

App per il Mobile Banking

Più della metà delle transazioni e-banking viene effettuata da smartphone o tablet. Solitamente si usa un'app del proprio istituto finanziario. Il Mobile Banking ha molti vantaggi, ma cela anche dei pericoli.

Ecco come utilizzare un'app per il Mobile Banking in modo sicuro:

- Proteggete il vostro dispositivo mobile con le nostre [«5 operazioni per la vostra sicurezza digitale»](https://www.ebas.ch/it/5-operazioni-per-la-vostra-sicurezza-digitale/) (<https://www.ebas.ch/it/5-operazioni-per-la-vostra-sicurezza-digitale/>). Solo un dispositivo pulito e sicuro rende possibile un Mobile Banking sicuro.
- Quando utilizzate le app per il Mobile Banking, non trasferite somme ingenti con la funzione di invio, ma sempre e solo con la funzione di richiesta. Così facendo, se viene commesso un errore di battitura o simili non sarà il denaro a giungere alla persona sbagliata, ma soltanto la richiesta.
- Installate l'app per il Mobile Banking (come pure tutte le altre app) solo dallo Store ufficiale.
- Installate soltanto le app di cui avete davvero bisogno e disinstallate tutte quelle che non usate (più).
- Limitate al minimo indispensabile i diritti d'accesso di tutte le app.
- Quando siete in viaggio, connettete il dispositivo soltanto a reti affidabili.
- Se lo smarrite, fate bloccare immediatamente il vostro dispositivo, e ripristinatelo correttamente prima di venderlo o smaltirlo.

Rischi e vantaggi delle app per il Mobile Banking

Smartphone e tablet sono come dei (piccoli) computer e quindi sono esposti a pericoli simili a quelli dei computer classici: perdita o furto di dati, infezione da malware, accessi non autorizzati ecc. Inoltre, dato che vengono utilizzati in movimento, si aggiungono rischi come lo smarrimento e il furto.

D'altra parte, offrono vantaggi come l'aspetto della mobilità e del poco spazio che occupano. Quando si utilizza un'app per il Mobile Banking si aggiunge un altro vantaggio decisivo: **a differenza dell'e-banking tradizionale tramite browser, il cliente riceve dall'istituto finanziario un software pronto all'uso e sviluppato appositamente per l'e-banking, dotato di conseguenza di buone protezioni.**

L'utente attento alla sicurezza, quindi, non ha più bisogno di preoccuparsi di compiti tediosi come l'inserimento manuale dell'indirizzo della banca nel browser e il controllo che la connessione sia sicura. A differenza del browser, infatti, l'app per l'e-banking esegue queste operazioni automaticamente in background, riducendo così al minimo il rischio di errori tipici come gli errori di digitazione e il phishing – naturalmente a condizione che l'utente osservi alcune regole di base.

Utilizzo sicuro di un'app per il Mobile Banking

Creare una protezione di base

Come prima cosa, quando si usa un dispositivo mobile bisogna ridurre al minimo i pericoli di carattere generale. Seguite quindi le nostre [«5 operazioni per la vostra sicurezza digitale»](https://www.ebas.ch/it/5-operazioni-per-la-vostra-sicurezza-digitale/) (<https://www.ebas.ch/it/5-operazioni-per-la-vostra-sicurezza-digitale/>) anche per i dispositivi mobili. Assicuratevi, in particolare, di attivare il blocco automatico dello

schermo tramite codice, password, impronta digitale o riconoscimento facciale.

Il bisogno di fare attenzione riguarda a maggior ragione gli smartphone e i tablet: non perdetevi mai di vista il vostro dispositivo. Fate attenzione a non comunicare a nessuno i vostri dati d'accesso come PIN, TAN e password, a nascondervi quando li immettete e a non farvi vedere da nessuno da dietro le spalle. Prestate attenzione quando aprite e-mail, allegati, chat (come i messaggi di WhatsApp) o MMS. Il malware si può diffondere anche tramite MMS e WhatsApp. Non fate clic su link sconosciuti ed eliminate immediatamente i messaggi provenienti da mittenti sconosciuti. Verificate i numeri sconosciuti prima di richiamare.

Fare attenzione all'origine delle app

Installate soltanto le app di cui avete davvero bisogno e accertatevi che provengano da una fonte affidabile, cioè dallo Store ufficiale (p. es. l'App Store di Apple o Google Play Store).

Non fidatevi delle app dalla reputazione scarsa o delle raccomandazioni di persone che non conoscete. Prima di installare un'app raccogliete informazioni sul fornitore, se non lo conoscete già.

Di tanto in tanto controllate quali app usate ancora, e disinstallate quelle obsolete e quelle che non usate più: ogni app è una potenziale falla di sicurezza in più.

Segnalate immediatamente al [vostro istituto finanziario \(https://www.ebas.ch/it/partner/\)](https://www.ebas.ch/it/partner/) eventuali messaggi di errore e funzionamenti insoliti della vostra app per l'e-banking.

Limitare i diritti d'accesso

Molte app si prendono, senza chiari motivi, ampi diritti. Per esempio, non è necessario che ogni singola app acceda ai dati della posizione, alla rubrica o allo stato del telefono. Per questo motivo, è consigliabile valutare con occhio critico se i diritti d'accesso sono realmente necessari per l'esecuzione delle funzioni e, se possibile, disattivare tutti i diritti non indispensabili.

Controllare da chi è gestita la rete

Lo smartphone o il tablet può connettersi in tanti modi al vostro istituto finanziario. Quando siete in viaggio, il dispositivo si connette a reti diverse. Se utilizzate una connessione WiFi o WLAN, accertatevi prima che sia affidabile: operatori poco raccomandabili di reti WiFi «gratuite» potrebbero indirizzare l'app per l'e-banking al server sbagliato e intercettare i dati d'accesso che inserite.

Per i dispositivi Android potete anche impostare un'app firewall per monitorare e proteggere le connessioni attive. Per i dispositivi iOS (iPhone/iPad), questo non è né possibile né necessario.

Gestire correttamente perdita, vendita e smaltimento

Se il vostro smartphone o tablet finisce nelle mani sbagliate, i file o i dati d'accesso che contiene potrebbero essere sfruttati e utilizzati in modo improprio.

Varie app permettono di bloccare in remoto i dispositivi persi o rubati. L'operazione cancella dal dispositivo i vostri dati personali, che quindi non saranno più consultabili. Dopo aver bloccato il dispositivo, è consigliabile contattare anche l'operatore telefonico per far bloccare la scheda SIM.

Se non volete che i dati che avete memorizzato nel dispositivo cadano nelle mani sbagliate quando lo vendete o smaltite, ricordate che potrebbero rimanere tracce di dati se non avete prima cancellato in modo sicuro tutti i supporti di archiviazione. La procedura è descritta per esempio sul [sito Internet di Apple \(https://support.apple.com/de-de/HT201274\)](https://support.apple.com/de-de/HT201274) e su una pagina della [SRF \(https://www.srf.ch/sendungen/kassensturz-espresso/services/handy-daten-sicher-loeschen-so-funktioniert-s\)](https://www.srf.ch/sendungen/kassensturz-espresso/services/handy-daten-sicher-loeschen-so-funktioniert-s). Naturalmente dovreste anche rimuovere la scheda SIM e, se non intendete continuare a uti-

lizzarla, distruggerla.

Con il termine «Mobile Banking» si intende l'esecuzione di operazioni bancarie attraverso dispositivi mobili come smartphone o tablet.

Potete accedere al vostro sistema di e-banking attraverso il browser oppure, sempre più spesso, con apposite app.

Promemoria: [Download \(PDF\) \(https://www.ebas.ch/wp-content/uploads/2019/10/mobilebankingSKP_it.pdf\)](https://www.ebas.ch/wp-content/uploads/2019/10/mobilebankingSKP_it.pdf)