Come non cadere dalle nuvole

Con le informazioni che transitano da computer e telefonini rendiamo pubblico ogni dettaglio della nostra vita, ma l'autodifesa digitale è possibile

di Serena Tinari

Alzi la mano chi utilizza una "cloud", la nuvola virtuale per conservare i dati. Siete tantissimi! C'è una brutta notizia: non siete al sicuro. L'ultimo caso che lo ha dimostrato è l'incidente capitato alla sorella della futura regina del Regno Unito. Pippa Middleton è rimasta vittima di un caso banale quanto eclatante di criminalità informatica del tipo "ransom", estorsione: ho i tuoi dati, quanto sei disposto a pagare per riaverli? Il caso è esemplare. Perché se è facile violare la sicurezza elettronica di una persona sorvegliata dai servizi segreti, pensate quanto può essere semplice entrare nell'account di un comune mortale.

Niente da nascondere? Pensateci un attimo. Nelle "nuvole" è archiviata ogni informazione che transiti per telefono e computer. Sms ed email, le ricerche effettuate su Internet, la rubrica e l'agenda. I viaggi che prenotate con l'App delle Ferrovie e quindi la carta di credito che avete inserito per comprare i biglietti. Magari ci sono anche delle password che avevate salvato nelle Note o inviato per sms alla fidanzata per fare una prenotazione? Oltre naturalmente a ogni documento di testo e ad ogni foto che possediate.

Nudi alla meta

Quando litigate con vostro marito, lo fate in pubblico? Diffondete con un altoparlante le confessioni all'amico del cuore? E i patemi dell'anima, li raccontate in ogni dettaglio al macellaio? Per come sono fatti il mondo di Internet e gli strumenti per accedere alla rete, usare senza prendere precauzioni computer e telefono corrisponde a trascrivere la vostra vita su un quaderno, che lascerete su una panchina pubblica. Vi sentite improvvisamente nudi? Fate bene. È il cambio di mentalità che la nuova era impone. L'insieme della nostra attività digitale consente, infatti, di farsi un'idea precisa di chi siamo e cosa facciamo. A immergersi nelle informazioni che spargiamo su Internet, ci scorre davanti tutta la nostra vita. Le lettere private spedite via email raccontano gioie e dolori della quotidianità. Un messaggio di frustrazione rivela che tipo di lavoratore sei. Cosa compri, in quale banca tieni i soldi, dove acquisti i biglietti aerei e persino che domande ti fai sulla vita e la morte, attraverso le stringhe di ricerca che hai digitato. Tutto viene registrato e immagazzinato.

Dimmi chi sei

Ci avrete fatto caso, sembra un prodigio. Non si fa in tempo a finire di inserire una frase in Google, che il sistema fornisce quello che cercavamo sotto l'ammiccante titolo "Mi sento fortunato". Non è fortuna. È che Google ci conosce benissimo, perché per ognuno di noi possiede un "profilo" aggiornato ogni volta che facciamo una ricerca, che usiamo una casella di posta Gmail o ci connettiamo ai social media. A identificarci sono il numero IP, che rivela il luogo da cui ci connettiamo, e l'indirizzo MAC ovvero la carta d'identità dell'apparecchio che utilizziamo. Le informazioni sono archiviate e messe a disposizione di operatori commerciali. È per questo che se in WhatsApp comunicate con una canadese, LinkedIn vi suggerirà di cliccare sul suo profilo e Twitter consiglierà di "seguire" utenti canadesi. Tutto ciò avviene grazie al magico mondo degli algoritmi e i calcoli che aggiornano i profili avvengono in tempo reale e ad una velocità impressionante. Lo scopo principe di cotanta sorveglianza è il marketing. Perché c'è un motivo, se Internet è gratis: i nostri profili producono denaro. Gli esperti la chiamano "pubblicità comportamentale": dimmi chi sei e ti proporrò prodotti che corrispondano ai tuoi interessi. Il "profiling" a fini commerciali è la madre dei nostri problemi di privacy online. Non siamo liberi, su Internet. Siamo un numero che produce denaro.

> Il primo passo è la presa di coscienza

L'autodifesa digitale inizia dalla presa di coscienza: prima di premere "invio", chiedetevi se state consegnando alla rete informazioni che vi darebbe fastidio trovare su una panchina al parco. E ponetevi qualche domanda sui fornitori dei servizi che utilizzate. I giganti di Internet offrono spazio e strumenti, gratis. Ma come ha dimostrato il recente caso di Yahoo, 200 milioni di caselle di posta elettronica violate e la sconcertante notizia data ai clienti con due anni di ritardo, questi servizi in realtà li paghiamo cari. Perché chi li fornisce garantisce solo la certezza che i nostri dati verranno generosamente utilizzati. Se potete, allora, preferite piccoli providers. Ce ne sono moltissimi e tanti sono gratuiti.

Una fondamentale arma di difesa è proteggere il computer dai "malware", i programmi malefici. Si nascondono in un link o in un documento dall'apparenza innocua. Prima di cliccare, chiedetevi se aspettavate quella email e quell'allegato. Se avete un dubbio telefonate al mittente per accertarvi che il suo account non sia compromesso. Un malware sa fare tante cose: può inviare una email plausibile eppure truffaldina ai vostri contatti e copiare cosa digitate sulla tastiera. Si impadronisce dei dati personali, per rivenderli o fare acquisti a vostro nome. Se siete una giornalista o un attivista, può essere usato per sorvegliarvi.

Grazie alle rivelazioni del whistleblower Edward Snowden sappiamo che i governi sono molto affaccendati nella raccolta estensiva di ogni forma di comunicazione elettronica. Grazie all'approvazione della Legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (Lscpt) e di quella sulle attività informative (LAIn) d'ora in poi si farà ufficialmente anche in Svizzera.

Per saperne di più

nexa.polito.it/come-funziona-internet.xx
Manuale "Come funziona Internet"
tinyurl.com/gnwqp4l
Trasformare uno smartphone in una spia
tinyurl.com/gvjxz9e
"Citizenfour", un film di Laura Poitras
tinyurl.com/zmmxkpw
"Citoyens sous surveillance", documentario di Alexandre Valenti

Consigli utili

Proteggere le e-mail

Spedire una email senza alcuna forma di crittazione è come inviare una cartolina senza busta. Chiunque si ritrovi in mano il vostro messaggio ne può leggere il contenuto. Utilizzare sistemi di crittografia corrisponde ad infilare la vostra lettera in una busta che solo il destinatario può aprire. Senza dover diventare un mago dell'informatica, è possibile proteggere le email grazie a PGP, OpenPGP e GPG. Una guida di facile lettura è disponibile nel sito dell'organizzazione italiana Autistici/ Inventati: http://tinyurl.com/zf53yfz

Alternative a Google

È un sano esercizio usare motori di ricerca alternativi a Google. DuckDuckGo funziona alla perfezione e non spia l'utente. Poiché non conserva alcun profilo personale, dovrete utilizzare termini di ricerca esatti e completi. Non aspettatevi, insomma, che DuckDuckGo conosca il vostro luogo di residenza, né le preferenze per cibi e commerci. Il sistema TOR è semplice da installare e garantisce l'anonimato: www.torproject.org

Browser più discreto

Il browser più amato da chi ci tiene alla libertà personale è Mozilla Firefox. Consente di aggiungere piccoli programmi che aumentano il tasso di sicurezza, a partire da "https everywhere". Per l'uso quotidiano delle comunicazioni elettroniche può essere comodo utilizzare un software per la posta elettronica: Thunderbird è il fratello di Firefox ed è da preferire ai cugini Mac e Microsoft. Sono programmi stabili, gratuiti e semplici da installare, prodotto di una comunità di sviluppatori impegnata sui temi della privacy digitale.

Un manager di password

Una parola chiave per ogni cosa. Ricordarle tutte è impossibile e per questo tendiamo ad usare sempre la stessa password, o al massimo password diverse che però si assomigliano molto. Il problema: trovata una, è un gioco da ragazzi risalire alle altre. Questo fumetto satirico spiega perché finora abbiamo sbagliato tutto: http://xkcd.com/936/ Utilizzate piuttosto un "manager di password" come KeePassX. Sarà lui a generare parole-chiave a prova di bomba per ogni esigenza e a voi rimarrà da ricordare solo una password, quella per attivare il programma.

Un po' di prudenza

Gli smartphone trasmettono dati a getto continuo e possono essere utilizzati come strumenti di sorveglianza. Fate attenzione a quali App installate, alcune sono poco utili e grandi ficcanaso. Non cliccate su link anomali ricevuti via email o messaggeria. Attivate il comando di "localizzazione" solo quando usate il Navigatore. È vero, che WhatsApp è crittata – ma le "chiavi di casa" le tiene il padrone ovvero Facebook. Alternative valide: Telegram, Threema e Signal. L'Electronic Frontier Foundation ne elenca pro e contra: https://www.eff.org/node/82654

Proteggere computer e dati

L'unica garanzia di non perdere i dati, neanche nel caso un virus infetti il computer, è eseguire regolarmente il back-up, la copia di sicurezza del vostro archivio. Va fatto su un hard-disk esterno e dedicato a questa attività. Installate solo programmi che conoscete ed eseguite regolarmente gli aggiornamenti. Ogni sistema operativo contiene un programma per crittare un computer. Si fa con pochi click e garantisce che in caso di furto o smarrimento il suo contenuto sia interessante quanto quello di un tostapane.