

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○○○○

Comunicacions

○○○○○○○○○○
○○○○○○○○
○○○○○○○○

Coordinació

○○○○○
○○○○
○○○○○○○○

Final

○○○
○
○

Anti-Repressió Digital

Protegir-nos és feina de totes!

Contacte:

projectenadki@protonmail.com

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○○○○

Comunicacions

○○○○○○○○○○
○○○○○○○○
○○○○○○○○

Coordinació

○○○○○
○○○○
○○○○○○○○

Final

○○○
○
○

Índex

Introducció

Seguretat física - Ordinador

Seguretat física - Mòbil

Comunicacions

Coordinació

Final

Introducció



Introducció

Seguretat física - Ordinador



Seguretat física - Mòbil



Comunicacions



Coordinació



Final



Projecte Nadki



Projecte Nadki

Projecte sense ànim de lucre, anònim i col·laboratiu que pretén difondre coneixements gratuïtament.

- ▶ Blog privacitat i anonimat
- ▶ Blog investigació online (OSINT, SOCMINT)
- ▶ Eines pròpies
- ▶ Formacions

Contacte:

- ▶ **Web:** <https://projectenadki.github.io/>
- ▶ **Email:** projectenadki@protonmail.com

Repressió digital





Repressió digital

Existeixen moltes formes de repressió digital:

- ▶ Intervenció de trucades (control dels ISP).
- ▶ Rastreig de dispositius mòbils.
- ▶ Confiscació de dispositius mòbils o ordinadors per analitzar-los.
- ▶ Infiltració a col·lectius utilitzant identitats falses.
- ▶ Atacs de Phishing o enginyeria social.
- ▶ Intervenció de recursos web (pàgines o comptes de xarxes socials).



Evaluació dels riscos

El primer pas és determinar quines són les amenaces per saber com afrontar-les.

Model d'amenaces, algunes preguntes a fer-se:

- ▶ Què val la pena protegir?
- ▶ De qui s'ha de protegir?
- ▶ Com de probable és que s'hagi de protegir?
- ▶ Quant de destructives són les conseqüències en cas de fallar?
- ▶ Quin esforç estàs disposat a fer?

Conceptes Bàsics



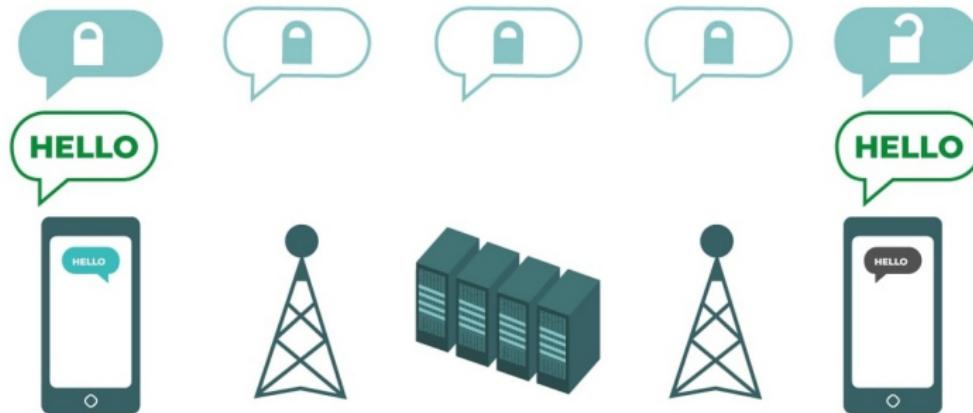
Centralització



Xifratge punt a punt



Xifratge extrem a extrem



Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

●○○○○
○○○○○
○○○○

Seguretat física

Seguretat física - Mòbil

○○○○
○○○○○○○○
○○○○○○

Comunicacions

○○○○○○○○
○○○○○○
○○○○○

Coordinació

○○○○
○○○○
○○○○○

Final

○○○
○○
○

Ordinador



Introducció

oo
ooo
oooo

Seguretat física - Ordinador

●○○○○
○○○○○
○○○○

Seguretat física

Seguretat física - Mòbil

oooo
oooooooooooo
oooooo

Comunicacions

oooooooooooo
oooooooo
oooooo

Coordinació

oooooo
oooo
oooooo

Final

ooo
o

Evaluació de riscos

Riscos

- ▶ Accés a documents emmagatzemats
- ▶ Accés a comptes amb contrasenya guardada
- ▶ Infecció de malware

Mitigacions

- ▶ Netejar fitxers temporals i navegadors
- ▶ Xifratge
- ▶ Antivirus
- ▶ Contrasenyes fortes

Introducció

○○
○○○
○○○○

Seguretat física

Seguretat física - Ordinador

○○●○○
○○○○○
○○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○○○○

Comunicacions

○○○○○○○○○○
○○○○○○○○
○○○○○○○○

Coordinació

○○○○○
○○○○
○○○○○○○○

Final

○○○
○
○

Sistemes operatius

Típics

- ▶ Windows
- ▶ OS X
- ▶ Linux

Especialitzats

- ▶ Whonix
- ▶ Tails
- ▶ Qubes OS



Antivirus

Protegeixen l'equipo d'infeccions.

- ▶ **Windows:** Windows Defender
- ▶ **OS X i Linux:** no és estrictament necessari
- ▶ Antivirus de pagament



Netejadors

Eliminació de cookies, historial, contrasenyes guardades i fitxers temporals.

- ▶ CCleaner
- ▶ BleachBit



Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
●○○○○
○○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○○

Comunicacions

○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Coordinació

○○○○
○○○○
○○○○○○

Final

○○○
○
○

Contrasenyes

Contrasenyes

0110101 NAME ADRES
01101001010010101101001001101
0110101 LOGIN **PASSWORD** 1
01101001010010101101001001101
01101010 NAME ADRES
01101001010010101101001001101
01101010110101011010110101101
01101001010010101101001001101.

```
oo
ooo
oooo
```

```
ooooo
o●ooo
oooo
```

```
ooooo
oooooooooooo
ooooooo
```

```
oooooooooooo
oooooooo
oooooo
```

```
ooooo
oooo
ooooooo
```

```
ooo
o
```

Atacs

Força bruta:

- ▶ només minúscules: 3:30 hores
- ▶ majúscules i minúscules: 1 mes i 9 dies
- ▶ alfanumèrica: 5 mesos
- ▶ alfanumèrica i símbols: 9 anys i 6 mesos

```
[ATTEMPT] target      - login "maria" - pass "0000" - 1 of 16 [child 0] (0/0)
[ATTEMPT] target      - login "maria" - pass "0001" - 2 of 16 [child 1] (0/0)
[ATTEMPT] target      - login "maria" - pass "0002" - 3 of 16 [child 2] (0/0)
[ATTEMPT] target      - login "maria" - pass "0003" - 4 of 16 [child 3] (0/0)
[ATTEMPT] target      - login "maria" - pass "0004" - 5 of 16 [child 4] (0/0)
[ATTEMPT] target      - login "maria" - pass "0005" - 6 of 16 [child 5] (0/0)
[ATTEMPT] target      - login "maria" - pass "0006" - 7 of 16 [child 6] (0/0)
[ATTEMPT] target      - login "maria" - pass "0007" - 8 of 16 [child 7] (0/0)
[ATTEMPT] target      - login "maria" - pass "0008" - 9 of 16 [child 8] (0/0)
[ATTEMPT] target      - login "maria" - pass "0009" - 10 of 16 [child 9] (0/0)
[ATTEMPT] target      - login "maria" - pass "0010" - 11 of 16 [child 10] (0/0)
[ATTEMPT] target      - login "maria" - pass "0011" - 12 of 16 [child 11] (0/0)
[ATTEMPT] target      - login "maria" - pass "0012" - 13 of 16 [child 12] (0/0)
[ATTEMPT] target      - login "maria" - pass "0013" - 14 of 16 [child 13] (0/0)
[ATTEMPT] target      - login "maria" - pass "9998" - 15 of 16 [child 14] (0/0)
[ATTEMPT] target      - login "maria" - pass "9999" - 16 of 16 [child 15] (0/0)
```



Atacs

Diccionaris (OSINT + SOCMINT):

- ▶ Noms de familiars o mascotes
- ▶ Dates importants
- ▶ Patrons reconeguts (ex. canviar les e per 3, les a per 4, ...)

```
[ATTEMPT] target      - login "maria" - pass "menorca" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target      - login "maria" - pass "paris" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target      - login "maria" - pass "2018" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target      - login "maria" - pass "1992" - 4 of 12 [child 3] (0/0)
[ATTEMPT] target      - login "maria" - pass "tobi" - 5 of 12 [child 4] (0/0)
[ATTEMPT] target      - login "maria" - pass "paris2018" - 6 of 12 [child 5] (0/0)
[ATTEMPT] target      - login "maria" - pass "Paris2018" - 7 of 12 [child 6] (0/0)
[ATTEMPT] target      - login "maria" - pass "Paris18!" - 8 of 12 [child 7] (0/0)
[ATTEMPT] target      - login "maria" - pass "Paris18" - 9 of 12 [child 8] (0/0)
[ATTEMPT] target      - login "maria" - pass "tobiparis92" - 10 of 12 [child 9] (0/0)
[ATTEMPT] target      - login "maria" - pass "menorca92" - 11 of 12 [child 10] (0/0)
[ATTEMPT] target      - login "maria" - pass "Menorca18" - 12 of 12 [child 11] (0/0)
```

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○●○
○○○○

Contrasenyes

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○○○○

Comunicacions

○○○○○○○○
○○○○○○○○
○○○○○○○○

Coordinació

○○○○○
○○○○
○○○○○○

Final

○○○
○○○
○

Contrasenyes segures

Recomanacions:

1. Més de 8 caràcters
2. Alfanumèrica: lletres i números (o símbols)
3. Majúscules i minúscules
4. Que no es pugui deduir per xarxes socials
5. No repetir contrasenyes

Suggerències:

- ▶ Frases (ex. laformaciomolamolt)
- ▶ Afegir complexitat (ex. La.Formacio.Mola.Molt!!)

Gestor de contrasenyes

Programes que emmagatzemem contrasenyes de manera segura.

- ▶ Contrasenyes xifrades
- ▶ Organització per carpetes
- ▶ Generació de contraseñes segures



KeePass



bitwarden

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○○
●○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○○

Comunicacions

○○○○○○○○○○
○○○○○○○○
○○○○○○

Coordinació

○○○○
○○○○
○○○○○○

Final

○○○
○○
○

Xifratge

Xifratge



Disc Dur

Métodes del propi sistema operatiu:

- ▶ **Windows:** BitLocker
- ▶ **OS X:** FileVault
- ▶ **Linux:** LUKS

Métode alternatiu:

- ▶ **Multiplataforma:** VeraCrypt



USB / Particions / Fitxers

VeraCrypt

- ▶ Permet xifrar particions
- ▶ Permet xifrar USB
- ▶ Permet xifrar fitxers
- ▶ Permet guardar tots els documents xifrats en un sol fitxer.
Facilita la movilitat.
- ▶ Tan per xifrar com per desxifrar, es necessari que el programa estigui instal·lat.

A tenir en compte

- ▶ Protegeix només contra atacants que tinguin accés físic, no d'atacs dirigits des de Internet.
- ▶ No es pot recuperar la contrasenya a no ser que es disposi d'una clau de recuperació.
- ▶ Un cop xifrat, no es poden recuperar les dades.
- ▶ Xifrar tot el disc evita filtracions.

Mòbil



Smartphone

Actualment els smartphones són ordinadors en miniatura capaços de fer gaire bé el mateix que un ordinador portàtil o de sobretaula.

Això implica que, igual que els ordinadors, tenen problemes de seguretat i la privacitat de l'usuari pot ser compromesa.

De fet, és més fàcil comprometre un dispositiu mòvil ja que els usuaris no estan concienciats.

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○●○
○○○○○○○○○○
○○○○○

Comunicacions

○○○○○○○○○○
○○○○○○○○
○○○○○

Coordinació

○○○○○
○○○○
○○○○○

Final

○○○
○
○

Introducció

Evaluació de riscos

Riscos

- ▶ Geolocalització
- ▶ Substracció del dispositiu
- ▶ Accés aplicacions sense necessitat d'introduir contrasenya
- ▶ Infecció de malware

Mitigacions

- ▶ Xifratge
- ▶ Contrasenya desbloqueig
- ▶ Gestió del sistema de localització
- ▶ Actualitzacions

Sistema operatiu



Securització



Xifratge

Android

- ▶ Opcions del telèfon - Seguretat - Xifratge
 - ▶ Sinó apareix l'opció, implica que ja està xifrat
- ▶ Fer una copia de seguretat abans
- ▶ El procés pot durar 1 hora
- ▶ Tenir el dispositiu amb més d'un 80% de bateria

iOS

- ▶ Mòbils superiors a Iphone3G ja té el disc xifrat per defecte

Cellebrite (Software Israelià)



Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○●○○○○○○
○○○○○

Comunicacions

○○○○○○○○
○○○○○○
○○○○○

Coordinació

○○○○
○○○
○○○○○

Final

○○○
○
○

Securització

GreyKey (Software EEUU)



Característiques software policial

1. Fer atacs de força bruta o diccionari per esbrinar el PIN
2. Evasió sistema de bloqueig després d'intents fallits
3. Instalació software maliciós
4. Comprometre el sistema aconseguint ser administrador

Característiques software policial - Protecció

Fer atacs de força bruta o diccionari per esbrinar el PIN

- ▶ Contrasenyes fortes
- ▶ Activar que el mòbil es bloquegi al cap de X intents

Per exemple:

- ▶ 3 intents: 30 segons
- ▶ 5 intents: 5 min
- ▶ 10 intents: 30 min
- ▶ 15 intents: 2h

Això incrementa exponencialment el temps que s'ha d'invertir per descobrir una contrasenya

Característiques software policial - Protecció

Evasió sistema de bloqueig després d'intents fallits

- ▶ Contrasenyes fortes

Asumint un codi decimal i evasió del SEP throttling:

- ▶ 4 díigits: 6.5 minuts
- ▶ 6 díigits: 11.1 hores
- ▶ 8 díigits: 46 dies
- ▶ 10 díigits: 12 anys

Característiques software policial - Protecció

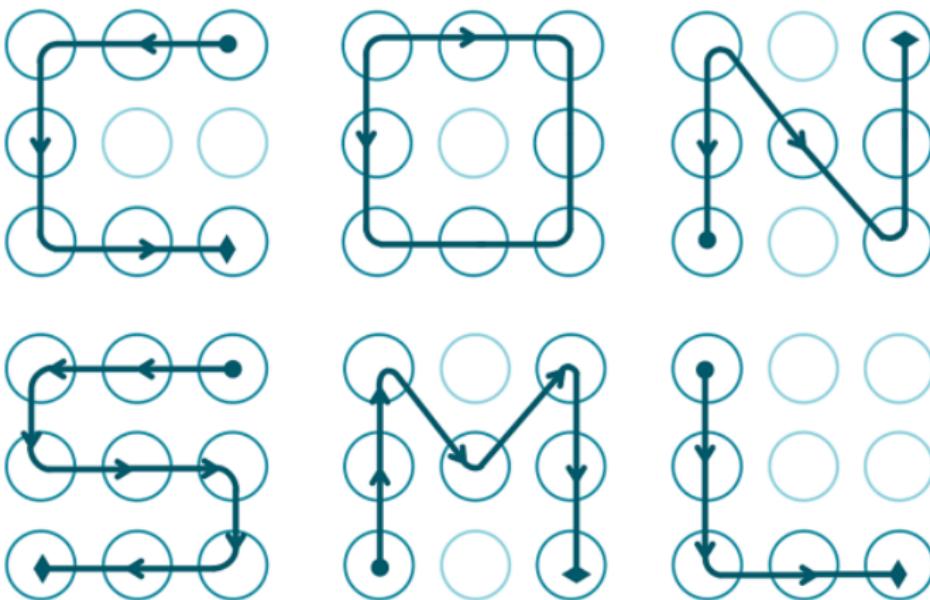
Instalació software maliciós

- ▶ Tenir el sistema actualitzat
- ▶ En cas de detenció, tirar o formatejar el telèfon.

Comprometre el sistema aconseguint ser administrador

- ▶ Tenir el sistema actualitzat

Patrons



Emprempta dactilar i reconeixement facial

Avantatges:

- ▶ No és necessari recordar una contrasenya
- ▶ No poden veure la contrasenya si es desbloqueja en públic
- ▶ Els atacs de força bruta passen a ser ineficients

Desvantatges:

- ▶ S'està investigant com extreure premses dactilars i cares de fotografies
- ▶ Molt fàcil d'immovilitzar i forçar a l'usuari per desbloquejar el telèfon

Conclusions

Contrasenya forta! – Alphanumèrica

Tenir el mòbil actualitzat sempre.

Evitar utilitzar mòbils amb sistemes operatius obsolets, anteriors a:

- ▶ **iPhone:** iPhone 6 (2018)
- ▶ **Android:** Oreo (8.0) (2017)

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
●○○○○

Comunicacions

○○○○○○○○○○
○○○○○○○○
○○○○○

Coordinació

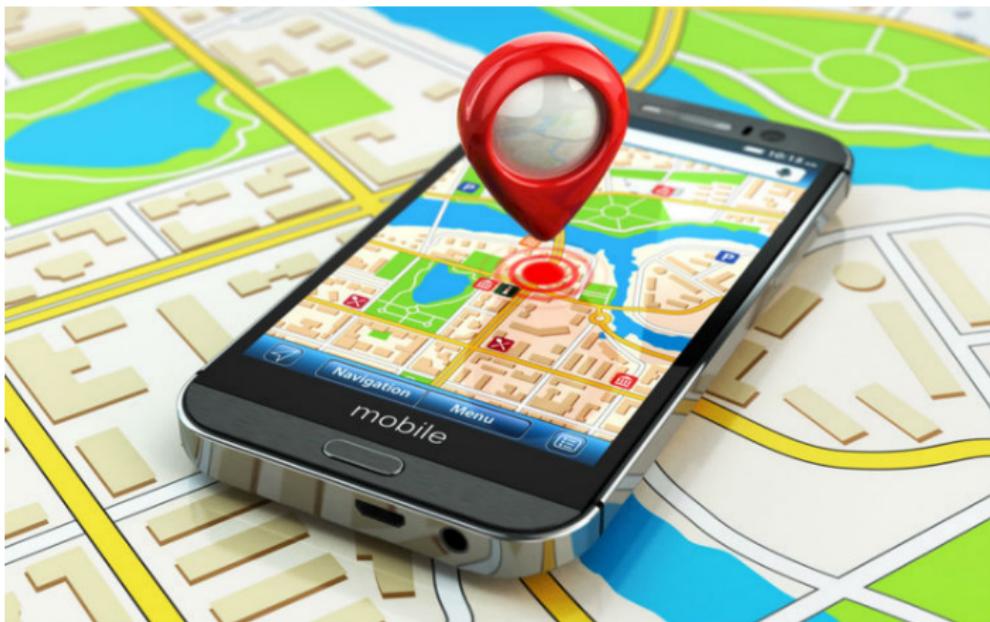
○○○○○
○○○○
○○○○○

Final

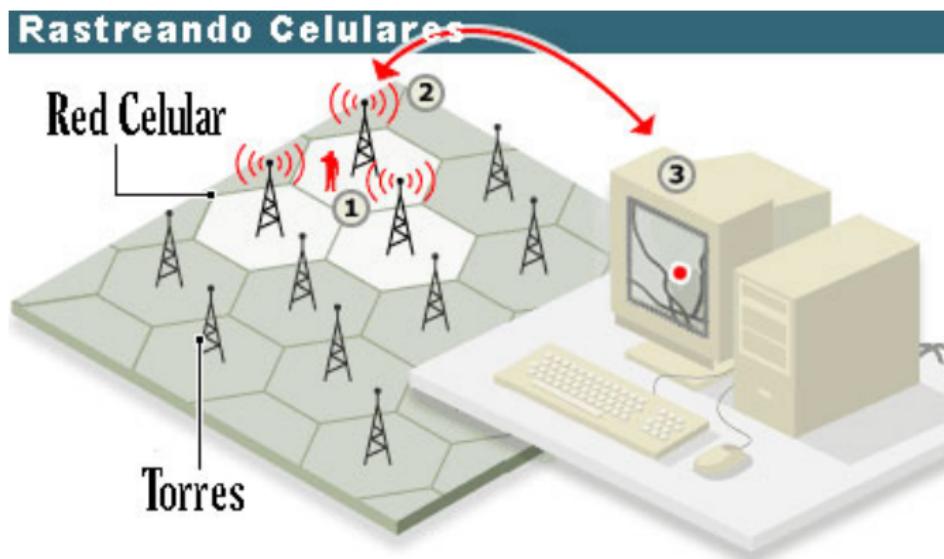
○○○
○○○
○

Rastreig de localització

Rastreig de localització



Torres de telefonia



Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○
○○○○
○○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○
○○●○○○

Comunicacions

○○○○○○○○
○○○○○○○○
○○○○○○○○

Coordinació

○○○○
○○○○
○○○○○○

Final

○○○
○○○
○

Rastreig de localització

Torres de telefonia

Un operador pot localitzar un telèfon si:

- ▶ El dispositiu està encés
- ▶ El dispositiu està registrat a la xarxa

Dades que emmagatzema:

- ▶ Personals: nom, dni, adreça vivenda
- ▶ Trucades: número origen, destí, data, durada i contingut
- ▶ Localització

Evasió

No hi ha cap manera de d'escapar d'aquest tipus de rastreig.

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○
○○○●○○

Comunicacions

○○○○○○○○
○○○○○○○○
○○○○○○○○

Coordinació

○○○○
○○○○
○○○○○○

Final

○○○
○○○
○

Rastreig de localització

Simulador de torre telefònica

El govern o les autoritats utilitzen torres de telefonia falses, IMSI (International Mobile Subscriber Identity) catcher, per obtenir la presència física i/o interceptar les comunicacions dels dispositius.

Detecció

Algunes aplicacions diuen de detectar els simuladors, però la detecció és imperfecta

Introducció

○○
○○○
○○○○

Rastreig de localització

Seguretat física - Ordinador

○○○○○
○○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○

Comunicacions

○○○○○○○○
○○○○○○○○

Coordinació

○○○○○
○○○○
○○○○○○

Final

○○○
○○○
○

GPS

El GPS (Global Position System) permet calcular la localització d'un dispositiu de manera ràpida i exacta.

El GPS opera basat en l'anàlisi de les senyals que envien uns satèl·lits al servei públic, operats pels EEUU.

Falsa Creença

Els satèl·lits NO observen ni tenen coneixement de l'ubicació dels dispositius dels usuaris, només emeten senyals.

GPS

Són les aplicacions que, si tenen permisos, fan les peticions al satèl·lit per obtenir la localització del dispositiu.

- ▶ Aplicacions instal·lades per l'usuari
- ▶ Aplicacions del proveidor d'Internet
- ▶ El sistema operatiu i software de tercers
- ▶ Navegant per Internet

On poden enviar la localització:

- ▶ Altres usuaris que utilitzin la app
- ▶ Proveedor d'Internet
- ▶ Servidors d'empreses privades

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○
○○○
○○○

Seguretat física - Mòbil

○○○
○○○○○○○○
○○○○○

Comunicacions

●○○○○○○○
○○○○○○
○○○○○

Coordinació

○○○○
○○○
○○○○○

Final

○○○
○
○

Anonimat

Anonimat



Introducció



Anònimat

Seguretat física - Ordinador



Seguretat física - Mòbil



Comunicacions



Coordinació



Final



Evaluació de riscos

Riscos

- ▶ Interceptació de les comunicacions.
- ▶ Identificació de la persona física.

Mitigacions

- ▶ Amagar les connexions.
- ▶ Serveis d'anonimització.

Introducció

○○
○○○
○○○○

Anònimat

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○○

Comunicacions

○○●○○○○○○
○○○○○○
○○○○○

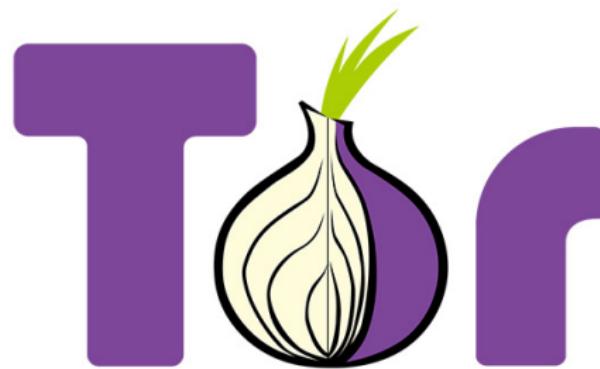
Coordinació

○○○○○
○○○○
○○○○○○

Final

○○○
○○○
○

Tor



Introducció

oo
ooo
oooo

Seguretat física - Ordinador

ooooo
oooo
oooo

Seguretat física - Mòbil

oooo
oooooooooooo
ooooooo

Comunicacions

oooo●ooooo
oooooooo
oooooo

Coordinació

ooooo
oooo
oooooo

Final

ooo
o

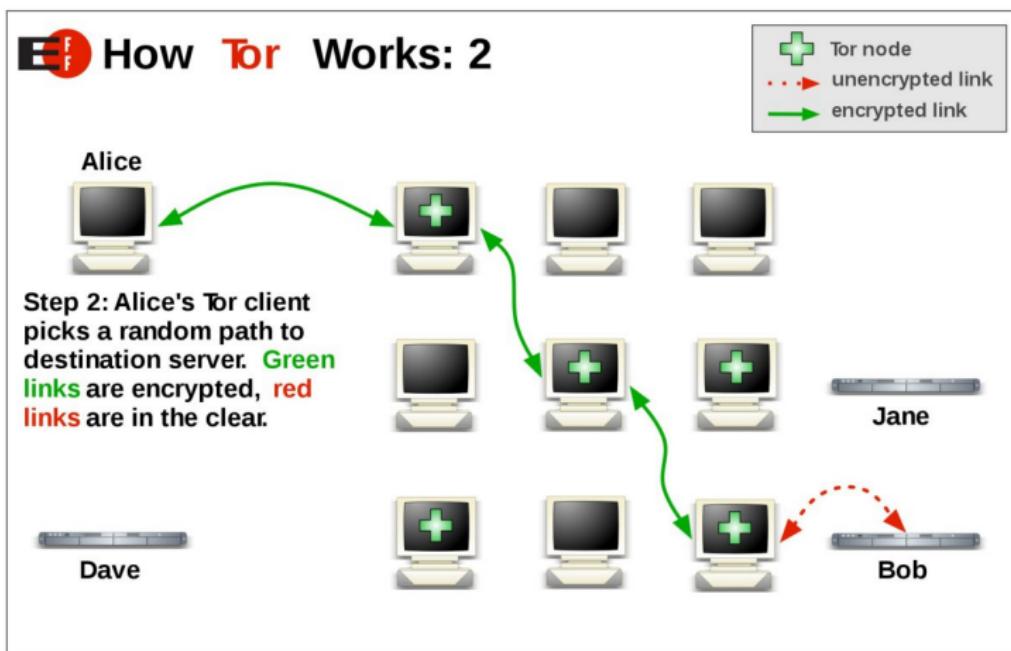
Anonimat

Què és?

"Promovemos los derechos humanos y defendemos tu privacidad en linea a través del software libre y las redes abiertas."

- ▶ Tor Project és una ONG 501(c)3 US
- ▶ Software lliure
- ▶ Sistema de proxys amb múltiples capes de xifratge
- ▶ Defensa contra la vigilància a la xarxa
- ▶ Evita que l'usuari sigui rastrejat
- ▶ Evadeix censura

Estructura



Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○

Comunicacions

○○○○○●○○○
○○○○○○○○
○○○○○

Coordinació

○○○○○
○○○○
○○○○○○

Final

○○○
○○○
○

Anonimat

VPN



Introducció



Anonimat

Seguretat física - Ordinador



Seguretat física - Mòbil



Comunicacions



Coordinació



Final



Què és?

Virtual Private Network

Xarxa virtual capaç de connectar diversos dispositius com si estiguessin físicament a un mateix lloc.

- ▶ Integritat: xifra les comunicacions entre el client i el servidor VPN
- ▶ Privacitat: amaga l'IP del client
- ▶ Permet evitar la censura (geolocalització)

Introducció



Anònimat

Seguretat física - Ordinador



Seguretat física - Mòbil



Comunicacions



Coordinació



Final



Estructura



Introducció



Anònimat

Seguretat física - Ordinador



Seguretat física - Mòbil



Comunicacions



Coordinació



Final



Conclusions

VPN

- ▶ Privacitat per política
- ▶ Permet escollir el servidor de sortida
- ▶ Més velocitat
- ▶ De pagament ja que és empresa privada

Tor

- ▶ Privacitat per disseny
- ▶ Menys velocitat
- ▶ Gratuït ja que és una ONG

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○

Comunicacions

○○○○○○○○○○
●○○○○○○
○○○○○

Coordinació

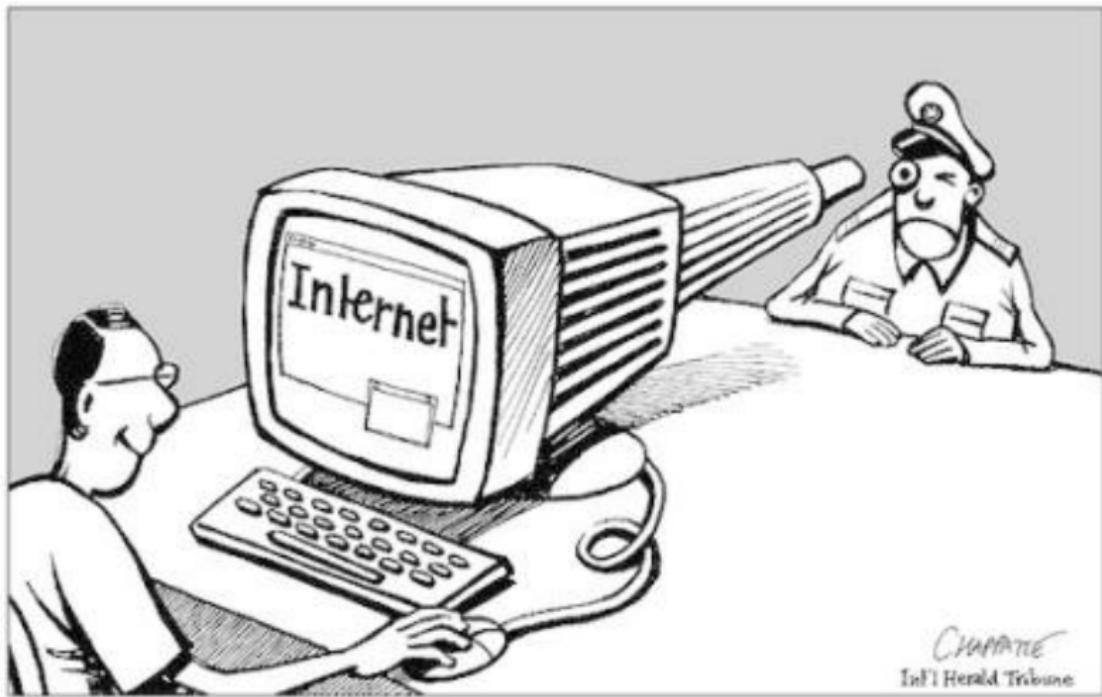
○○○○
○○○
○○○○○

Final

○○○
○
○

Comunicacions

Comunicacions



Protegir-nos és feina de totes!

Anti-Repressió Digital

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○

Comunicacions

○○○○○○○○○○
○●○○○○○○
○○○○○

Coordinació

○○○○○
○○○○
○○○○○

Final

○○○
○○○
○

Comunicacions

Evaluació de riscos

Riscos

- ▶ Interceptació de les comunicacions.
- ▶ Emmagatzematge insegur.
- ▶ Aplicacions insegures.

Mitigacions

- ▶ Utilitzar protocols segurs.
- ▶ Utilitzar aplicacions segures.
- ▶ Saber què utilitzar en cada situació.

Trucades i SMS

La policia pot:

- ▶ Localitzar el dispositiu sense ordre judicial
- ▶ Obtenir el llistat de trucades sense ordre judicial
- ▶ Interceptar trucades amb ordre judicial

Important

Evitar-ho sempre que sigui possible o parlar en clau (no gaire segur).

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○

Comunicacions

○○○○○○○○○○
○○○●○○○
○○○○○

Coordinació

○○○○
○○○○
○○○○○

Final

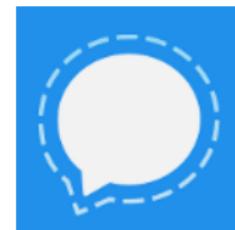
○○○
○
○

Comunicacions

Alternativa trucades

Protegeixen la privacitat:

- ▶ Signal
- ▶ Jitsi



Altres:

- ▶ Telegram
- ▶ Whatsapp



Missatgeria instantània

Protegeixen la privacitat:

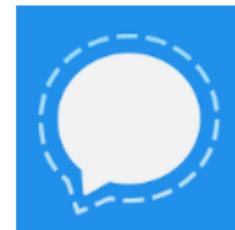
- ▶ Signal
- ▶ Wire

Alternatives:

- ▶ Sistema federats: Element
- ▶ Sistemes P2P: Briar o Jami

Altres

- ▶ Telegram
- ▶ Whatsapp



Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○○○○

Comunicacions

○○○○○○○○○○
○○○○●○○○○○
○○○○○○○○○○

Coordinació

○○○○
○○○○
○○○○○○○○

Final

○○
○

Comunicacions

Email

ProtonMail

- ▶ Xifratge extrem a extrem (entre ProtonMails)
- ▶ No xifra l'assumpte
- ▶ Seu a Suïssa



Tutanota

- ▶ Xifratge extrem a extrem
- ▶ Seu a Alemanya



Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○

Comunicacions

○○○○○○○○○○
○○○○○●
○○○○○

Coordinació

○○○○
○○○
○○○○○

Final

○○○
○
○

Comunicacions

Núvol



Online

- ▶ Cryptpad
- ▶ Sync



Self-Hosted

- ▶ NextCloud



Alternativa

- ▶ Mega

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○○

Comunicacions

○○○○○○○○○○
○○○○○○○○
●○○○○○

Coordinació

○○○○
○○○○
○○○○○○

Final

○○○
○
○

Aplicacions

Aplicacions



Navegadors

Problemàtics

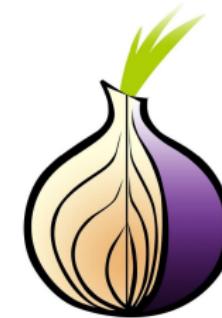
- ▶ Chrome
- ▶ Safari
- ▶ Internet Explorer



I'm Watching You

Protegeixen la privacitat

- ▶ Firefox
- ▶ Brave
- ▶ Tor Browser



Cercadors

Problemàtics

- ▶ Google
- ▶ Bing
- ▶ Yahoo



Protegeixen la privacitat

- ▶ DuckDuckGo (Estats Units)
- ▶ StartPage (Països Baixos)
- ▶ searx (software lliure)
- ▶ Swisscows (Suïssa)



Introducció

○○
○○○
○○○○

Aplicacions

Seguretat física - Ordinador

○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○○○○

Comunicacions

○○○○○○○○○○
○○○○○○○○○○
○○○●○○

Coordinació

○○○○
○○○○
○○○○○○

Final

○○○
○○○
○

Tor

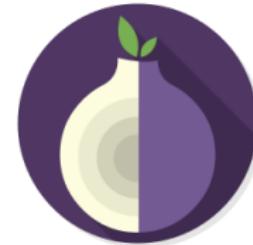
Navegador Tor

- ▶ Software lliure
- ▶ Navegador multiplataforma



Orbot

- ▶ Software lliure
- ▶ Tot el tràfic del mòvil passa per un proxy
- ▶ Utilitza Tor per xifrar i anonimitzar el tràfic



VPN

ProtonVPN

- ▶ Pla gratuït i desde 4 euros/mes
- ▶ Seu a Suïssa



IVPN

- ▶ 15 euros/mes
- ▶ Seu a Malta



Mullvad

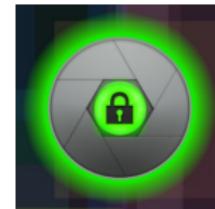
- ▶ 5 euros/mes
- ▶ Seu a Suècia



Càmera i metadades

ObscuraCam

- ▶ Guardian Project
- ▶ Elimina metadades que poguessin comprometre la privacitat



Elimina metadades:

- ▶ Photo EXIF Editor (Mòbil)
- ▶ MAT2 (PC)
- ▶ ExifCleaner (PC)



Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○○○○

Comunicacions

○○○○○○○○○○
○○○○○○○○
○○○○○○○○

Coordinació

●○○○○
○○○○
○○○○○○

Final

○○○
○

Coordinació

Coordinació



Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○
○○○○○○○○

Comunicacions

○○○○○○○○
○○○○○○○○
○○○○○○○○

Coordinació

○●○○○
○○○○
○○○○○○

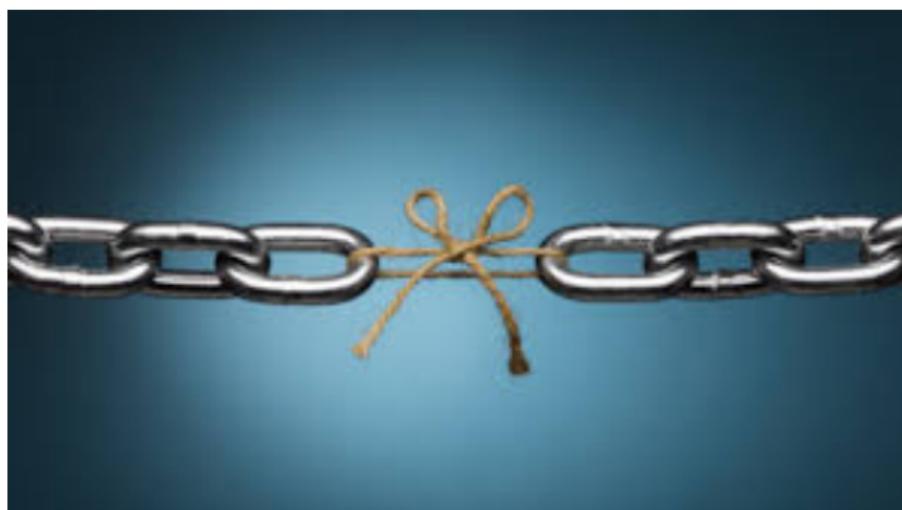
Final

○○○
○

Coordinació

Una cadena és tan forta com el seu enllaç més dèbil

Per molt segur que sigui un sistema, sempre té un punt dèbil.
L'atacant sempre intentarà accedir a través d'aquest.



Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○

Comunicacions

○○○○○○○○
○○○○○○○○
○○○○○○○○

Coordinació

○○●○○
○○○○
○○○○○○

Final

○○○
○

Coordinació

Príncipi del mínim privilegi

El príncipi de mínim privilegi és una disciplina de seguretat que s'assegura que a un usuari, sistema o aplicació no se li otorgui cap privilegi adicional dels que són necessaris perquè duguin a terme la seva funció.

- ▶ Redueix el risc en cas de compromís
- ▶ Redueix el risc de fuga d'informació

Preparació pla de seguretat

Decidir un pla de seguretat que s'ajusti al nivell determinat i a les necessitats específiques dels membres.

- ▶ **Nivell de seguretat:** telegram, signal, gmail, protonmail...
- ▶ **Pla per cada situació:** reunions, accions...
- ▶ **Detecció**
- ▶ **Concienciació**
- ▶ **Preparació estructura tecnològica:** grups, usuaris, permisos carpetes...

A tenir en compte:

- ▶ **Limitacions tecnològiques**
- ▶ **Limitacions organitzatives / accions**

Pla de contingència

Determinar les accions a dur a terme si es detecta que algun membre o sistema ha sigut compromés.

- ▶ Detectar el sistema o persona compromesa
- ▶ Determinar l'abast

Accions

- ▶ Solució sense pèrdues
- ▶ Eliminar sistema o informació específica
- ▶ Eliminar-ho tot

Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○○○
○○○○○○○○

Comunicacions

○○○○○○○○○○
○○○○○○○○
○○○○○○○○

Coordinació

○○○○○
●○○○
○○○○○

Final

○○○
○

Exemple proposta

Exemple proposta

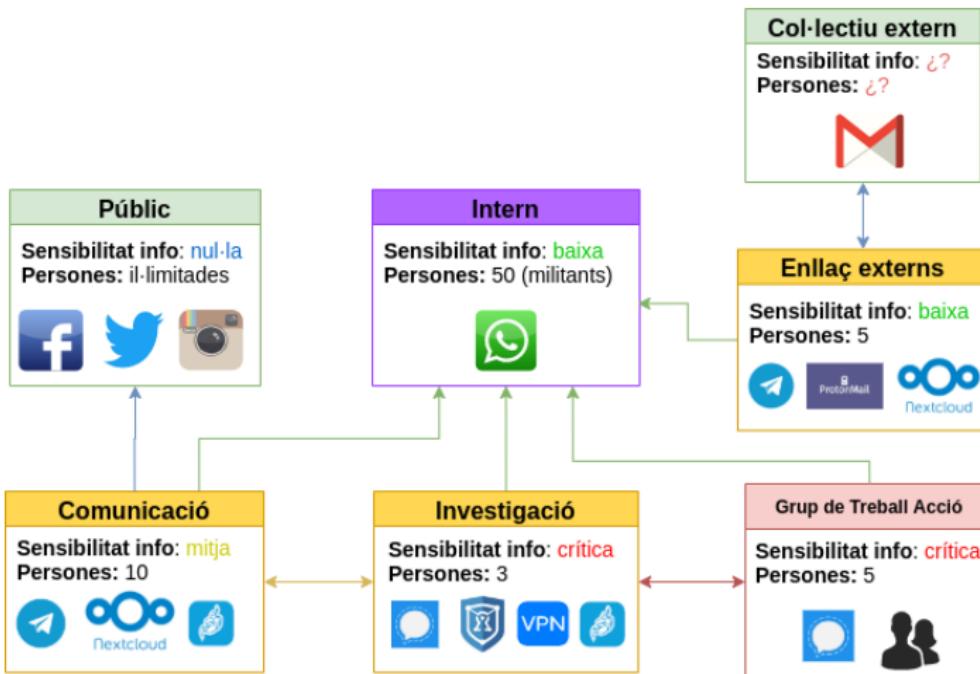


Introducció

Seguretat física - Ordinador
 ○○
 ○○○
 ○○○○

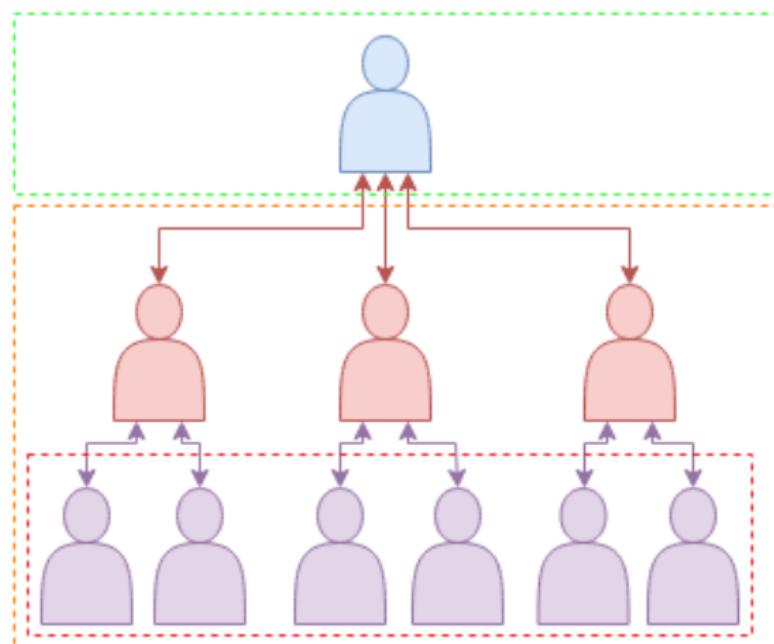
Exemple proposta

Diagrama proposta seguretat



Exemple proposta

Diagrama proposta accions



Introducció



Seguretat física - Ordinador



Seguretat física - Mòbil



Comunicacions



Coordinació



Final



Exemple proposta

Conclusions

Resumint:

- ▶ Determinar nivell de seguretat.
- ▶ Determinar canals de comunicació segons necessitat i seguretat.
- ▶ Una persona que no està a un grup de treball no necessita saber els detalls.
- ▶ Tothom hauria de col·laborar en ajudar a protegir la privacitat i poder detectar filtracions o compromisos.
- ▶ Encara que existeixi una jerarquia en algunes situacions, tot es pot decidir a nivell assambleari.

Manifestacions i reunions



Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○
○○○○○○○○

Comunicacions

○○○○○○○○
○○○○○○○○
○○○○○○○○

Coordinació

○○○○○
○○○○
○●○○○○

Final

○○○
○○○
○

Manifestacions i reunions

Reunions

Recomanacions respecte els mòbils al fer reunions on es parlin coses sensibles:

- ▶ **Més segur:** deixar o apagar el mòbil a casa.
- ▶ **Segur:** apagar el mòbil durant el trajecte.
- ▶ **Localització lloc reunió:** apagar el telèfon abans de la reunió.
- ▶ **Localització participants i lloc:** Deixar el telèfon a una altra habitació.

Ordinadors

Ordinadors es podríen arribar a considerar segurs si no han estat compromesos.

Manifestacions: Abans

- ▶ Deixar el telèfon a casa o portar-lo apagat.
- ▶ Assegurar-se que el mòbil està xifrat.
- ▶ Fer una còpia de seguretat.
- ▶ Eliminar fotos, documents o converses sensibles (si és possible).
- ▶ Mantenir-lo en mode avió o desactivar GPS, WiFi, Bluetooth.
- ▶ Canviar el codi de desbloqueig per un temporal però segur.

Manifestacions: Durant

- ▶ Tenir el telèfon sempre controlat.
- ▶ Fer fotos i vídeos sense desbloquejar el telèfon.
- ▶ Utilitzar aplicacions que tapin les cares o eliminin les metadades instantàniament al fer fotos.
- ▶ Evitar comunicar-se més del necessari.
- ▶ Anar amb la cara tapada per evitar els sistemes de reconeixement facial (buff o mascareta).

Introducció



Seguretat física - Ordinador



Seguretat física - Mòbil



Comunicacions



Coordinació



Final



Manifestacions i reunions

Manifestacions: Després

- ▶ Eliminar les metadades, sobretot nom i marca del dispositiu i geolocalització.
- ▶ Tapar les cares si es publiquen fotos o vídeos a les xarxes socials.
- ▶ Assegurar-se que ningú de l'entorn hagi estat compromés.

Manifestacions: Detenció

- ▶ Trucar a un advocat.
- ▶ No dir res sense la presencia de l'advocat.
- ▶ No donar contrasenyes ni desbloquejar el dispositiu.
- ▶ Poden agafar el dispositiu com a evidència.
- ▶ Amb ordre judicial podrien obligar a desbloquejar el dispositiu.

Introducció



Bonus Track

Seguretat física - Mòbil



Comunicacions



Coordinació



Final



Introducció

○○
○○○
○○○○

Seguretat física - Ordinador

○○○○
○○○○
○○○

Seguretat física - Mòbil

○○○○
○○○○○○○○
○○○○○

Comunicacions

○○○○○○○○
○○○○○○
○○○○○

Coordinació

○○○○
○○○
○○○○○

Final

○○○
○○
○

Bonus Track

Bonus Track 1

Phishing a col·lectius de l'esquerra independentista per part de la policia.

- ▶ És il·legal.
- ▶ No ho poden utilitzar davant d'un jutge.
- ▶ Els hi serveix per obtenir informació sensible i sobre militants per ampliar l'investigació.

Important

Assegurar-se sempre que la persona de l'email o missatge és qui diu ser. Preguntar a gent del voltant abans d'enviar informació confidencial o donar-li accés.

Introducció



Bonus Track

Seguretat física - Ordinador



Seguretat física - Mòbil



Comunicacions



Coordinació



Final



Bonus Track 2

Vigileu que compartiu a les xarxes socials.

- ▶ Les companyies poden accedir a tots els missatges privats que envies i al teu perfil privat.
- ▶ Amb una ordre judicial, la policia pot aconseguir tots els teus missatges privats i perfil privat.
- ▶ Els tweets o publicacions poden utilitzar-se com a prova a un judici.
- ▶ És legal publicar vídeos i fotos sobre actuacions policials a les xarxes socials sempre i quant no es posi en perill a l'agent ni a la seva família.

Introducció



Seguretat física - Ordinador



Seguretat física - Mòbil



Comunicacions



Coordinació



Final



Anti-Repressió Digital

Protegir-nos és feina de totes!

Contacte:

projectenadki@protonmail.com