Sicurezza, privacy e smartphone: 5 consigli per proteggersi

Parlare di privacy e di smartphone sembra quasi un ossimoro: è chiaro che per poter utilizzare tutte le funzionalità di un dispositivo avanzato dobbiamo rinunciare ad una parte di essa, dagli spostamenti che facciamo ogni giorno all'attività fisica, dai siti che ci piace consultare spesso ai social network. Questo, però, non significa che dobbiamo arrenderci ad essere spiati 24 ore su 24, in ogni momento del giorno e della notte: la **consapevolezza** di come funziona il nostro amato/odiato dispositivo è **il primo passo da fare per evitare di renderlo ancora più invasivo e, in certi casi, anche pericoloso**. Ecco, quindi, 5 consigli utili per proteggersi dalle minacce più diffuse e per vivere più serenamente, senza necessariamente installare antivirus, antispam e altri tool pesanti sul vostro dispositivo.

Spegnete Wifi, GPS, NFC e Bluetooth se non si utilizzano

Lo so, siamo pigri e addirittura alcuni sistemi operativi oggi decidono per noi quando attivare e disattivare tali funzionalità. Tuttavia dobbiamo abituarci a farlo manualmente, perché in questo modo non solo risparmieremo batteria, ma ci difenderemo da alcuni rischi potenziali, come ad esempio:

- accessi indesiderati da Bluetooth e Wifi (ovviamente se state sfruttando hotspot sicuri e le reti delle vostre **offerte ADSL e fibra di casa**, nessun problema);
- allaccio a reti senza fili realizzate ad hoc per attaccare e/o per appropriarsi di dati personali in modo

illecito;

- furto di denaro attraverso l’NFC (sempre più possibile con la maggior diffusione dei pagamenti contactless);
- localizzazione continua attraverso il GPS (che sia Google o un criminale informatico, **è davvero necessario far sapere a tutti dove siamo in qualsiasi istante della nostra esistenza?**).

Occhio ai social network

Per questo punto sarebbe necessario scrivere un trattato in merito: i social network vivono e guadagnano con la raccolta dati ed è l’utente stesso a fornirli, **più o meno volontariamente** (il recente caso di **Facebook sotto inchiesta penale per la cessione di dati ad altre aziende** dovrebbe fare riflettere). Se, però, non potete fare a meno di Facebook, Twitter, Instagram, etc…, cercate di utilizzarli in modo intelligente, **evitando di condividere informazioni e contenuti particolarmente personali e/o sensibili**.

Ricordate, inoltre, che pubblicare sui social network **non è mai privato**, pur impostando le opzioni privacy in modo restrittivo: **ogni amico o follower può potenzialmente condividere a loro volta i vostri post, le vostre foto e i vostri dati**, sia sullo stesso social network che all’esterno, con screenshot e altri sistemi. Insomma, prima di scrivere o pubblicare qualcosa, fatevi prima la seguente domanda: ne vale davvero la pena?

Occhio alle app

Gli store di Apple e Google vengono controllati regolarmente eppure non mancano casi, anche eclatanti, di app spia e/o particolarmente affamate di dati personali presenti all'interno dei cataloghi ufficiali e scovate in ritardo: **pensate, quindi, cosa potrebbe nascondersi negli store alternativi**. Se da questo lato Apple ha una politica di chiusura abbastanza stringente sulle app esterne (anche se con qualche metodo è possibile aggirare i blocchi), Android è molto più esposto alle app più pericolose.

-

Evitate, quindi, di installare applicazioni sconosciute, provenienti da fonti a rischio, ma dubitate anche quelle app che vi richiedono troppi permessi "strani" al momento dell'installazione. Un esempio: se state installando un'applicazione per la navigazione stradale è chiaro che sarà necessario l'accesso al GPS per poterla utilizzare, ma se state scaricando un'app per gli sfondi del telefonino che vi richiede la localizzazione geografica, beh, passate ad altro.

Evitate di rispondere o richiamare numeri esteri

Se fate un lavoro che implica anche le comunicazioni con l'estero, ovviamente saprete già con quali Paesi sarete in contatto. Tuttavia, se non avete alcun interesse al di fuori dei confini nazionali e vi ritrovate chiamate con prefissi stranieri, evitate di rispondere o di ricontattarli. Spesso, infatti, **potrebbero nascondersi vere e proprie truffe**, che potrebbero scalarvi denaro e aprire la strada ad altri tipi di attacchi. Tra i servizi truffa via telefono più diffusi ultimamente, quelli provenienti da Tunisia ed est europeo

(molto frequenti i seguenti prefissi: **+216, +373 e +383**);

Evitate siti e banner dubbi

Se state navigando su Internet dal vostro smartphone e vi si aprono pagine con annunci di vincite (iPhone, viaggi, pc, etc…), inviti alla compilazione di test o sondaggi mai richiesti, **quasi certamente si tratta spam** o, ancora peggio, un metodo per attaccare il vostro dispositivo e, quindi, i vostri dati. **Evitateli come la peste** e, se sono particolarmente frequenti, utilizzate browser più sicuri e dotati di ad block.

Non cliccate sui link

Che vi arrivino sulla mail, su WhatsApp, su Facebook, su Skype, non ha importanza: prima di cliccare su qualsiasi indirizzo Internet, anche proveniente da una fonte sicura, **chiedete conferma che sia stata quella specifica fonte ad averlo inviato**. Se ciò non è possibile, analizzate attentamente il link che avete ricevuto: è un indirizzo attendibile? Ha un dominio verosimile? Ha senso che il vostro amico, collega o familiare ve lo abbia inviato?

Sembra quasi paranoico doversi preoccupare di controllare qualsiasi link che vi venga spedito, ma sappiate che spesso le minacce peggiori si nascondono su questi innocenti indirizzi. Attraverso link "malevoli" i criminali informatici **possono sfruttare i bug e gli accessi dei sistemi operativi e violarne la sicurezza**, consentendo il furto dati, l'accesso ai file o addirittura prendere il comando a distanza del dispositivo stesso (ad esempio attivando la fotocamera, cancellando o creando dati sulla memoria, etc…). Riuscite ora a percepirne le devastanti potenzialità? Bene, probabilmente il controllo dei link prima di un click ora vi sembrerà meno esagerato.

Ecco, quindi, 5 consigli per proteggervi dalle minacce sul

vostro smartphone: non sono certamente gli unici ma possiamo considerarli certamente tra i più importanti e utili. Perché **il primo antivirus e il primo sistema d’allarme per i nostri dispositivi – è importante tenerlo a mente e averne consapevolezza – siamo noi**.

https://www.key4biz.it/sicurezza-privacy-e-smartphone-5-consigli-per-proteggersi/250792/