

Quanto è sicuro il tuo dispositivo mobile?

Quasi tutti ormai possiedono uno smartphone, ma quanti di noi prendono sul serio le minacce alla sicurezza di questi dispositivi mobili? I dispositivi mobili sono vulnerabili a diversi tipi di minacce. Gli attacchi contro i dispositivi mobili sono in aumento e i truffatori li prendono di mira utilizzando applicazioni dannose. Tramite questi metodi sono in grado rubare informazioni personali e aziendali senza che l'utente se ne renda minimamente conto.

Anche se hai scaricato un'applicazione di sicurezza o un antivirus, la sicurezza del tuo smartphone va oltre ciò che può essere garantito da questi servizi. Migliorare le prassi di sicurezza sui dispositivi mobili è la tua migliore difesa contro gli attacchi alla privacy e alla sicurezza del tuo dispositivo mobile.

Cosa fare per migliorare le prassi di sicurezza sui dispositivi mobili?

Per ridurre al minimo il rischio di exploit sui dispositivi mobili, applica sempre queste buone prassi:

1. **Assicurati che il sistema operativo del tuo telefono sia sempre aggiornato.** I sistemi operativi vengono spesso aggiornati per risolvere i problemi di sicurezza. Molte minacce sono causate da falle nella sicurezza non risolte dovute al mancato aggiornamento del sistema operativo.
2. **Fai attenzione alle app dannose presenti negli app store.** Gli app store ufficiali rimuovono regolarmente le applicazioni contenenti malware, ma a volte alcune app malevole sfuggono ai controlli e possono essere scaricate da utenti ignari. Fai delle ricerche, leggi le recensioni e presta attenzione al numero di download. Non scaricare mai applicazioni da fonti diverse dagli app store ufficiali.
3. **Verifica che le applicazioni non chiedano l'accesso a elementi del tuo telefono non rilevanti per le loro finalità.** Solitamente le applicazioni chiedono un elenco di autorizzazioni per file, cartelle, altre applicazioni e dati prima di essere scaricate. Non concedere queste autorizzazioni alla leggera. Se le richieste di autorizzazione non sembrano necessarie, cerca un'applicazione alternativa all'interno dell'app store.
4. **Assenza di password o password debole.** Molte persone non usano una password per bloccare il telefono. Se il dispositivo viene smarrito o rubato, i ladri avranno facile accesso a tutte le informazioni contenute nel telefono.
5. **Fai attenzione al Wi-Fi pubblico.** I truffatori utilizzano tecnologie che permettono loro di vedere cosa stai facendo. Evita di accedere ai servizi online o di eseguire transazioni sensibili (come quelle bancarie) tramite il Wi-Fi pubblico.



Il team di sicurezza KnowBe4