

OUCH!

La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per te

# Smaltimento dei tuoi dispositivi mobili

## In sintesi

I dispositivi mobili, come gli smartphones, gli smart watches e i tablets, continuano ad innovarsi e progredire in maniera sempre più rapida. Di conseguenza molte persone sostituiscono i loro dispositivi mobili anche ogni anno. Sfortunatamente le persone spesso non si accorgono di quante informazioni personali si trovino su questi dispositivi. Di seguito ti illustreremo quali dati possono trovarsi sul tuo dispositivo mobile e come eliminarli in modo sicuro prima di sostituirlo. Se usi un dispositivo mobile aziendale, o che contenga dati di lavoro, chiedi al tuo supervisore quali sono le procedure di backup e smaltimento appropriate.

## I tuoi dati

I dispositivi mobili contengono più dati sensibili di quanto crediamo, spesso ancora più di un computer.



- Dove abiti, lavori e i luoghi che visiti
- I dettagli di ogni contatto nella tua rubrica, inclusi familiari, amici e colleghi di lavoro
- L'elenco delle chiamate ricevute, inviate, senza risposta e dei messaggi vocali
- I messaggi di testo e le sessioni di chat in applicazioni come Secure chat, i giochi e i social media
- La cronologia dei siti visitati, delle ricerche, i cookies e le pagine salvate nella cache
- Le foto personali, i video e i files audio
- Le password salvate e gli accessi ai tuoi account, come quelli della banca, dei social media e della posta elettronica
- Informazioni sulla salute, inclusi la tua età, la frequenza cardiaca, l'attività fisica svolta o la pressione del sangue

## Pulizia dei dati sul dispositivo

Indipendentemente dal metodo utilizzato per smaltire il tuo dispositivo mobile, ad esempio donarlo, scambiarlo con uno nuovo, darlo ad un altro membro della famiglia, rivenderlo o semplicemente buttarlo via, devi prima assicurarti di cancellare tutti i dati sensibili. Eliminare i dati non è sufficiente, dovresti invece eseguire una cancellazione sicura di tutti i dati sul tuo dispositivo. Il modo più semplice per farlo è quello di eseguire un reset del tuo dispositivo. La funzione di reset varia a seconda del dispositivo; di seguito elenchiamo i passaggi per quelli più comuni. Come ulteriore misura di sicurezza accertati di aver attivato la crittografia dei

dati prima di eseguire il reset. Sui dispositivi mobili più recenti il modo più semplice per farlo è quello di attivare un blocco schermo (cosa che speriamo tu abbia già fatto). Infine, è vivamente consigliato di eseguire un backup del tuo dispositivo prima di eseguire il reset.

- Dispositivi Apple iOS: Impostazioni | Generali | Ripristina | Inizializza contenuto e impostazioni
- Dispositivi Android: Impostazioni | Privacy | Ripristino dati di fabbrica

## SIM e Schede Esterne

Oltre al tuo dispositivo, devi considerare anche cosa fare della tua scheda SIM (Subscriber Identity Module). Una scheda SIM è quella che viene usata dai dispositivi mobili per connettersi alla rete cellulare o dati. Quando elimini i dati sul tuo dispositivo, la scheda SIM conserva le informazioni del tuo account e rimane collegata a te. Se vuoi mantenere il tuo numero quando sostituisci il dispositivo, dovrai chiedere al tuo operatore telefonico come effettuare il trasferimento della scheda SIM. Se questo non fosse possibile, assicurati di distruggere la tua vecchia scheda SIM, per evitare che altri possano usare la tua identità per accedere alle tue informazioni e accounts. Infine, alcuni dispositivi Android utilizzano una scheda rimovibile SD (Secure Digital) come spazio di archiviazione aggiuntivo. Rimuovi queste schede di archiviazione esterna dal tuo dispositivo mobile prima di eliminarlo. Queste schede spesso possono essere riutilizzate sui nuovi dispositivi mobili, oppure come spazio di archiviazione sul tuo computer tramite un adattatore USB. Se non fosse possibile riutilizzare la tua scheda SD, allora come nel caso della vecchia scheda SIM, ti raccomandiamo di distruggerla fisicamente.

Se hai dei dubbi su qualcuno dei passaggi che ti abbiamo illustrato, o se le opzioni di reset del tuo dispositivo sono diverse, portalo al negozio dove lo hai acquistato e fatti aiutare da un tecnico specializzato. Infine, se stavi pensando di buttare il tuo dispositivo, prova piuttosto a donarlo. Ci sono molte organizzazioni di beneficenza che accettano dispositivi mobili usati e molti negozi di telefonia offrono opzioni per lo smaltimento degli stessi.

## L'autore di questo articolo

**Christopher Crowley** (@CCrowMontance) è un consulente indipendente nell'area di Washington DC, specializzato in operazioni di sicurezza. Occasionalmente pubblica su blog e twitter. Di prossima uscita un suo libro riguardante i Centri Operativi di Sicurezza. E' Istruttore Capo al SANS Institute.



## Risorse

SANS Course: Pen Testing Mobile Devices: <https://sans.org/sec575>

SANS Course: Advanced Smartphone Forensic Course: <https://sans.org/for585>

FTC Advice on Disposing Your Mobile Device: <https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device>

*OUCH!* è pubblicato da SANS Security Awareness ed è distribuito sotto licenza [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). Siete liberi di distribuire questa newsletter o di utilizzarla nel vostro programma di sensibilizzazione purchè non ne venga modificato il contenuto. Per traduzioni o ulteriori informazioni, si prega di contattare [www.sans.org/security-awareness/ouch-newsletter](http://www.sans.org/security-awareness/ouch-newsletter). Direzione Editoriale: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley