🕵 C1b3rWall - OPSEC Autodefensa Digital

- Asegurando Hardware
  - Windows
    - Antivirus
    - Firewall
      - Glasswire
    - Bitlocker
    - Apps
  - Mac
    - Antivirus
    - Firewall
      - Little Snitch, controla que sale de tu máquina hacia internet
      - Micro Snitch, vigilancia de audio
    - Filevault
    - Apps
  - Android/iOS
    - Antivirus
      - https://www.av-test.org/es/antivirus/moviles/
    - VPN
    - Cryptomator
    - Cifrado de dispositivo
  - Linux
    - Antivirus
    - Firewall
      - Opensnitch
    - LUKS
  - En general
    - DNSCrypt/DoH/DoT, DNS cifrado para evitar ataques de DNS poisoning
      - En este hilo de Twitter explico como configurarlo en diferentes dispositivos: https://twitter.com/soydelbierzo/status/1131806956669276160
    - Adblocking
      - uBlock Origin, disponible para la mayoría de navegadores web, incluyendo Firefox para Android
    - Tapa para la webcam
      - Hasta la frontal del móvil
- Email personal
  - Protonmail, en Suiza, leyes de privacidad muy fuertes, mensajes cifrados en reposo, solo el usuario puede acceder a ellos. Tienen una versión gratuita limitada a 500MB de espacio
  - Startmail, situado en Holanda, GDPR europea, datos cifrados en reposo
  - Tutanota, Alemanes, más o menos igual, bajo GDPR
  - Gmail ni en broma, es una herramienta de marketing para obtener información personal
- Gestión de logins
  - Lastpass
  - 2FA
    - Yubikey
    - Google Authenticator
    - Symantec VIP Access para Paypal
    - Duo Security
  - Passwordless Yubikey 5 NFC
  - KeepassXC
    - Alternativa libre, disponible para casi todas las plataformas, usa un formato estándar que lo hace interoperable con aplicaciones para Android como Keepass2Android o Kypass en iOS
- Internet of Shit
  - Aplicaciones running
  - Termostatos inteligentes
  - Robots de cocina
- SMS - SS7
  - Mensajería segura
    - Signal, Wire
    - Whatsapp
    - Telegram, ni en broma
- Red TOR
  - Tor Browser con OBFSProxy permite saltar limitaciones para acceder a internet en países con acceso limitado
- Llamadas seguras
  - Linphone, software libre, podemos usar su software de código abierto para montar nuestro propio servidor
  - Signal, código abierto, podemos fiscalizarlo e incluso montar un servicio propio, por ejemplo Noise, la versión de Signal para dispositivos con CopperHead OS que no necesita Google Play para enviar notificaciones
  - Whatsapp
    - De momento usan el cifrado punto a punto de Signal, sigue teniendo acceso a los metadatos
- Drive/Dropbox seguro
  - https://cryptomator.org/
  - Mountain Duck permite montar unidades remotas de Drive, Box, Dropbox, S3, Nextcloud y usarlas en remoto como si se tratase de un disco local
- Backups en la nube
  - https://www.idrive.com/idrive/signup/el/get90 backups cifrados zero knowledge
- WiFi pública
  - VPN
    - Private Internet Access
    - ProtonVPN
    - NordVPN
    - Proxy.sh
  - Firewall
    - Caso ES File Explorer
      - https://github.com/fs0c131y/ESFileExplorerOpenPortVuln
  - Mini router
    - GI iNet AR750 - AR750S
- WiFi doméstica