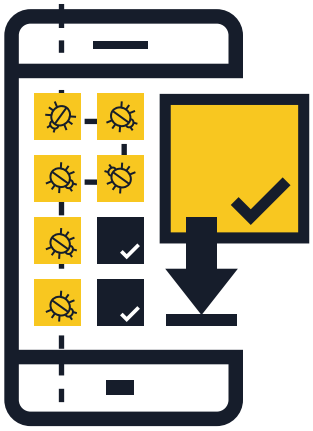
MALWARE MOBILE

SUGGERIMENTI E CONSIGLI PER PROTEGGERSI



1 Installate applicazioni provenienti solo da fonti attendibili

- **Acquistate le vostre app solo da store affidabili** — Prima di scaricare un'app, fate una ricerca sia sull'app che sugli autori. Siate cauti con i link che ricevete per e-mail e fate attenzione ai messaggi di testo che potrebbero indurvi a installare app di terze parti o fonti sconosciute.
- **Date un'occhiata alle recensioni di altri utenti,** se disponibili.
- **Verificate le autorizzazioni di un'app** — Controllate a quali tipologie di dati può accedere l'app e se può condividere i vostri dati con parti esterne. Se avete dei sospetti o non vi fidate delle condizioni, non scaricate l'app.

2 Non fate clic sui link o sugli allegati contenuti in e-mail o messaggi di testo non richiesti

- **Non fidatevi dei link contenuti in e-mail o messaggi di testo non richiesti** (SMS e MMS). Eliminateli non appena li ricevete.
- **Fate un controllo incrociato degli URL abbreviati e dei codici QR** in quanto potrebbero condurre a siti dannosi o scaricare direttamente del malware sul vostro dispositivo. Prima di fare clic, cercate di visualizzare l'anteprima dell'URL per verificare che l'indirizzo web sia affidabile. Prima di effettuare la scansione di un codice QR, selezionate un lettore di codici QR in grado di visualizzare l'anteprima dell'indirizzo web a cui fa riferimento e utilizzate un software per la sicurezza mobile in grado di segnalare la presenza di link rischiosi.

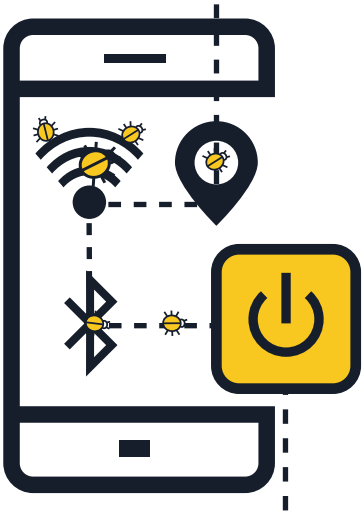
3 Disconnettetevi da un sito dopo aver effettuato un pagamento

- **Non salvate mai username e password nel browser o nelle app del vostro dispositivo mobile** — In caso di smarrimento o furto del vostro telefono o tablet, chiunque potrebbe accedere ai vostri account. Una volta completata una transazione, disconnettetevi dal sito invece di chiudere semplicemente il browser.
- **Non effettuate operazioni bancarie o acquisti online utilizzando connessioni Wi-Fi pubbliche** — Effettuate operazioni bancarie e acquisti online utilizzando esclusivamente reti note e attendibili.
- **Fate un controllo incrociato dell'URL del sito** — Assicuratevi che l'indirizzo web sia corretto prima di effettuare l'accesso o inviare dati sensibili. Valutate la possibilità di scaricare l'app ufficiale della vostra banca per essere certi di collegarvi sempre al sito autentico.

4 Tenete sempre aggiornati il vostro sistema operativo e le app

- **Scaricate gli aggiornamenti per il sistema operativo del vostro dispositivo mobile non appena vi viene chiesto** — Installando gli ultimi aggiornamenti, il dispositivo non solo è più sicuro ma garantisce anche prestazioni migliori.

5 Disattivate il Wi-Fi, i servizi di localizzazione e il Bluetooth se non li usate



- **Disattivate il Wi-Fi se non lo utilizzate** — I cybercriminali possono accedere ai vostri dati se la connessione non è protetta. Se possibile, utilizzate una connessione dati 3G o 4G anziché un hotspot. Potete anche optare per un servizio di rete privata virtuale (VPN) per mantenere i dati in transito crittografati.
- **Non consentite alle app di utilizzare i servizi di localizzazione, a meno che non sia indispensabile** — Queste informazioni possono essere condivise o trapelare ed essere utilizzate per l'invio di annunci basati sulla località in cui vi trovate.
- **Disattivate il Bluetooth quando non lo utilizzate** — Assicuratevi che sia completamente disattivato e non solo in modalità invisibile. Le impostazioni predefinite sono spesso preimpostate per consentire ad altri di connettersi al dispositivo a vostra insaputa. Eventuali utenti malintenzionati potrebbero potenzialmente copiare i vostri file, accedere ad altri dispositivi collegati o addirittura accedere in remoto al vostro telefono per effettuare chiamate e inviare messaggi di testo e far lievitare i costi della vostra bolletta.

6 Evitate di fornire i vostri dati personali

- **Non rispondete mai fornendo i vostri dati personali** a messaggi di testo o e-mail che apparentemente sono stati inviati dalla vostra banca o un da un'altra azienda affidabile. Cercate invece di contattare direttamente l'azienda in questione per verificare che la loro richiesta sia autentica.
- **Controllate periodicamente il dettaglio del vostro traffico mobile per verificare la presenza di eventuali spese sospette** — Se doveste individuare spese che ritenete di non aver mai effettuato, contattate immediatamente il vostro gestore telefonico.

7 Non effettuate il jailbreak del vostro dispositivo

- Il jailbreak consiste nella rimozione delle limitazioni di sicurezza imposte dal fornitore del sistema operativo per acquisire l'accesso completo al sistema operativo stesso e alle sue caratteristiche. **Effettuando il jailbreak del vostro dispositivo, la sua sicurezza può essere compromessa in modo significativo** e aprire falle a livello di sicurezza che potrebbero non risultare subito evidenti.

8 Effettuate il backup dei vostri dati

- **Molti smartphone e tablet sono in grado di effettuare il backup dei dati in modalità wireless** — Verificate le opzioni esistenti a seconda del sistema operativo del vostro dispositivo. Effettuando il backup del vostro smartphone o tablet potrete ripristinare facilmente i vostri dati personali in caso di smarrimento, furto o danneggiamento del dispositivo

9 Installate un'app per la sicurezza mobile

- Tutti i sistemi operativi sono a rischio di infezione. Se possibile, **utilizzate una soluzione di sicurezza mobile** in grado di rilevare e proteggere dal malware, dallo spyware e da applicazioni dannose, oltre ad offrire altre funzionalità a tutela della privacy e antifurto.