



Smartphone sicuro

Per un cellulare a prova di hacker, bisogna inserire pin di accesso e di sblocco tastiera, disattivare la pubblicazione automatica di foto e video sul web, ma anche il posizionamento automatico tramite Gps che consente di seguire i nostri spostamenti. Esistono poi siti per bloccare il cellulare o cancellarne i contenuti



Cronologia e mail

Il sistema di posta Gmail si è reso protagonista del primo arresto per pedopornografia, grazie a un software che individua foto illecite nelle mail dei suoi utenti. Le conversazioni dovrebbero essere al sicuro, ma varie piattaforme di fatto utilizzano già le conversazioni per scopi pubblicitari



Facebook e i social

È possibile modificare il livello di privacy attraverso le impostazioni del proprio account, fino a renderlo invisibile per i motori di ricerca. Non tutti sanno, però, che Facebook è di fatto proprietario di tutto ciò che viene pubblicato dai suoi utenti e può utilizzare foto e scritti a suo piacimento, anche senza interpellare l'utente.

Occhio ai selfie, il web non perdona Gli scudi per difendere i segreti

Evitare password semplici, cautela nelle chat. Memorie da cancellare



■ ROMA

NON C'È porta che non si possa aprire, anche quelle virtuali. In un mondo sempre più connesso, proteggere la nostra vita on line è sempre più difficile. Tutte le maggiori piattaforme di archiviazione dati e di messaggistica, oltre ai social network, utilizzano ormai protocolli di sicurezza complessi e sofisticati. Ma l'anello debole, il tallone d'Achille di questa fortezza virtuale, è proprio in mano all'utente e spesso è rappresentata da un'unica parola: la password. Siamo molto attenti all'affidabilità delle serrature di casa nostra, ma non siamo altrettanto accorti con le parole di accesso ai nostri account. Qualsiasi codice che si rifà alla nostra vita è facilmente individuabile attraverso il *social engineering*, la ricostruzione delle nostre generalità attraverso semplici ricerche o mail fasulle con richieste di dati

apparentemente innocue. È meglio usare combinazioni di lettere e numeri difficili da ricostruire, meglio ancora se non sono di senso compiuto. Gli hacker, infatti, usano spesso una tecnica chiamata *dictionary attack*: un sistema automatizzato mette in atto continui tentativi di inserimento basati su uno o più dizionari.

INUTILE specificare che le password non andrebbero mai salvate sul proprio *smartphone*: in caso di furto sarebbe come regalare al ladro l'intero mazzo di chiavi della nostra vita digitale. Per fortuna esistono siti e applicazioni attraverso i quali è possibile bloccare in remoto l'accesso al cellulare rubato o cancellarne i contenuti: tra questi, CM security, AndroidLost, Wheres my Droid o Lookout. Per l'appunto, lo *smartphone*: molti dei nostri dati e delle nostre foto passa-

no proprio per questo dispositivo, inviati via mail, via messaggio, o caricati su social network e piattaforme on line. Un buon modo per proteggere la propria privacy è innanzitutto verificare le impostazioni del proprio dispositivo, evitando la pubblicazione automatica di foto e contenuti su social o piattaforme come Google Plus o iCloud. È meglio evitare di accedere ai nostri account o inviare informazioni da reti Wifi pubbliche, più a rischio di intercettazione. Per quanto riguarda le chat e le app di messaggistica, dopo recenti attacchi da parte di hacker alcune hanno aggiornato i propri sistemi di protezione, come WhatsApp. Per tutto il resto resta valida la regola aurea: non diffondere con leggerezza ciò che potrebbe danneggiarci. E forse è proprio questa la parte più difficile.

Valeria Melloni



Protezione on line

Tra le più recenti falle ai protocolli di sicurezza dei siti c'è Heartbleed che l'anno scorso ha intaccato il sistema. Molti siti hanno 'tappato' e corretto la falla, ma non tutti. Per fortuna alcune piattaforme hanno messo a punto pagine e programmi in grado di verificare la protezione di un sito semplicemente inserendone l'url. Tra questi. Heartbleedtest di McAfee, Chromebleed Checker per Chrome e ProactiveRisk per Firefox



Messaggi personali

Le chat non offrono il massimo della sicurezza. Basti pensare che i messaggi inviati con WhatsApp fino a pochi mesi fa non erano criptati (ora l'app è stata aggiornata, ma resta sconosciuto l'uso che la società, acquistata da Facebook, farà delle conversazioni salvate). E' comunque più prudente non inviare messaggi o accedere ai propri account da reti Wifi pubbliche, meno protette.