MANUAL DE CIBERSEGURETAT PER A ACTIVISTES

Davant l'espionatge de l'Estat espanyol,
protegim-nos!

CATALANGATE

ÒMNIUM

catalangate.omnium.cat

T'HO POSEM FÀCIL. POSA-HO DIFÍCIL

En l'era de la informació, les noves tecnologies ofereixen grans oportunitats però també riscos per a la defensa de la democràcia i els drets humans. L'activista de base o qualsevol persona que vulgui defensar les seves idees lliurement ha de protegir-se davant l'intent de tercers d'interceptar les comunicacions de forma il·lícita per boicotejar la seva feina o activitats, com s'ha demostrat en el cas del Catalangate. **En aquest sentit, hi ha una premissa bàsica: la seguretat total no existeix.**

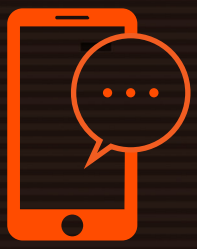
Llavors, què entenem doncs per ciberseguretat? **En les eines de comunicació, protegir-se és posar les coses difícils a qui vulgui espiar**. En altres paraules, vetllar per la privacitat individual i tenir clar exactament què es vol protegir:

Què fas? On treballes? On vas? Què consumeixes? Amb qui et relaciones? Què dius, escrius o fas que pugui ser tergiversat i utilitzat en contra teva?

També és molt important poder controlar la informació que sí que vols que tinguin tercers. Però sobretot hi ha una actitud bàsica per protegir-se: **la disciplina i la consistència en el temps a l'hora de prendre mesures de protecció**. És precisament la inconsistència el que t'exposa, ja que si et relaxes s'obre una escletxa de seguretat i tota la bona feina prèvia que hagis pogut fer pot quedar en no res en qüestió de minuts.

L'objectiu d'aquesta guia no és un altre que aportar consells bàsics per millorar el control sobre la teva privacitat i la seguretat en les eines de comunicació que utilitzes en el teu dia a dia. Les recomanacions d'aquest manual t'ajudaran a crear una primera capa de ciberseguretat imprescindible per a qualsevol activista de base que vulgui exercir els seus drets i llibertats sense estar sota vigilància.

T'animem a fer-les servir!



MISSATGERIA MÒBIL

La majoria de persones fan servir sistemes de missatgeria mòbil tipus Whatsapp, Telegram o SMS. Tots aquests programes presenten vulnerabilitats, però aplicant bones pràctiques les teves converses estaran més protegides:

Bones pràctiques

- **Activa l'opció de missatges efímers als xats de la missatgeria mòbil**. Apps com WhatsApp, Telegram i Signal permeten l'autodestrucció dels missatges d'un xat o d'un grup. Per activar-ho, cal anar a la configuració del xat. Convé fer-ho de seguida, abans d'escriure cap missatge a un xat o grup. Es pot triar entre uns pocs minuts o, fins i tot, mesos. 3 dies acostuma a ser un bon efímer pel dia a dia. Per a més informació de com establir efímers, clica aquí.

- **Descarta WhatsApp per missatges o qüestions que vulguis protegir.** És molt més segur fer servir Signal o els Secret Chat de Telegram. Recorda que, tot i que els missatges d'aquests canals no es puguin arribar a llegir mai, així i tot, queda registrat qui hi ha en una determinada conversa. Això ho pot saber l'empresa proveïdora del servei de missatgeria i qui tingui accés al mòbil en cas de substracció o segrest del dispositiu. Vols saber com crear un **Secret Chat** a Telegram? Clica aquí

NIVELL AVANÇAT

- **També pots fer servir Element, Matrix, Wire o KeyBase**. Són sistemes de missatgeria i d'enviament d'informació sensible (per exemple, si vols compartir el número de la teva targeta de crèdit amb algú) perquè permet fer el registre a l'aplicació sense donar cap número de telèfon o correu electrònic. En cas que et decantis per alguna d'aquestes opcions, fes servir un pseudònim en un idioma que no sigui el teu per a major privacitat.

- **Per a temes molt compromesos, fes servir un aparell on mai s'hi hagi instal·lat una targeta SIM**.

- **Si vols enviar fitxers segurs a través d'un servei de missatgeria cal fer-ho havent-los encriptat prèviament amb PGP**, tipus Kleopatra o similar. L'encriptació PGP (GNU Privacy Guard) és un sistema d'encriptació asimètric mitjançant el qual l'emissor encripta les dades amb una clau pública, coneguda per tercers, però que només la pot desencriptar el receptor amb una clau privada.

Males pràctiques

Les següents pràctiques, molt habituals en la majoria d'usuaris, et fan molt vulnerable a l'espionatge:

- Enregistrar àudios (notes de veu) o vídeos per comunicar-te.
- Enviar documents compromesos per missatgeria mòbil.
- Trucar per telefonia convencional. És recomanable trucar sempre a través de missatgeria tipus Telegram o Signal.
- Obrir SMS de números desconeguts o de remitents estranys o inesperats (un comanda que no has demanat, una informació sospitosa, etc). La majoria de víctimes del #Catalangate es van infectar clicant enllaços de SMS.
- Millor enviar adreces a documents protegits amb contrasenya o amb permisos que no pas adjuntar un document en PDF. Els documents, quan s'envien en obert, queden desats al mòbil de forma permanent.

CORREU ELECTRÒNIC

Enviar un correu electrònic mitjançant proveïdors convencionals és, a la pràctica, com enviar una postal per correu tradicional. És a dir, és molt fàcil de llegir pel distribuïdor i també per qualsevol que vulgui interceptar la teva informació.

Bones pràctiques

- **Fes servir serveis de correu electrònic que permetin fer un registre anònim.** Aquest tipus de proveïdors no et demanen ni número de telèfon ni un segon correu electrònic per registrar-te. Això exclou Gmail com a correu electrònic a utilitzar en l'activitat de tot activista. Hi ha diverses opcions segures com Protonmail, tot i que no es pot descartar que aquest proveïdor pogués facilitar les teves dades. Per tant, una recomanació vàlida és fer servir Telios.
- **Configura i utilitza claus PGP per protegir el teu correu electrònic**. Si ho fas, encriptes el contingut dels teus correus i només el receptor que tingui una clau privada podrà desxifrar-lo. El Thunderbird és un bon client de correu per a consultar els teus comptes que permet posar PGP a qualsevol adreça de correu que tinguis.

- **Fes servir correus on l'adreça no contingui cap element que es pugui relacionar amb tu**. Això inclou, per descomptat, nom i cognoms; però també pseudònims o dates que d'alguna manera o altra puguin ajudar a revelar la teva identitat.

Males pràctiques

- Fer servir el teu pseudònim, amb el que signes els correus electrònics, també en el nom de la teva adreça de correu. Diferenciar-ho ajuda a posar-ho més difícil al rastrejador.

- Fer servir els correus amb pseudònim en llocs on hagis de fer pagaments amb targeta de crèdit. En aquest cas, és millor fer-ne servir d'oficials. Podrien creuar les dades del titular del pagament com a responsable del correu molt fàcilment.

TRUCADES TELEFÒNIQUES

Les trucades convencionals són totalment transparents i vulnerables a l'espionatge i existeixen sistemes de tractar-les totes, com ara reconeixement de veu o significats. És relativament fàcil per l'interceptor identificar trucades i fer-ne seguiment.

Bones pràctiques

- **No donis gaires detalls en les trucades convencionals:** noms de persones, activitats concretes, ubicacions específiques, horaris... Evita fer comentaris, frases o expressions que es puguin tergiversar o et puguin comprometre.

- **Acostuma't a fer les teves converses convencionals mitjançant missatgeria mòbil.** Es recomana sobretot Signal i Telegram, però en aquest cas Whatsapp també pot ser una opció.

- **Fes servir JITSI per converses que vulguis que siguin totalment privades i anònimes.** Pots intercanviar una adreça de JITSI per missatgeria o correu electrònic on tu i el teu interlocutor pugueu entrar amb pseudònim. En aquest cas, no es recomana fer servir trucades a partir de missatgeria mòbil perquè WhatsApp, Signal i Telegram t'identifiquen pel número de telèfon.

- **Utilitza auriculars en les teves trucades perquè no puguin escoltar la conversa completa.** Això és rellevant per a pisos, oficines i cotxes.

Males pràctiques

- Trucar per telefonia convencional o smartphone. Sempre missatgeries que permetin trucada (WhatsApp, Signal, Telegram,...) o via videotrucada.
- Despenjar trucades d'origen desconegut excepte les que estiguem esperant. Sempre poden deixar un missatge de veu o enviar un missatge per identificar-se.

VIDEOTRUCADES

Amb la normalització del teletreball, les videotrucades són ara un dels canals més utilitzats per a reunions de treball o d'activisme. Però cal ser conscients que tenir un ordinador i una càmera al davant ens exposa al 100%, per això cal prendre mesures.

Bones pràctiques

- **Posa't auriculars quan facis una videoconferència.** Si ho fas, només podran enregistrar una part de la conversa.
- **Apaga o tapa la càmera del teu ordinador, ja sigui PC o portàtil.**
- **Fes servir un pseudònim.** Ja sigui el nom que apareix en pantalla o el nom que fas servir per relacionar-te amb el teu interlocutor.
- **Utilitza serveis sense autenticació tipus JITSI** que no demana usuari per accedir-hi.

Males pràctiques

- Posar el nom real, tenir la càmara oberta i tenir els altaveus posats.
- Parlar més del compte, donar massa detalls, referir-se innecessàriament a tercers pel seu nom....

CERQUES PER INTERNET

Quan fas una cerca a través del teu navegador habitual vas deixant un rastre molt fàcil de traçar, però posant en pràctica algunes mesures, navegaràs amb més seguretat.

Bones pràctiques

- **Fes servir un navegador que no enviï informació.** Un bon exemple és el LibreWolf.
- **Obre sempre una pestanya de navegació d'incògnit.** Si no ho fas, encara que utilitzis una VPN per evitar que el proveïdor d'internet sàpiga per on navegues, l'empresa del teu navegador - sigui Google Chrome, Firefox o Safari - poden saber tot el què has visitat.
- **No desis les contrasenyes al navegador.** Cal tenir en compte que a "Configuració", les contrasenyes es poden consultar. Aquestes no queden encriptades, només estaran protegides per la contrasenya del ordinador. A més, si tens el perfil sincronitzat, Google també les tindrà.

Males pràctiques

- Fer servir navegadors que envien informació com Chrome, FireFox, Opera, Safari, Brave...

EMMAGATZEMATGE D'ARXIUS

L'encriptació d'arxius és un dels passos que pot marcar clarament la diferència entre estar protegit o estar exposat. Prèn consciència!

Bones pràctiques

- **Posa els fitxers sempre encriptats a dins del propi dispositiu o al núvol.** En cas d'haver de compartir fitxers fer servir cryptpad.fr o similar, però protegir sempre els fitxers amb contrasenya i activar l'"enable access list" per poder controlar qui hi té accés i qui no. Cal recordar que qualsevol adreça d'internet és accessible des de tot internet.

Males pràctiques

- Compartir fitxers al GoogleDrive, OneDrive o iCloud sense haver-los encriptat prèviament amb un programa de PGP com pugui ser Kleopatra.
- Enviar fitxers per internet sense encriptar amb PGP.

REUNIONS O TROBADES PRESENCIALS

Les reunions són dels espais més sensibles per a qualsevol activista. No només perquè són un dels objectius del possible interceptor o espia, sinó també perquè interactuem amb més d'una persona, multiplicant les possibilitats d'exposar-nos o exposar als altres participants. Prendre mesures, en aquest cas, és protegir-nos individualment i col·lectiva.

Bones pràctiques

- **Apaga el telèfon i el portàtil abans de desplaçar-te cap a la reunió i deixa'l fora de la sala de la reunió.** Això és important no només per la geolocalització, sinó perquè quan fas un desplaçament existeix la possibilitat que et segrestin els equips. I, si estan en obert o en mode suspensió, no estan encriptats i són vulnerables.
- **Portàtil sí o portàtil no?** Només es poden portar a reunions que funcionin amb Linux i si és estrictament necessari. Un ordinador no deixa de ser un equip multimèdia molt potent.
- **Com prendre notes: amb ordinador o amb llibreta?** Si cal prendre notes millor fer-ho amb un ordinador (protegit) perquè un cop encriptat no el podran obrir.

Males pràctiques

- Dur el teu smartphone a les reunions.
- Deixar-ho tot anotat en una llibreta.
- Parlar excessivament alt.

RECOMANACIONS GENERALS EN DISPOSITIUS DE COMUNICACIÓ

Entenem per dispositius de comunicació els telèfons mòbils, PCs, ordinadors portàtils i tauletes.

Utilitza una VPN

- **Per no revelar quines pàgines web, adreces d'internet i programes fas servir, cal tenir sempre connectada una Virtual Private Network (VPN)**. Et comuniquis amb un smartphone o bé amb un ordinador portàtil, és 100% recomanable treballar sempre amb una VPN. Són fàcilment descarregables a Internet o a través del teu proveïdor d'Apps: n'hi ha de gratuïtes com **RiseupVPN** (agraeixen els donatius per fer possible aquest projecte) o de pagament: **NordVPN**, **ExpressVPN**, **SurfShark**... La VPN et protegeix de l'espionatge que algú pugui fer a través de la teva operadora d'accés a Internet (ISP). És important fer un ús molt responsable d'una VPN perquè davant d'un requeriment judicial el teu proveïdor del programa sí que podria acabar informant sobre quines pàgines web has visitat o utilitzat.

Encripta els teus dispositius

- **Els dispositius de comunicació mòbil haurien d'estar sempre encriptats i els ordinadors portàtils han d'estar encriptats d'arrel per protegir els fitxes que hi tinguis.** En el primer cas, l'encriptació s'aconsegueix a través de la configuració del mateix telèfon mòbil. En el segon, s'aconsegueix a través de programes com **VeraCrypt**, **Bitlocker** o **FileVault**. Per saber-ne més de com encriptar els teus dispositius, consulta els ENLLAÇOS D'INTERÈS al final d'aquest manual.

Fes ús de dispositius no habituals

- **Per a qüestions sensibles, com accions d'activisme en el marc de la llibertat d'expressió i el dret a la protesta, cal fer servir aparells que no s'utilitzin habitualment.** És a dir, aparells en els quals mai t'hagis identificat en cap servei (Gmail, Google Play, Apple Store, etc), que reserves només per qüestions molt concretes. Cal tenir en compte que si estàs intervingut amb un spyware com Pegasus, recomanacions com la VPN o l'encriptació no són suficients per evitar que t'enregistrin la pantalla o la veu.

Apaga el telèfon si no vols ser geolocalitzat

- **Si no vols que et geolocalitzin ni sàpiguen amb qui estàs, has d'apagar el dispositiu.** Et poden geolocalitzar per la targeta SIM, pel GPS de localització del mòbil i per les WIFI on et connectis. Fàcilment poden cercar coincidències de geolocalització i saber amb qui et relaciones.

Fes ús de contrasenyes alfanumèriques al teu telèfon mòbil

– Per evitar que accedeixin a la informació del teu telèfon mòbil és bàsic no fer servir l'accés per biometria ni un patró de desbloqueig (perquè deixa rastre dels dits a la pantalla). Cal fer servir un password alfanumèric de més de 8 caràcters i si conté caràcters especials millor.

Desactiva les notificacions del teu smartphone

– Perquè no es pugui veure qui es comunica amb tu, encara que el dispositiu estigui bloquejat, cal desactivar les notificacions de pantalla al mòbil.

ENLLAÇOS D'INTERÈS

Descarregar VPN - Riseup VPN (clicar aquí)

Configurar FileVault - Encriptació Mac (clicar aquí)

Configurar BitLocker - Encriptació Windows (clicar aquí)

Configurar VeraCrypt - Encriptació Windows (clicar aquí)

Activar efímers a WhatsApp (clicar aquí)

Activar efímers Signal (clicar aquí)

Activar efímers Telegram (clicar aquí)

Activar "Secret Chats" a Telegram (clicar aquí)

Correus electrònics anònims via Telios.io (clicar aquí)

Instal·lar PGP/GPG Kleopatra (clicar aquí)

Instal·lar Thunderbird i PGP (clicar aquí)

Instal·lar Thunderbird portable dins VeraCrypt (clicar aquí)

Per a qualsevol dubte sobre ciberseguretat, no dubtis en contactar amb ciberseguretat@omnium.cat

ÒMNIUM

catalangate.omnium.cat