SICUREZZA INFORMATICA

SICUREZZA DEI DISPOSITIVI MOBILI

Consigli per la protezione dei dati personali

Ver.1.0, 21 aprile 2015

Pagina lasciata intenzionalmente bianca

I rischi per la sicurezza e la privacy connessi all'uso dei dispositivi mobili

I moderni dispositivi mobili sono sempre più spesso utilizzati come veri e propri computer portatili.

Leggere le Email, accedere ai *social network* e ai servizi di *online banking* sono diventate attività che svolgiamo ormai abitualmente tramite i nostri *smartphone*, nei quali memorizziamo, spesso inconsapevolmente, una grande quantità di informazioni personali, anche sensibili, tra cui ad esempio:

- nomi, indirizzi (Email e fisici) e numeri di telefono di amici e parenti;
- cronologia della navigazione in Internet;
- informazioni sulla propria posizione e sui propri spostamenti;
- SMS, Email e messaggi inviati e ricevuti;
- PIN e password (se memorizzati accidentalmente in chiaro);
- foto e documenti personali o di lavoro, contenenti potenzialmente informazioni riservate, magari sincronizzati tramite servizi Cloud non affidabili;
- dati delle applicazioni, che possono includere credenziali di accesso ad account di servizi online.

Tutte queste informazioni, in caso di smarrimento, furto o compromissione del dispositivo, potrebbero cadere in mano di estranei o criminali informatici con gravi rischi per la sicurezza dei nostri dati, la privacy e spesso anche per il portafoglio. Pensiamo ad esempio ad acquisti che un malintenzionato potrebbe fare a nostro nome usando servizi collegati alla nostra carta prepagata o anche tramite acquisti *in-app*.

Perfino la nostra stessa incolumità e i nostri beni fisici possono essere messi a rischio dalla quantità di informazioni sulle nostre abitudini che tendiamo a condividere online.

Anche le app che spesso installiamo ed utilizziamo con superficialità, solo per provarle, possono presentare potenziali rischi, specialmente se non si pone attenzione alla loro provenienza e alle informazioni a cui consentiamo loro di accedere.

Consigli per la messa in sicurezza del proprio *smartphone*

Di seguito si elencano alcuni semplici suggerimenti su come configurare ed utilizzare in maniera sicura i nostri *smartphone*, in modo da evitare la maggior parte dei rischi.

Le indicazioni fornite non si intendono naturalmente esaustive di tutte le possibili minacce per la sicurezza e la privacy derivanti dall'uso dei dispositivi mobili, ma costituiscono un elenco di buone pratiche volto ad aumentare l'attenzione e la consapevolezza degli utenti nei riguardi tali problematiche.

Le modalità tecniche specifiche per configurare opportunamente le opzioni di sicurezza degli *smartphone* dipendono dalla piattaforma utilizzata e non sono dettagliate in questa guida. Si consiglia di fare riferimento alle istruzioni e agli *help online* forniti dai singoli produttori.

1. Bloccare sempre lo *smartphone* con una password

Questo è uno degli accorgimenti di sicurezza più elementari, ma che è spesso completamente ignorato a favore di tecniche di blocco più semplici, come l'uso di sequenze da tracciare col dito sullo schermo. Attenzione, perché, oltre ad essere questo un metodo intrinsecamente insicuro, le tracce di grasso sullo schermo potrebbero rivelare la sequenza usata molto facilmente.

Usando un PIN di quattro cifre si ottiene già un buon livello di protezione, ma l'ideale è utilizzare una password alfanumerica abbastanza robusta e non facilmente indovinabile.

2. Configurare opportunamente il blocco automatico dello schermo

Dover continuamente sbloccare il telefono può essere considerato da alcune persone molto scomodo, ma un tempo di inattività troppo lungo prima del blocco dello schermo potrebbe risultare eccessivamente rischioso e vanificare il beneficio della password. Si consiglia di impostare tempi non superiori al minuto.

3. Utilizzare la crittografia dei dati

Anche se il vostro *smartphone* è protetto da una password, in caso di furto un *hacker* potrebbe essere in grado, collegando il dispositivo ad un computer, di accedere a tutte le vostre informazioni personali.

L'uso della crittografia sullo *smartphone* può aiutare a prevenire il furto di dati. Per maggiore sicurezza si suggerisce anche di effettuare un backup periodico dei dati.

4. Evitare di scaricare applicazioni da fonti non fidate

Ove possibile, scaricare le app solamente dagli *store* ufficiali come, a puro titolo esemplificativo, il Google Play Store e l'App Store di Apple. In linea di principio, le applicazioni disponibili da questi canali sono maggiormente controllate, anche lato sicurezza. Spesso, quando un'app presenta problemi di sicurezza viene ritirata dallo *store*. Anche le recensioni e i commenti degli utenti posso fornire indizi sulla sicurezza di un'app. In caso di dubbio, meglio non scaricare.

5. Controllare le autorizzazioni richieste dalle applicazioni

Diffidare in generale di app che richiedono l'accesso a funzioni del sistema che non sembrano avere molto a che vedere con gli scopi dell'app stessa.

Se, ad esempio, è normale e ragionevole che un'app di messaggistica richieda l'accesso agli SMS o che un'app che presenta delle mappe voglia rilevare la posizione GPS, non lo è altrettanto se una semplice sveglia richiede di accedere alla rubrica dei contatti. In questo caso, è necessario esercitare estrema cautela e, in caso di dubbio, evitare l'installazione.

6. Tenere il sistema operativo sempre aggiornato

Gli aggiornamenti di sistema spesso includono *patch* di vulnerabilità ed è quindi importante installarli non appena vengono rilasciati.

Può essere conveniente configurare gli aggiornamenti per essere avvisati della loro presenza, piuttosto che installarli automaticamente (in rari casi un aggiornamento può introdurre nuovi problemi, anche solo riguardo la compatibilità di alcune app).

7. Diffidare di qualsiasi link si riceve via Email o SMS

Attacchi di *phishing* non arrivano solo tramite Email, ma possono essere veicolati anche da SMS e messaggi che arrivano su app di messaggistica istantanea, in alcuni casi anche provenienti da contatti conosciuti. In ogni caso, evitare di aprire allegati ad Email o cliccare su link di dubbia provenienza.

8. Non lasciare la connessione Wi-Fi sempre attiva

I moderni *smartphone* hanno la capacità di connettersi automaticamente ad Internet ricercando continuamente reti wireless attive, ma questa funzione potrebbe rivelare informazioni sulla vostra identità e posizione. Inoltre, la connessione automatica a punti di accesso non protetti potrebbe comportare il rischio di consentire l'accesso al telefono e alle nostre attività online da parte di malintenzionati. Molti *hotspot* Wi-Fi pubblici, come quelli che si trovano in luoghi di ristoro, aeroporti e hotel, non cifrano le informazioni che inviamo su Internet e non sono sicuri.

Per ridurre al minimo i rischi, si suggerisce di far dimenticare allo *smartphone* le reti wireless non più utilizzate e di attivare/disattivare manualmente il Wi-Fi solo in determinati luoghi (ad esempio a casa) oppure sfruttando le funzioni di apposite app.

Se si ha la necessità di collegarsi ad un *hotspot* pubblico, evitare di visitare siti non protetti da una connessione sicura HTTPS e, soprattutto, di effettuare operazioni bancarie o altre attività ad alto rischio.

9. Spegnere Bluetooth e NFC quando non in uso

Bluetooth e NFC (*Near Field Communication*) possono essere utili in termini di connettività, consentendo di utilizzare accessori come auricolari e tastiere wireless o effettuare pagamenti *contactless*.

Anche questi servizi potrebbero essere sfruttati per accessi illeciti al dispositivo, per cui si raccomanda di tenerli spenti e attivarli solo quando serve o mettere il dispositivo in modalità "non rilevabile", ove possibile. Inoltre, fare molta attenzione quando si associa il proprio *smartphone* ad altri dispositivi e non accettare mai richieste da dispositivi sconosciuti.

10. Installare un software di sicurezza

Come già evidenziato, lo *smartphone* non è poi così dissimile da un computer ed esistono virus, trojan e altri tipi di *malware* anche per le piattaforme mobili più diffuse.

Per questo motivo si consiglia di installare un software antivirus (ce ne sono molti di provata efficacia e anche gratuiti). Spesso queste app forniscono utili servizi aggiuntivi, quali ad esempio la rilevazione di app con problemi per la privacy, la localizzazione e il blocco (o la cancellazione) da remoto del telefono.