Utilizzo prudente del vostro smartphone o phablet

Sono sempre di più i possessori di telefoni cellulari multimediali (smartphone) o tablet collegati ad Internet (phablet) in grado di comunicare sulla rete. Questi dispositivi sono dei PC in miniatura e contengono molte informazioni riservate sul proprietarie e sulle persone o istituzioni (banche, Servizio sanitario nazionale, ecc) a cui si collega, informazioni che possono fare gola ai malintenzionati e che è necessario proteggere con cura. Questo articolo, pubblicato su Hardware Upgrade, offre 10 utili consigli per un uso consapevole del proprio smartphone (per i fortunati che lo posseggono).

Smartphone, croce e delizia

Sono passati molti anni dalla prima apparizione sul mercato dei cosiddetti smartphone, di fatto dei telefoni cellulari evoluti che assomigliano davvero molto a PC in miniatura, grazie alla possibilità di connettersi al web e a tutto l'universo di applicazioni disponibili per l'utente, che spaziano praticamente in qualsiasi ambito. Se nei primi tempi questi apparecchi si vedevano nelle mani soprattutto degli appassionati, oggi la situazione è molto diversa, grazie a una vastissima offerta di modelli per qualsiasi tasca.
La grande diffusione di smartphone però non è andata di pari passo con la consapevolezza di avere fra le mani un dispositivo che contiene moltissime informazioni che ci riguardano, che possono dire molto sulle nostre abitudini o peggio ancora essere utilizzate in maniera illecita. Se gli appassionati sono consapevoli dei rischi (anche se a volte li sottovalutano), non sarebbe giusto farne una colpa a chi utilizza regolarmente lo smartphone senza avere particolari conoscenze del web e dei potenziali pericoli ad esso legati: il mondo per molti è cambiato troppo in fretta e lo smartphone viene visto come un vecchio cellulare, che non richiedeva attenzioni particolari.
La maggior parte degli utilizzatori, insomma, ha nozioni scarse o anche nulle dei possibili rischi collegati a un utilizzo superficiale dello smartphone. Il pensiero va a molti utilizzatori over 50 che, pur con eccezioni, si sono trovati letteralmente travolti da un'evoluzione tecnologia senza precedenti: aver passato buona parte della vita senza PC, internet, GPS e via dicendo costringe a un grande sforzo per stare al passo, e non sempre ci si riesce.
Da recenti statistiche comunque il problema non è solo anagrafico, poiché anche fra le nuove generazioni vi sono persone con una conoscenza del mondo tecnologico davvero basilare. Tutti però, praticamente senza eccezioni, possiedono uno smartphone. Eccoci quindi a commentare un recente rapporto di Protect Your Bubble, compagnia assicurativa USA, che stila una classifica delle 10 abitudini più pericolose legate all'utilizzo degli smartphone. Le analizzeremo insieme poiché il tema è interessante e potrebbe metterci al riparo da sgradevoli sorprese in un futuro.
Alcune abitudini riportate possono sembrare allarmistiche, ma non mancano nell'elenco alcune regole colme di buonsenso, che richiedono davvero poco tempo per essere adottate nell'uso quotidiano da parte di tutti.

10 consigli utili sull'uso consapevole del proprio smartphone.

Dove non arriva il buonsenso non sono mai sprecati i consigli e la segnalazione di alcuni problemi più o meno evidenti, che sono in agguato anche per chi utilizza lo smartphone in perfetta buona fede e al meglio delle proprie capacità. Occorre però ricordarsi sempre che lo smartphone è ormai un contenitore di dati personali, ancora più del nostro PC, con la differenza che con lo smartphone si tende ad avere la guardia molto più bassa. In età avanzata mancano normalmente le basi tecnologiche e l'esperienza nell'utilizzo di strumenti molto sofisticati ed in continua evoluzione, con maggiori rischi per l'utilizzatore.

Problema 1: nessuna password. La ricerca evidenzia un dato abbastanza significativo, secondo cui ben il 62% degli utilizzatori non adotta una password per proteggere il proprio dispositivo. Stiamo parlando della password che serve a riabilitare l'utilizzo dello smartphone dopo lo spegnimento del display o lo stato di standby, per intenderci. Quasi 2/3 degli utilizzatori ritiene superfluo adottarla, vuoi per pigrizia, vuoi perché non sa che si può abilitare. Il consiglio è quindi quello di abilitarla, poiché in caso di smarrimento costituisce un prima barriera molto importante per i nostri dati e anche per il nostro portafogli, qualora venga ritrovato da una persona che inizia ad utilizzarlo con il nostro credito.

Problema 2: memorizzazione user e password. Questo è un punto per certi versi critico e su cui non vi è una grande percezione di rischio specie per i meno esperti. Risulta sicuramente comodo, quando navighiamo in generale (PC o smartphone), delegare al browser il compito di memorizzare utenze e password in modo da non doverle riscrivere ogni volta che ci colleghiamo a un sito che richiede autenticazione. Molti però non sanno che è possibile dare consenso a questa pratica solo per alcuni siti, mentre per altri scegliere l'inserimento manuale ad ogni accesso. Il 32% degli utenti sfrutta il completamento automatico dei campi user e password anche per i siti bancari, esponendosi a gravi rischi in caso di smarrimento (e nel caso non vi sia una password all'accesso). Il consiglio è quindi di leggere attentamente ciò che la app che utilizziamo per navigare ci propone, senza dire "sì" ad ogni cosa. Le conseguenze di questa negligenza possono essere davvero spiacevoli anche sul piano personale e più frivolo, qualora qualcuno si divertisse a fare il bello e il cattivo tempo con il nostro account Facebook, Twitter o mail.

Problema 3: foto osé sullo smartphone. Circa il 20% dei teenager USA, ma verosimilmente anche da noi, è solito utilizzare lo smartphone per farsi foto osé da spedire poi ad alcuni contatti. Il 17% di chi riceve questi scatti è solito condividere quando ricevuto con altri, ad insaputa della persona ritratta. In questo caso non vi sono le scusanti per un mondo cambiato troppo in fretta o via dicendo. Il buonsenso dovrebbe essere alla base di un utilizzo proprio e consapevole del dispositivo ma non siamo certo qui a fare del moralismo, quanto a cercare di sensibilizzare sui possibili rischi di diffusione non voluta. Ognuno usi il proprio smartphone come desidera, ma ne tenga presente i rischi. Come si sa, servono anni a farsi una reputazione e cinque minuti per mandare tutto all'aria. Data l'età media dei Soci Apve dovrebbe essere un problema che non li riguarda, ma la senilità a volte fa brutti scherzi.

Problema 4: rispondere a mail false che vogliono truffarci. Sono circa 156 milioni al giorno le email apparentemente mandate da mittenti sicuri, spesso banche o assicurazioni, che invece nascondono una truffa ai nostri danni per farci scrivere dati personali e numeri di carte di credito. Il fenomeno viene chiamato phishing ed è alla base del 4% di tutti i furti di identità. Un numero che sembra piccolo ma che in realtà non lo è. In questo noi italiani siamo più fortunati: per ora mail di questo tipo sono di solito goffe e scritte in un italiano discutibile, spesso senza accenti e quasi sempre destinati alla cartella "spam". Negli USA le cose sono completamente diverse, con modelli e sintassi praticamente perfette. Molto più facile cadere nell'inganno.

Problema 5: postare foto in tempo reale quando siamo in vacanza. Un problema che suona eccessivo e probabilmente lo è, ma ha il suo fondamento. Oltre il 75% di persone condannate per furto ha ammesso di aver tenuto traccia dello spostamento delle proprie vittime anche seguendo i social network. Insomma, molti ladri non solo si appostano per vedere se in casa non c'è nessuno, ma possono comodamente controllare dove si trova una famiglia semplicemente aprendo Facebook. Il tutto dal divano di casa.

Problema 6: postare foto con la geolocalizzazione attivata. Un problema simile al precedente del quale non vi è spesso consapevolezza da parte degli utilizzatori. Praticamente tutti gli smartphone, a prescindere dal sistema operativo, chiedono al momento del primo avvio cosa si vuole fare con la geolocalizzazione, mantenendola attiva salvo caso contrario. Questo significa che se scattiamo una fotografia e la mettiamo su Facebook, apparirà un "nei pressi di ...", senza che magari l'utente ne sia consapevole, poiché quando ha acquistato lo smartphone ne sapeva poco o nulla delle potenzialità. Mettendoci nei panni di chi non sappia minimamente cosa significhi *geolocalizzazione* applicata agli smartphone, appare chiaro che quel *sì* o *no* in fase di configurazione sia una questione simile a un testa o croce.

Problema 7: furto di dati via telefono. In questo caso il problema è generalizzabile e non riferito ai soli utenti di smartphone, ma in virtù dell'utilizzo sempre più massiccio del telefono mobile a svantaggio di quello fisso, la problematica è ricaduta anche in questo settore. Il 27% dei furti di identità e dati importanti avviene per via telefonica, dove fantomatici dipendenti di banche, gentilissimi, chiedono agli utenti conferme di dati e molto altro. Anche in questo caso gli USA sono più soggetti al problema perché là sono pratiche più diffuse, mentre da noi raramente le banche ci chiamano se non per segnalarci uno scoperto sul conto. Anzi, a volte passiamo decine di minuti in attesa per parlare con qualcuno.

Problema 8: non utilizzare una cover protettiva. Il 25% degli utenti non utilizza una cover per il proprio smartphone poiché la ritiene antiestetica. In realtà è stato dimostrato che una cover può garantire un surplus di protezione non trascurabile, oltre a scongiurare in molti casi la rottura dello schermo in caso di caduta accidentale.

Problema 9: accesso disinvolto a reti Wi-Fi non protette. Risulta in ascesa il problema che vede coinvolti molti smartphone a cui sono stati sottratti dati importanti semplicemente perché sono stati connessi a Wi-Fi aperte, posizionate ad hoc da malintenzionati, specie in grossi centri urbani. In questo caso sono gli appassionati le vittime predilette, felici di aver trovato una Wi-Fi aperta dove meno se lo aspettavano. Chi si tiene alla larga dalla tecnologia in senso ampio rischia molto meno in questi casi: non sa nemmeno dove partire per connettersi, nella maggior parte dei casi. Ben il 52% degli utenti non perde occasione di collegarsi a una rete Wi-Fi aperta non appena ne trova una, fidandosi molto più di quanto dovrebbe e talvolta senza che ve ne sia necessità. Il problema suona allarmistico e probabilmente in parte lo è, poiché la quasi totalità degli hot spot gratuiti non costituisce una minaccia. Il problema sta nel "quasi", e il fenomeno è in ascesa.

Problema 10: assenza di assicurazione sul proprio smartphone. Esistono coperture assicurative che garantiscono la sostituzione del display o dell'intero dispositivo in caso di furto, smarrimento o caduta accidentale, il tutto in tempi rapidissimi, oltre ad offrire servizi accessori. Prendiamo questo decimo problema un po' con le pinze, ma ciò non toglie che l'elenco delle potenziali minacce ci abbia guidato in un utilizzo più consapevole del nostro smartphone.