APPS

SOLO UN GIOCO?

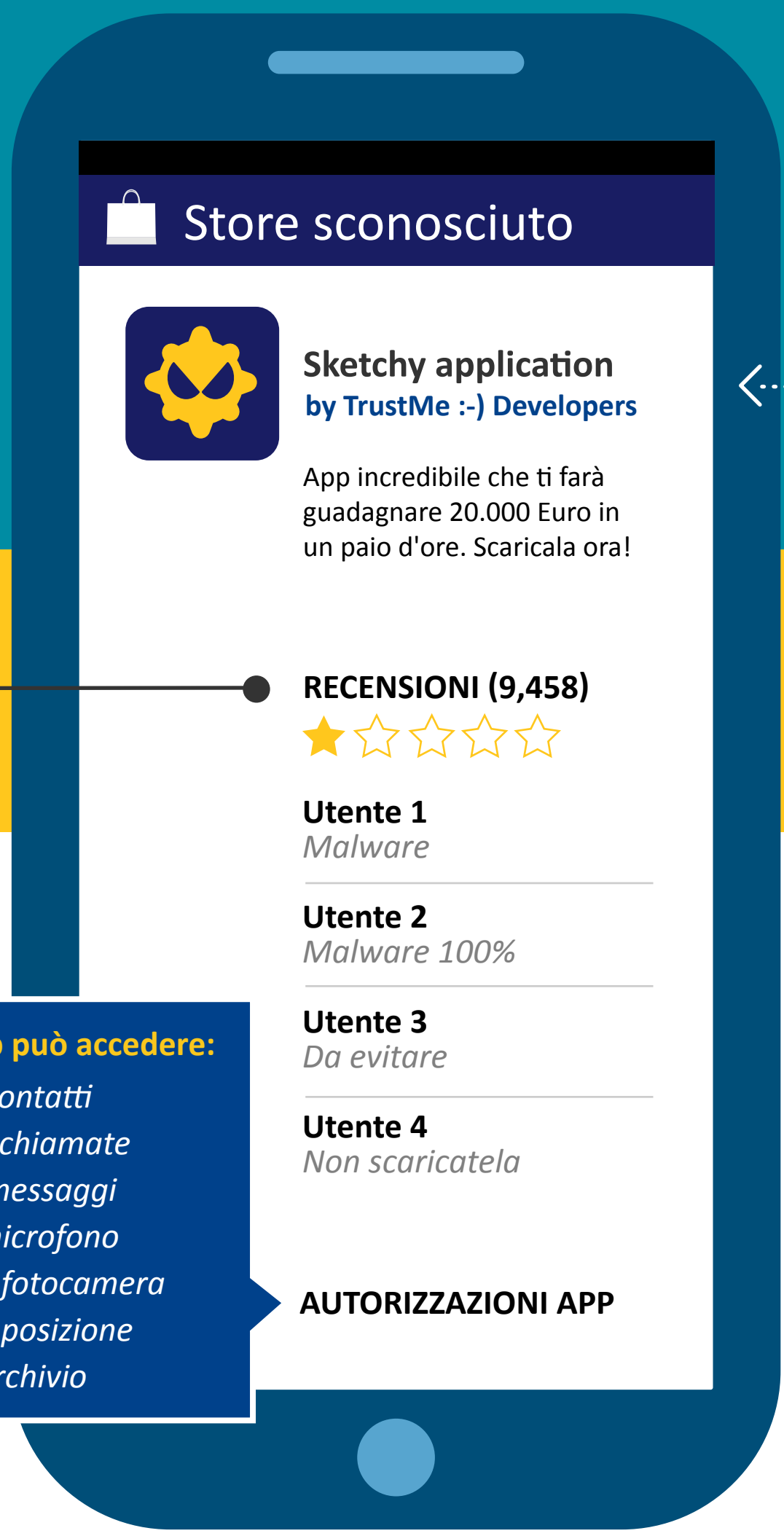
Installate solo applicazioni provenienti da app store ufficiali

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 ad installare app di terze parti o fonti sconosciute.

DATE UN'OCCHIATA ALLE RECENSIONI DI ALTRI UTENTI

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. Un'app ha proprio bisogno di tutte quelle autorizzazioni? Nel dubbio, non scaricate.



INSTALLATE UN'APP PER LA SICUREZZA MOBILE

Questa esaminerà tutte le app presenti sul vostro dispositivo e ogni app nuova che installerete successivamente avvisandovi nel caso in cui dovesse essere rilevato un software dannoso.

EUROPOL EC3 European Cybercrime Centre

Polizia di Stato

#MobileMalware

MALWARE CHE COLPISCE L'INTERNET BANKING SUI DISPOSITIVI MOBILI

UN MALWARE PUÒ COSTARVI CARO

Un malware che colpisce l'internet banking è appositamente studiato per rubare i dati finanziari eventualmente memorizzati su un dispositivo mobile.

COME SI DIFFONDE?

Visitando siti dannosi

Scaricando app dannose

Tramite phishing

QUALI SONO I RISCHI?

Furto dei dati di autenticazione personale

Prelievi non autorizzati

COSA POTETE FARE PER PROTEGGERVI?

https://

Scaricate l'app mobile ufficiale della vostra banca e assicuratevi ogni volta di visitare il sito autentico della vostra banca.

Evitate di connettervi automaticamente al vostro sito o alla vostra app di internet banking.

Non condividete con né rivelate a nessuno il vostro numero di carta di credito o la vostra password.

Se possibile, installate un'app di mobile security in grado di segnalare eventuali attività sospette.

Se perdete il vostro telefono cellulare o cambiate il vostro numero, contattate la vostra banca per fare aggiornare i vostri dati personali.

Non condividete alcun dato relativo al vostro account tramite messaggi di testo o e-mail.

Utilizzate sempre una rete Wi-Fi protetta per connettervi al sito mobile o all'app della vostra banca. Non fatelo mai utilizzando una rete Wi-Fi pubblica!

Controllate frequentemente i vostri estratti conto.

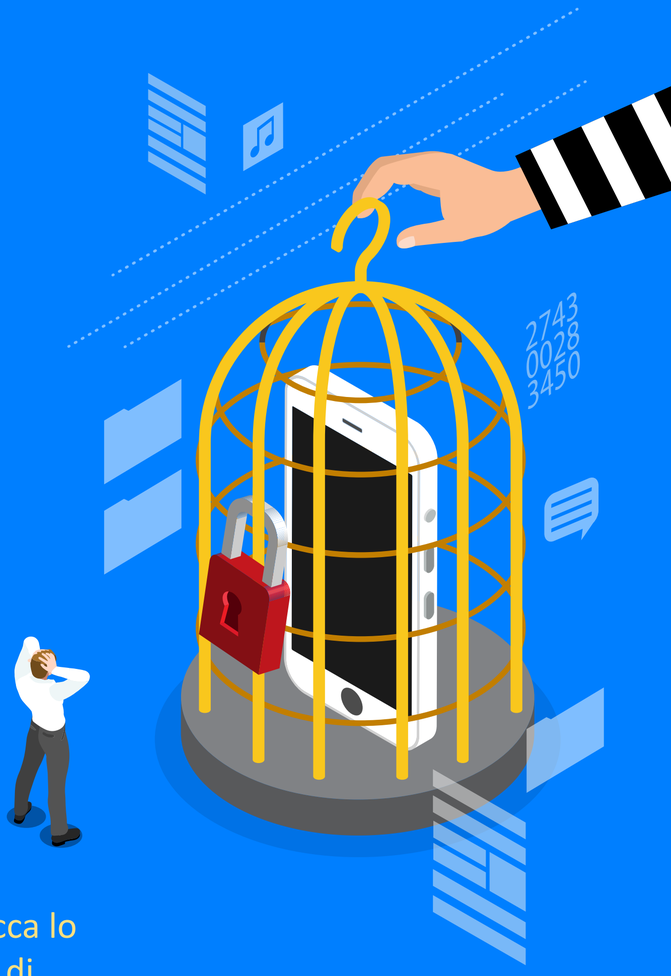
EUROPOL EC3 European Cybercrime Centre

Polizia di Stato

#MobileMalware

RANSOMWARE
MOBILE

DITE ADDIO AI VOSTRI FILE PERSONALI



Il ransomware è un tipo di malware in grado di tenere in ostaggio un dispositivo mobile ed i dati in esso contenuti fino al pagamento di un riscatto. Questo tipo di malware blocca lo schermo del dispositivo o impedisce di accedere ad alcuni dei file e delle sue funzioni.

COME SI DIFFONDE?

Visitando siti compromessi.

Scaricando versioni falsificate di app normali.

Facendo clic su link malevoli e allegati alle e-mail di phishing.

QUALI SONO I RISCHI?

Potrebbe rendersi necessario il ripristino alle impostazioni di fabbrica del dispositivo con conseguente perdita di tutti i dati.

Un utente malintenzionato può avere accesso completo al vostro dispositivo e condividere i vostri dati con soggetti terzi.

COSA POTETE FARE PER PROTEGGERVI?

Effettuate un backup frequente dei vostri dati e aggiornate regolarmente tutte le vostre app e il sistema operativo.

Evitate di acquistare app presso app store di terze parti.

Se possibile, installate un'app di mobile security in grado di segnalare se il dispositivo è stato compromesso.

Diffidate di e-mail e siti sospetti o che sembrano troppo belli per essere veri.

Non concedete a nessuno i diritti di amministratore del dispositivo.

Non pagate alcun riscatto. Se lo fate, finanzierete dei criminali incoraggiandoli a continuare le loro attività illegali.

EUROPOL EC3 European Cybercrime Centre

Polizia di Stato

#MobileMalware

MINACCE VIA INTERNET

VALUTATE BENE PRIMA DI FARE CLIC

Se il vostro dispositivo smette di funzionare, potreste perdere il vostro denaro e i vostri dati personali oltre ai dati memorizzati. Non fatevi raggirare!

COME PUÒ SUCCEDERE?

ATTACCHI DI PHISHING: gli utenti vengono ingannati e convinti a fornire i propri dati presentandosi come un'entità affidabile. Si diffondono tramite e-mail, messaggi di testo o piattaforme di social network.

ESPLORAZIONE DI SITI: il vostro dispositivo mobile potrebbe infettarsi semplicemente visitando un sito non sicuro.

DOWNLOAD DI FILE: un'e-mail può contenere link e allegati dannosi.

PERCHÉ È EFFICACE?

I dispositivi mobili sono COSTANTEMENTE CONNESSI a Internet.

Le DIMENSIONI RIDOTTE DELLO SCHERMO DI UN DISPOSITIVO MOBILE rappresentano un limite generale. I browser dei dispositivi mobili visualizzano gli URL su uno schermo dallo spazio limitato, pertanto è difficile vedere se un determinato dominio è autentico.

L'UTENTE NUTRE UNA FIDUCIA IMPLICITA nella natura personale di un dispositivo mobile.

COSA POTETE FARE PER PROTEGGERVI?

Siate sospettosi se ricevete un SMS o una telefonata da un'azienda che vi chiede di fornire i vostri dati personali. Potete verificare l'autenticità della chiamata o del messaggio ricevuto richiamando direttamente l'azienda al loro numero.

Quando navigate su Internet con il vostro dispositivo mobile, assicuratevi che la connessione sia protetta tramite HTTPS. Potete sempre controllare la parte iniziale dell'URL.

Non fate mai clic su un link o un allegato contenuto in un'e-mail o un SMS indesiderato. Eliminatelo immediatamente.

^BE:%}
W@RY
*)Z#$=

Diffidate dei siti dalla grammatica povera, con errori ortografici o a bassa risoluzione.

Se possibile, installate un'app di mobile security in grado di segnalare eventuali attività sospette.

EUROPOL EC3 European Cybercrime Centre

Polizia di Stato

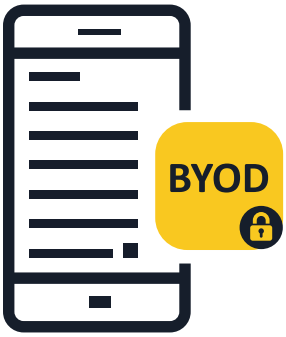
#MobileMalware

MALWARE NEI DISPOSITIVI MOBILI

SUGGERIMENTI E CONSIGLI PER LE AZIENDE

1 Informate il vostro personale sui rischi esistenti in mobilità

- Quando si lavora da remoto, i confini tra uso aziendale e uso personale diventano poco chiari. In caso di attacco inizialmente diretto al dispositivo mobile di un individuo, le conseguenze per un'impresa possono essere catastrofiche. Un dispositivo mobile è un computer e come tale deve essere protetto.



2 Attuate una politica aziendale di tipo "bring your own device" (BYOD)

- I dipendenti che utilizzano i propri dispositivi mobili per accedere ai dati ed ai sistemi aziendali (anche se solo e-mail, calendari o database di contatti) devono attenersi alle politiche aziendali. Selezionate attentamente quali tecnologie devono essere utilizzate per gestire e proteggere i dispositivi mobili ed esortate il vostro personale ad agire con cautela.

3 Cercate di includere politiche di protezione mobile nel vostro piano di sicurezza globale

- Se un dispositivo non è conforme alle politiche di sicurezza aziendale, non dovrebbe essere autorizzato a connettersi alla rete aziendale e ad accedere ai dati aziendali. Tutte le aziende dovrebbero implementare soluzioni di Mobile Device Management (MDM) o Enterprise Mobility Management (EMM).
- A completamento di queste soluzioni, è fondamentale installare una soluzione di Mobile Threat Defence. Ciò consentirà di avere una maggiore visibilità e consapevolezza contestuale delle minacce a livello di app, rete e sistema operativo.

4 Diffidate delle reti Wi-Fi pubbliche per accedere ai dati aziendali

- In generale, le reti Wi-Fi pubbliche non sono sicure. Se un dipendente accede ai dati aziendali utilizzando una connessione Wi-Fi gratuita presso un aeroporto o un locale pubblico, i dati potrebbero essere esposti a utenti malintenzionati. È consigliabile che le aziende sviluppino politiche per un "utilizzo efficace" in questo senso.

5 Tenete sempre aggiornati i sistemi operativi e le app dei dispositivi

- Raccomandate al vostro personale di scaricare gli aggiornamenti software per il sistema operativo dei loro dispositivi mobili non appena viene loro richiesto. Soprattutto per Android, cercate di acquisire informazioni sui gestori di telefonia mobile e i produttori di cellulari per conoscere la loro politica relativa agli aggiornamenti. Installando gli ultimi aggiornamenti, un dispositivo non solo è più sicuro ma ha prestazioni migliori.

6 Installate applicazioni provenienti solo da fonti attendibili

- Le aziende dovrebbero autorizzare esclusivamente l'installazione di app provenienti da fonti ufficiali sui dispositivi mobili che si connettono alla rete aziendale. In alternativa, vi consigliamo di valutare l'introduzione di uno store aziendale di app attraverso il quale gli utenti finali possono accedere, scaricare e installare app approvate dall'azienda. Consultate il vostro fornitore di soluzioni per la sicurezza per avere dei consigli per la configurazione o l'allestimento di uno store interno.

7 Impedite il jailbreak dei dispositivi

- 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. I dispositivi di tipo "root-enabled" non dovrebbero essere autorizzati ad accedere all'ambiente aziendale.

8 Valutate alternative per l'archiviazione cloud

- I dipendenti in remoto desiderano spesso accedere a documenti importanti non solo tramite il PC che usano al lavoro ma anche dal loro telefono o tablet privato al di fuori dell'ufficio. Le aziende dovrebbero valutare l'allestimento di una soluzione di archiviazione sicura basata sul cloud e l'introduzione di servizi di sincronizzazione di file per soddisfare queste esigenze in modo sicuro.

9 Incoraggiate il vostro personale a installare un'app per la sicurezza mobile

- Tutti i sistemi operativi sono a rischio di infezione. Se possibile, verificate che i vostri dipendenti utilizzino una soluzione per la sicurezza mobile in grado di rilevare e proteggere da malware, spyware e applicazioni dannose, oltre ad offrire altre funzionalità a tutela della privacy e antifurto.

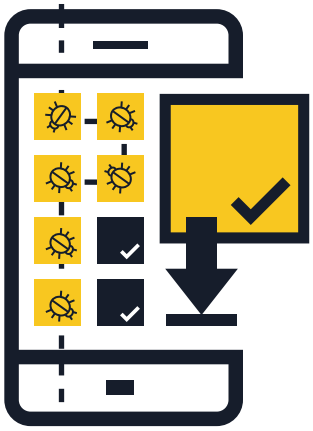
EUROPOL EC3 European Cybercrime Centre

Polizia di Stato

#MobileMalware

MALWARE NEI DISPOSITIVI MOBILI

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 un 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.

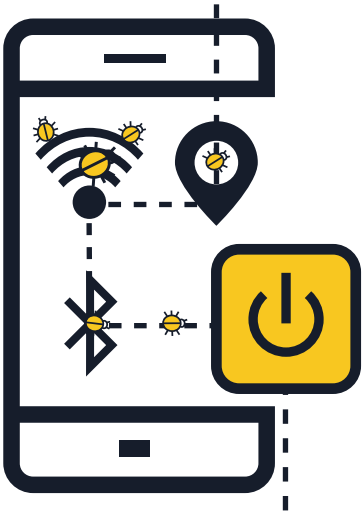
3 Disconnettetevi da un sito dopo aver effettuato un pagamento

- **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.

EUROPOL EC3 European Cybercrime Centre

Polizia di Stato

#MobileMalware