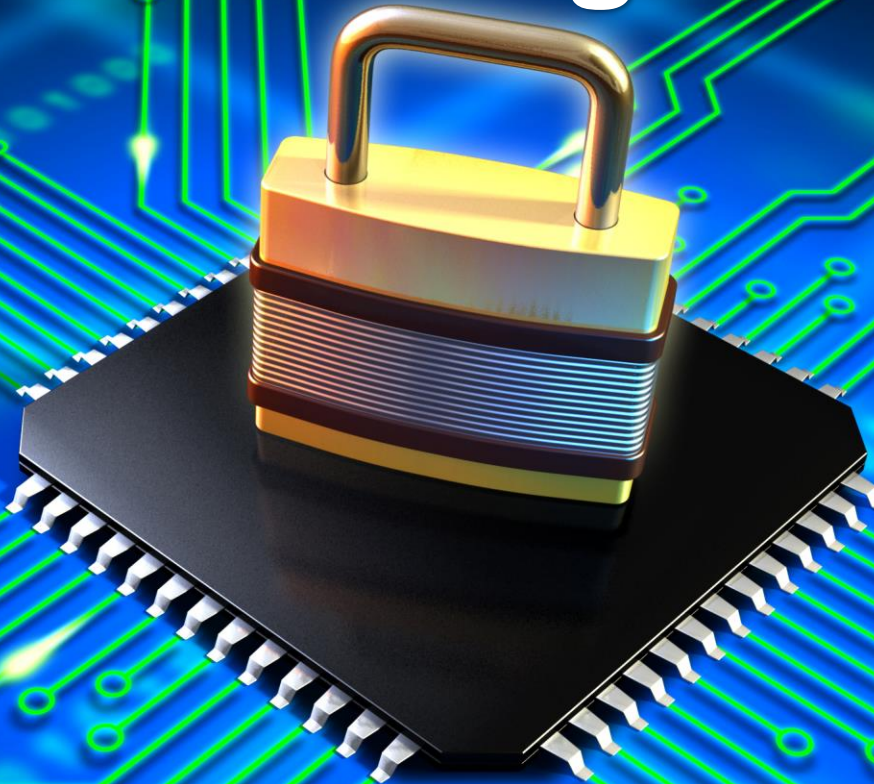
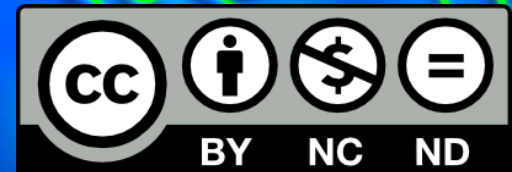


Seguretat en les comunicacions digitals



**Informàtics compromesos
amb la República (ICR)**



Atecedents



- Revalacions d'Edward Snowden (2014)
 - Espionatge massiu. Col·laboració entre operadors i empreses.
- Aliats per l'espionatge
 - Manca de “cultura i consciència digital”
 - Traça digital
 - Patrons de comportament
- “Jo no tinc res a amagar”
 - Segur? I en el futur?

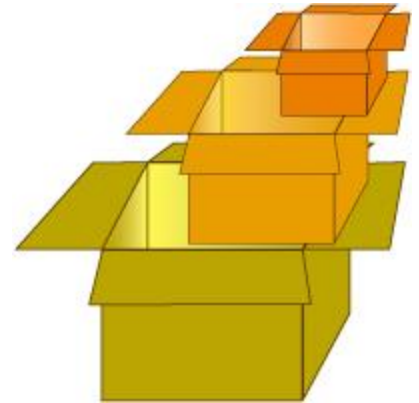
Index

- Estratègia
- Fonts d'informació
- Robatori d'aparells
- Infiltració de programari no desitjat
- Intercepció de comunicacions
- Altres traces
- Conclusions



Estratègia

- És impossible impedir l'accés a la informació
- Dificultar i/o retardar l'accés a la informació
- Compromís entre seguretat i comoditat
- Normalitzar l'ús d'aplicacions segures



Estratègia



- Accions petites que augmentin molt la seguretat
- Detectar el punt mes dèbil de la cadena i enfortir-lo
- Fer ús de criptografia de clau pública i privada
- Fer ús de programari lliure (en mesura del possible)
 - Firefox millor que Internet Explorer
 - Libreoffice millor que Microsoft Office
 - Qualsevol distribució de Linux millor que Windows o Mac

Fonts d'informació



■ Informació que donem nosaltres

- Conscientment: Xarxes socials, xats, e-mails, etc.
- Inconscientment: Metadades, geoposicionament, etc.

■ Informació que ens roben



Robatori d'aparells



Infiltració de programari no desitjat



Intercepció de comunicacions



Robatori d'aparells











- Accés a tota la informació de l'aparell
- Notificacions de la pantalla de bloqueig
- Extracció de maquinari
- Injecció de programari maliciós



Robatori d'aparells



- Bloquejats quan no s'usin 
- Deshabilitem les notificacions a la pantalla de bloqueig 
- Xifratge en el sistema i de les dades   
- Gestionar les actualitzacions  
- Molta atenció a les repliques descontrolades 



Infiltració de programari no desitjat







- Instal·lats sense el nostre consentiment
- Afecten a qualsevol dispositiu
- Els més famosos:
 - Screen recorders (grabadors de pantalla)
 - Sound recorders (grabadors de so)
 - Cam controllers (controlen la càmera)
 - Bots (exploren dades internes del dispositiu)
 - Trojan (prenen el control total del dispositiu)





Infiltració de programari no desitjat



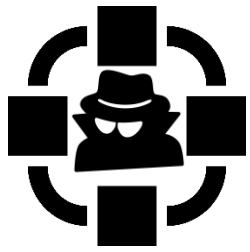
■ Ordinadors

- SOs i antivirus actualitzats actualitzats 
- Firewalls  
- Detecció de comportaments anòmals 

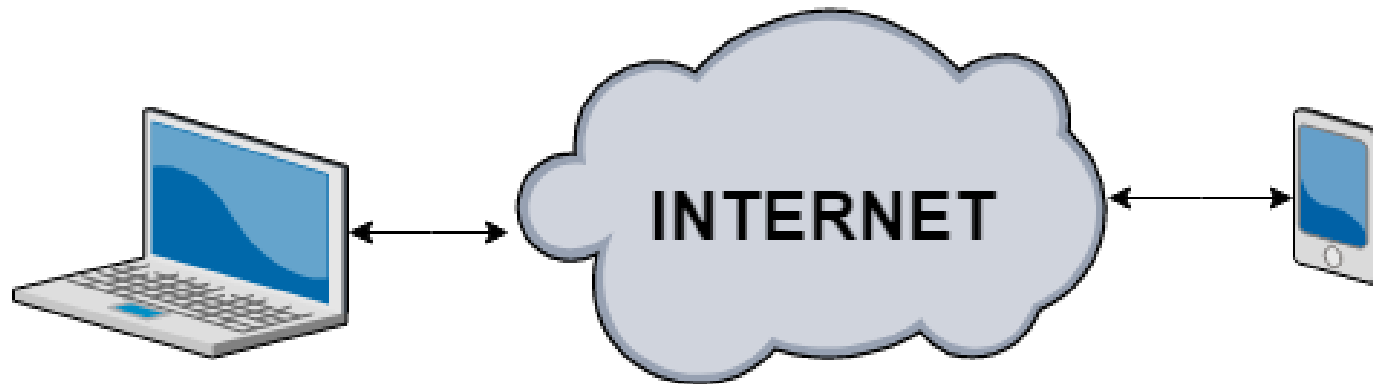
■ Mòbils i Tauletes

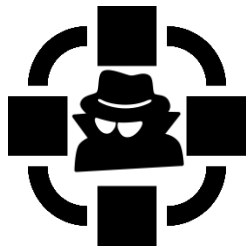
- Android: seguretat → origens desconeguts 
- Consum exagerat de bateria o dades a internet 

■ Evitar tenir els mòbils amb nosaltres quan parlem d'informació sensible

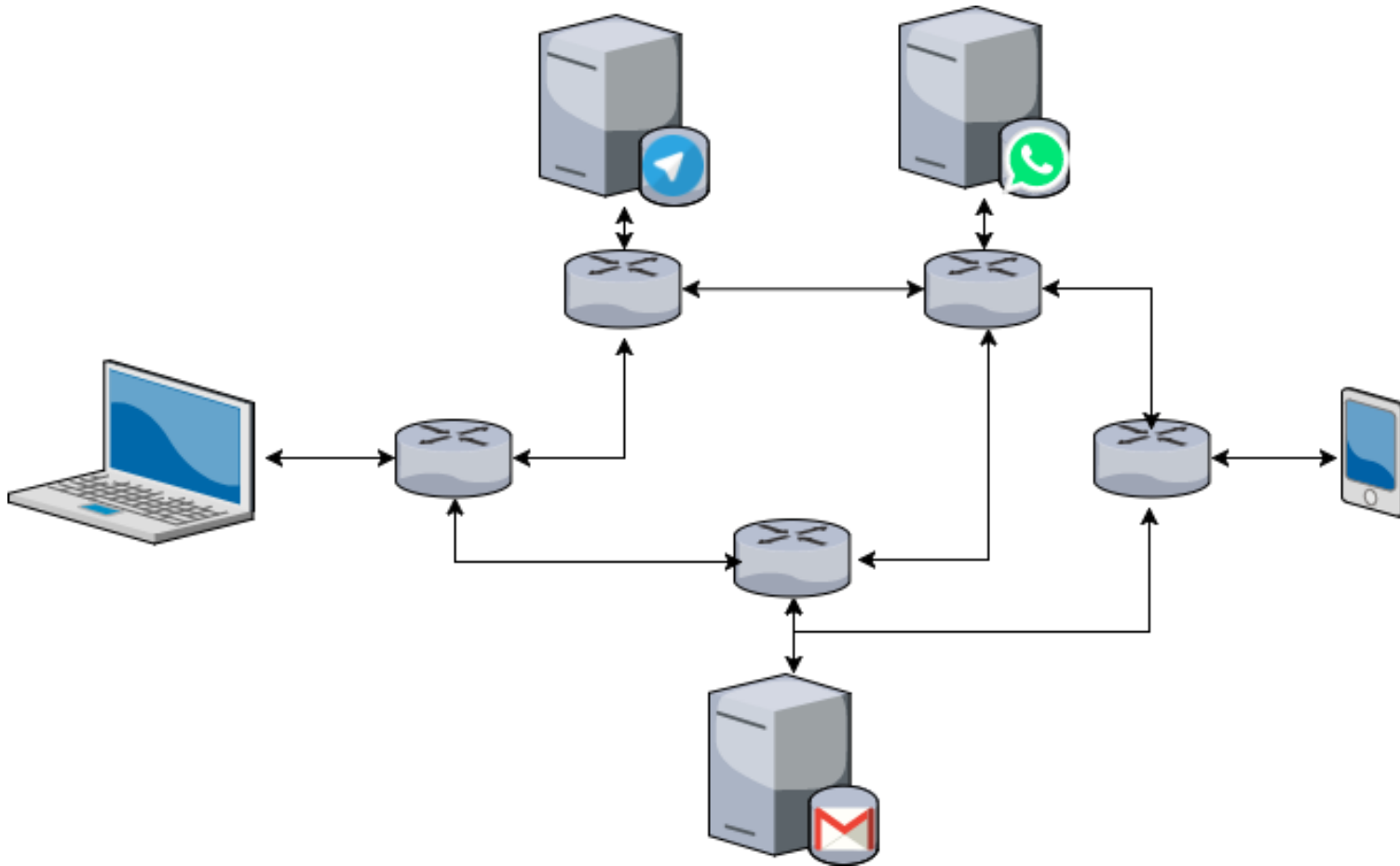


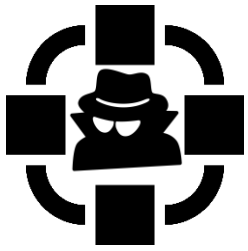
Intercepció de comunicacions



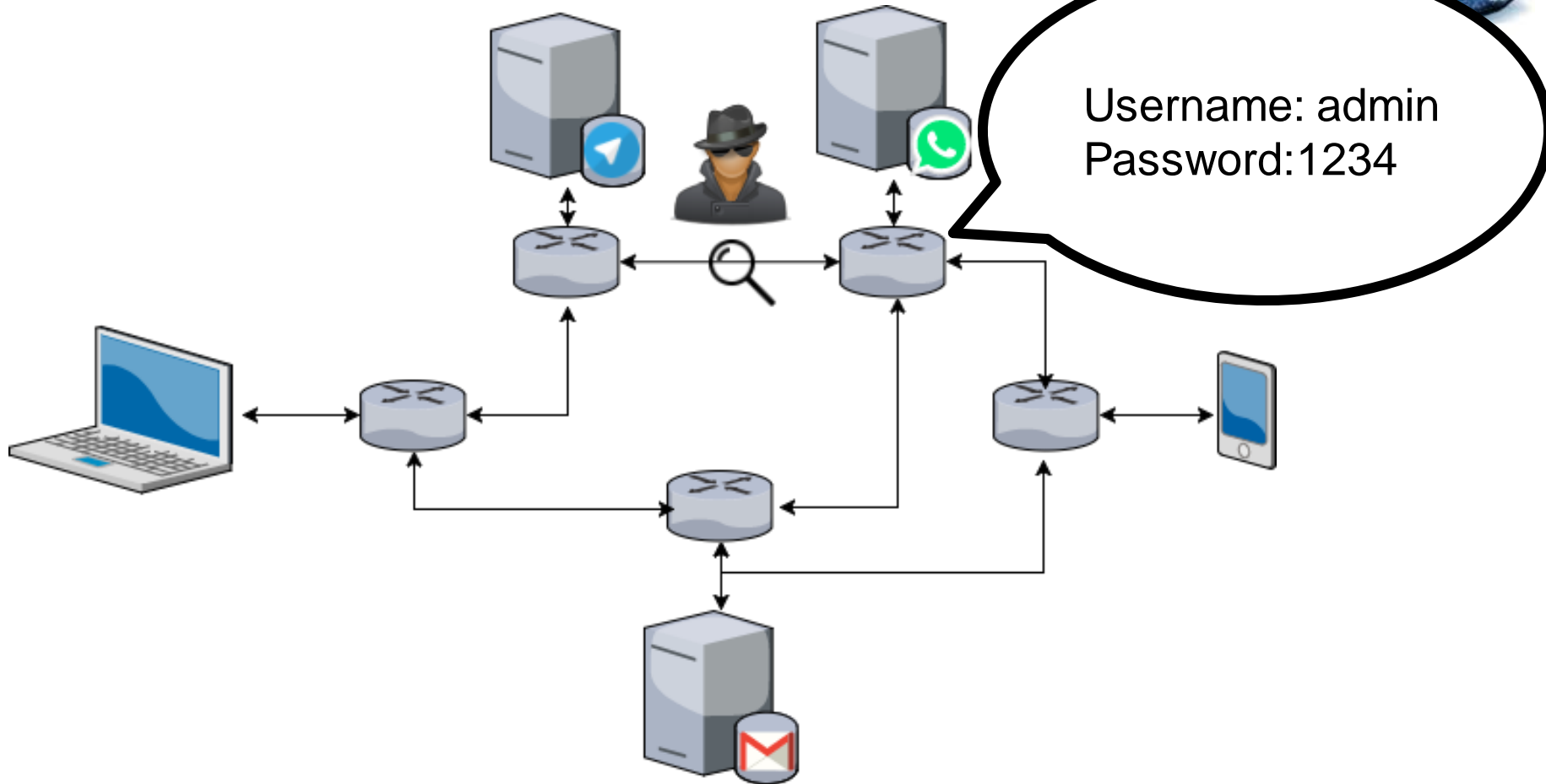


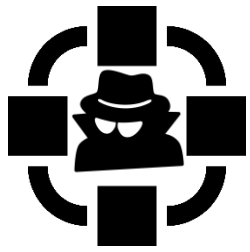
Internet és vulnerable



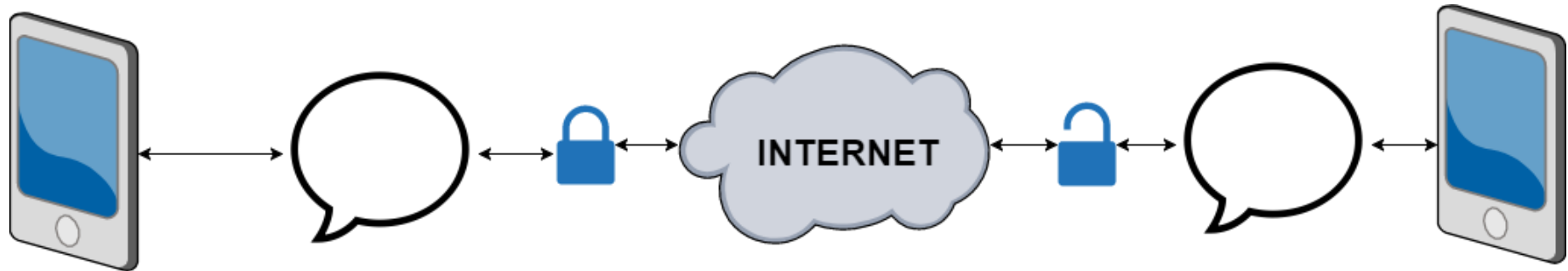


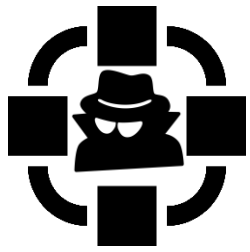
Punts de vulnerabilitat



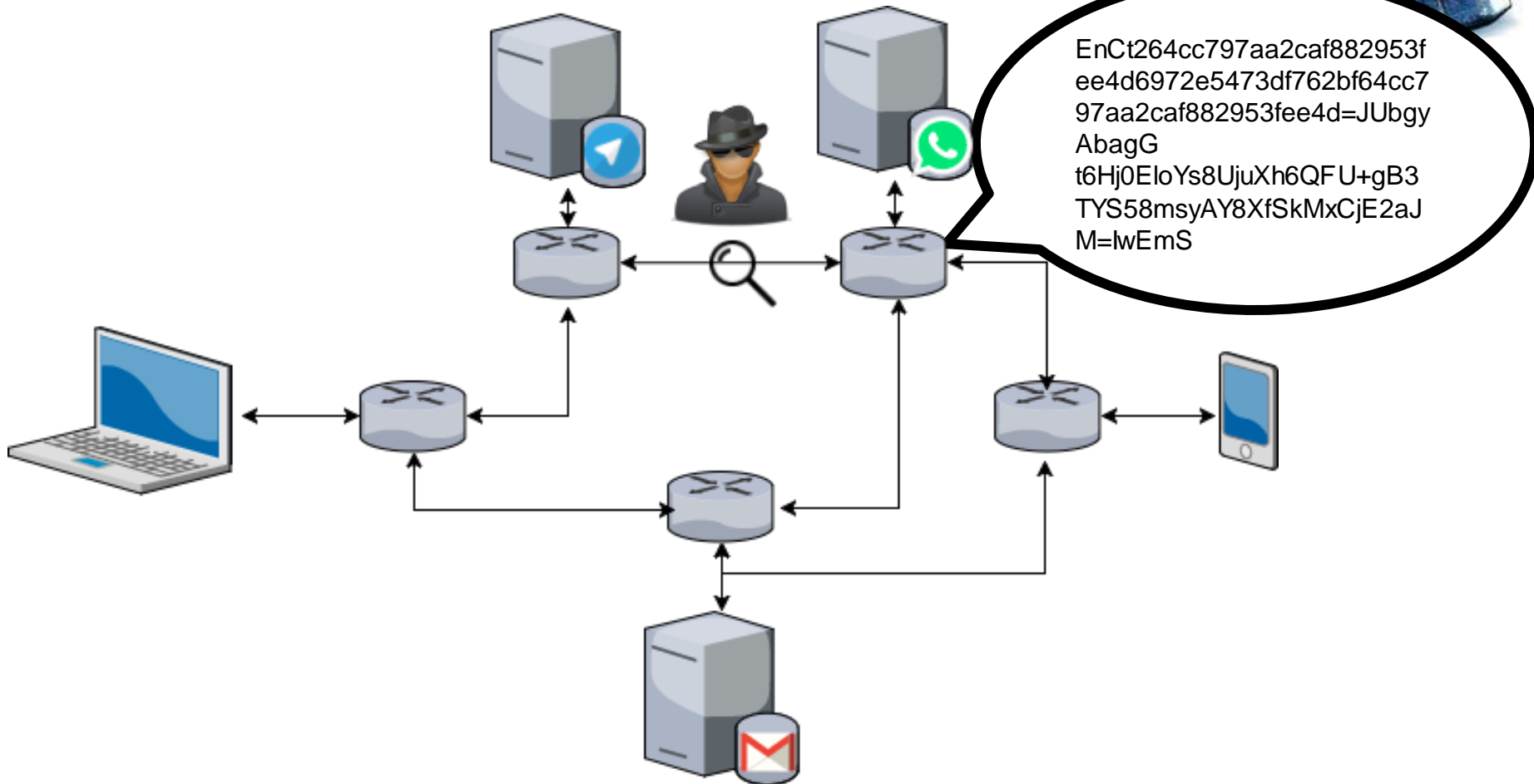


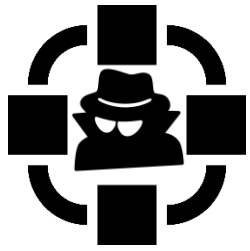
Seguretat a nivell d'aplicació





Xifratge

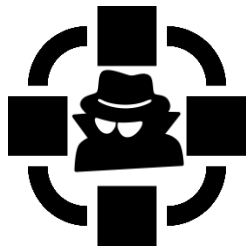




Apps de xat i veu



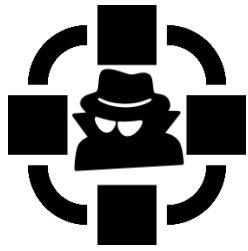
- Riot – molt segur, però ús incòmode
- Signal – bon compromís seguretat i ús;
 - recomanat per ús estàndard; moltes opcions de seguretat
- Telegram – es considera segur; força popular;
 - els “canals” permeten arribar a gran quantitat de gent (canals dels CDR, Assamblea, Òmnium, EnPeuDePau, etc.)
- Whatsapp – no es considera segur;
 - no recomanat



Apps de xat i veu



App	Popularitat	Missatges temporals	Xifartge entre dos terminals	Xifrage en grups	Seguretat
Riot	Baixa	Manualment	Per defecte	Per defecte	Molt alta
Signal	Conegut	Automàtic	Per defecte	Per defecte	Alta
Telegram	Alta	Automàtic	Xats secrets	No	Normal
WhatsApp	Molt Alta	No	Per defecte	No	Baixa



Correu

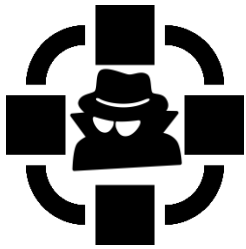


■ Serveis de correu (Gmail, Hotmail, etc.)

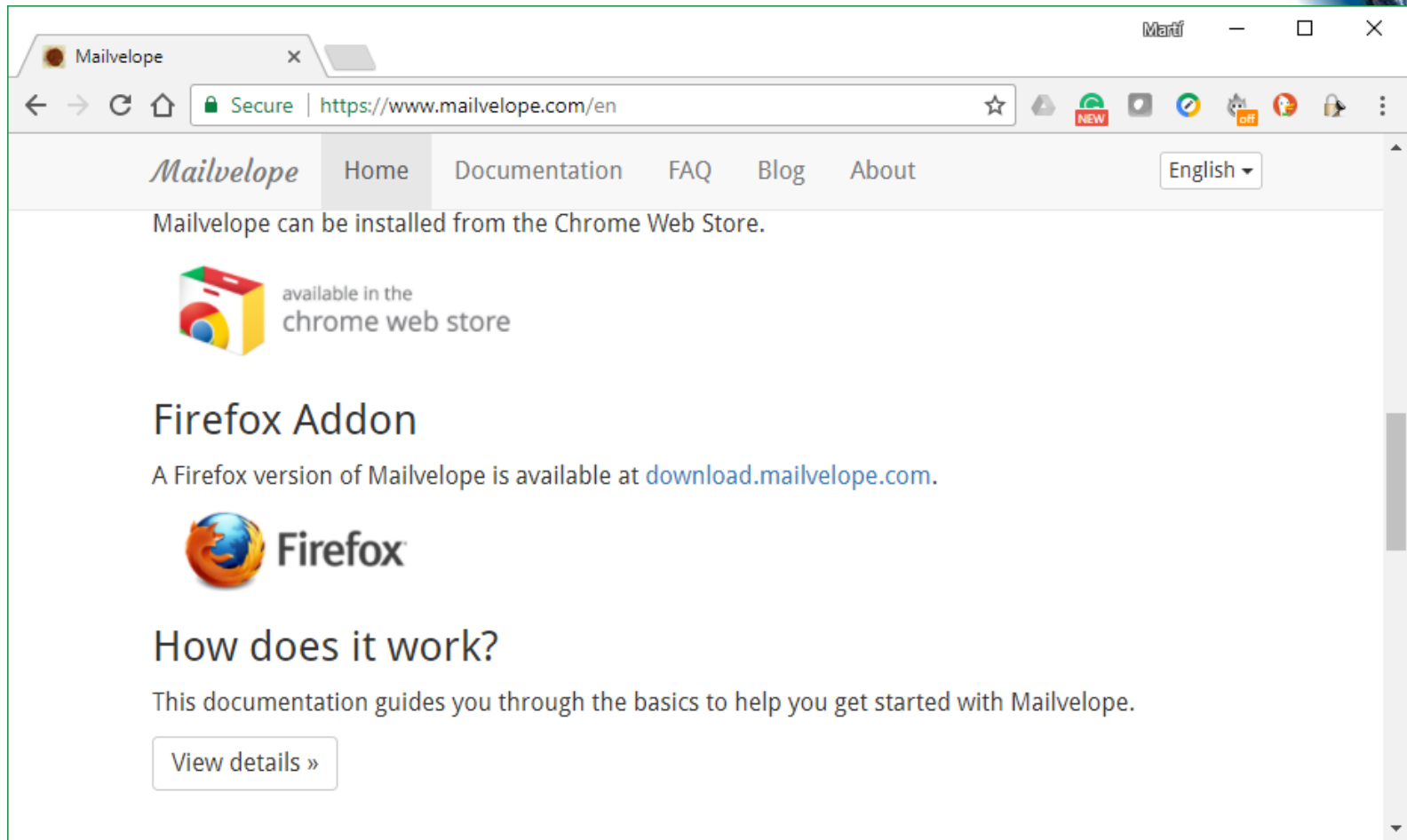
- Enviament de missatges NO xifrats
- Gestionats per una empresa
- Robots llegeixen e-mails per treure beneficis

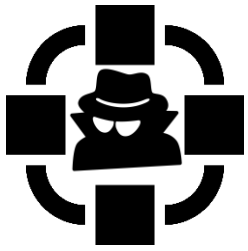
■ Mailvelope.com

- Xifratge per clau PGP (clau pública – privada)
- S'adapta a correus com Gmail, hotmail, yahoo, etc.
- No pot fer-se servir des del mòbil fàcilment

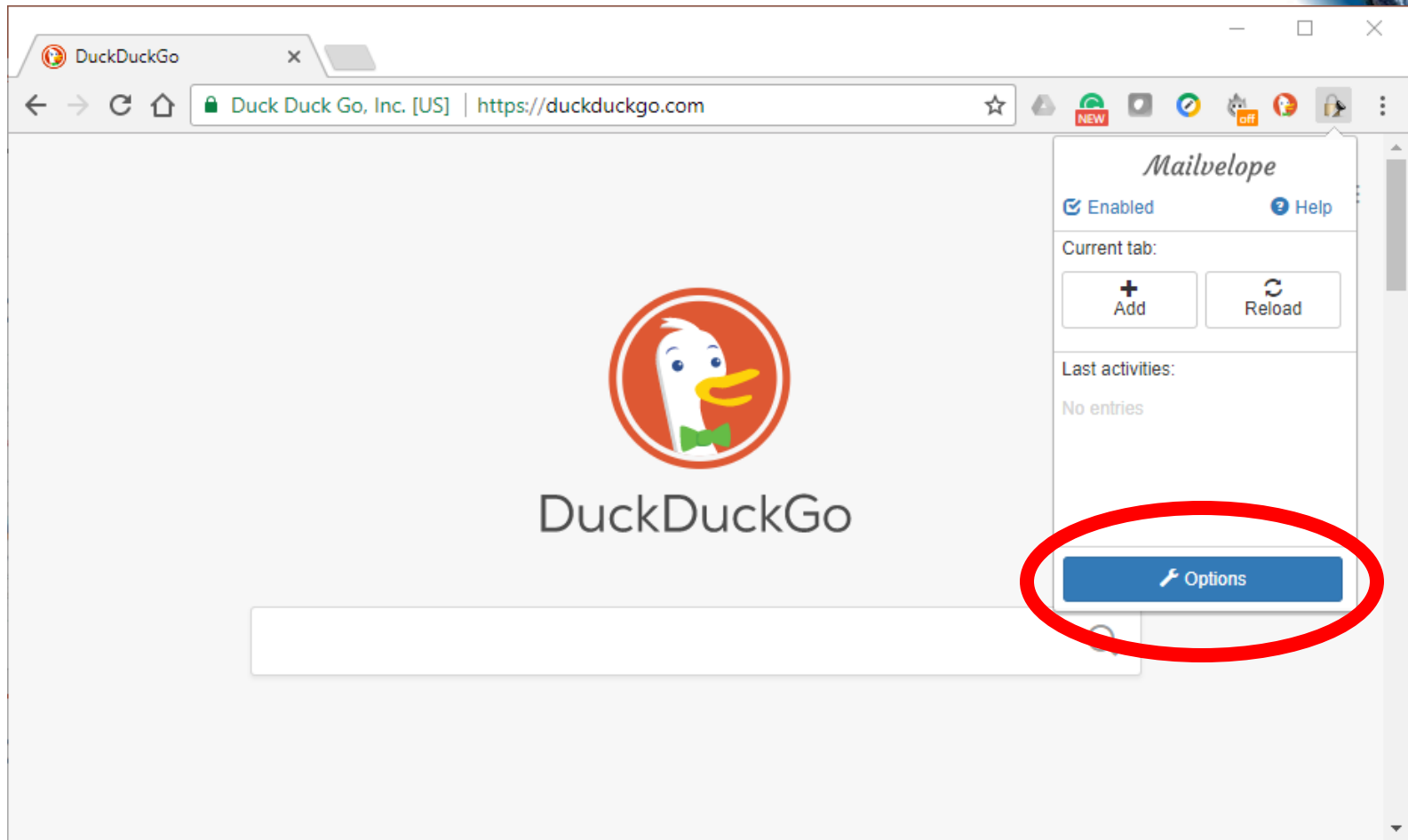
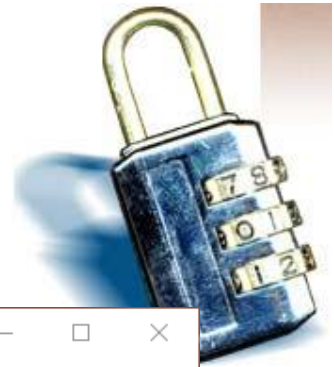


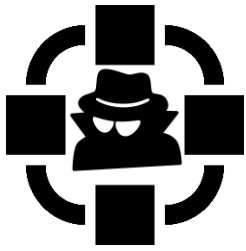
Correu



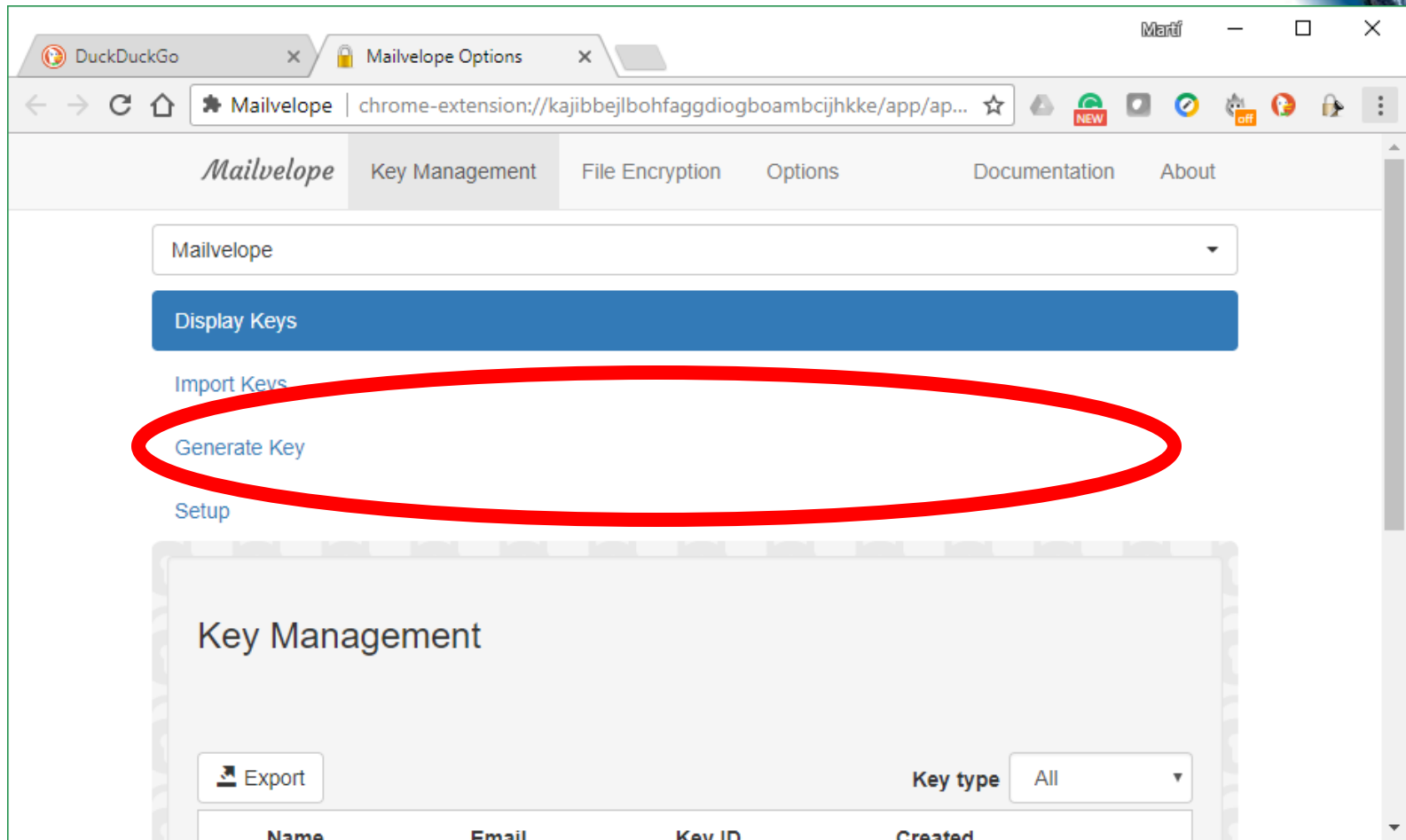


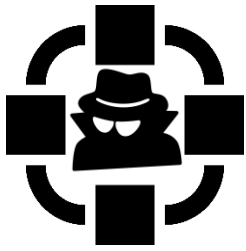
Correu





Correu





Correu



DuckDuckGo x Mailvelope Options x

Mailvelope | chrome-extension://kajibbejlbohfgagdiogboambcijhkke/app/app.ht... ☆

Mailvelope Key Management File Encryption Options Documentation About

Generate Key

Name

Full name of the key owner

Email

Advanced >>

Enter Password

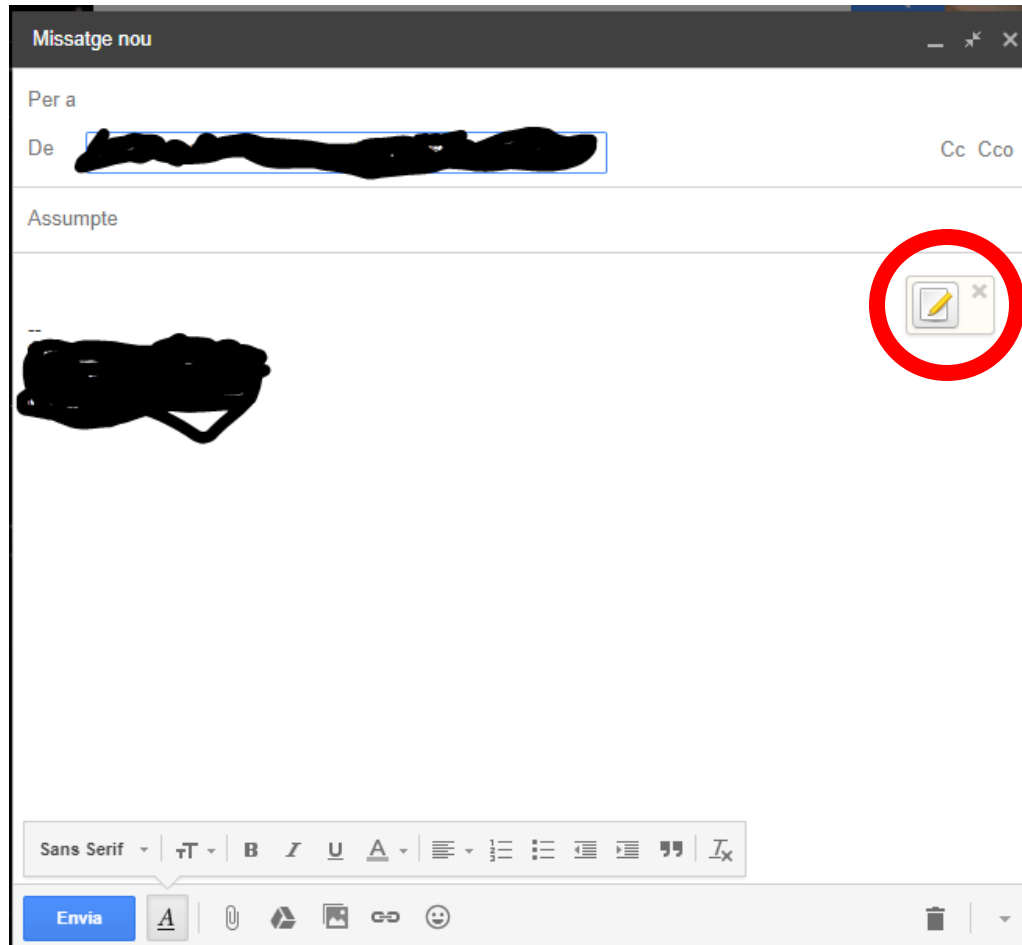
Password field is empty

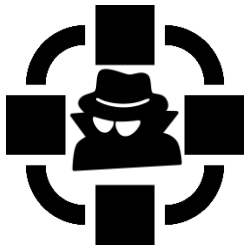
Re-enter Password

☒ Upload public key to Mailvelope Key Server (can be deleted at any time). [Learn more](#)

Generate Clear

chrome-extension://kajibbejlbohfgagdiogboambcijhkke/app/app.html#/keyring/setup





Correu



Compose Email

Compose Email

Add recipient

—
|

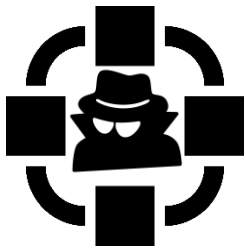
Encrypt files

Options

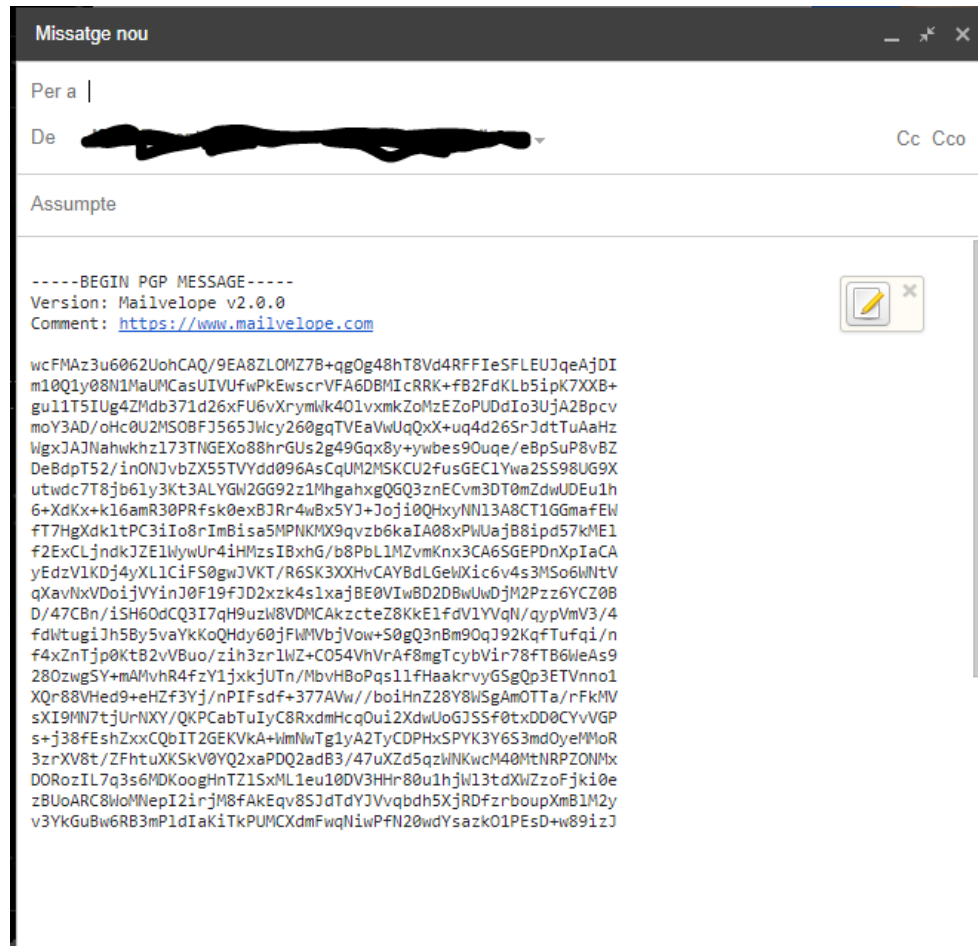
Sign Only

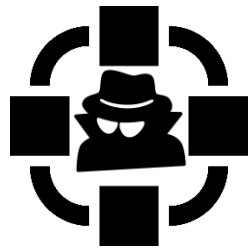
Cancel

Encrypt










Correu





Navegadors WEB



- Navegar en mode incògnit 
- Utilitzar navegadors dedicats 
- Esborrar historial quan acabem 
- Buscador recomanat: <https://duckduckgo.com> 
- Navegador TOR 
- Android: Orfox  



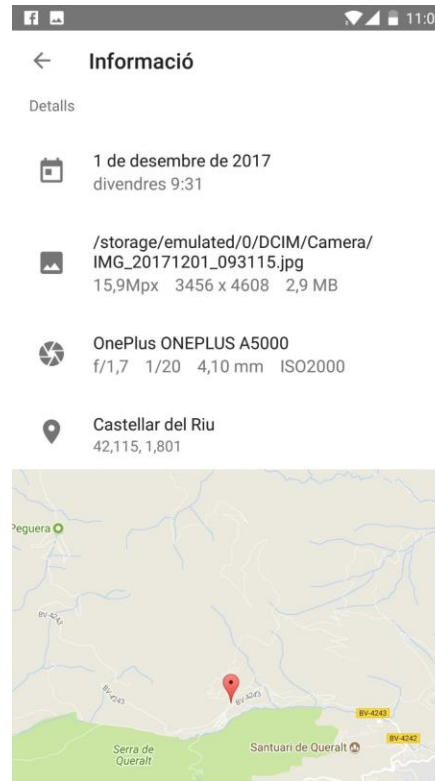
- Proporciona una xarxa virtual anònima
- Orbot: app android que es connecta a la xarxa Tor
 - Permet reidreccionar tràfic d'altres apps per la xarxa Tor
 - Hi ha aplicacions que permeten utilitzar el proxy local d'Orbot



Metadades



- Dades que no es veuen però es camuflen amb els arxius.
- Geolocalització, autor, etc.
- Accés a les metadades difereix en funció del document.



Conclusions



- No hi ha comunicacions 100% segures
- Hàbits segurs
 - Dificultar accés a les dades
 - No aixecar sospites
- Els millors mètodes són els que ens podem inventar nosaltres.

Conclusions



- Començar a utilitzar des d'avui:
 - Signal
 - Mailvelope.com

Moltes gràcies



icr@tutanota.com

<http://github.com/martit/icr>