VADEMECUM PER LA LIBERTA' DIGITALE

(Titolo e classificazione documento): "Vademecum libertà digitale R2020" (DOC1DIGITALE) – non confidenziale, non ad uso interno R2020
(Riferimenti bibliografici ed link approfondimento): https://r2020.info/commissioni/commissione-sovranita-digitale/
(Licenza Creative Commons): BY,NC,SA - R2020
(Autore e revisore): Commissione R2020 Sovranità digitale
(Ultimo aggiornamento del documento): n.13 data 14/09/20 orario 23.45.16
(Stato attuale del documento): FINALE ***versione soggetta ad integrazioni e variazioni***

STEP 1) **DIFENDITI !** ***noob level***

usa software libero, naviga senza lasciare dati in rete, proteggi la tua privacy digitale

-Invece che Microsoft Office, scarica e utilizza LibreOffice (https://it.libreoffice.org/).
-Quando navighi, cancella sempre cookies e cronologia, ci sono varie applicazioni che lo fanno. -Disabilita OneDrive (https://www.windowsblogitalia.com/2015/09/come-disabilitare-o-rimuovere-onedrive-in-windows-10/).
-Passa da Microsoft Edge o Google Chrome a Mozilla Firefox (https://www.mozilla.org/it/firefox/new/), installando l'estensione Facebook Container (https://addons.mozilla.org/en-US/firefox/addon/facebook-container/): impedisci a Facebook di raccogliere informazioni su di te e le tue abitudini. Ti protegge isolando Facebook quando sei su Internet. Attiva l'opzione automatica di invio ai siti web del segnale "Do Not Track" (https://support.mozilla.org/it/kb/impedire-tracciamento-siti-web).
Inoltre verifica nel pannello protezioni di Firefox il livello di protezione antitracciamento avanzata (normale o restrittiva), soprattutto per i social media. Attiva il monitor per le violazioni sui tuoi indirizzi mail.
-Scarica SurfShark (https://surfshark.com/it/download): ti permette di cambiare la tua posizione per evitare il tracciamento. Blocca anche annunci pubblicitari, trackers e malware.
-Verifica lo stato di tutte le porte lasciate aperte o eventuali backdoors tramite OpenPorts, da riga di comando.

STEP 2) **LIBERATI !** ***hacktivist level***

cambia sistema operativo, diventa indipendente, passa a strumenti alternativi che puoi pienamente controllare

SISTEMA OPERATIVO: molla Windows. Trova un qualsiasi altro sistema operativo Linux, come Ubuntu (https://www.ubuntu-it.org/). Al massimo partiziona il disco utilizzando Windows solo per le applicazioni fondamentali che non trovi per altri sistemi operativi, o utilizza all'occorrenza una macchina virtuale (https://www.virtualbox.org/).

INTERNET e DEEP WEB: Per navigare scarica Tor (https://www.torproject.org/it/). Hai un accesso privato in rete senza censura. Il network ha migliaia di relays gestiti da volontari e milioni di utenti in tutto il mondo per garantire privacy e libertà online. Alternativa a Tor è Orfox (https://guardianproject.info/apps/orfox/). Cerca con Torch, DuckDuckGo o Onion search. Per Apple puoi usare Red Onion II o Onion browser.
Per maggiore sicurezza è meglio utilizzare una VPN (https://openvpn.net/) sulla quale si appoggino Tor o altri software.

SOCIAL: Passa da Facebook a social alternativi come Mewe (https://mewe.com/) e Mastodon. R2020 e Byoblu hanno un proprio social basato proprio su Mastodon (https://social.byoblu.com/web/accounts/22767).

MAPPE: OpenStreetMap (https://www.openstreetmap.org) alternativo a Google Maps

MESSAGGISTICA: Telegram (https://telegram.org/) è preferibile a WhatsApp e Messenger, ma attenzione perché gruppi e canali Telegram non hanno la crittografia end-to-end. Installa Signal (https://signal.org/it/) oppure Theema (https://threema.ch/en) . Quest' ultima è totalmente sicura perché ogni conversazione viene eliminata dal server non appena trasmessa, ma purtroppo è ancora a pagamento tramite Bitcoin o Paypal.

POSTA e DATI CRIPTATI: lascia Google. Puoi installare Gpa o Kleopatra per crittografare la posta. GNUPG (https://gnupg.org/) (openpgp) è la soluzione migliore e può essere utilizzata all'interno di Thunderbird mail client o in k9mail per Android. Utilizza dischi e chiavette usb criptate (ottimo VeraCrypt https://www.veracrypt.fr/en/Home.html).

PAGAMENTI ONLINE: Paypal o criptovalute (creando un tuo wallet con Bitcoin o altre monete, tramite Coinbase). Nota che i servizi di wallet sono monitorati e al momento dell'iscrizione fornisci i tuoi documenti di identità per l'identificazione cliente si fini dell'antiriciclaggio. Maggior sicurezza ovviamente se si usa un wallet personale su PC (con tutte le sicurezze del caso a livello di password e cifratura).

Note:

1) Su ANDROID un'operazione complessa (effetto collaterale: invalidazione della garanzia del dispositivo) ma efficace è l' eliminazione dei bloatware e l' ottenimento root del dispositivo.Si può effettuare sui vecchi dispositivi al fine di dargli nuova vita. Una necessità impellente, alla luce della problematica ecologica, come anche della lotta geopolitica sulle terre rare.Scegliendo il giusto cellulare si può sostituire la ROM (Sistema operativo) con una derivata da AOSP (Android Open Source Progetto) che è la medesima base di Google privato dei Google Play Services ed altri componenti proprietari di bigG. LineageOS la più famosa

2) Alternativo all' APP STORE c'è F-Droid, curato dalla comunità di XDA-Developers. Occhio ai problemi di hw, malware,SMS jacker.