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 consiència 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

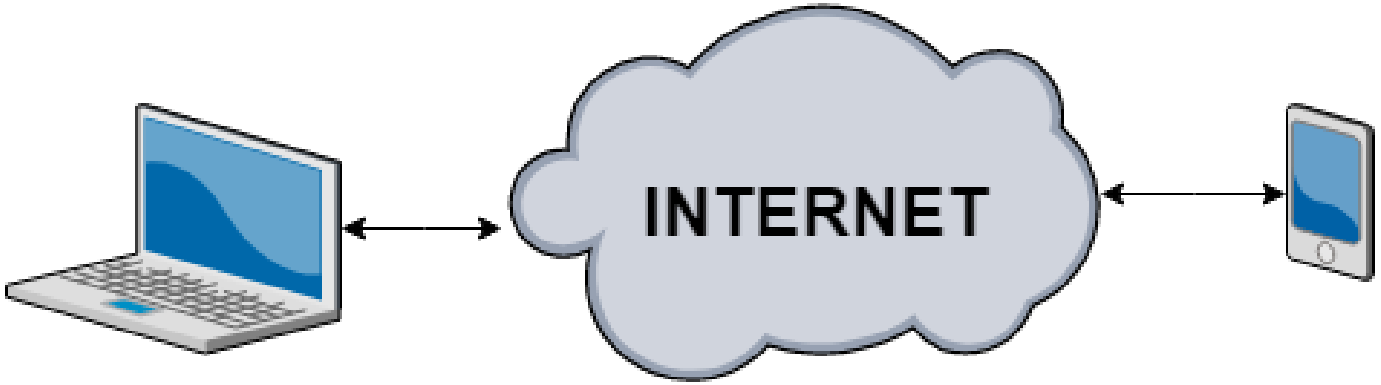
Infiltració de programari no desitjat

- Instal·lats sense el nostre conscentiment
- 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)

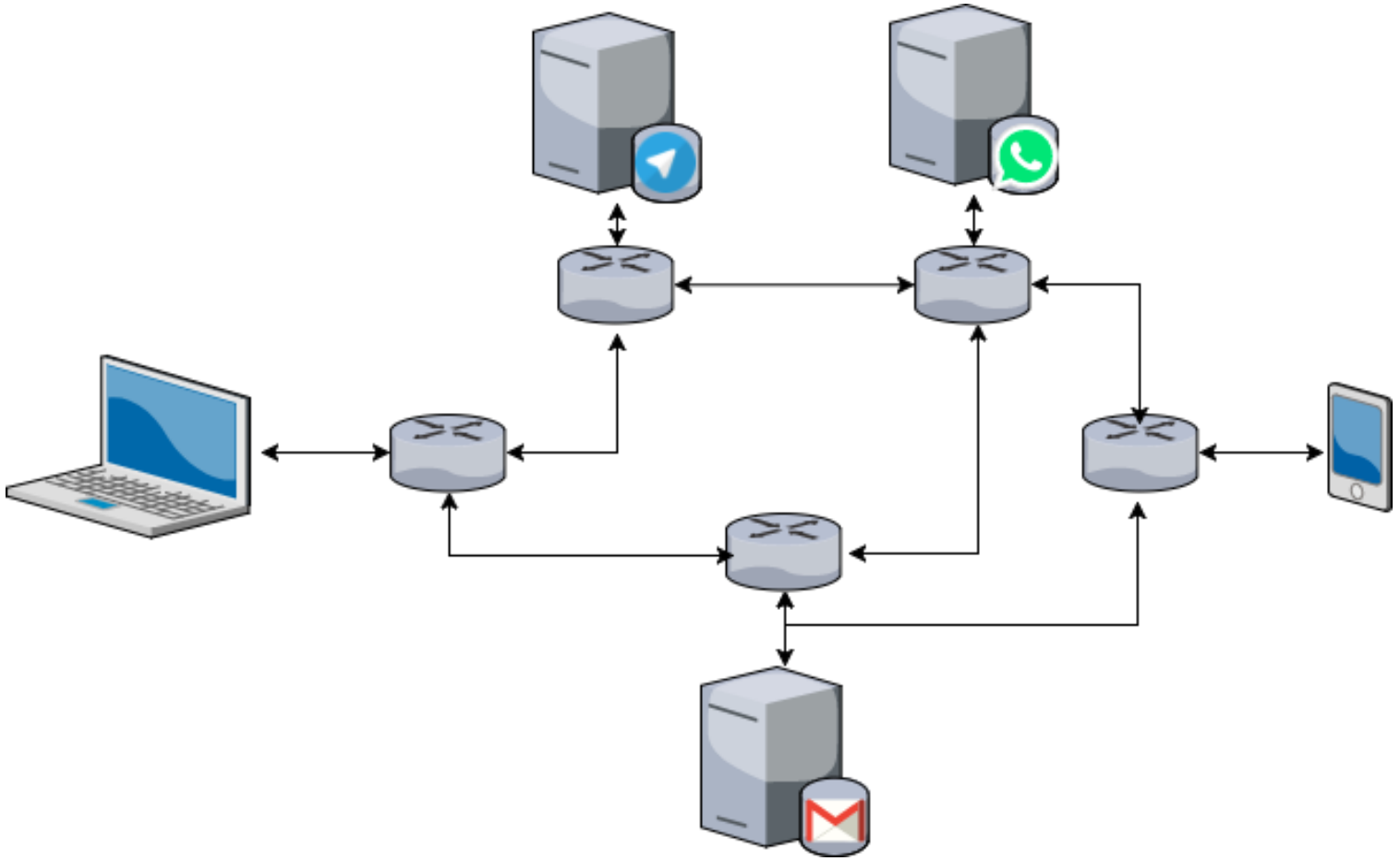
Infiltració de programari no desitjat

- Ordinadors
  - SOs i antivirus actualitzats actualitzats
  - Firewalls
  - Detecció de comportaments anòmals
- Mòbils i Tauletes
  - Android: seguretat → origens desconneguts
  - Consum exagerat de bateria o dades a internet
- Evitar tenir els mòbils amb nosaltres quan parlem d'informació sensible

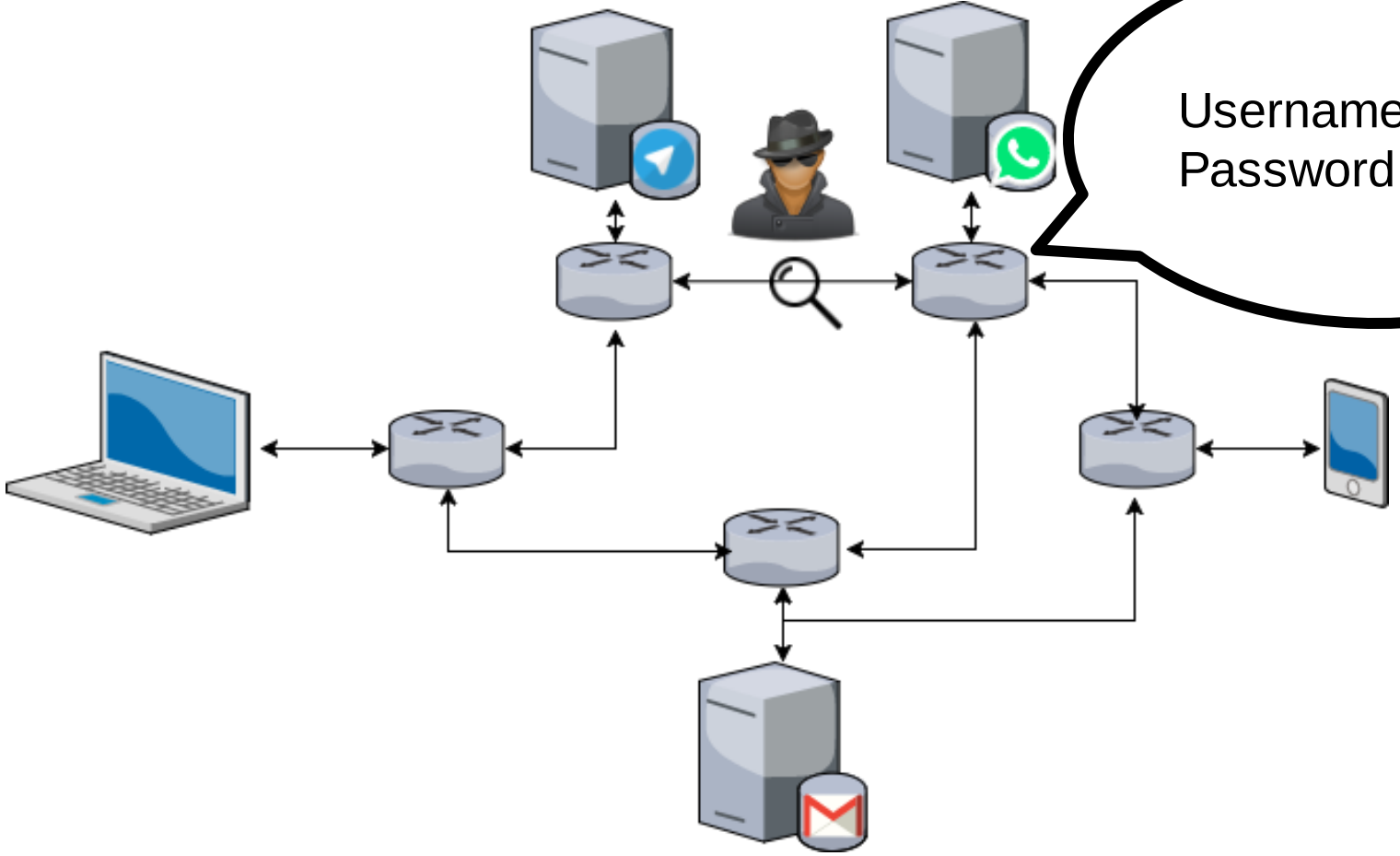
Intercepció de comunicacions



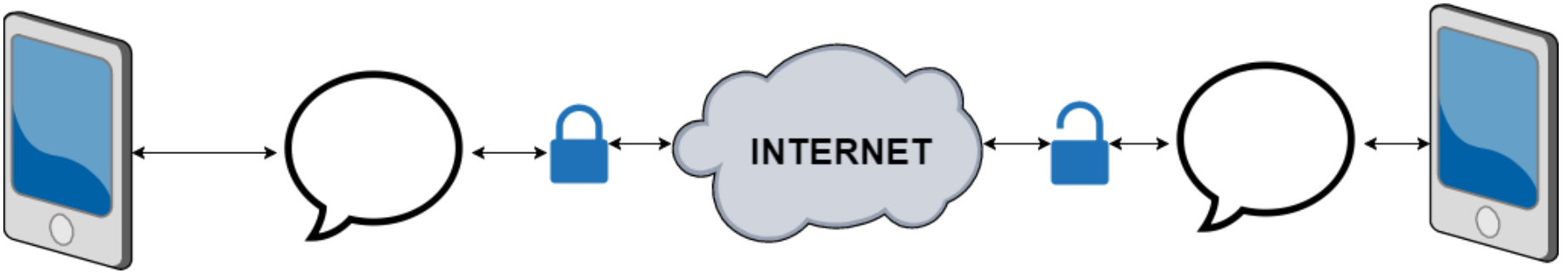
Internet
és vulnerable



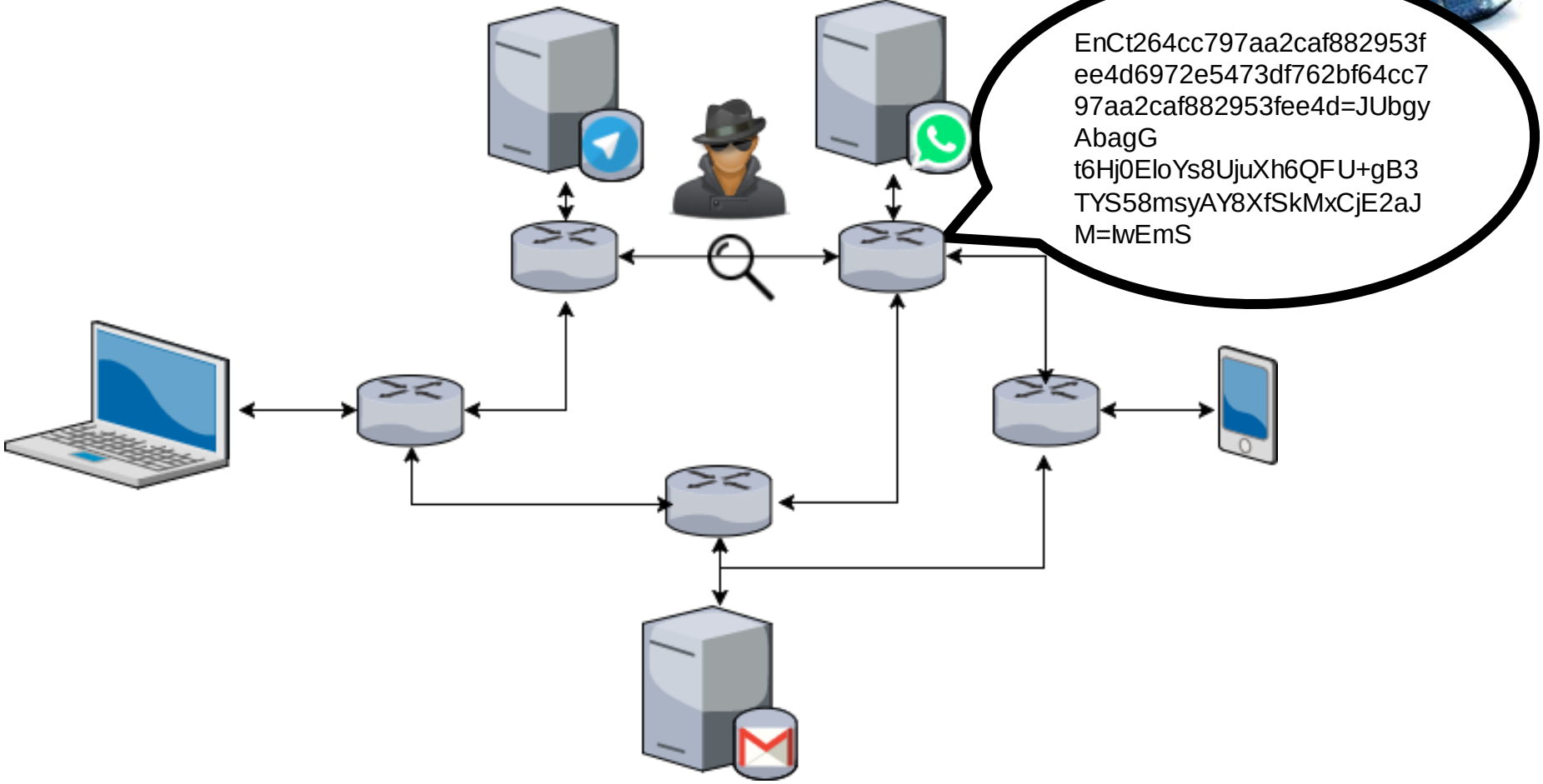
Punts de vulnerebilitat



Seguretat a nivell d'aplicació



Xifratge


EnCt264cc797aa2caf882953f
ee4d6972e5473df762bf64cc7
97aa2caf882953fee4d=JUbgy
AbagG
t6Hj0EloYs8UjuXh6QFU+gB3
TYS58msyAY8XfSkMxCjE2aJ
M=lwEmS

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 benefeicis

- 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

Mailvelope

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

Mailvelope 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.

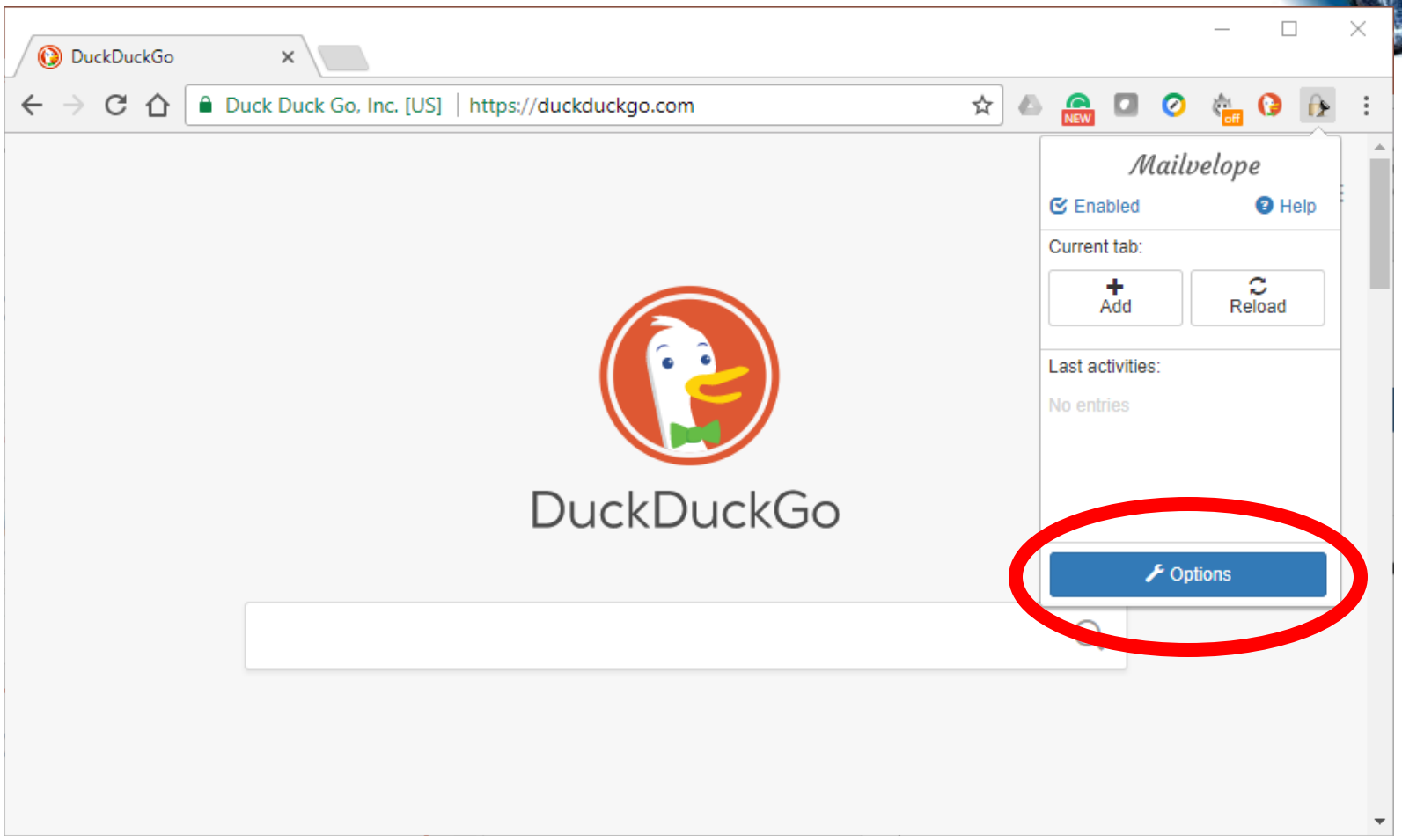
Firefox

How does it work?

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

View details »

Correu


DuckDuckGo
Duck Duck Go, Inc. [US] | https://duckduckgo.com
Mailvelope
Enabled
Help
Current tab:
Add
Reload
Last activities:
No entries
Options
DuckDuckGo

Correu

DuckDuckGo | Mailvelope Options

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

Mailvelope | Key Management | File Encryption | Options | Documentation | About

Mailvelope

Display Keys

Import Keys

Generate Key

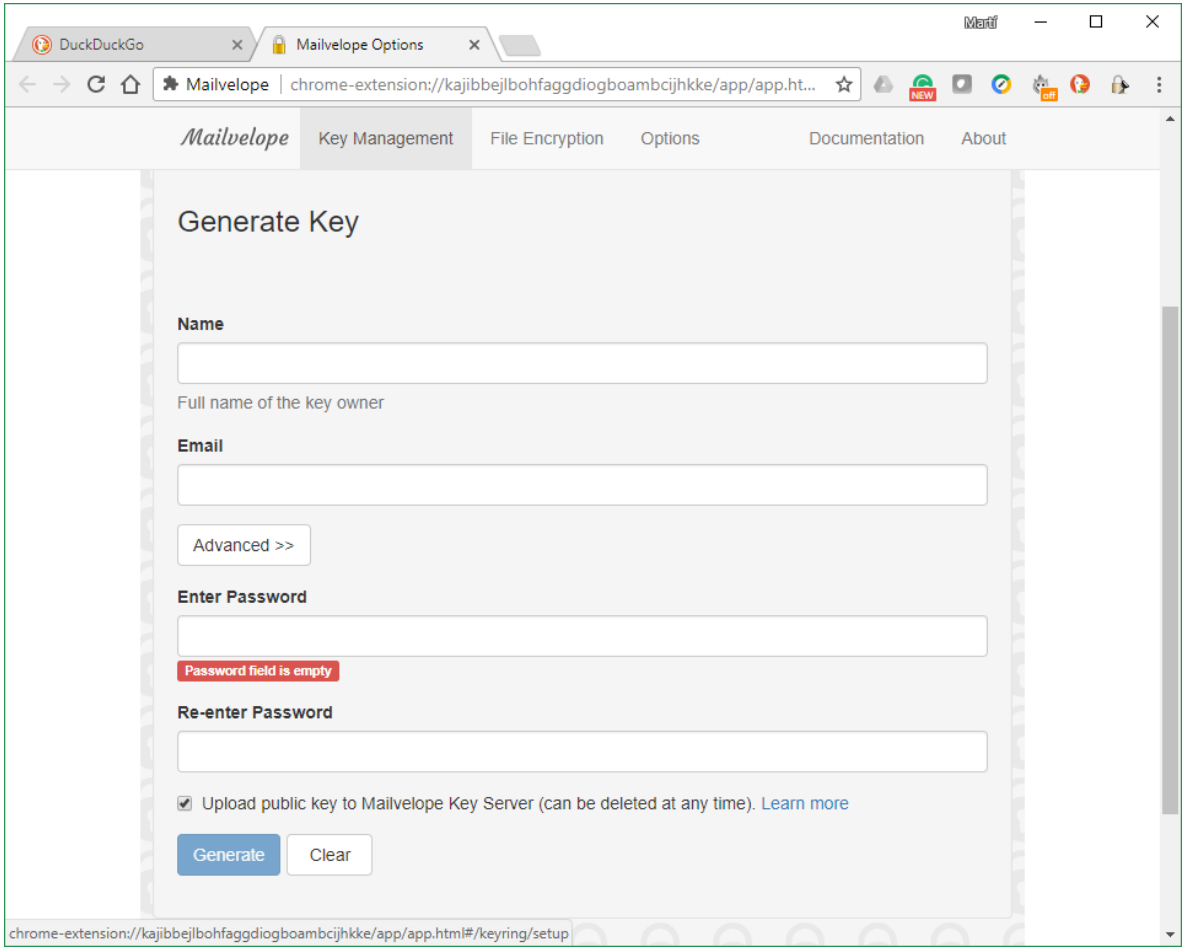
Setup

Key Management

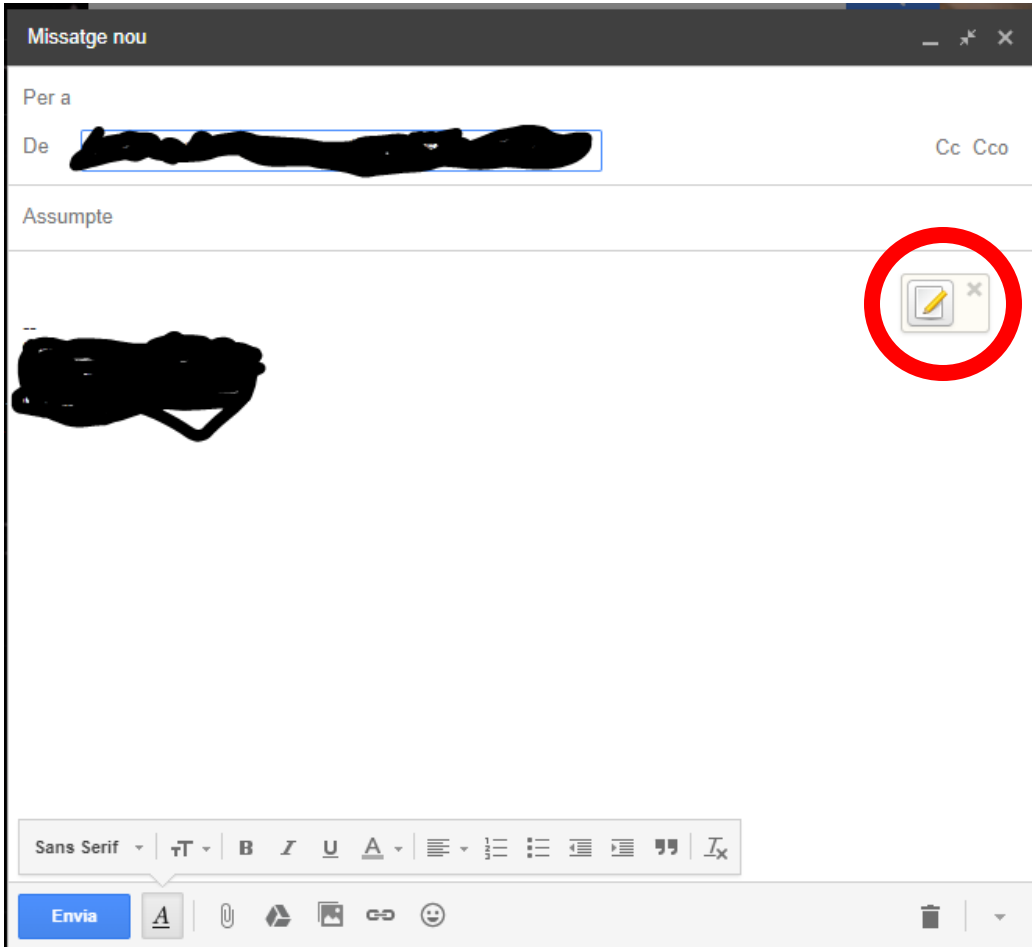
Export | Key type: All

Name | Email | Key ID | Created

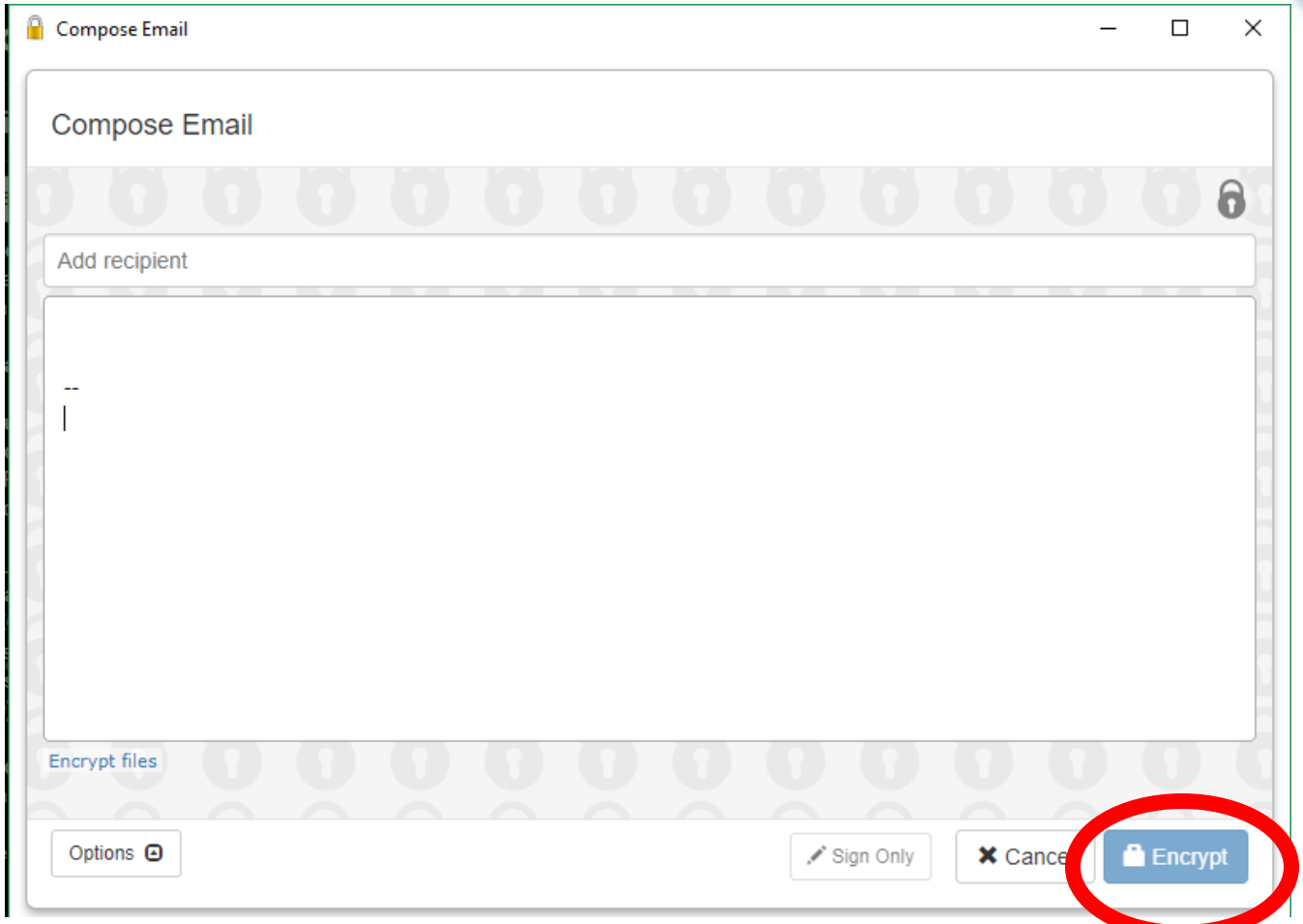
Correu


DuckDuckGo
Mailvelope Options
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



Correu


Compose Email
Compose Email
Add recipient
--
Encrypt files
Options
Sign Only
Cancel
Encrypt

Correu

Missatge nou

Per a

De [redacted] Cc Cco

Assumpte

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

wcFMAz3u6062UohCAQ/9EA8ZLOMZ7B+qgOg48hT8Vd4RFFIeSFLEUJqeAjDI
m10Q1y08N1MaUMCasUIVUfwPkEwscrVFA6DBMIcRRK+fB2FdKLb5ipK7XXB+
gul1T5IUg4ZMdb371d26xFU6vXrymWk4OlvxmkZoMzEZoPUDdIo3UjA2Bpcv
moY3AD/oHc0U2MSOBFJ565JWcy260gqTVEaVwUqQxX+uq4d26SrJdtTuAaHz
WgxJAJNahwkhzl73TNGEXo88hrGUs2g49Gqx8y+ywbes9Ouqe/eBpSuP8vBZ
DeBdpT52/inONJvbZX55TVYdd096AsCqUM2MSKCU2fusGECl1Ywa2SS98UG9X
utwdc7T8jb6ly3Kt3ALYGW2GG92z1MhgahxgQGQ3znECvm3DT0mZdwUDEu1h
6+XdKx+kl6amR30PRfsk0exBJRr4wBx5YJ+Joji0QHxyNNl3A8CT1GGmafEW
fT7HgXdkltPC3iIo8rImBisa5MPNKMX9qvzb6kaIA08xPWUajB8ipd57kME1
f2ExCLjndkJZElWywUr4iHMzsIBxhG/b8PbLlMZvmKnx3CA6SGEPDnXpIaCA
yEdzV1kDj4yXL1CiFS0gwJVKT/R6SK3XXHvCAYBdLGeWXic6v4s3MSo6WNtV
qXavNxVDoijVYinJ0F19fJD2xzk4slxajBE0VIwBD2DBwUwDjM2Pzz6YCZ0B
D/47CBn/iSH6OdCQ3I7qH9uzW8VDMCAkzcteZ8KkE1fdV1YVqN/qypVmV3/4
fdWtugiJh5By5vaYkKoQHdy60jFWMVbjVow+S0gQ3nBm9OqJ92KqfTufqi/n
f4xZnTjp0KtB2vVBuo/zih3zrlWZ+CO54VhVrAf8mgTcybVir78fTB6WeAs9
28OzwgSY+mAMvhR4fzY1jxkjUTn/MbvHBoPqsllfHaakrvyGSgQp3ETVnno1
XQr88VHed9+eHZf3Yj/nPIFsdf+377AVw//boiHnZ28Y8WSgAmOTTa/rFkMV
sXI9MN7tjUrNXY/QKPCabTuIyC8RxdmHcqOui2XdwUoGJSSf0txDD0CYvVGP
s+j38fEshZxxCQbIT2GEKVkA+WmNwTg1yA2TyCDPHxSPYK3Y6S3mdOyeMMoR
3zrXV8t/ZFhtuXKSkV0YQ2xaPDQ2adB3/47uXZd5qzWNKwcM40MtNRPZONMx
DORozIL7q3s6MDKoogHnTZlSxML1eu10DV3HHr80u1hjWl3tdXWZzoFjki0e
zBUoARC8WoMNepI2irjM8fAkEqv8SJdTdYJVvqbdh5XjRDfzrboupXmBlM2y
v3YkGuBw6RB3mPldIaKiTkPUMCXdmFwqNiwPfN20wdYsazkO1PEsD+w89izJ
```

Navegadors WEB

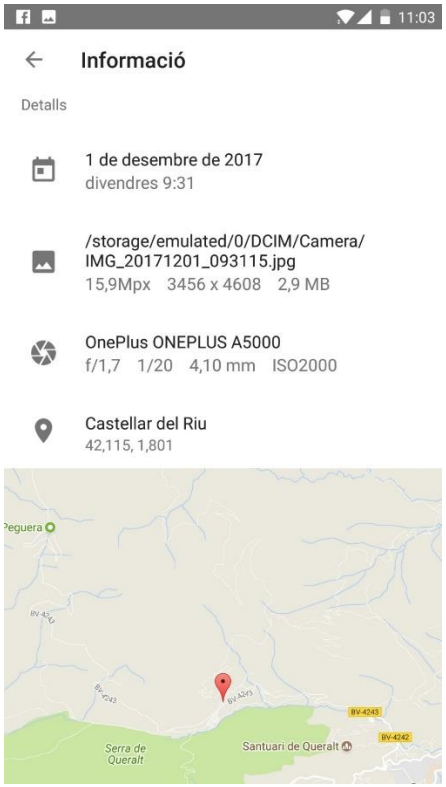
- Navegar en mode incògnit
- Utilitzar navegadors dedicats
- Esborrar historial quan acabem
- Buscador recomanat: https://duckduckgo.com
- Navegador TOR
- Android: Orfox

Tor

- 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.
- Acces a les metadedes 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

https://tinyurl.com/y8gexcd8

icr@tutanota.com