Il Federal Bureau of Investigation, a fronte della forte crescita degli attacchi informatici ai danni dei dispositivi mobili, ha lanciato una specie di allerta. Il documento dell'Fbi parla di due nuovi virus, Loozfon e FinFisher, entrambi mirati alla piattaforma Android. Ma le raccomandazioni pubblicate dall'agenzia federale (che qui sotto abbiamo riassunto e commentato in corsivo) interessano in buona parte anche i possessori di iPhone.

Proteggete il dispositivo mobile con una password: è il primo passaggio per la sicurezza. Poi, attivate la funzione che blocca lo schermo dopo qualche minuto di inattività.

A seconda del modello, il sistema operativo potrebbe avere la possibilità di criptare i dati: in caso di furto o di smarrimento, può aiutare a proteggere i contenuti del telefono.

Fate attenzione alla geo-localizzazione: alcune applicazioni tracciano gli spostamenti del telefono. Autorizzate solo quelle che vi servono veramente.

Leggere le recensioni sulle applicazioni che volete scaricare e sui loro sviluppatori.

Questo consiglio riguarda soprattutto i possessori di telefoni Android, visto che il mercato digitale delle app per iOS è rigidamente controllato e verificato da Apple.

Evitate il jailbreaking o il rooting. Questa procedura, usata dagli utenti per prendere il controllo totale dell'apparecchio, sfrutta comunque le vulnerabilità dei sistemi operativi e accresce considerevolmente le possibilità di un attacco.

Questo invece riguarda anche gli utenti iPhone e iPad che con il jailbreaking (usato per poter installare app non autorizzate da Apple) aprono le porte a problemi di sicurezza che prima non avevano. Nel mondo Android l'analoga operazione si chiama rooting.

Non collegatevi a network sconosciuti: potrebbero essere punti di accesso che catturano le informazioni trasmesse mentre siete collegati a un qualsiasi server.

Quando una rete wifi si chiama «Free Wifi», state alla larga: potrebbe essere un modo per attirarvi a collegarsi. In ogni caso, mai fare un'operazione bancaria tramite un network che non si conosce.

Aggiornate il sistema operativo: dimenticarsene vuol dire esporsi al rischio di attacchi.

Gli aggiornamenti includono i patch (letteralmente: le toppe) alle vulnerabilità che vengono via via scoperte nei sistemi operativi.

Acquistate software per la protezione dal malware: cercate antivirus che aiutino a proteggere il sistema dal malware.

Se vendete il telefono, prima cancellate tutto: riportando l'apparecchio alle condizioni di fabbrica (factory default) si evita di lasciare in giro i dati personali.

In realtà, non è così semplice. Anche il factory reset, lascia dietro di sé dati che mani esperte possono recuperare. Se il telefono contiene una memory card estraibile (l'iPhone non ce l'ha) toglietela.

Evitate di cliccare link di origine sconosciuta o di scaricare software da fonti ignote o poco chiare.

Un sistema di attacco molto usato (che in questo caso interessa anche gli iPhone) è un Sms, o un avviso di sistema, che chiede di approvare il download o l'installazione di qualcosa: meglio stare alla larga.

Usate le stesse precauzioni che usate con il Pc anche con gli apparecchi mobili.

In realtà, sarebbe meglio usarne di più.