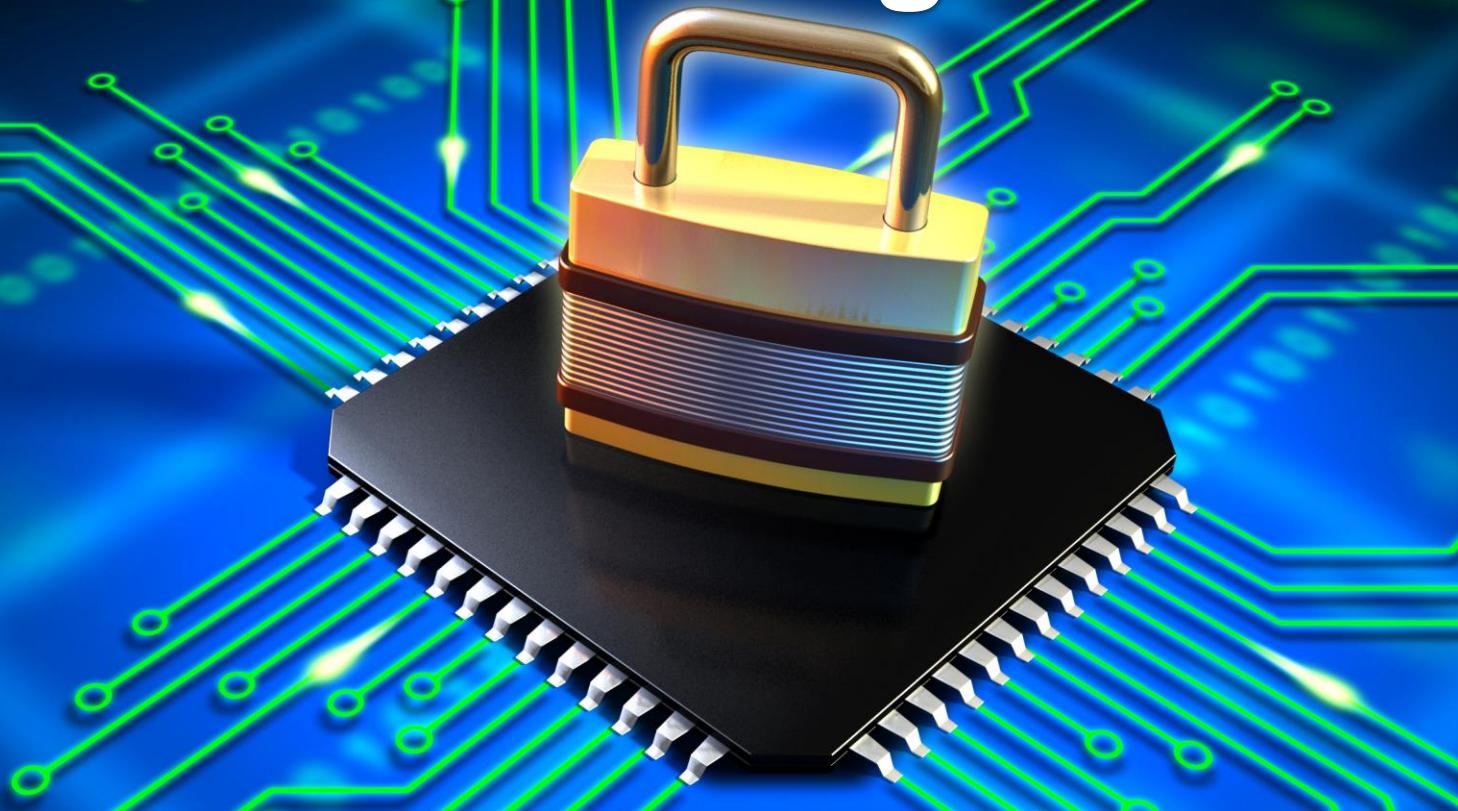


Seguretat en les comunicacions digitals



Informàtics compromesos
amb la Repùbilca (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?

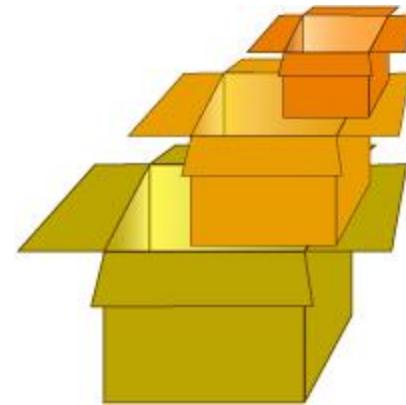
Index



- 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 
- Desabilitem 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



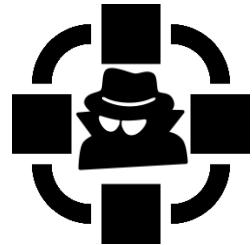
■ Ordinadors

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

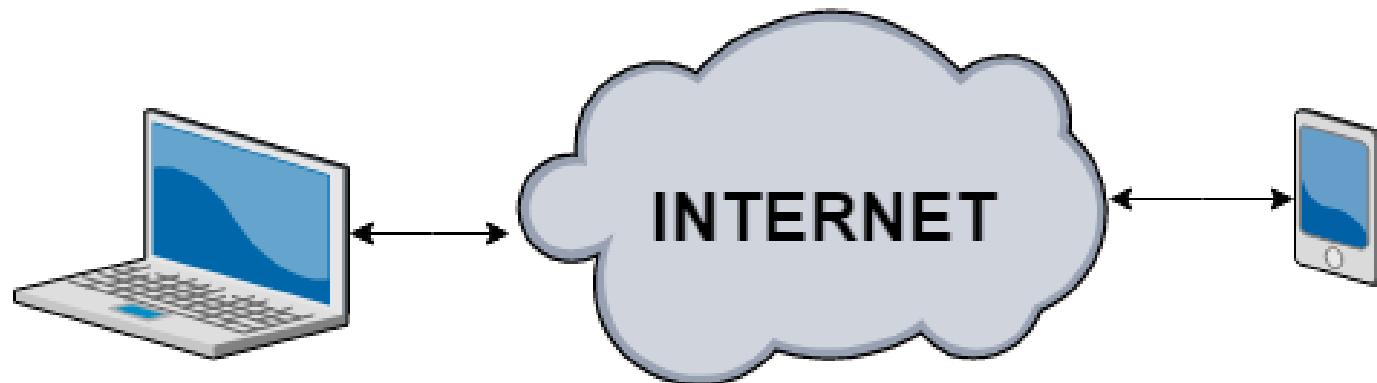
■ Mòbils i Tauletes

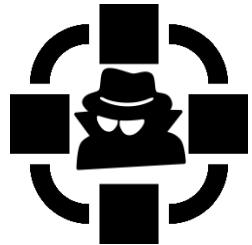
- Android: seguretat → origens desconeguts
- Consum exagerat de bateria o dades a internet

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

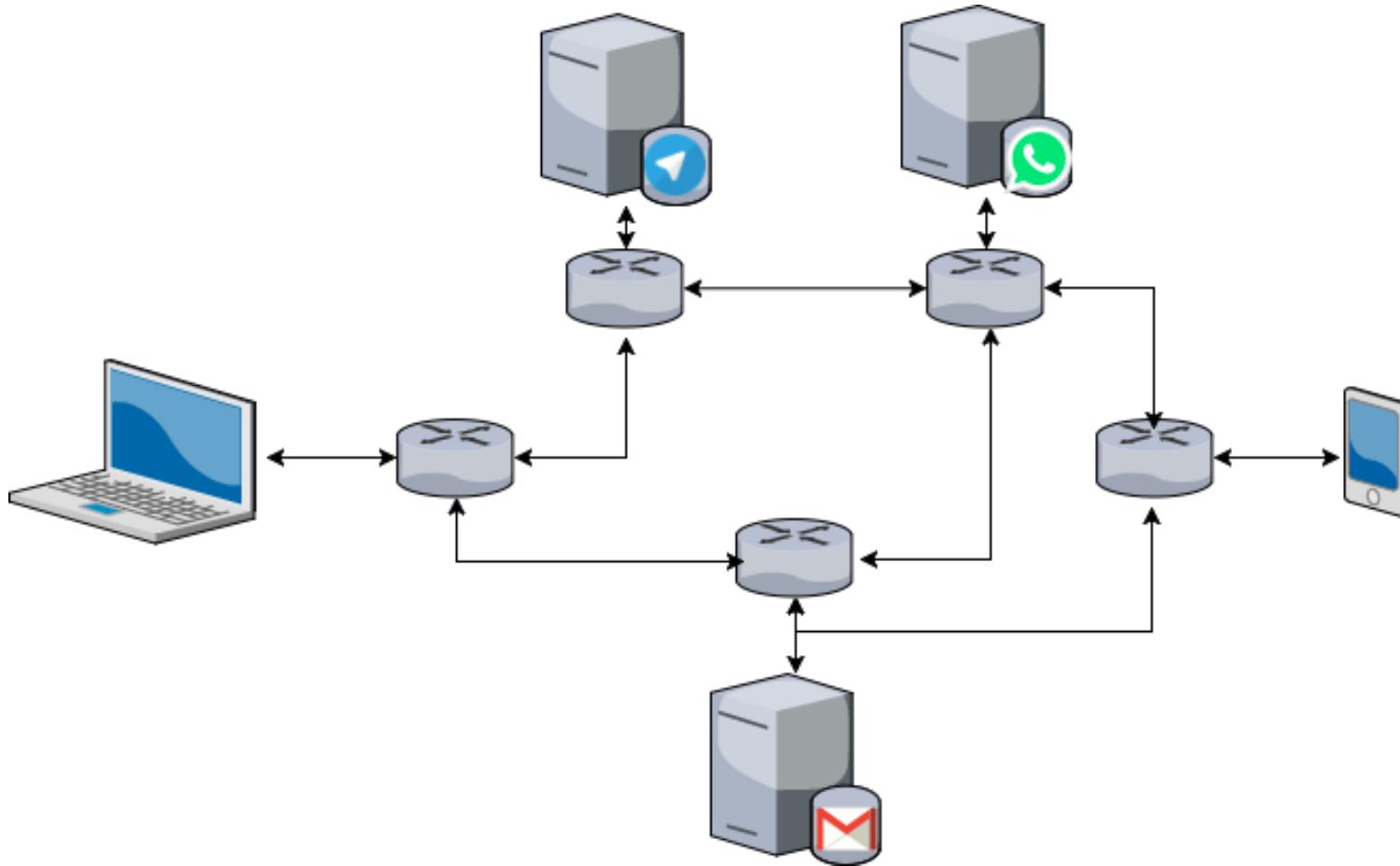


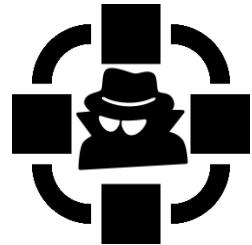
Intercepció de comunicacions



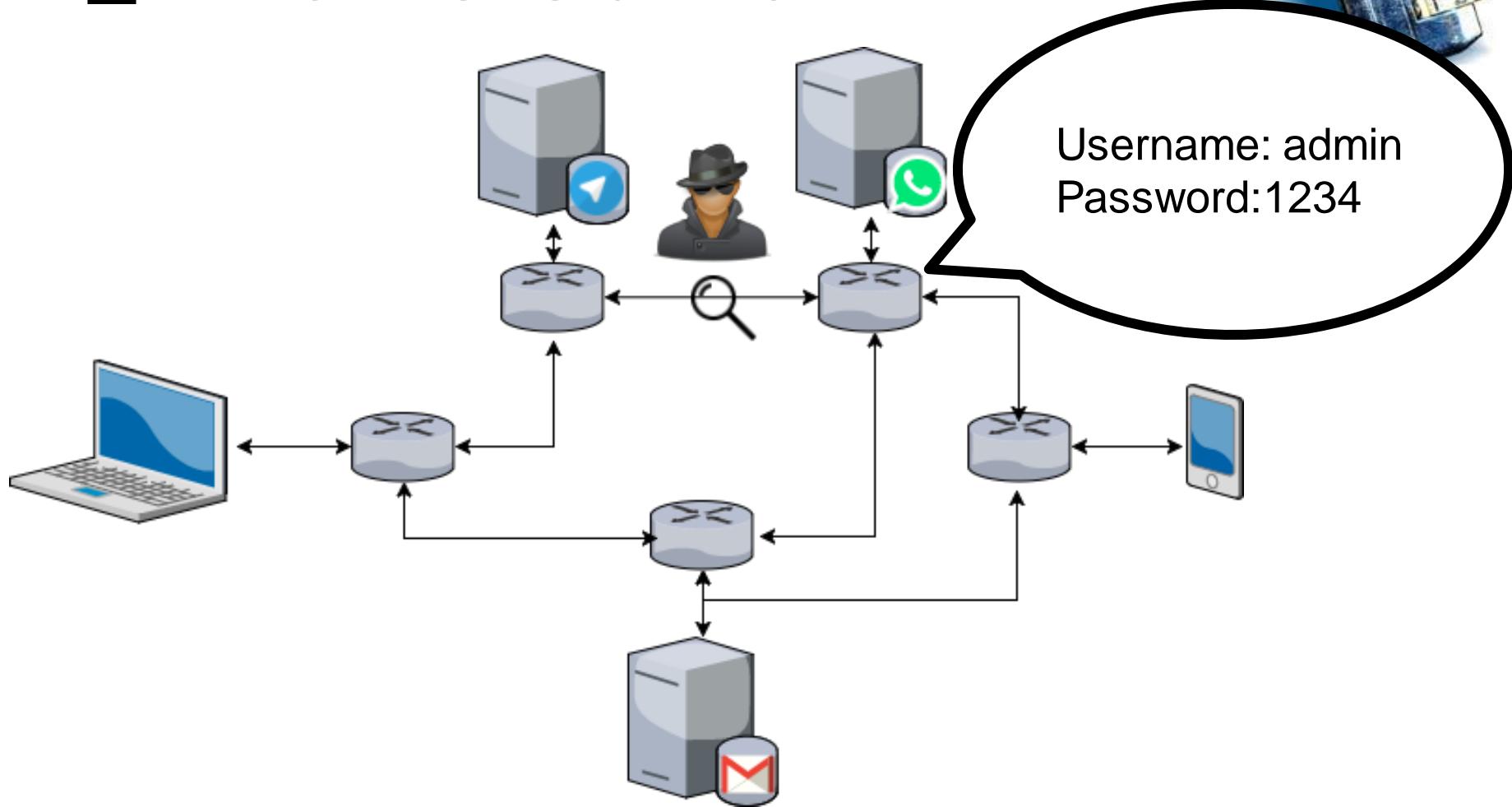


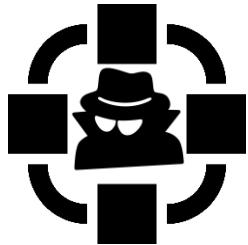
Internet és vulnerable



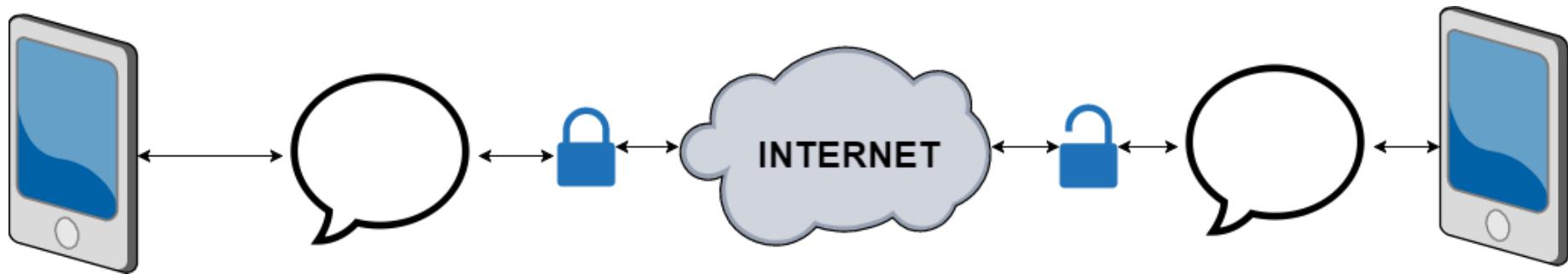


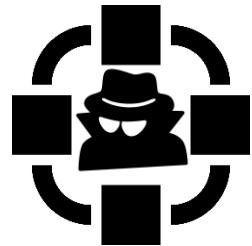
Punts de vulnerabilitat



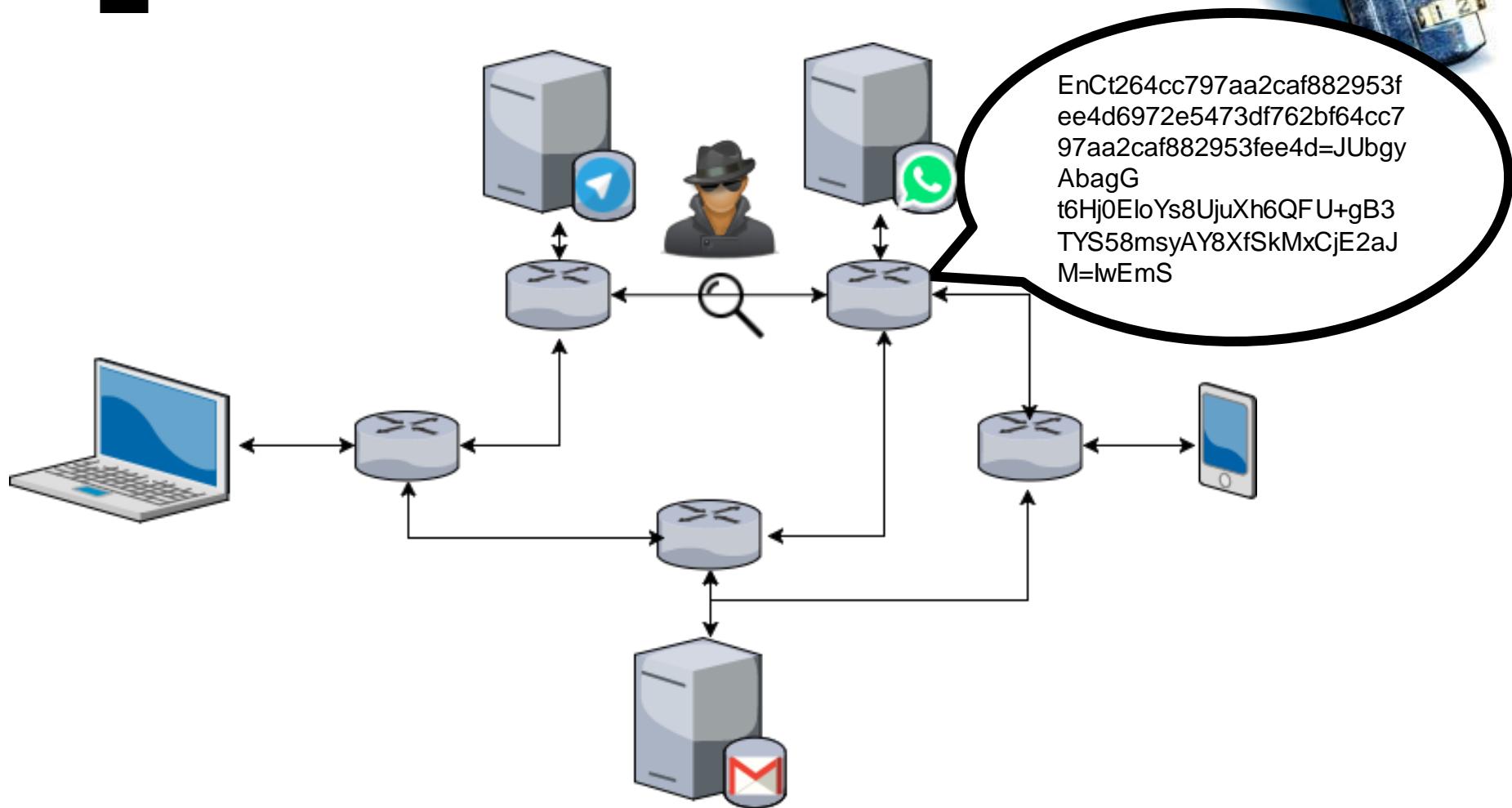


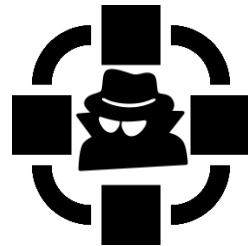
Seguretat a nivell d'aplicació





Xifratge

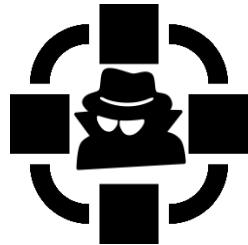




Apps de xat i veu



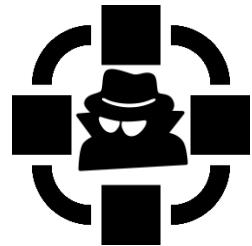
- Riot – molt segur, però ús incòmode
- Signal – bon compromís seguretat i ús;
 - recomanat per ús estàndard; moltes opcions de seguretat
- Telegram – es considera segur; força popular;
 - els “canals” permeten arribar a gran quantitat de gent (canals dels CDR, Assamblea, Òmnium, EnPeuDePau, etc.)
- 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

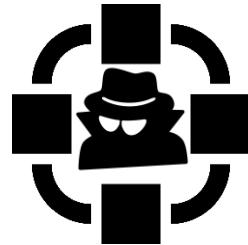


■ Serveis de correu (Gmail, Hotmail, etc.)

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

■ Mailvelope.com

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



Correu



The screenshot shows a web browser window with the title bar "Mailvelope". The address bar indicates a secure connection to <https://www.mailvelope.com/en>. The page content includes a navigation menu with "Home" selected, and links for "Documentation", "FAQ", "Blog", and "About". A language dropdown shows "English". Below the menu, a message states "Mailvelope can be installed from the Chrome Web Store." followed by a "chrome web store" badge. A section for "Firefox Addon" is present with a "Firefox" logo and a link to "download.mailvelope.com". A "View details »" button is at the bottom left. The background of the slide features a large, semi-transparent watermark of the Mailvelope logo.

Mailvelope

Secure | <https://www.mailvelope.com/en>

Home Documentation FAQ Blog About English

Mailvelope can be installed from the Chrome Web Store.

available in the chrome web store

Firefox Addon

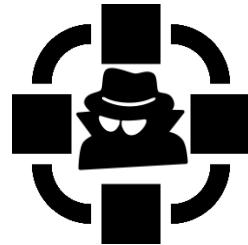
A Firefox version of Mailvelope is available at download.mailvelope.com.

Firefox

How does it work?

This documentation guides you through the basics to help you get started with Mailvelope.

[View details »](#)



Correu



DuckDuckGo

Enabled [Help](#)

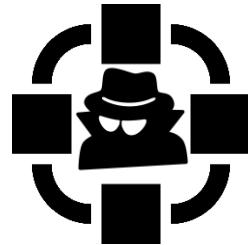
Current tab:

[Add](#) [Reload](#)

Last activities:

No entries

[Options](#)



Correu



DuckDuckGo Mailvelope Options

Mailvelope | chrome-extension://kajibbejlbohfaggdiogboambcijhkke/app/ap... NEW

Marti

Mailvelope Key Management File Encryption Options Documentation About

Mailvelope

Display Keys

Import Keys

Generate Key

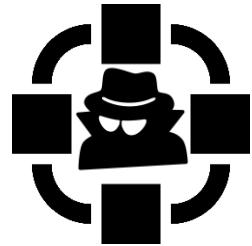
Setup

Key Management

Export

Key type All

Name	Email	Key ID	Created
------	-------	--------	---------



Correu



DuckDuckGo Mailvelope Options Martí

Mailvelope | chrome-extension://kajibbejlbohfaggdiogboambcijhkke/app/app.ht...

Mailvelope Key Management File Encryption Options Documentation About

Generate Key

Name
Full name of the key owner

Email

Advanced >>

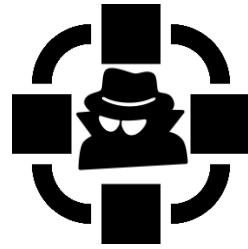
Enter Password
Password field is empty

Re-enter Password

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

Generate **Clear**

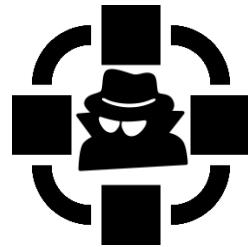
chrome-extension://kajibbejlbohfaggdiogboambcijhkke/app/app.html#/keyring/setup



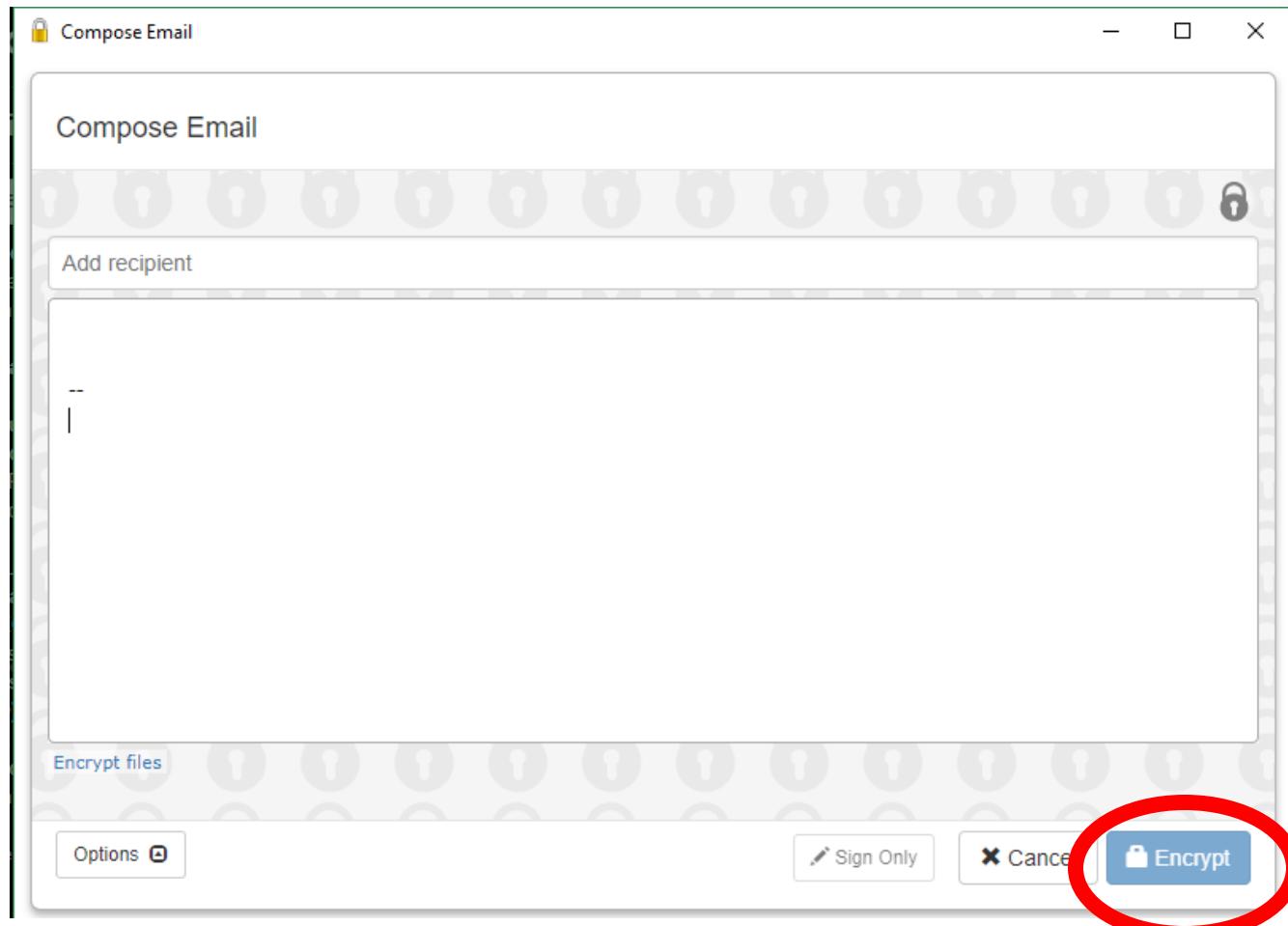
Correu

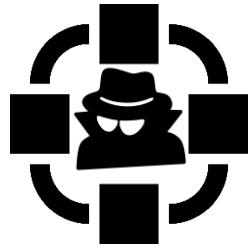


A screenshot of a mobile messaging application interface. At the top, there's a header bar with the text "Missatge nou". Below it, the message fields show "Per a" (To), "De" (From) with a redacted name, and "Cc Cco" (Carbon Copy). The message body contains the text "Assumpto" followed by a large black redaction box. In the bottom right corner of the message body area, there is a small icon representing a drawing or sketch tool, which is highlighted with a thick red circle. At the very bottom of the screen, there is a toolbar with various icons for font selection, bold, italic, underline, and other text styles, along with a blue "Envia" (Send) button.



Correu





Correu

Missatge nou

Per a |

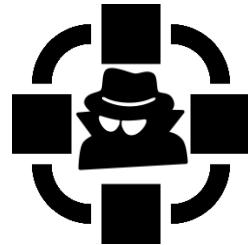
De [REDACTED] Cc Cco

Assumpte

-----BEGIN PGP MESSAGE-----
Version: Mailvelope v2.0.0
Comment: <https://www.mailvelope.com>

```
wcFMAz3u6062UohCAQ0/9EA8ZLOM7B+qgOg48hT8Vd4RFFIeSFLEUJqeAjDI
m1001y08N1MaUMCasUIVUfwPKeWscrVFA6DBM1cRRK+fB2fKLb5ipk7XXB+
gu11T5IUg4ZMdb371d26xFU6vXrymlk401vxmkZoMzEzoPUddIo3UjA28pcv
moY3AD/Hc0U2MS0BFJS565JWcy260gaTVEaVuUqQxx+uq4d265rJdtTuAaHz
WgxJAJNahwhz173TNGEx088hrGU$2g49Gqx8y+ywbes90uqe/eBpSuP8vBZ
De8dpT52/inONJvbZX55TVYdd0096AsCqUN2MSKCU2fusGEC1Ywa2SS98UG9X
utwdc7T8jb61y3Kt3ALYGW2GG92z1MhgahxgQGQ3znEcvm3DT0mZdwUDEu1h
6+XdKx+k16amR30PRfsk0exBjRr4wBxSYJ+Joi0OHxyNN13A8CT1GmaFEW
ft7HgXdkltPC3iIo8rImBisa5MPNKMIXqvzb6kaIA08xPWUaj88ipd57kME1
f2ExCLjndkJZE1wywUr4iHMzsIBxhG/b8PbL1MZvmKnrx3CA6SGEPDnXpiCa
yEdzV1KDj4yXL1Cif50gwJVKT/R6SK3XHvCAYBdLGelXic6v4s3MSo6lnNtv
qXavNxVdoijVvinJ0F19fJD2zxk4s1xajBE0IVwBD2DBwUwDjm2Pzz6YCZ0B
D/47CBn/iSH60dCQ317qh9uzl8VDMCAkzcteZKKxE1fdv1VYqN/qypVmV3/4
fdltugz1jh5vaYkko0Hdy60jFMMvbjVow+S0gQ3nBm90qJ92kqftufq1/n
f4xZnTjp0KtB2vVBuo/zih3zr1Wz+C054hVrAf8mgTcybv1r78FTB6WeAs9
280zgS8y+mAmvhR4fzY1jkjUtN/MbvHB0Pqs11fhakrvyG5gQp3ETVnno1
XQr88VHed9+eHZf3Yj/nPIf sdf-377AW/ /boiHn228Y8WSgAmOTTa/rFkMV
sXI9MN7tjUrnXY/QKPCabTuIyC8RxdmHcqOui2XdwUoGJSSf0txD0CYvVGP
s+j38fEshZxxCqbIT2GEKVKA+lmflwTg1yA2TyCDPHxSPYK3Y6S3mdOyeMloR
3zrXV8t/ZFhtuXKSv0YQ2xaPDQ2adB3/47uXzd5qzWNKwcM40MtNRPZONMx
DORozIL7q3s6MDKoogHnTZ15xML1eu10DV3Hhr80u1hjw13tdXhIZzoFjki0e
zBUoARC8WoMNepI2irjm8fAKEqv85JdTdYJvVqbdh5XjRDfzrboupXmB1M2y
v3YkGuBw6RB3mPlIdaK1TkPUMCXdmFwqNiwPFN20wdYsazkO1PEsD+w89izJ
```

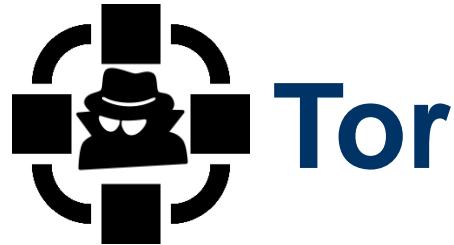




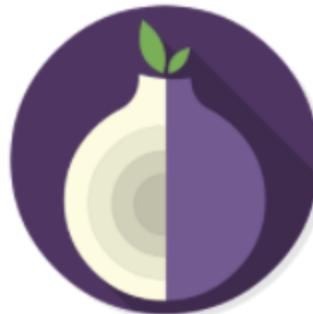
Navegadors WEB



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



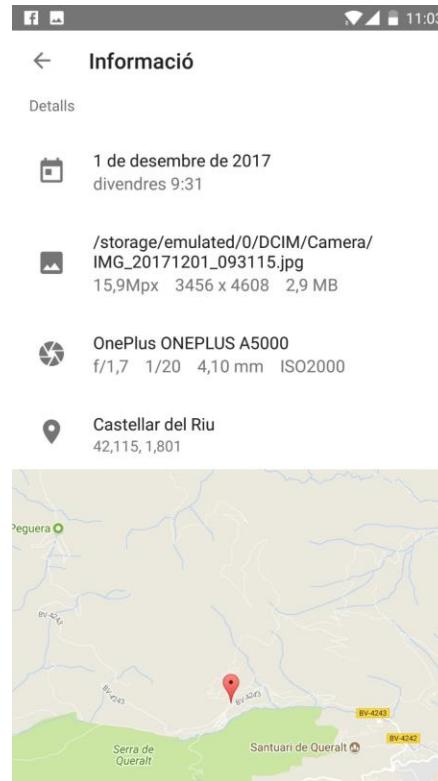
- Proporciona una xarxa virtual anònima
- Orbot: app android que es connecta a la xarxa Tor
 - Permet reidrecccionar tràfic d'altres apps per la xarxa Tor
 - Hi ha aplicacions que permeten utilitzar el proxy local d'Orbot



Metadades



- Dades que no es veuen però es camuflen amb els arxius.
- Geolocalització, autor, etc.
- Acces 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>