



Percorso di consapevolezza digitale: Problemi e soluzioni pratiche

Daniele Piccoli
(daniele.piccoli@riseup.net)

<https://www.linuxtrent.it>



Premessa

- LinuxTrent si è dato come obbiettivo quello di sensibilizzare il più possibile le persone sugli aspetti inerenti i temi della privacy e dei diritti digitali
 - Serate informative e talk
 - Serate sulla sicurezza e crittografia
 - Serate divulgative di più ampio respiro
- Sportelli Linux per chi ha bisogno di aiuto:
 - <https://www.linuxtrent.it/iniziative/sportello-linux>
- È importante cercare di aumentare la propria consapevolezza riguardo a tutto quello che si fa in rete, per poi cercare di diffonderla anche alle altre persone
- Non fermatevi a quello che dico io, prendevi del tempo per verificare ed approfondire

Scaletta argomenti – parte 1° - introduzione

Introduzione generale

- Cos'è Internet e quali sono i suoi principi fondanti
- L'evoluzione della rete e gli attori in gioco
- Connessione alla rete
- Introduzione al software libero
- Libero vs gratuito
- Desktop vs mobile
- On-premise vs cloud
- Sistemi centralizzati vs sistemi distribuiti

Scaletta argomenti – parte 2° - problemi

Problematiche

- Di gratis non c'è nulla
- Quali sono i rischi a cui siamo esposti
- Termini e condizioni
- Autenticazione
- Tracciamento e raccolta dati
- Sorveglianza governativa di massa
- Perdita di controllo e del diritto alla privacy

Scaletta argomenti – parte 3° – possibili soluzioni

Soluzioni

- Cosa possiamo fare: consigli in pillole
- Come scegliere il proprio device
- Come scegliere il sistema operativo
- Gestione sicura dell'autenticazione e delle password
- I browser e le estensioni
- Decidere quali servizi usare e quali no
- Quali app usare da mobile
- Buone pratiche

Prima parte

Introduzione e concetti di base

Cos'è Internet e i suoi obiettivi

- Internet è una rete di reti (federazione di reti)
- È in grado di mettere in comunicazione qualsiasi dispositivo basato su protocolli aperti e conosciuti (TCP/IP)
- Gli obiettivi in cui credevano i suoi creatori:
 - Condivisione del sapere
 - Scambio di idee e informazioni
 - Decentralizzazione del potere
 - Maggiori opportunità di democrazia
 - Libertà di espressione
 - Diritto alla riservatezza

Dalla nascita di Internet ai giorni nostri

- Inizialmente veniva utilizzata per scopi militari
 - Successivamente venne usata in ambiente accademico
 - Nascita del WWW (Tim Berners-Lee e Robert Cailliau) (1989 - 1994)
 - Gradualmente tutte le aziende si affacciarono su Internet (1995 – 2001); internet inizia a diffondersi nelle abitazioni
-
- Nuovi servizi del web 2.0 (interattività, e-commerce, social-network)
 - Dispositivi sempre più veloci e connettività sempre più accessibile
-
- Collegamento in rete degli smartphone (app, IM)
 - Collegamento in rete dei dispositivi IoT

(le linee rappresentano la perdita di controllo sui dati e sulla privacy)

Chi sono gli attori in gioco

- Operatori telefonici e ISP (Internet Service Provider)
- Fornitori di servizi e aziende del settore IT
- Governi e agenzie governative
- Utenti
- Organi e istituzioni
- Organizzazioni per la privacy e i diritti umani
- Attivisti, whistleblower e giornalisti

Connessione alla rete

- Tutti i nostri device che usiamo oggi giorno sono connessi ad una rete: cablata o wireless
 - Desktop: connessioni via cavo, wifi
 - Mobile (smartphone e tablet): wifi, 3G/4G/5G
 - IoT (Smart TV, giochi per bambini, Smartwatch, frigoriferi, pneumatici): wifi, 3G/4G/6G
- Dal momento in cui il nostro device è connesso, è potenzialmente in grado di raggiungere qualsiasi destinazione che sia attiva e connessa in Internet e quindi di avere un scambio bidirezionale di dati
- Ogni dispositivo affinché possa raggiungere e possa essere raggiunto dal resto dei dispositivi ha bisogno di usare un indirizzo IP univoco
- Gli indirizzi IP vengono assegnati e gestiti dagli ISP (Internet service provider)

Introduzione al software libero

- Il software libero è un software pubblicato sotto i termini di una licenza libera, ovvero che ne incoraggia l'utilizzo, lo studio, la modifica e la redistribuzione.
- Il Software è Libero se possiamo:
 - Utilizzarlo per qualsiasi scopo
 - Studiarlo vedendo com'è fatto al suo interno
 - Farne copie senza limiti e distribuirle al prossimo
 - Modificarlo e ridistribuirne le modifiche a chiunque
- [Software Libero - Wikipedia](#)
- [Disciplinare Software libero - Economia Solidale Trentina](#)

Libero vs gratuito

- Il software libero non è gratuito, e secondo me è necessario evitare di veicolare questa associazione, come primo passo
- Donare al software libero che si ritiene utile alle proprie attività è il secondo
- Se puoi usare un software libero e portare a termine le tue attività è perché qualcun altro ci ha messo tempo e risorse
- Se sei soddisfatto di quel prodotto, finanziarlo: è un ottimo modo per contribuire (ma non il solo) per te e soprattutto per gli altri
- Altri modi per contribuire sono partecipare attivamente al progetto, ad esempio con le traduzioni, aiutando con la documentazione, segnalando bug, ecc...

Desktop vs mobile

- Per desktop si intendono i computer fissi e i portatili
- Per mobile gli smartphone, tablet, smartwatch
- È tendenzialmente più facile gestire il sistema operativo e i software sui desktop che non sul mobile
- In entrambe le categorie riceviamo già il prodotto con il sistema operativo e i software/app preinstallati
- Nei dispositivi mobile le app sono sempre connesse e autenticate e questo vedremo, è un problema

On-premise vs cloud

- On-premise: si implementano e/o si usano servizi sotto il proprio controllo, ovvero che vengono gestiti direttamente dall'utente/organizzazione
 - È la cosa che preferisco, ma capisco che ognuno non si possa fare tutto in casa. Ma certamente si possono fare a livello comunale/provinciale/nazionale
 - O affidarsi a provider che garantiscano la privacy (<https://www.privacytools.io/>)
- Cloud: si usano servizi che vengono erogati da terzi, spesso poco trasparenti: non sappiamo come vengono gestiti e che fine fanno i nostri dati

Sistemi centralizzati vs distribuiti

- In un sistema centralizzato, ci sono dei server che erogano il servizio e i client si connettono a loro per usufruirne
 - I server sono controllati da chi eroga il servizio
- In un sistema distribuito non ci sono server (o meglio possono esserci, ma non gestiscono tutti il traffico), ma i client si scambiano informazioni tra loro
 - Peer to peer
 - Peertube
 - WebRTC

Seconda parte

Problematiche

Di gratis non c'è nulla

- La quasi totalità dei servizi basati su cloud che utilizziamo ci viene apparentemente offerta in modo del tutto gratuito...mhhh...sarà proprio così?
- Proviamo a chiederci quanto e come guadagnano i giganti del web?
 - <https://www.visualcapitalist.com/how-tech-giants-make-billions/>
 - <https://www.lealternative.net/2020/10/14/come-guadagnano-le-grandi-aziende/>

Servizi web e cloud 1/2

- I servizi che vengono messi a disposizione dai principali fornitori del web, sono nella maggior parte dei casi gratuiti; di seguito alcuni esempi:
 - Motori di ricerca
 - Posta elettronica
 - Storage di dati
 - Social network e social media
 - IM
- Per far funzionare questi servizi, considerando la mole enorme di utenti, e quindi di flussi che è necessario gestire, sono necessari degli investimenti enormi in infrastrutture, personale, assistenza tecnica, competenze, ecc..

Servizi web e cloud 2/2

- Ora vorrei provaste a porvi (e a porre) questa domanda:
 - Conoscete delle persone che hanno versato una qualche somma in denaro per usare tutti questi servizi?
 - Come è stato possibile realizzare e adesso mantenere questi datacenter (centinaia) senza che nessuno abbia mai pagato nulla?
- Dobbiamo abbandonare la convinzione dell'equazione “pagare = dare soldi”
- In realtà noi siamo il prodotto: i nostri dati sono il nuovo oro



By Global Access Point [Public domain], via Wikimedia Commons

Termini e condizioni dei servizi

- Li leggiamo? NO
- Li approviamo e li sottoscriviamo? SEMPRE
- Ognuno di noi dovrebbe iniziare a fare degli sforzi in questa direzione
- Fermiamoci un attimo prima di accettare qualsiasi cosa per default
- Spesso sottoscriviamo termini di cui non abbiamo consapevolezza
- Accettiamo clausole e vincoli che nella vita offline ci farebbero storcere il naso
- Ecco un test per vedere come questi termini vengono talvolta proposti in maniera subdola: <https://termsandconditions.game/>

Autenticazione

- È un dovere custodire in modo ragionevolmente sicuro i propri accessi
 - Possono essere tanti, ma è un problema che va gestito
- Mi capita spesso di vedere persone con lo smartphone senza nessun sistema di sicurezza all'accesso
- Si continuano ad usare sempre le solite password per tutti i servizi
 - Sondaggio Bitdefender: un utente su due usa la stessa password ovunque:
<http://attivissimo.blogspot.com/2021/10/un-utente-su-due-usa-la-stessa-password.html>
- Non si attivano sistemi a doppio fattore
- Non si presta attenzione a fare il logout correttamente

Quali sono i rischi

- Tracciamento, raccolta dei dati e profilatura [1]
 - Fornitori mainstream del web – GAFAM - (Google, Apple, Facebook, Amazon and Microsoft)
 - Aziende terze e istituti privati (Nielsen Co, InfiniGraph, Cambridge Analytica) [2]
 - 47 aziende conoscono la posizione di 2 miliardi di utenti [38]
- Intercettazioni e sorveglianza di massa [3]
 - Agenzie governative in collaborazione con ISP e fornitori dei servizi
- Censura e repressione del dissenso [4]
- Perdita di controllo sui nostri dati [5]
- Indebolimento della crittografia [6]
- Leggi che vanno contro i nostri diritti
- Contribuire (spesso inconsapevolmente) agli attacchi che vengo perpetrati da organizzazione criminali [7]

Raccolta dati e profilatura

- I guadagni di tutte queste aziende derivano (in buona parte) dalla raccolta, catalogazione, e vendita dei dati degli utenti
- Ogni volta che facciamo una ricerca, consultiamo siti web, mandiamo email o messaggi con le app, quando usiamo i social-network lasciamo tracce del nostro passaggio [8]
- Anche i metadati vengono raccolti e catalogati
- Gli algoritmi raccolgono, catalogano ed elaborano questi dati al fine di stilare un profilo il più possibile fedele della nostra persona [9]:
- Algoritmi e bolle: <https://tracking.exposed>
- Per descrivere questa mole enorme di dati è stato introdotto il termine BigData: <https://www.valigiablu.it/illusione-big-data/>

Quali dati e come vengono raccolti

- Dati relativi al nostro device: <https://www.deviceinfo.me/>
- Fingerprinting: <https://www.nothingprivate.ml/>
- I cookie
- Gli URL traccianti
 - URL accorciati
 - URL che contengono elementi aggiuntivi
- Pixel di tracciamento <https://www.lealternative.net/2020/10/30/phantom-analyzer/>
- Telecamere e riconoscimento facciale
 - <https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9>
 - <https://www.valigiablu.it/riconoscimento-facciale-emozioni-diritti-umani/>
- Geolocalizzazione
- Computer in prestito per spiare studenti [10]

Uso dei dati raccolti

- Tutta questa mole enorme di informazioni viene usata per venderci pubblicità e prodotti
- Ma vengono anche usati per controllarci; i principali governi del mondo hanno accesso a questi dati, fanno leggi per poter accedervi [11], per poter sorvegliare
- Se è vero che tutti i dati raccolti potrebbero non venire mai usati, è altrettanto vero che sono a disposizione per un tempo potenzialmente infinito, e potrebbero essere usati in qualsiasi momento, contro di noi
- Sempre più spesso ci viene detto che la sorveglianza serve per bloccare gli attacchi terroristici [12]

Sorveglianza di massa

- Datagate: Edward Snowden rilascia molti documenti top secret [13] in cui vengono evidenziate delle pratiche di sorveglianza di massa da parte dell'NSA e di altri enti governativi in altri paesi [44]
- Vengono a galla programmi di sorveglianza [14] come PRISM, Xkeyscore, Tempora, Boundless Informant, Muscular e tanti altri
- Five Eyes: U.S.A. (NSA), U.K (GHCQ), Australia, Canada, Nuova Zelanda
- Intercettazione del traffico dati e telefonico in molti paesi, anche al di fuori degli Stati Uniti
- A tal proposito l'esperto di crittografia Bruce Schneier [15]

Censura e repressione del dissenso

- Il controllo e la sorveglianza vengono utilizzati per incastrare i dissidenti e gli attivisti, per reprimere il dissenso
 - Emirati Arabi, Bahrain, Egitto, Russia e altri
- I governi sono spesso aiutati da aziende che forniscono gli strumenti in grado di monitorare tutte le attività del target scelto (o di accedere ai dati in esso custoditi)
 - HackingTeam (Italiana) [16]
 - Cellebrite (Israeliana), Mslab (Svedese), NSO Group
- In alcuni stati vengono censurati siti web e servizi di Internet
 - Cina
 - Turchia
 - EAU
 - Russia

Perdita di controllo e del diritto alla privacy

- Ricapitolando affidiamo (volontariamente e involontariamente) sempre più spesso e in maniera sempre più estesa i nostri dati a dei fornitori di servizi, su cui non abbiamo controllo e che sottostanno a leggi in vigore dove risiedono fisicamente i loro server
- È facile dimenticarsi velocemente di quanto si è condiviso il giorno prima, mentre per i sistemi informatici è facile tenere traccia di tutto quello che è stato inserito
- Ma queste sistemi sono gestiti da persone, che possono commettere errori, e a quel punto i dati (personali e sensibili) che ci riguardano potrebbero finire online
 - Yahoo [17] [18]
 - Ashley Madison [19]
 - Equifax [20]

Indebolimento e bypass della crittografia

- I governi premono affinché la crittografia venga indebolita, affinché vengano inserite delle backdoor di servizio, così da poter accedere ai contenuti in via privilegiata
 - Apple vs FBI [21]
 - Attentati di Londra del 4 giugno 2017 [22]
 - Saggio di Cory Doctorow [23] [24]
- Indebolire la crittografia vuol dire minare la sicurezza degli utenti [25]

Minacce alla privacy

- Italia luglio 2017: estensione dei termini di memorizzazione dei dati raccolti dai provider (la cosiddetta data retention) a 72 mesi (6 anni) [26]
- USA aprile 2017: Il Congresso USA svende la privacy degli americani [27]
- UK (dicembre 2016): Il Regno Unito verso la sorveglianza totale: “Un attacco alla democrazia” [28]
- Apple, gli abusi sui minori e l’incubo della sorveglianza globale:
- <https://www.valigiablu.it/apple-abusi-minori-sorveglianza/>

Altri spunti

<http://www.valigiablu.it/netneutrality/>

<https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>

<https://blog.mozilla.org/press-it/2016/02/16/aiuta-mozilla-a-spargere-la-voce-la-crittografia-e-importante/>

<http://espresso.repubblica.it/visioni/tecnologia/2017/06/28/news/l-utopia-di-internet-oggi-e-morta-e-anche-i-guru-della-rete-si-sono-pentiti-1.304708>

http://www.repubblica.it/tecnologia/2014/03/14/news/nsa_violazioni_privacy-81012739/

<https://www.valigiablu.it/progetto-pegasus-spionaggio/>

<https://www.valigiablu.it/category/diritti-digitali/>

<https://www.lealternative.net/2021/10/15/gli-smartphone-android-ci-tracciano-in-continuazione/>

3° parte

Possibili soluzioni

Cosa possiamo fare: consigli in pillole

Possiamo cercare di migliorare la nostra sicurezza e privacy:

- Non dando nulla per scontato
- Usando sistemi operativi e software liberi al posto dei proprietari
- Usando servizi rispettosi degli utenti e della loro privacy
- Installando tutti gli aggiornamenti, soprattutto quelli di sicurezza
- Usando software di controllo/protezione
- Usando password sicure, diverse per ogni servizio e cambiandole regolarmente
- Configurando i browser in maniera opportuna e usando le estensioni
- Usando la crittografia E2E, la rete anonima* TOR e le VPN
- Usando app e app-store per smartphone alternativi
- Prestando attenzione a quello che condividiamo e immettiamo in rete
- Verificando le fonti
- Non fidarsi dei punti di accesso liberi

Come scegliere il proprio device

- Informarsi e chiedere nelle community prima di acquistare un qualsiasi device
- Scegliere device che hanno la miglior compatibilità con quello che poi si vorrà installare
 - Ad esempio se si vuole installare LineageOS, meglio preventivamente verificare la lista di compatibilità e scegliere il device di conseguenza: <https://wiki.lineageos.org/devices/>
- Scegliere device usati o ricondizionati è una buona idea, sia per sé stessi sia per l'ambiente
 - <https://iode.tech/en/>
 - <https://esolutions.shop/>

Come scegliere il sistema operativo

- Sui desktop si può installare Linux senza particolari problemi (UEFI non lo è più)
 - Noi di Linux Trent consigliamo Ubuntu e derivate
 - Sistemi operativi Debian-based
- Su mobile bisogna avere alcune accortezze:
 - Scegliere con cura il device (vedi slide precedente)
 - Scegliere un device con già a bordo un sistema lineageos o un suo fork
 - Affidarsi a qualcuno di un po' competete per l'installazione, in quanto non è cosa così banale
 - Video serata informativa:
<https://video.linuxtrent.it/videos/watch/04ccd67c-347b-4f95-a0f6-2b756001710c>

Aggiornamenti sistema operativo

- Tenere aggiornato il sistema operativo è di fondamentale importanza, ma spesso è la prima cosa che viene trascurata
- Controllare sempre se sono disponibili aggiornamenti e installarli
- Gli aggiornamenti di sicurezza sono critici e vanno sempre fatti
- Nel mondo mobile (Android) spesso e volentieri i produttori non rilasciano aggiornamenti, costringendo gli utenti a restare con versioni obsolete e vulnerabili; valutare anche questo prima di fare un acquisto

Gestione dell'autenticazione

- Non usare password semplici (da dizionario); una buona password, al giorno d'oggi, deve avere almeno 12 caratteri alfanumerici e casuali o usare passphrase
- Non usare MAI la stessa password più volte
- Cambiare le password dei servizi on-line regolarmente
- Usare un gestore delle password (KeePassX)
- Usare, dove possibile, l'autenticazione a 2 fattori

KeepassX – gestore password

- <https://www.keepassx.org/>
- Software libero e multi-piattaforma
- È necessario creare un database
- Impostare una password solida e robusta (sarà quella che proteggerà tutte le altre password)
- Per aumentare la sicurezza è possibile creare una chiave da associare ad database
- Impostare la chiusura automatica in caso di non utilizzo e la cancellazione dei dati dagli appunti
- Necessario eseguire il backup del database
- Usare database diversi per necessità diverse (personale e lavoro, ad esempio)

Quale browser scegliere

- Firefox (consigliato): multi-piattaforma, sviluppato e supportato dalla fondazione Mozilla Foundation, la quale si batte da sempre per un web libero

Pagina ufficiale: <https://www.mozilla.org/it/>

- Iridium: recente progetto basato sul codice di Chromium che estende e migliora la privacy durante la navigazione

Pagina ufficiale: <https://iridiumbrowser.de/>

* Chromium (which Iridium is based on) is a very secure browser, yes. But it does call home to Google. And we did even more to enhance security to the maximum extent possible.

- Ungoogled-chromium: progetto su github che rimuove i riferimenti al mondo Google

Pagina ufficiale: <https://github.com/Eloston/ungoogled-chromium>

Browser – consigli generali 1/2

- HTTP: traffico in chiaro
- HTTPS: traffico protetto (cifrato), compare lucchetto
 - Non fermarsi al lucchetto, verificare il certificato (possibili attacchi MITM)
- È buona cosa tenere sotto controllo la barra dell'indirizzo (URL), per essere consapevoli del tipo di protocollo usato, e su quale sito stiamo navigando
- È buona cosa non cliccare sui link senza pensare (il nome del link non corrisponde quasi mai all'URL vero e proprio); un buon metodo per vedere dove punta il link è quello di passarci sopra con il mouse e in basso (tipicamente) comparirà l'URL di destinazione (non funziona con i link abbreviati)

Browser – consigli generali 2/2

- Verificare che l'opzione Do Not Track sia abilitata: chiede ai siti web di non eseguire il tracciamento; l'opzione può essere ignorata dai server
- Cronologia e cookie: valutare come gestirli, di solito si accettano i cookie dai siti (di sessione o tecnici); si consiglia invece di disabilitare i cookie di 3° parti (abilitare solo i domini strettamente necessari)
- Password: evitare di salvare le password nel browser può tanti motivi: si dimenticano e sono a rischio

Firefox settaggi 1/2

Menu preferenze → Privacy

- Tracciamento: firefox dalla versione 42 ha migliorato le opzioni per la privacy, introducendo l'anti-tracciamento nella modalità “Navigazione anonima” che di default è abilitato
- Usare la “Navigazione anonima” vi permette di non lasciare tracce sull'account del PC che state usando (in rete restano)
- Cronologia: Impostazioni cronologia
 - Accetta i cookie dai siti: SI
 - Accetta i cookie di terze parti: MAI
 - Conservali fino: Alla chiusura di firefox

Firefox settaggi 2/2

Menu preferenze → Sicurezza

- Ricorda i dati di accesso ai siti: disattivare (più scomodo ma più sicuro)
- Utilizza una password principale: permette di impostare una password unica per proteggere tutti i dati di autenticazione che sono salvati nel browser
- Accessi salvati: vi permette di vedere quali sono stati salvati in precedenza

Firefox – Componenti aggiuntivi

- Menu → Componenti aggiuntivi → Estensioni
- È possibile estendere le funzionalità di Firefox attraverso alcuni componenti: ecco i più interessanti..
 - Ublock Origin: filtraggio dei contenuti e ad-blocker (blacklist)
 - Multi-account container: permette di tenere i contenuti delle schede separati
 - Cookie AutoDelete: elimina i cookies automaticamente al termine della sessione
 - ClearURL: pulisce gli url dagli elementi traccianti
 - HTTPS Everywhere: dove possibile tenta di redirigere le richieste http in https; su alcuni siti può causare problemi
 - Privacy Badger: blocca tutti gli elementi traccianti che vengono trovati nella pagina che si sta visualizzando, permettendo il loro sblocco selettivo
 - Privacy redirect: redirige gli url su backend alternativi
 - NoScript e uMatrix (avanzati): bloccano tutti gli script che vengono caricati nella pagina; in alcuni casi impediscono di visualizzarla
 - Unshort.link: espande gli url accorciati e mostra dove portano

Dispositivi mobile

- Sempre più utenti usano i propri dispositivi mobile per usufruire dei servizi web
 - In ottobre 2016 per la prima volta il traffico mobile ha superato il traffico desktop
- Se possibile evitare il framework Google e tutte le relative librerie
 - Esistono alternative: microG [29]
- Attenzione alle autorizzazioni delle App: controllarle e settare solo le necessario e ogni tanto fare un check
- Attenzione alla condivisione della nostra posizione (GPS, reti wi-fi)
- Installare poche app e verificare la loro affidabilità
- Permessi di root: parliamone

App suggerite su mobile

- Usare app-store alternativi: F-droid [30], Aurora Store
- DNS 66 o Blokada
- Tracker Control, Exodus, ClassyShark3exodus
- UntrackMe
- OpenContacts
- AFWall+, NetGuard
- Uso comune: NewPipe, AntennaPod, Twidere, NextCloud, VLC, K-9 Mail

Motori di ricerca

- I motori di ricerca più comuni e usati spesso non tutelano la nostra privacy
- Alcune alternative:
 - <https://duckduckgo.com> [31]
 - <https://www.startpage.com/> [32]
- Controlla se il tuo account di posta risulta nei database dei siti compromessi:
 - <https://haveibeenpwned.com/>
- Shodan (motore di ricerca host connessi in rete):
<https://www.shodan.io/>

Servizi di posta più sicuri

- Anche i servizi di posta più conosciuti spesso non rispettano la nostra privacy
- Alcune valide alternative:
 - <https://posteo.de/en>
 - <https://www.riseup.net>
 - <https://protonmail.com/>
 - DA LEGGERE: <https://www.resolutions.it/nextcloud/index.php/s/bDJfD2Z6XtKB8wm>
 - <https://www.autistici.org/en/index.html>
- Per saperne di più:
 - <http://www.prxbx.com/email>
 - <https://www.privacytools.io/>

Servizi di cloud più sicuri

- OwnCloud, NextCloud
- Scegliere servizio che supportino la crittografia zero-knowledge
- Crittografare i dati prima di inviarli in cloud che non controllate
- Avete delle reali necessità di condivisione dei file [33]?

Servizi di localizzazione

- Openstreetmap è un progetto libero, a cui tutti possono contribuire
- Contribuendo al progetto aiuti la comunità
- I dati vengo messi a disposizione di tutti per poter essere usati
- <https://www.openstreetmap.org>
- Esempio uso OSM [34]:

Un passo in più

- Usare una VPN per navigare e per proteggere la propria privacy (pro e contro)
- Usare TOR per navigare in maniera molto anonima
 - <https://www.torproject.org>
- Rendere sicura la vostra posta elettronica con GnuPG
 - <https://gnupg.org/>
- Configurare e usare un firewall anche sul proprio PC/Smartphone

Leggi e sentenze pro privacy

- Garanti della privacy
- Corte Europea
 - La Corte europea dice che la sorveglianza di massa è illegittima. Di nuovo [35]
 - Sentenza Schrems [36]
 - La Corte europea invalida l'accordo Privacy Shield sul trasferimento dei dati europei e declassa gli Usa:
<https://www.valigiablu.it/corte-giustizia-europa-privacy-shield/>
 - https://it.wikipedia.org/wiki/Scudo_UE-USA_per_la_privacy
- Regolamento in materia di protezione dei dati personali (GDPR)
- Proposta di regolamento ePrivacy [37]
 - Si occupa specificamente della tutela delle comunicazioni elettroniche, della sicurezza dei dispositivi digitali e della protezione dei dati personali nel mondo online

Chi si batte: attivisti/whistleblower e organizzazioni

- Edward Snowden
- Julian Assange
- Chelsea Manning
- Ahmed Mansoor
- Daphne Caruana Galizia
- Mozilla Foundation
- Noyb
- Amnesty International
- Citizen Lab
- EFF

Chi ne parla

- Spesso gli argomenti riguardanti i temi che abbiamo toccato passano in sottofondo, non venendogli attribuito il peso che meritano
 - Italiani: Stefania Maurizi, Carola Frediani, Fabio Chiusi
 - Internazionali: Glenn Greenwald, Laura Poitras, Bruce Schneier, Cory Doctorow
 - Testate giornalistiche italiane: ValigiaBlu, Il Post
 - Testate giornalistiche internazionali: The Guardian, The Intercept
- Altri siti interessanti:
 - <https://www.lealternative.net/>
 - <https://www.3x1t.org/>
 - <https://guerredirete.it/>

Lecture interessanti

- NetNeutrality (Fabio Chiusi) [39]
- La risorsa più preziosa al mondo sono i dati (The Economist) [40]
- Mozilla: la crittografia non è un optional, ma un diritto [41]
- L'utopia di internet oggi è morta. E anche i guru della rete si sono pentiti (Fabio Chiusi) [42]

Riferimenti e Link utili 1/4

- [1] https://it.wikipedia.org/wiki/Profilazione_dell%27utente
<http://www.valigiablu.it/trump-privacy/>
- [2] <http://www.ilpost.it/2010/10/13/privacy-internet-dati/>
<https://www.valigiablu.it/cambridge-analytica-big-data-trump-facebook/>
- [3] https://it.wikipedia.org/wiki/Divulgazioni_sulla_sorveglianza_di_massa_del_2013
- [4] https://it.wikipedia.org/wiki/Censura_di_Internet
- [5] <https://www.tedxcambridge.com/talk/the-battle-for-power-on-the-internet/>
- [6] <https://www.agendadigitale.eu/sicurezza/nessuno-tocchi-la-crittografia-ecco-perche-e-pericoloso-indebolirla-e-quali-alternative-ci-sono-per-l-e-indagini/>
<https://www.agendadigitale.eu/sicurezza/privacy/se-i-governi-vogliono-rompere-la-crittografia-per-spiarci-meglio/>
- [7] <http://attivissimo.blogspot.com/2016/10/lattacco-delle-centomila-telecamere-che.html>
- [8] <https://coveryourtracks.eff.org/>
- [9] <http://www.valigiablu.it/cambridge-analytica-big-data-trump-facebook/>
- [10] <https://www.theguardian.com/commentisfree/2021/oct/11/us-students-digital-surveillance-schools>
- [11] <http://www.valigiablu.it/uk-legge-sorveglianza/>
- [12] <http://espresso.repubblica.it/internazionale/2015/11/18/news/terrorismo-perche-la-sorveglianza-di-massa-ha-fallito-1.239855>
- [13] <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>
- [14] <https://www.valigiablu.it/grazie-mr-snowden-datagate-nsa/>
- [15] <http://www.bernardi.cloud/2013/09/09/bruce-schneier-come-rimanere-sicuri-contro-la-sorveglianza-della-nsa/>

Riferimenti e Link utili 2/4

- [16] <https://attivissimo.blogspot.it/2015/07/lo-spione-spiato-hacking-team-si-fa.html>
- [17] <http://attivissimo.blogspot.com/2016/09/yahoo-oltre-500-milioni-di-password.html>
- [18] <https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached>
- [19] <http://www.lastampa.it/2015/08/20/tecnologia/hacker-attaccano-il-sito-di-incontri-ashley-madison-diffusi-i-dati-di-milioni-di-fedifraghi-xFlxr8ZoyxQtIKEvDmvilL/pagina.html>
- [20] <http://attivissimo.blogspot.com/2017/09/rubati-i-dati-di-meta-degli-americani.html>
- [21] <https://attivissimo.blogspot.com/2016/02/perche-apple-va-contro-Ifbi.html>
- [22] <https://www.gov.uk/government/speeches/pm-statement-following-london-terror-attack-4-june-2017>
- [23] <https://www.theguardian.com/technology/2015/may/01/encryption-wont-work-if-it-has-a-back-door-only-the-good-guys-have-keys-to>
- [24] <http://attivissimo.blogspot.com/2017/06/cory-doctorow-perche-bandire-la.html>
- [25] <http://www.datamanager.it/2016/02/indebolire-la-crittografia-vuol-dire-minare-la-sicurezza-degli-utenti/>
- [26] <http://www.valigiablu.it/ascensori-dati-sorveglianza-massa/>

Riferimenti e Link utili 3/4

- [27] https://www.repubblica.it/tecnologia/sicurezza/2018/01/12/news/il_congresso_usa_vota_per_rinnovare_la_sorveglianza_di_massa_denunciata_da_snowden-186368275/
- [28] <http://www.valigiablu.it/uk-legge-sorveglianza/>
- [29] <https://microg.org/>
- [30] <https://f-droid.org/>
- [31] <http://www.tecnoandroid.it/2015/06/18/cresce-duckduckgo-motore-ricerca-tutela-privacy-128882>
- [32] <https://www.ixquick.com/ita/aboutixquick/>
- [33] <https://lifehacker.com/the-best-cloud-storage-services-that-protect-your-privacy-729639300>
- [34] http://sky.mappeelettorali.it/_sky/referendum2016/comuni.html
- [35] <http://www.valigiablu.it/corte-europea-sorveglianza-massa/>
- [36] <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117it.pdf>
- [37] <http://www.valigiablu.it/regolamento-europeo-privacy/>
- [38] <https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data>

Riferimenti e Link utili 4/4

- [39] <http://www.valigiablu.it/netneutrality/>
- [40] <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>
- [41] <https://blog.mozilla.org/press-it/2016/02/16/aiuta-mozilla-a-spargere-la-voce-la-crittografia-e-importante/>
- [42] <http://espresso.repubblica.it/visioni/tecnologia/2017/06/28/news/l-utopia-di-internet-oggi-e-morta-e-anche-i-guru-della-rete-si-sono-pentiti-1.304708>
- [44] http://www.repubblica.it/tecnologia/2014/03/14/news/nsa_violazioni_privacy-81012739/

Grazie per l'attenzione



Associazione LinuxTrent

www.linuxtrent.it