

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

- Le tue informazioni
- Cancellare il contenuto del dispositivo
- SIM e schede di memoria

Sostituire un dispositivo mobile

Introduzione

La tecnologia dei dispositivi mobili, come smartphone, tablet e smart watch, evolve a ritmi impressionanti. Come conseguenza di questo molte persone sostituiscono il proprio dispositivo sempre più frequentemente, anche una volta all'anno. In troppi però si disfano di esso senza rendersi conto di quanti dati personali ancora conservi. In questa newsletter illustreremo quali tipi di informazioni personali possono essere presenti nei dispositivi mobili e come cancellarli in modo sicuro prima di disfarsene. Se il dispositivo ti è stato consegnato dalla tua azienda, o conserva dati aziendali, verifica con il tuo responsabile la presenza di salvataggi e di procedure di smaltimento adeguate prima di seguire i passi che ti illustreremo.

L'autore di questo numero

Heather Mahalik ([@HeatherMahalik](#); [+HMahalik](#)) è Principal Forensic Scientist presso ManTech CARD. È co-autrice e gestore del corso Advanced Smartphone Forensics per il SANS Institute per il quale insegna anche Windows Forensic Analysis. Potete leggere il suo blog su smarterforensics.com.

Le tue informazioni

I dispositivi mobili conservano molti più dati sensibili di quanto tu possa immaginare, spesso più di quanti ne conservi il tuo computer. Tra queste informazioni troviamo:

- il luogo in cui vivi, lavori e i posti che frequenti;
- i dettagli di contatto di chiunque sia presente nella tua rubrica e nelle tue applicazioni, compresi i famigliari, gli amici e i colleghi;
- la storia delle tue telefonate, ricevute, fatte e perse;
- messaggi SMS e multimediali;
- sessioni in chat di varie applicazioni,
- i tuoi spostamenti, basati su coordinate GPS o delle celle di rete;
- la cronologia della navigazione, delle ricerche, i cookie e le pagine in cache;
- foto personali, video, registrazioni audio e email;
- password memorizzate e accessi agli account personali, come l'email o la tua banca online;
- accessi a foto, file o informazioni nel Cloud;
- dati sanitari di vario tipo.

Sostituire un dispositivo mobile

Cancellare il contenuto del dispositivo

Come avrai potuto vedere, c'è una quantità impressionante di dati sensibili nel tuo dispositivo mobile. Indipendentemente da come te ne disferai (donandolo, scambiandolo per uno nuovo, dandolo a un altro membro della tua famiglia, rivendendolo o buttandolo via) devi essere sicuro di cancellare le informazioni personali in esso presenti. La semplice cancellazione dei dati non è abbastanza, poiché essi possono essere recuperati facilmente con strumenti gratuiti reperibili in Internet. È invece necessario cancellare in modo sicuro tutti i dati sul dispositivo, con un processo chiamato wiping che permette di sovrascrivere le informazioni in modo che non possano più essere recuperate. Ricorda che prima di cancellare tutti i tuoi dati, è opportuno eseguire un backup, in modo da poterli ripristinare sul dispositivo nuovo.

Il metodo più semplice per cancellare il tuo dispositivo in modo sicuro è il ripristino dei dati di fabbrica. In questo modo ritornerà alla situazione del momento in cui è entrato in tuo possesso. Il ripristino dei dati di fabbrica offre il metodo più semplice e sicuro per rimuovere i dati dal dispositivo. L'applicazione di questa funzione varia tra i vari dispositivi, per cui elenchiamo di seguito come accedervi dai due tipi di dispositivo più utilizzati:

- Apple iOS: Impostazioni | Generali | Ripristina | Inizializza contenuto e impostazioni
- Android: Impostazioni | Account e backup | Backup e ripristino | Ripristina dati di fabbrica

Sfortunatamente, la rimozione dei dati personali dai Windows Phone non è semplice come per gli altri tipi di dispositivi: tutt'ora si stanno svolgendo ricerche per cancellare i dati in modo sicuro. Se vuoi sapere come fare con il tuo dispositivo, verifica il manuale o il sito del produttore.

Ricorda: la semplice cancellazione dei dati personali non è sufficiente, in quanto essi possono essere facilmente recuperati.

SIM e schede di memoria

In aggiunta ai dati memorizzati sul dispositivo, devi pensare anche alla scheda SIM, la scheda utilizzata dal dispositivo per collegarsi alla rete cellulare. Quando effettui un ripristino dei dati di fabbrica, la scheda SIM continua a conservare informazioni sul tuo account e continua ad essere, in qualche modo, collegata a te. Se mantieni lo stesso numero di telefono usando un nuovo dispositivo, chiedi al tuo fornitore di servizio informazioni su come trasferire la carta SIM. Se questo non



Quando ti disferai del tuo dispositivo mobile, assicurati di ripristinare i dati di fabbrica, rimuovere la scheda SIM ed eventuali schede SD.

Sostituire un dispositivo mobile

fosse possibile, perché, ad esempio, il nuovo telefono usa una SIM di una dimensione diversa, tieni la vecchia SIM e distruggila fisicamente per impedire che qualcuno la possa riutilizzare.

Parliamo infine dei dispositivi che usano una scheda SD separata, come memoria aggiuntiva. Queste schede contengono immagini, applicazioni e altro contenuto sensibile. Ricorda di rimuovere ogni scheda esterna dal tuo dispositivo mobile prima di disfartene (in alcuni dispositivi, la scheda SD potrebbe essere nascosta nel vano della batteria, a volte dietro la batteria stessa).

Questa scheda può essere riutilizzata in nuovi dispositivi, o come dispositivo di memorizzazione generico su computer con un'interfaccia USB. Se la scheda non dovesse essere riutilizzabile ti raccomandiamo di distruggerla fisicamente. Se hai bisogno di ulteriori informazioni, porta il tuo dispositivo al negozio dove l'hai acquistato e chiedi l'aiuto di un tecnico professionista. Se invece te ne stai disfacendo ti consigliamo di donarlo a un'associazione caritatevole che accetti dispositivi usati.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito

securingthehuman.sans.org/ouch/archives

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguilta su www.advancement.com e su Twitter([@advanction](https://twitter.com/advanction)).

Risorse

Tablet e sicurezza: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_it.pdf

Salvataggi e ripristino: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_it.pdf

OUCH! è pubblicata dal progetto Securing The Human del SANS Institute e viene distribuita con licenza [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Sei libero di distribuire questa newsletter o utilizzarla nei tuoi programmi di awareness senza però modificarne i contenuti. Per traduzioni o ulteriori informazioni, contatta ouch@securingthehuman.org.

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley



securingthehuman.sans.org/blog



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.sans.org/gplus](https://plus.google.com/securethehuman.sans.org/gplus)