Promemoria

«L’uso di app su dispositivi mobili impiegati a scopi di servizio nell’Amministrazione federale»

Cosa devo sapere?

L’uso di applicazioni TIC della Confederazione su dispositivi mobili è disciplinato nella direttiva «Smartphone/Smarttablet Sync E021» (disponibile in tedesco e francese).
E021 - Einsatzrichtlinie Smartphone/Smarttablet Sync

Il presente promemoria contiene raccomandazioni della Confederazione per l’uso di app su dispositivi mobili aziendali e privati impiegati a scopi di servizio ed è destinato ai collaboratori della Confederazione.

04/2023

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Centro nazionale per la cibersicurezza NCSC

Installare app con moderazione

Ogni app in più rappresenta un potenziale rischio per la sicurezza, perciò le app non più necessarie devono essere eliminate. Tenere poche app permette di avere una visione d'insieme migliore e di ridurre i rischi per la sicurezza. Controllate regolarmente le app installate.	Raccomandazione • Installate soltanto le app indispensabili. • Eliminate le app non più necessarie.

Aggiornare regolarmente le app

Le app non aggiornate sono un potenziale rischio per la sicurezza. Verificate regolarmente se sono disponibili aggiornamenti e installateli subito.	Raccomandazione • Fate in modo che le app siano sempre aggiornate. La cosa migliore è impostare l'aggiornamento automatico.

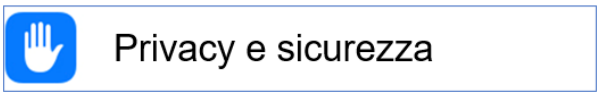
Autorizzazioni

Al primo utilizzo di un'app, talvolta anche dopo un aggiornamento, ci viene chiesto se autorizzare gli accessi. Molte app chiedono di accedere ai dati personali. Nelle impostazioni del dispositivo gli accessi possono essere limitati o negati.	Raccomandazione • Concedete solo gli accessi (ad es. all'elenco dei contatti) indispensabili per il funzionamento dell'app. In caso di dubbi si raccomanda di rifiutare l'autorizzazione. Nelle impostazioni è sempre possibile modificare gli accessi. • Verificate gli accessi per ogni app.

Le app di social media

Non è proibito installare app di social media sui dispositivi mobili aziendali (Instagram, Facebook, TikTok ecc.). Tuttavia, tali app spesso ottengono autorizzazioni estese ed è noto che raccolgono grandi quantità di dati, ad esempio quelli relativi ai contatti.	Raccomandazione • Accertatevi che le app installate sul dispositivo mobile impiegato a scopi di servizio siano davvero necessarie. • Limitate i diritti d'accesso allo stretto indispensabile. • In merito all'uso dei social media si rinvia anche alla relativa guida dell'UFPER.

Servizi di localizzazione

Oltre a intaccare la sfera privata, i servizi di localizzazione consumano molta batteria. Alcune app non funzionano senza accesso a determinate funzioni quali i servizi di localizzazione. Gestite l'accesso manualmente quando utilizzate l'app. Nel menu «Servizi di localizzazione» sono elencate tutte le app che chiedono l'accesso alla posizione e potete gestirle manualmente.	**Raccomandazione** • Se non è necessario per il funzionamento di una determinata app, si raccomanda di disattivare del tutto il servizio di localizzazione. A tal fine, nelle «Impostazioni» selezionate il menu «Privacy e sicurezza».  • Nella maggior parte dei casi è sufficiente cambiare l'opzione di localizzazione da «Mai» a «mentre usi l'app». 

Comunicazioni confidenziali

Per le comunicazioni vocali confidenziali (telefono, note vocali, chat), sui dispositivi mobili gestiti con MDM può essere scaricata l'app Threema Work.	**Raccomandazione** • I contenuti sensibili e confidenziali vanno discussi via Threema Work o Skype for Business. • Per le conversazioni confidenziali utilizzate solo Threema Work. • Fatta eccezione per quelli appena menzionati, non è consentito usare altri servizi di messaggistica per le comunicazioni di lavoro. **Direttiva** E027 – Direttiva concernente le comunicazioni vocali crittografate

Simboli di stato

La barra di stato si trova in alto a destra dello schermo. I simboli indicano se un'app sta raccogliendo dati di localizzazione o ha attivato interfacce. Se figurano attività che non avete avviato intenzionalmente, verificate le app attive.

Raccomandazione

Prestate sempre attenzione ai simboli che figurano nella barra di stato del dispositivo.

	Un'app o un sito web sta utilizzando la posizione (servizi di localizzazione).
	Un'attività di rete è in corso (ad es. tramite un'app).
	L'inoltro delle chiamate è attivo.
	Un'app sta utilizzando il microfono del dispositivo.
	Un'app sta utilizzando la videocamera (con o senza microfono) del dispositivo.
09:41	Il dispositivo sta registrando l'audio o sta facendo uno screenshot.

Se sospettate anomalie contattate il Service Desk del vostro fornitore di prestazioni.

Uso dei dispositivi mobili all’estero

Durante i viaggi all’estero è d’obbligo la massima prudenza con le app. In determinati Paesi le autorità doganali possono controllare le app. Per evitare che ciò accada, le app Secure MDM (Secure Mail, Secure Notes, Secure Tasks) devono essere disinstallate prima di entrare nel Paese. Le app obbligatorie (ad es. secondo le direttive del Paese) devono essere installate su un altro dispositivo mobile.	Raccomandazione • Nei viaggi all’estero portate con voi solo i dispositivi indispensabili. • Per le persone esposte in viaggio con statuto diplomatico valgono disposizioni particolari, soprattutto per quanto concerne la messa a disposizione di informazioni. Informatevi sulle direttive e le possibilità presso il vostro ufficio di riferimento o il supporto VIP. • Consigli di viaggio del DFAE: DFAE - Consigli di viaggio in breve • Sito web NCSC - Viaggi all’estero: NCSC - Viaggi all’estero

Sostituzione del dispositivo mobile

Quando un dispositivo mobile viene sostituito, molti dati rimangono memorizzati sul vecchio dispositivo.	Raccomandazione • Cancellate i dati dal vecchio dispositivo.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Centro nazionale per la cibersicurezza NCSC