Digital Education. Come difendere la nostra privacy online?

Privacy online, come difendersi in rete e non solo? Se ormai va quasi di moda dire, peraltro non a torto, che la sicurezza dei nostri dati è un'illusione, limitiamoci qui alle ultime news: che ci mostrano tra i nuovi, inattesi paladini della privacy il «**vecchio gigante Firefox»,** tornato prepotentemente agli onori delle cronache. E non smette di stupirci. Già qui segnalavamo due importanti novità: l'estensione **Facebook Container**, che isola l'identità **Facebook** di ognuno in una tab separata, per evitare che il social ti tracci anche fuori dalla piattaforma, separando la navigazione su social da quella su qualsiasi link non appartenente alla piattaforma, per far sì che l'attività online extra rimanga protetta; in secondo luogo, l'integrazione con Pocket, per scoprire contenuti di maggiore qualità all'apertura di ogni nuova pagina, in alternativa alla logica del News Feed.

Di poche ore fa, poi, un nuovo annuncio: l'arrivo di un tool che userà il database di Have I Been Pwned per indicare quali account siano stati hackerati. «Dallo shopping ai social media, gli utenti hanno centinaia di account che richiedono password», dichiarano da Mozilla. *«Allo stesso tempo il numero di furti dei dati continua a crescere drammaticamente. È comprensibile che la gente ora sia ben più preoccupata per la sua sicurezza su Internet e su crimini informatici che coinvolgono informazioni personali e finanziarie. Per mantenere al sicuro tutto questo, stiamo testando un nuovo strumento che consentirà di controllare se i propri dati siano stati compromessi nelle operazioni di qualche hacker».*

Nello specifico, grazie alla partnership con **Troy Hunt**, uno dei più rinomati e rispettati esperti di sicurezza nel mondo, già creatore del celebre servizio HIBP – «Sono stato vittima di hacker?», che include un database di indirizzi e-mail noti per essere stati compromessi e violati – ed alla creazione dell'apposito strumento di sicurezza Firefox Monitor, sarà possibile controllare, inserendo un indirizzo e-mail, se questo sia già inserito nel database di Have I Been Pwned, con informazioni dettagliate sui siti e altre fonti di violazione o riguardanti i dati personali esposti in ogni operazione di hackeraggio. Saranno anche inviati agli utenti appositi alert in caso di eventuali nuove violazioni.

La partnership includerà anche 1Password, «la sola password sicura che non puoi ricordare», dichiara Hunt. La loro stretta collaborazione già da marzo aveva fruttato la creazione delle «Pwned Passwords», presenti nelle App desktop per Mac e Windows. Stavolta però, grazie all'inserimento di un «database di migliaia di utenti», il passo avanti è molto maggiore.

Se i browser si danno finalmente una mossa, le App non stanno a guardare. **Telegram** in particolare, fondata da **Pavel Durov** il 17 agosto 2013, in diffusione rapidissima con i suoi 200 milioni di utenti attivi, 700.000 nuovi al giorno e che ha fatto della difesa di libertà e democrazia una bandiera, non solo nelle dichiarazioni ma nella sostanza, con la sua infrastruttura distribuita, basata su un cloud «frantumato su più datacenter attorno al globo, controllati da differenti entità legali a loro volta sono distribuite sotto diverse giurisdizioni, che rende così impossibile l'accesso di fatto alle informazioni crittografate scambiate tra gli utenti», ha fatto molto parlare di sé giusto ieri. E non ci riferiamo al

#TelegramDown che, nel primo pomeriggio, ha fatto impazzire la rete, bensì alle novità trapelate, e subito viralmente rilanciate da tutti i principali canali vicini alle fonti ufficiali di Telegram, circa Telegram Passport, nuovo servizio presto in arrivo sulla piattaforma. Una sorta di borsellino, portadocumenti digitale, con il vantaggio della protezione assoluta garantita. Grazie ad esso «si potrà facilmente iscriversi ai siti e ai servizi che richiedono verifica dell'identità, senza però il rischio della compromissione di dati». In barba al Facebook Connect, di cui solo ora ognuno si è accorto delle potenziali, dannose conseguenze in termini di privacy, con Telegram Passport «informazioni, dati personali e documenti sono protetti dalla crittografia *end-to-end* e nessuno, inclusa Telegram, potrà mai accedervi senza il tuo permesso».

Ritenuto ormai da mesi la via preferenziale per conservare quei dati personali e bancari richiesti al fine di autenticarsi sull'imminente piattaforma di criptomoneta Telegram Open Network, terza generazione di blockchain e già record per aver raccolto oltre 2,6 miliardi di dollari ancora prima dell'uscita pubblica della richiesta capitali – la cosiddetta ICO – promette di essere un plus per tutti. Una volta creata la password di protezione, si potrà aggiungere, e accedere poi in maniera totalmente sicura, a documenti e dati, dalle informazioni anagrafiche al numero della carta credito e a dati bancari. Telegram, aggiornatasi giusto ieri alla Versione 4.8.10 – con piccole ma interessanti news quali la possibilità di segnare le chat come lette/non lette, sostituire i media quando si modifica un messaggio, annullare l'invio dei messaggi prima che vengano inviati e usare «crea link» nel menu di formattazione per creare URL dal testo – mostra di voler andare avanti sulla propria linea di difesa della privacy.

Per il resto? In modo apparentemente paradossale, la rete è piena di risorse utili per difenderci, scoprendo ciò che i Big sanno di noi, e attaccare, proteggendoci in maniera proattiva. Basta voler cercare e saper dove farlo. Un «luogo» su tutti, regalo da [pre]weeekend? Guide come questa, da stampare, leggere con calma e appendere accanto alla scrivania. Non scoprono niente se non ciò che dovremmo da sempre sapere. L'Educazione Civica Digitale, d'altronde, è anzitutto questo: partire dal quotidiano per rintracciare nelle nostre abitudini di ogni giorno «le cretinate che ci rovinano la vita».

The post Digital Education. Come difendere la nostra privacy online? appeared first on Key4biz.

https://www.key4biz.it/digital-education-come-difendere-la-nostra-privacy-online/225755/