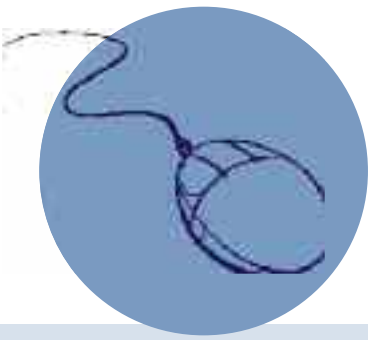


La Borsa *della* Spesa
Edizione 1.14

Doppioclick: Instagram, attenzione a non farsi pedinare

Instagram sta diventando molto popolare fra gli utenti dei social network: permette di condividere fotografie e commentarle in modo semplice, senza tutte le complicazioni e opzioni di Facebook (che è proprietario di Instagram dal 2012). L'apparente semplicità, tuttavia, tende a nascondere il fatto che tutte le foto su Instagram sono geolocalizzate, ossia indicano pubblicamente il luogo nel quale sono state scattate. Siti come Gramfeed.com permettono così di vedere tutte le foto di Instagram realizzate in un luogo oppure di sapere dove è stata scattata ogni foto di un utente.

Questo significa che è facile lasciare tracce che possono essere abusate, per esempio dai molestatori o dai ficcanaso, per sapere dove abita, lavora o va a scuola una persona presa di mira. Per evitare di includere la localizzazione nelle foto di Instagram bisogna disattivare l'opzione Aggiungi alla mappa foto dopo ogni scatto fatto con l'app di questo social network, oppure disattivare preventivamente la geolocalizzazione nel telefonino: negli iPhone, per esempio, si va nelle Impostazioni, si sceglie Privacy e poi Localizzazione, e infine si disattiva la voce "Instagram".

Togliere i dati di localizzazione dalle foto già pubblicate è possibile ma non è intuitivo: occorre andare nella galleria di foto dell'app di Instagram, toccare l'icona della localizzazione, poi l'icona della griglia, poi l'icona delle opzioni, scegliere Modifica e infine toccare le foto alle quali si vuole togliere l'informazione geografica. Toccando Fine e poi Conferma si conclude l'operazione.

Come mai un dato delicato come la propria posizione geografica è attivato automaticamente e difficile da disattivare? Semplice: è un'informazione molto desiderata dai pubblicitari, e i social network, essendo gratuiti, devono mantenersi vendendo questo genere d'informazione.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 2.14

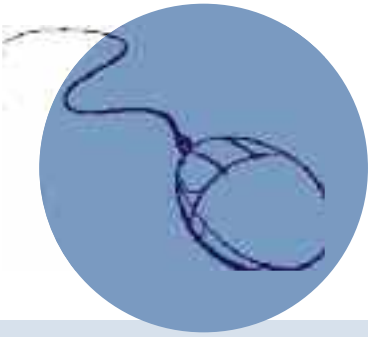
Doppioclick: Smartphone: spegnere il WiFi prolunga la batteria e aumenta la privacy

Se siete utenti degli "smartphone", i telefonini evoluti come Android, iPhone o Windows Phone, avrete notato che la loro batteria dura decisamente meno di quella dei telefoni mobili convenzionali. In parte è colpa delle funzioni WiFi, che cercano costantemente reti alle quali collegarsi per accedere a Internet e ai suoi servizi. Questa ricerca ininterrotta consuma energia anche quando non ha successo perché siamo lontani dalle reti alle quali abbiamo il permesso di collegarci.

Spegnere il WiFi sul telefonino, quindi, allunga la durata della carica della batteria. Dato che la maggior parte dei contratti per smartphone oggi include la trasmissione dati sulla rete cellulare (che è separata da quella WiFi), questo spegnimento non impedisce al telefonino di scambiare dati via Internet gratuitamente. Inoltre le reti WiFi sono spesso utilizzate da ladri di password e da sistemi di monitoraggio delle presenze, per cui tenere disattivato il WiFi è un beneficio anche in termini di sicurezza e privacy.

La soluzione ideale sarebbe accendere il WiFi dello smartphone soltanto dove c'è una rete WiFi sicura che possiamo usare, per esempio a casa o sul posto di lavoro, ma non è facile ricordarsi di spegnere e accendere ogni volta. Per gli smartphone Android ci sono varie app, come Tasker oppure Smart WiFi Toggler, che lo fanno per noi in base a dove siamo e senza dover attivare il GPS, altra funzione che consuma molta energia; per iPhone e Windows Phone, purtroppo, per ora non ci sono app altrettanto servizievoli.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 3.14

Doppioclick:
Il WiFi non fa male alla salute: nuove conferme

C'è una diffusa e crescente apprensione per la presunta nocività del WiFi, il sistema che trasmette via radio i dati delle connessioni a Internet e tra i vari dispositivi digitali: spesso si citano a sproposito parole come "radiazioni" che evocano paure profonde. Ma i fatti parlano chiaro: tutta la rigorosa sperimentazione condotta sull'argomento indica senza alcun dubbio che il WiFi non ha effetti sulla salute. L'importante è rispettare le norme di sicurezza, come per qualunque cosa. Anche l'acqua, se ingerita in eccesso, è tossica.

La conferma più recente arriva dalla Royal Society canadese, incaricata dalle autorità sanitarie di valutare se gli standard vigenti sul WiFi sono adeguati. Il rapporto della Royal Society ribadisce che i limiti di esposizione attuali sono adeguati: persino i livelli massimi ammessi causano soltanto lo stesso effetto termico di un lieve esercizio fisico. Chi teme di trovarsi con il cervello "cotto dalle microonde" del WiFi può, insomma, smettere di preoccuparsi. Il rapporto canadese aggiunge che gli altri effetti sulla salute finora ipotizzati sono privi di qualunque conferma oggettiva e che la cosiddetta "elettrosensibilità" dichiarata da alcune persone non ha alcun nesso concreto con l'esposizione a segnali WiFi ma è dovuta ad altre circostanze.

Se c'è un problema con le emissioni del WiFi, nota la Royal Society, è che le basi scientifiche solide sulle quali si fondano le norme di sicurezza non vengono divulgate adeguatamente. Si potrebbe cominciare ricordando una semplice regola di fisica: l'intensità di qualunque emissione elettromagnetica diminuisce con il quadrato della distanza. In altre parole, se si triplica la distanza dall'antenna del WiFi, l'intensità del segnale diventa nove volte minore. Basta insomma tenere una distanza ragionevole dalle antenne per rientrare nei limiti di sicurezza. Una precauzione che vale anche per i telefonini.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 4.14

Doppioclick:
Aiuto, qualcuno finge di essere me su Facebook!

Su Facebook è molto facile creare un profilo falso copiando le foto e i messaggi di un altro utente e usando il suo stesso nome e cognome. Lo fanno per esempio i criminali informatici, per inviare ai nostri amici richieste di denaro spacciandosi per noi, e lo fanno i molestatori, per tormentare le proprie vittime. Spesso, oltretutto, questi impostori si rendono invisibili alle persone delle quali assumono l'identità: le vittime si accorgono del falso profilo soltanto quando i loro amici glielo segnalano.

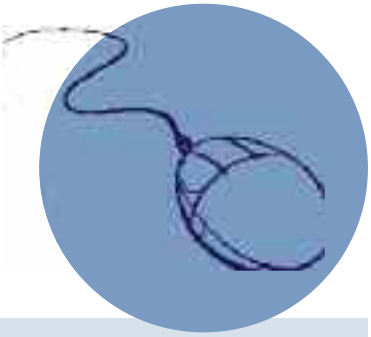
Se usate Facebook e vi accorgete che qualcuno vi sta impersonando, entrate in Facebook usando un computer (non un telefonino o un tablet) e visitate il profilo dell'impostore. Cercate il pulsante "Messaggio" nell'immagine principale del Diario: accanto ad esso c'è un pulsante con tre puntini. Cliccatelo e scegliete "Segnala/blocca", poi "Invia una segnalazione" e "Segnala l'account".

Confermate e poi scegliete "Questo diario finge di essere me o qualcuno che conosco" e poi sull'opzione "Finge di essere me". Cliccate su "Continua" e poi su "Invia una segnalazione".

Se non avete un profilo Facebook o se volete intervenire per conto di un'altra persona (per esempio un figlio), trovate un formulario apposito in italiano presso https://www.facebook.com/help/contact/169486816475808.

In entrambi i casi, il Centro Assistenza di Facebook vi chiederà una scansione completa a colori di un documento d'identità che includa nome completo, foto e data di nascita (vostri o, rispettivamente, della persona che state aiutando). Questo è un dato che l'impostore normalmente non può fornire e consente a Facebook di cancellare il profilo falso. Nel frattempo, comunque, è prudente avvisare del problema i propri amici usando un canale differente da Facebook: per esempio il telefono o un incontro di persona.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 5.14

Doppioclick:
Paura dei sensori d'impronte sui cellulari?

Chi ha uno smartphone porta in giro con sé molti dati personali, come fotografie, indirizzi, numeri di telefono di lavoro e le password delle caselle di mail e dei social network, che vanno protetti contro occhi indiscreti, contro gli amici burloni (immaginate che danni e imbarazzi può fare una foto oscena o un'invettiva pubblicata a vostro nome su Facebook) e contro il furto d'identità.

Di solito la protezione consiste in un codice di sblocco: un PIN oppure un gesto che collega in una sequenza particolare una griglia di punti. Ma questi codici sono scomodi, perché vanno digitati ogni volta che si consulta il telefonino, e sono facili da sbirciare e scavalcare. Per questo gli smartphone di fascia alta di Apple, Samsung e altre marche integrano un lettore d'impronte digitali: una volta impostato, riconosce soltanto le impronte delle dita del proprietario, dando accesso immediato al contenuto dello smartphone senza dover digitare codici. E rubare un'impronta non è facile.

Funziona piuttosto bene, ma molti utenti sono riluttanti ad usarlo e consegnare al telefonino le proprie impronte digitali: temono di essere in qualche modo schedati. In effetti molti esperti storcono il naso, non per il rischio di schedatura (se siamo andati in vacanza negli Stati Uniti, per esempio, abbiamo già affidato ai controlli di frontiera le nostre impronte) ma perché il sensore usa come password un dato non modificabile, che è tecnicamente un controsenso. Oltretutto per scavalcarlo basta per esempio aspettare che il proprietario s'addormenti e appoggiargli delicatamente il dito sul sensore.

In pratica, però, è questione di gradi di sicurezza. Il sensore d'impronte non è perfetto, ma è meno insicuro di un PIN o (peggio ancora) di un telefonino senza codice di blocco. Usato consapevolmente offre una buona protezione in condizioni normali. L'importante è non appisolarsi in pubblico.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 6.14

Doppioclick:
Ingiurie su Facebook, che fare?

I recenti casi di cronaca riguardanti ingiurie pubblicate su Facebook sollecitano un ripasso delle strade disponibili quando si è vittima di questi atti d'inciviltà. La via più diretta è l'uso degli strumenti appositi di Facebook, preferibilmente da un computer e non da un telefonino o un tablet: per esempio, potete bloccare subito l'utente che ha espresso l'ingiuria, così non potrà mandarvi altri messaggi, "taggarvi" o vedere quello che pubblicate sul vostro Diario. Potete anche segnalare l'utente a Facebook, descrivendo le ragioni della segnalazione e chiedendo facoltativamente l'intervento di un amico fidato. Se molti utenti fanno la stessa segnalazione, i gestori di Facebook solitamente prestano più ascolto: chiedete ai vostri amici di aiutarvi segnalando l'utente o il messaggio d'ingiuria.

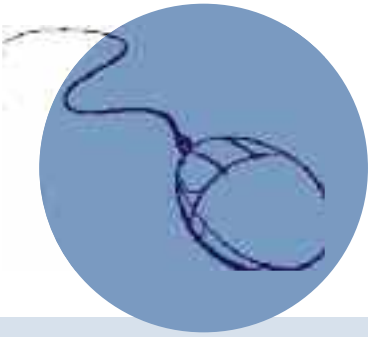
Potete anche inviare una mail, tassativamente in inglese, ad abuse@facebook.com, fornendo i dettagli del caso e in particolare il nome Facebook esatto dell'utente che vi ingiuria. Per ottenere questo nome, che è spesso diverso da quello visualizzato, andate nel profilo dell'utente e guardate il link che compare nella casella dell'indirizzo del vostro browser: per esempio, se compare https://www.facebook.com/mario.bernasconi.3, il nome Facebook dell'utente è mario.bernasconi.3.

Il blocco o la segnalazione, tuttavia, non sempre ottengono la cancellazione da Facebook dell'ingiuria, che può restare visibile agli altri anche se a voi è nascosta. Inoltre, se il messaggio è ingiurioso secondo voi ma rispetta gli standard di Facebook (www.facebook.com/communitystandards), che non sempre sono allineati alle leggi svizzere, non verrà rimosso.

Se preferite le vie legali, è importante documentare tutto, per esempio con fotografie o stampe del messaggio d'ingiuria effettuate in presenza di testimoni, e poi rivolgersi prontamente a un legale. Per le emergenze, la Polizia ha un canale apposito di contatto con Facebook, che vale anche per Instagram (www.facebook.com/records).

Per chi invece pensa di potersi permettere ingiurie perché protetto dall'anonimato di Internet o da uno pseudonimo, va ricordato che ogni messaggio su Facebook è tracciato, anche dopo la cancellazione: pertanto le forze dell'ordine possono risalire all'indirizzo IP e quindi all'identità di chi l'ha pubblicato.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 7.14

Doppioclick:
Aiuto, la polizia mi ha bloccato il telefonino. Ma è una truffa

Un lettore di Doppioclic, Diego, ha segnalato che il suo smartphone (un Windows Phone) è stato bloccato dalla polizia con un avviso perentorio: il dispositivo era stato usato per scaricare contenuti illegali e bisognava pagare una multa.

La polizia sapeva dove Diego si trovava: nell'avviso era indicata con esattezza la sua città insieme ad altri dati personali. I normali comandi per uscire dalla navigazione Web erano in effetti bloccati e quindi non era possibile abbandonare la schermata di avviso se non pagando la multa immettendo i dati della propria carta di credito.

Ma la polizia non c'entra nulla: si tratta di una nuova variante di una truffa già vista sui computer e ora in circolazione in versione per smartphone e tablet. La vittima viene convinta con l'inganno (una mail o un messaggio di Facebook apparentemente proveniente da un amico o un collega) a visitare una pagina-trappola, gestita dai criminali, che prende i dati di geolocalizzazione forniti dal telefonino e li usa per visualizzare una schermata di avviso che varia da paese a paese e in base al tipo di smartphone o tablet. I truffatori contano sulla coscienza sporca delle vittime e sul fatto che lo smartphone sembra davvero bloccato.

In realtà si può rimuovere il blocco abbastanza facilmente: si va nelle impostazioni e si scollega il dispositivo da Internet, disattivando la connessione Wi-Fi e l'eventuale connessione dati cellulare. Poi si toccano i pulsanti per ricaricare la pagina Web: essendo scollegato, il dispositivo non riesce a ricaricarla e mostra una schermata vuota.

A questo punto si va nelle impostazioni dell'app di navigazione e si chiede di cancellare la cronologia e la "cache" (memoria temporanea dei siti visitati). Fatto questo, ci si può ricollegare a Internet senza più problemi.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 8.14

Doppioclick:
A che età esporre un bambino a Internet?

Secondo l'indagine Minori e Internet di Michele Mainardi e Lara Zgraggen (2012), il 90% dei bambini delle scuole elementari ticinesi afferma di usare Internet; alle scuole medie questa percentuale sale al 98% e raggiunge il 99.5% nelle scuole superiori. L'età media del primo utilizzo di Internet è sette anni. il 34% dei bambini delle elementari è scritto a un social network, in violazione della regola che prevede un'età minima di 13 anni: un sintomo chiaro del fatto che l'uso della Rete spesso non è supervisionato da un adulto.

Molti genitori, inoltre, affidano tablet e smartphone ai figli giovanissimi perché pensano di farne degli esperti d'informatica.

In realtà affidare a un bambino molto piccolo un oggetto fragile, costoso e connesso a Internet non farà del figlio un informatico più di quanto farlo giocare in un parcheggio lo farà diventare un bravo automobilista.

Visto che i dispositivi informatici commerciali di oggi sono sempre più sigillati e semplificati, un bambino che li usa finirà per essere semplicemente un bravo cliccatore di icone.

Inoltre Internet è una risorsa preziosa di conoscenza, ma offre anche inganni, trappole e contenuti scioccanti: per questo organizzazioni come Santé Bernoise e Cybersmart.ch propongono alcune regole pratiche per esporre progressivamente a Internet un minore:

– sotto i tre anni d'età, è meglio evitare l'esposizione agli schermi di computer, tablet, smartphone (e proporre invece giochi che sviluppino la manualità)
– da 4 a 10 anni, un periodo di tempo limitato (dapprima 30 minuti al giorno, poi 60) per la navigazione accompagnata da un genitore o da un adulto
– da 11 a 13 anni, 90 minuti giornalieri con sorveglianza (tramite per esempio programmi di monitoraggio o controllo parentale)
– dai 14 anni in su, regole non più imposte, ma concordate, e senza abbandonare le altre attività.

PAOLO ATTIVISSIMO