1. Introducció:

Aquest document és un recull de recomanacions d'autoprotecció online.

Sovint mantenir un nivell de seguretat alt i consistent pot arribar a dificultar l'ús. És per això que des de la comissió tècnica d'ANC Deutschland hem creat dos perfils d'usuari amb diferents recomanacions de seguretat.

Aquest document descriu les **recomanacions de seguretat per usuaris de risc**. Aquest grup inclou persones amb responsabilitats organitzatives o amb projecció pública.

El segon grup, amb unes recomanacions mínimes, està orientat a membres de l'ANC Deutschland o simpatitzants sense responsabilitats organitzatives.

2. Gestió de dispositius:

- Mantenir els ordinadors, tauletes i telèfons sempre actualitzats.
- Evitar iPhones o Androids antics que ja no es poden actualitzar fàcilment.
- Establir una contrasenya per desbloquejar els dispositius. L'ús de les empremtes dactilars pot no ser recomanable depenent del tipus d'informació que tinguem en el dispositiu. La vulnerabilitat principal de l'empremta és que podríem estar forçats físicament a desbloquejar el dispositiu.
- No repetir mai contrasenyes. Emprar sempre contrasenyes diferents per a cada compte, programa o dispositiu, no repetint-les mai. Es recomanar fer servir gestors de contrasenyes com Keepass (https://keepass.info/) o LastPass (https://www.lastpass.com/)* o BitWarden (https://bitwarden.com/).

3. Encriptació:

Assegurar que els dispositius que fem servir tinguin les dades encriptades**:**

- **Windows:** Microsoft Pro Edition permet encriptació. Cercar el disc dur o "C":, botó dret del ratolí i seleccionar "Turn on Bitlocker", ens demanarà introduir una nova contrasenya.
- **Mac:** System Preferences > Security & Privacy > Filevault > Turn On Filevault
- **iPhone:** No cal fer res ja que encripta el telèfon per defecte.
- **Android:** Per certes versions cal fer-ho de forma manual:
  - Android > Security > Encrypt device
  - Android > Security > Encrypt SD-card

(*) Producte comercial

4. Comunicacions

- Per trucades de veu fer servir Signal.
- No fer servir trucades normals o SMS. Ni fent servir paraules clau. Sovint en saber a qui es truca ja és suficient independentment del contingut. Tot i que Signal hauria de ser l'estàndard és millor altres programes com Telegram o WhatsApp abans que trucades normals.
- Evitar el correu electrònic per compartir informació confidencial. Si cal enviar infromació confidencial encriptar-los fent servir PGP/GPG (https://gnupg.org/)
- El problema principal de la missatgeria és sobretot els missatges oblidats al telèfon. És per això que es recomana fer servir Signal posant sempre un temps d'expiració dels missatges.
- En el cas de comunicacions entre persones de forma anònima podrem fer servir Telegram (ja que només cal compatir l'àlies) però en aquest cas mantindrem la disciplina d'esborrar els missatges de forma regular.
- Configuració Telegram potenciant l'anonimat: (impedir que Telegram tingui accés als nostres contactes).

  iOS: Configuració de Telegram > Privadesa i seguretat > Configuració de dades > Desactivar les opcions "Sincronitza els contactes" i "Suggereix contactes freqüents" i fer clic a "Elimina els contactes sincronitzats".

  Android: Configuració de Telegram > Privadesa i seguretat > Contactes > Desactivar les opcions "Sincronitza els contactes" i "Suggeriments de contactes freqüents" i fer clic a "Elimina els contactes sincronitzats".

5. Navegació:

És important emprar un navegador segur com Chrome, Firefox o Brave. Per poder accedir a webs censurades en zones concretes fer servir TorBrowser (https://www.torproject.org) disponible per Windows, Mac, Android i iPhone entre d'altres. Assegurar-nos que els navegadors s'actualitzen de forma periòdica.

TorBrowser no només serveix per evitar la censura sinó també per evitar el seguiment. Si cal accedir a una pàgina web de forma anònima fer-lo servir.

(*) Producte comercial

6. **Connexions segures:**

Evitar connexions a xarxes públiques d'internet (com per exemple aeroports o hotels) sense una VPN (Virtual Private Network). Això ens permetrà ocultar el tràfic i evitar que el manipulin. Fer servir la VPN d'ANC-DE al mòbil sempre.

Si encara no teniu accés a la VPN d'ANC-DE poseu-vos en contacte amb la comissió tècnica.

7. **Avaluar riscos:**

Una eina molt important per avaluar riscos en les nostres comunicacions és el nostre sentit comú. Hem de saber identificar quins llocs poden ser segurs i quins poden contenir riscos.

Com a persona de risc és possible que algú intenti instal·lar un programa de seguiment i escolta als vostres dispositius.

Algunes recomanacions:

- Cal estar alerta als enllaços rebuts per correu i especialment SMS. Mai accedir a un enllaç rebut per SMS.
- Valorar i revisar els arxius adjunts d'un correu electrònic. Mai accedir a enllaços rebuts que no estiguéssim esperant (encara que sembli que arriben de contactes coneguts).
- Actualitzar aplicacions periòdicament per a evitar fallades en la seguretat.

8. **Eines de detecció:**

Si feu servir iPhone o iPad és recomanable instal·lar l'aplicació "iVerfy" de Trail of Bits i seguir-ne els consells (https://apps.apple.com/us/app/iverify/id1466120520)

En cas de dubte poseu-vos en contacte amb la comissió tècnica a tecnica@anc-deutschland.cat o al canal #seguretat de l'Ancora (https://ancora.assemblea.net/channel/seguretat)

(*) Producte comercial