suprimeix un fitxer, l'ordinador oblida el lloc on aquest es guarda encara que sempre romandrà en el disc dur. Per suprimir-lo definitivament, es pot descarregar gratuïtament un programari de supressió permanent (com *CC-Cleaner*) que permetrà la supressió definitiva del fitxer. Però és important tenir en compte que no n'hi ha prou amb eliminar el fitxer en qüestió, és necessari suprimir igualment les múltiples còpies que se n'han anat fent quan se l'ha anat modificant i que generalment es troben en una carpeta que aplega els fitxers temporals.
2.– Recuperació de dades. Els periodistes poden utilitzar en el seu favor les falses supressions. Si qualsevol autoritat obliga a eliminar unes fotos, es poden recuperar tècnicament amb posterioritat. Solament fa falta un programari específic (com *Recuva*) per fer-ho.
3.– Gestionar, modificar o suprimir **les metadades:** les metadades són informacions tècniques sobre les propietats d'un arxiu (document o foto) i proporcionen indicacions precises sobre el tipus d'aparell utilitzat, la data i el lloc de les visualitzacions,… Proporcionen molta informació sobre l'usuari i de com s'ha creat l'arxiu. Si vols mantenir l'anonimat o protegir les teves fonts, elimina o edita les metadades.
4.– Crear una **protecció segura de les dades.** S'hauria de disposar sempre d'un sistema de protecció de les informacions importants però és preferible emmagatzemar-los en un servidor segur i encriptat (com *Mega.co.nz)*. Si no es volen portar damunt les dades sensibles durant els desplaçaments, es poden guardar sobre aquest tipus de servidors que els encripten automàticament.
5.– Encriptar dades i comunicacions. Es pot descarregar gratuïtament el programari (com *TrueCrypt* o *BoxCryptor*) per xifrar les dades abans d'enviar-les o guardar-les en un servidor. Aquestes aplicacions permeten crear una *caixa de cabals secreta* que solament és visible per a la persona que coneix la contrasenya i la localització d'un arxiu a l'ordinador. Així, no cal tenir coneixements tècnics sobre l'encriptació de dades per protegir els arxius més sensibles.
6.– Què fer si s'és obligat per la força, sigui per l'autoritat o per una altra persona, a revelar la contrasenya que permet obrir el dossier encriptat? El programari *TrueCrypt* permet crear un *forat amagat* dins de la *caixa de cabals secreta*, una espècie de doble fons on guardar les dades que es cregui. En aquest cas, la *caixa de cabals secreta* es converteix en un truc per enganyar l'atacant si s'és forçat a revelar la contrasenya.

Certes veritats difícils d'acceptar a propòsit de les comunicacions a Internet
La veritat sobre l'anonimat a la xarxa és que és molt difícil mantenir les activitats totalment

privades. Avui, ja no és possible l'anonimat a Internet excepte si es prenen mesures específiques extremadament pesades i difícils d'aplicar per amagar la identitat, el seu ús i les comunicacions. Algú, en algun indret, sempre intentarà, per diferents raons, vigilar l'activitat de qualsevol a la xarxa.
Segons el dret comunitari europeu sobre la conservació de les dades, els proveïdors d'accessos a Internet (ISP) i els operadors telefònics han de conservar la totalitat de les dades per proporcionar-les, en cas de petició, als serveis de seguretat o a les autoritats judicials. El passat 19 de gener, un article revelava que una agència d'informació britànica havia espiat milers de correus de periodistes que treballen per a mitjans de comunicació internacionals.

Tot i que sigui pràcticament molt difícil protegir les comunicacions en un entorn digital, hi ha algunes mesures que es poden adoptar per protegir la confidencialitat dels correus, les converses a través de missatgeria instantània o els debats per vídeo o audioconferència.
1.– Xifrat i encriptat del correu. Es poden descarregar mòduls complementaris del navegador *Firefox* o *Chrome* (com *Mailvelope*) per encriptar els correus perquè ningú (al marge, és clar, d'un mateix i el destinatari) pugui llegir-los. Ara com ara, *Mailvelope* només encripta el contingut dels missatges i no els fitxers adjunts.
2.– Protecció de les converses instantànies per àudio o vídeo. Les plataformes més populars de missatgeria instantània (com *Skype*, *Facebook Chat*, *Google Hangout*, etc.) són gestionades per grans empreses la reputació de les quals és més que dubtosa en matèria de respecte a la privadesa dels usuaris. Per preservar la confidencialitat de les converses, s'han d'utilitzar eines alternatives eficaces basades en tecnologia *punt a punt* (com *Cryptocat, Jitsi, Talky.io*, *Whispersystems,* etc.). Per llegir un resum de les característiques de cada plataforma, es pot visitar la web de l'Electronic Frontier Foundation que ha auditat totes les darreres que han aparegut.
3.– Algú ha sentit un col·lega dir que prefereix posar el mòbil a la nevera per evitar escoltes indiscretes? No és un acudit. Els mòbils poden ser activats a distància i utilitzats com a eina d'espionatge a la nostra esquena. **Ja no podem ser anònims amb els mòbils** perquè fins i tot apagats envien un senyal per indicar la seva ubicació. En molts països, cal facilitar un document d'identitat per poder comprar una targeta SIM. La societat WhisperSystems ha desenvolupat una aplicació per als usuaris de smartphones amb l'objectiu de garantir la confidencialitat dels missatges i de les localitzacions dels usuaris.
4.– Què fer per esquivar la **censura a Internet**? Als països on la censura és una pràctica habitual per oprimir els periodistes o les veus crítiques, l'accés a la informació o als mitjans de comunicació pot ser un problema per als periodistes. Avui, hi ha mitjans tècnics fàcils d'utilitzar per esquivar la censura. Es pot llogar una cobertura privada virtual (*VPN*) per encriptar i redirigir la totalitat del vostre ús sobre Internet.
5.– Alguns periodistes utilitzen **adreces electròniques temporals** per ser anònims. . Si es vol evitar el correu brossa o no es vol donar l'adreça electrònica real a desconeguts, es pot utilitzar el servei de correu electrònic temporal (com *GuerrillaMail* o *Mailinator)* per ser anònim. El servei proporciona una única adreça electrònica.
6.– La privadesa de la navegació. La neteja de les *cookies* i de l'historial de navegació no és suficient. Si es desitja reduir al mínim la vigilància a Internet, es pot fer servir el programari *Tor* on ningú pot veure els llocs que s'han visitat ni rastrejar-ne la ubicació. També permet l'accés a llocs web que no estan disponibles per als navegadors normals.

Més informació sobre la ciberseguretat:
https://securityinabox.org
https://www.level-up.cc
http://saferjourno.internews.org/
https://learn.equalit.ie

Programaris d'emmagatzematge de les contrasenyes: http://keepass.info
Servidor de seguretat: http://mega.co.nz
Encriptació del correu amb Firefox o Chrome; https://www.mailvelope.com/
Electronic Frontier Foundation: https://www.eff.org
Protecció de les comunicacions en el mòbil: https://whispersystems.org/