

Cyber Security Brochure

Utilizzo sicuro dei dispositivi mobili

Nuove sfide:
connettività e sicurezza
dei dispositivi mobili



Sommario

Cosa troverai in questa brochure

01

Introduzione

Perché è fondamentale proteggere i dispositivi mobili?

02

Quali sono i rischi?

Riconoscerli e adottare misure di difesa

03

Come difendersi?

Buone pratiche per la protezione dei dispositivi mobili

04

Security Trend

Casi di attacchi reali contro i dispositivi mobili

Introduzione

Smartphone e tablet custodiscono una quantità sempre maggiore di informazioni personali e professionali, consentendo di accedere rapidamente a numerosi servizi digitali. Dalla comunicazione alla gestione delle attività quotidiane, fino all'utilizzo di applicazioni e piattaforme online, questi dispositivi **rivestono un ruolo** sempre più **centrale nella vita di tutti i giorni**.

La **continua evoluzione delle funzionalità**, la **connessione costante alla rete** e la **crescente integrazione con i servizi digitali** offrono importanti opportunità, ma richiedono al tempo stesso una maggiore attenzione alla protezione dei dati e alla sicurezza delle informazioni.

Promuovere un utilizzo sicuro dei dispositivi mobili significa valorizzarne i benefici, sviluppando al contempo una maggiore consapevolezza delle buone pratiche da adottare nell'ambiente digitale. L'adozione di **comportamenti responsabili** contribuisce infatti a **ridurre i rischi** connessi alle minacce informatiche, **tutelare la privacy** e **proteggere dati e dispositivi** utilizzati quotidianamente.

Mobile Threats 2025

+116%

Aumento degli indirizzi IP univoci coinvolti in infezioni informatiche

+29%

Aumento degli attacchi informatici su smartphone

Le fasi di un attacco ai dispositivi mobili:



Diffusione del contenuto malevolo

Link malevoli, allegati dannosi o app infette possono essere distribuiti tramite SMS, email, social network o store non ufficiali.

Interazione e installazione da parte dell'utente

L'utente clicca su un link malevolo o installa un'applicazione infetta, innescando il processo di compromissione del dispositivo.



Esecuzione nascosta del malware

Una volta installato, il software malevolo opera in background, raccogliendo dati e comunicando con l'esterno.

Sfruttamento del dispositivo compromesso

Le informazioni vengono rubate o il dispositivo viene usato per frodi e altri attacchi.



Fonte: Kaspersky, Mobile Threat Landscape 2025 (H1 2025); Rapporto Clusit - Operational Summary - 2026

Quali sono i rischi?

Rischi

01 Compromissione

I malware possono **compromettere il corretto funzionamento del dispositivo mobile**, consentire l'accesso non autorizzato a contenuti personali e alle attività dell'utente, nonché esporre il dispositivo e la rete aziendale o personale a **minacce e attacchi informatici** più complessi.

02 Violazione dei dati

Attraverso tecniche di manipolazione psicologica (c.d. *social engineering*) o autorizzazioni concesse dall'utente con leggerezza, i criminali possono **ottenere informazioni sensibili** quali credenziali, dati bancari, messaggi privati, foto, video e audio.

03 Perdite finanziarie

Una volta **ottenuto l'accesso** al dispositivo o ai dati, i criminali possono effettuare **transazioni** non autorizzate, **attivare servizi a pagamento** o **sottrarre fondi** tramite app bancarie e metodi di pagamento salvati, con conseguenze rilevanti dal punto di vista economico.

Contromisure

Installa app solo da **store ufficiali**, mantieni il **sistema operativo** e le **app** sempre **aggiornate**, evita link o allegati sospetti e **limita le autorizzazioni concesse**.

Usa **password complesse**, attiva l'**autenticazione a più fattori**, **blocca lo schermo** dei tuoi dispositivi quando non li utilizzi e utilizza **backup crittografati**.

Evita di salvare metodi di pagamento su dispositivi poco protetti, **attiva notifiche** in tempo reale e **monitora** costantemente i **movimenti sulle app bancarie**

Come difendersi?

*Mantieni il dispositivo
protetto e aggiornato*

Mantieni sempre **aggiornati** il **sistema operativo** e le **applicazioni** installate, abilitando, ove possibile, gli aggiornamenti automatici. Le nuove versioni **correggono vulnerabilità** note, migliorano le funzionalità di sicurezza e **riducono il rischio** che il **dispositivo** venga **compromesso** da malware o altre minacce informatiche.

Proteggi accessi e dati

Utilizza **password robuste**, uniche per ogni servizio, difficili da indovinare e, ove possibile, attiva l'**autenticazione a più fattori** (MFA). Inoltre, proteggi le informazioni sensibili presenti sul dispositivo, mediante le funzionalità di **cifratura** e sicurezza integrate per tutelare i dati.

*Adotta comportamenti
consapevoli*

Presta attenzione a messaggi, email, link e allegati sospetti e scarica applicazioni soltanto da fonti affidabili, limitando la condivisione di informazioni sensibili. Infine, effettua regolarmente il **backup** dei dati importanti per garantirne il recupero in caso di guasto, perdita del dispositivo o incidente informatico.



Security Trend

Il malware nascosto nelle false app

Nel **maggio 2026** è stata identificata una nuova variante di **TrickMo**, un sofisticato **malware** per dispositivi Android diffuso tramite applicazioni contraffatte che imitano servizi molto popolari, come **TikTok** o **piattaforme di streaming**. Il malware viene condiviso tramite social media o app di messaggistica, inducendo gli utenti a installarle al di fuori degli store ufficiali.

Una volta installato, lo stesso è in grado di **sottrarre credenziali di accesso, intercettare SMS e codici di verifica, acquisire schermate e consentire il controllo remoto del dispositivo**. L'aspetto più preoccupante della nuova variante è l'utilizzo di una **rete decentralizzata** (TON - The Open Network) per comunicare con gli attaccanti, rendendo più complesso individuare e bloccare le comunicazioni malevole e aumentando la capacità del malware di rimanere nascosto.

Questo caso evidenzia ancora una volta l'importanza di **scaricare applicazioni solo dagli store ufficiali, verificare attentamente i permessi richiesti dalle app e mantenere sempre aggiornati sistema operativo e applicazioni**.



maggio 2026

Il caso della rete criminale Sality

Nel **settembre 2026** un'importante operazione internazionale coordinata da **Europol** ha portato al contrasto di **Sality**, una rete di dispositivi infetti attiva da oltre vent'anni. Secondo le indagini, questa infrastruttura criminale era stata utilizzata per diffondere malware e **coinvolgere migliaia di dispositivi compromessi** in attività dannose in tutto il mondo.

I dispositivi colpiti venivano utilizzati all'insaputa dei proprietari per **distribuire ulteriori minacce informatiche, sottrarre informazioni e supportare altre attività criminali online**.

L'operazione ha portato al sequestro di numerosi domini utilizzati dagli attaccanti e all'interruzione delle comunicazioni tra i dispositivi **compromessi**, impedendo ai criminali di continuare a controllare la rete, rendendo inefficace una delle infrastrutture criminali più longeve e resilienti degli ultimi anni.

Questo caso dimostra come anche **un singolo dispositivo non adeguatamente protetto** possa essere sfruttato dai criminali informatici senza che l'utente se ne accorga.



settembre 2026



CYBER
SAPERE

*Restate sintonizzati:
nuovi approfondimenti
sulla cybersecurity vi aspettano
nelle prossime pubblicazioni.*