BASTARDI SENZA GOOGLE

"Il gruppo BsG (Bastardi senza Google) nasce con lo scopo di aiutare le persone a trovare soluzioni alternative, valide e concrete per utilizzo di pc e smartphone con programmi non riconducibili a Microsoft, Apple o Google e bigh tech di questo calibro. In pratica tutti quei programmi, servizi, social network, piattaforme e hardware che tracciano i nostri dati ed i nostri metadati, utilizzandoli a fini di lucro e soprattutto a fini “politici” di controllo, e indirizzamento del pensiero. Oltre a ciò, negli ultimi anni, si sono dimostrati feroci censori di tutto quello che non era in linea con il pensiero dominante imposto dalle elite economiche, finanziare e politiche del capitalismo globale e sovranazionale. La libertà di espressione, di pensiero e di informazione praticamente soppressa da questi “tecno-mostri” privati.

Le soluzioni esistono, c’è un vasto mondo di software open source, dove il codice sorgente è a disposizione di tutti, controllabile da una intera comunità di sviluppatori che credono nel software libero e trasparente. Libero, precisiamo, non significa per forza gratuito e gratuito non significa sempre essere il prodotto. Crediamo che dove è possibile sia giusto contribuire al mantenimento di queste comunità per far crescere consapevolezza e libertà.

La finalità dunque è la seguente: uscire dal controllo diretto delle grandi aziende, dalla cessione inconsapevole di ogni nostro dato sensibile, riprendendo il controllo sul dispositivo, sulla nostra privacy, sul nostro tempo e sul possesso dei nostri dati. Tra i nostri dati in un futuro molto prossimo potrebbero finirci anche i nostri soldi e molto altro ancora.

Il passo da compiere per essere digitalmente liberi richiede un piccolo impegno ma anche e soprattutto un grosso sforzo psicologico. Abbandonare le vecchie abitudini nell’uso di questi strumenti che ci seguono quotidianamente, addirittura ora per ora, minuto per minuto non è semplice. Per affrontare questo passo verso la riconquista di uno spazio di libertà è necessario, prima di tutto, essere consapevoli dell’atto “politico” di libertà che si compie. Togliere la linfa vitale a chi ci vuole solo schiavi a cui mungere dati personali, a cui vendere prodotti, a cui far fruire solo informazioni mediate e necessarie al mantenimento del pensiero unico scientificamente, tecnologicamente e politicamente corrotto. Corretto volevo dire...corretto.
Rimodulare l’utilizzo personale della tecnologia perché sia uno strumento di servizio per l’utilizzatore e non mezzo di asservimento.

Per tutto questo BSG organizza incontri per far comprendere al meglio i suoi scopi, le sue proposte e per quanto sarà possibile dare un supporto a chi condividerà questo progetto.

BSG è un gruppo di volontari appartenenti a Uniamoci Trentino APS di cui condivide gli scopi sociali ed i regolamenti interni.

Se vuoi saperne di più contattaci.

Email: uniamocibsg@proton.me

PC e sicurezza

Sistemi Operativi: è vivamente consigliato installare Linux. Tutte le distribuzioni di Linux contengono già svariati programmi open source per l'utilizzo comune come la suite di Libre Office, il browser Firefox ed altri che elencheremo in seguito. Se non potete abbandonare del tutto Windows e non volete o potete utilizzare 2 PC vi è la possibilità di installare Linux a fianco di Windows. La cosa è possibile anche sui sistemi Apple che si basano su processori Intel ma personalmente ci sentiamo di sconsigliarlo.

Linux può essere installato nelle varie distibuzioni: Ubuntu, Mint, KDE e molte altre. Linux Tails è un sistema operativo portatile utile per protgeggersi da censura e sorveglianza.
Nelle installazioni Linux trovate già pronti da installare centinaia di programmi per ogni esigenza.

Consigli utili per tutti i sistemi utilizzati:

Password: inserite password sicure - ogni sito o servizio deve avere PWD diverse – Utilizzate PWD manager. Accessi piu sicuri con autenticazione a 2 o piu fattori.

Backup: eseguite backup dei vostri dati su supporti esterni a quelli del sistema.

VPN: le VPN sono servizi che instradano il vostro traffico internet utilizzando un IP address del server VPN cosi che il vostro traffico non possa essere riconosciuto come proveninte dal vostro IP. Ve ne sono di gratuiti ma i più affidabili sono a pagamento. Con le VPN è possibile superare anche il Geo Blocking. (Private Internet Access, Mullvad)

Motore di ricerca: modificate il motore di ricerca nel browser (DuckDuckgo, Startpage, Qwant)

Browser: tenete aperta una scheda per volta quando possibile e chiudete sempre le sessioni attive e fate il logout dei siti dove vi siete loggati. Alcuni software sono in grado di leggere le altre schede. Utilizzate degli AdBlocker per bloccare pubblicità e finestre inutili. (Brave, Mozilla Firefox)

Mail: utilizzate provider che garantiscono la crittografia totale non solo end to end ma anche che il provider non possa leggere i vostri contenuti.

Crittografia: Gnu-Pg è un sistema per crittografare file, note, contenuti di email. Un interfaccia grafica di gestione crittografica utile è Kleopatra scaricabile per tutti i sistemi operativi compreso Android.

Social Network: sono montagne di informazioni per male intenzionati e per i proprietari dei social. Se proprio dovete, meglio utilizzarli da browser piuttosto che dalle App proprietarie. Fate il logout quando non lo utilizzate.

Permessi delle App: prima di scaricare un'App controllate i permessi che richiede. Che motivo ha un giochino di avere accesso alla vostra rubrica o alla vostra fotocamera ?

Email: uniamocibsg@proton.me

Blutooth: attivo solo per il tempo necessario all'uso. Il Blutooth è utilizzato ormai su miliardi di dispositivi dal telefonino all'auto ed all'internet of thing (IOT). La sua universalità e facilità d'uso è anche la causa della sua estrema vulnerabilità.

Virtual Machine: per una sicurezza ancora maggiore è possibile utilizzare delle macchine virtuali. All'interno di una macchina virtuale installata sul vostro PC o su un server è possibile far girare un intero sistema virtualizzato totalmente isolato dal sistema ospite.

Rete: Preferire sempre connessioni cablate, sono più sicure di wi-fi e 4G e nel caso foste sensibili all'argomento di sicuro non rischiate l'inquinamento elettromagnetico.
Una delle cose che vi espone a ad alti livelli di rischio attacco informatico sono le reti wi-fi pubbliche. Utilizzatele solo se disponete di un servizio VPN serio.

Telefoni

Google: contrariamente a quanto possa apparire, non è necessario attivare l'account google per far funzionare il telefono e le applicazioni. Potete tranquillamente discontterlo e togliere (disattivare) le app google dopo esservi salvati i dati che vi interessano, per esempio la rubrica.

Rubrica contatti: alternative Open Source come OpenContact

Tastiera: la tastiera dei telefoni raccoglie tutto ciò che digitate e con il vostro permesso inconsapevole se ne fa proprietario. La grandissima maggioranza delle tastiere in uso sui telefoni Android è quella di Google ed a seguire quella del produttore del device. Esistono tastiere open source che non salvano i dati e non li elaborano come OpenBoard o altre. Basta installarle andare nelle impostazioni e sostituire la tastiera.

App preinstallate: lo stesso discorso fatto per le tastiere vale in gran parte anche per le app, apparentemente innoque, che trovate preinstallate sul telefono, come il calendario, le note o le app di Health Care che vanno tanto di moda oggi.
In generale sui telefoni conviene controllare tutte le app preinstallate e nel caso sostituirle con altre sicure.

Email: uniamocibsg@proton.me