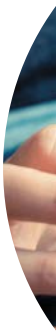
Mobile Banking e Mobile Payment

Ecco come rendere sicuri i pagamenti effettuati con il vostro dispositivo mobile!

La vostra polizia e la Prevenzione Svizzera della Criminalità (PSC) – un servizio intercantonale della Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP)

Effettuate transazioni bancarie con il vostro tablet e alla cassa preferite pagare senza contanti con lo smartphone?



Ormai il Mobile Banking e il Mobile Payment sono due funzioni molto diffuse sui dispositivi mobili. Ma a cosa bisogna fare attenzione dal punto di vista della sicurezza e come si possono evitare danni finanziari?

I vantaggi dei dispositivi mobili come gli smartphone e i tablet sono evidenti: sono pratici, sempre a portata di mano e connessi a Internet. Come per il vostro computer di casa, però, anche l'uso quotidiano dei dispositivi mobili cela rischi e pericoli. Questi suggerimenti vi mostrano come proteggere al meglio il vostro dispositivo mobile.

Tenete il vostro dispositivo mobile aggiornato e in perfetto stato di funzionamento!

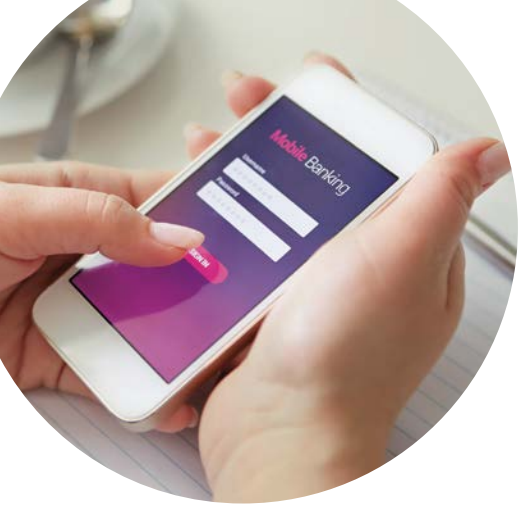
- **Installate le app scaricandole esclusivamente dallo store ufficiale!** Scaricate le app soltanto dall'App Store di Apple o da Google Play Store. Non fidatevi delle app che non presentano valutazioni o commenti. Prima di installare un'app raccogliete informazioni sul fornitore, se non lo conoscete già.
- **Installate gli aggiornamenti regolarmente!** Attivate sul vostro dispositivo mobile la funzione di aggiornamento automatico e installate immediatamente gli aggiornamenti disponibili per il sistema operativo e le app installate. Disinstallate le app obsolete o quelle che non usate più, così da evitare ulteriori rischi per la sicurezza.
- **Siate prudenti nell'aprire i messaggi di mittenti sconosciuti!** Non cliccate mai sui link e non scaricate gli allegati contenuti in e-mail, messaggi di instant messaging (come WhatsApp) o MMS di mittenti sconosciuti. Potrebbero nascondere del software dannoso (malware). Installate sul vostro dispositivo Android anche un'app antivirus. Sui dispositivi iOS non è possibile ma non è nemmeno necessario.
- **Abilitate soltanto le connessioni necessarie e affidabili!** Il vostro dispositivo mobile è in grado di connettersi a Internet o ad altri dispositivi tramite WiFi/WLAN, NFC, Bluetooth, infrarossi, 3G/4G/5G, USB, ecc. Attivate sempre solo il tipo di connessione che desiderate utilizzare e non accettate richieste di connessione da dispositivi sconosciuti.

Osservate alcune regole di base quando configurate il vostro dispositivo mobile!

- **Limitate i diritti d'accesso delle varie app!** Valutate con occhio critico se i diritti d'accesso sono realmente necessari per l'esecuzione delle funzioni e disattivate tutte le autorizzazioni non indispensabili. Non tutte le app hanno bisogno di ricevere diritti completi, come l'accesso ai dati di geolocalizzazione, alla fotocamera o alla rubrica.
- **Agite con cautela quando condividete le informazioni sulla vostra posizione geografica!** Utilizzate i servizi di geolocalizzazione con attenzione e non memorizzate le informazioni sulla vostra posizione geografica nelle foto che poi caricate ad esempio sui social media.
- **Non memorizzate dati confidenziali sul vostro dispositivo mobile o nel cloud!** Non salvate mai sul dispositivo mobile o nel cloud dati d'accesso come PIN, TAN e password che utilizzate nel browser o nello Store. Utilizzate un password manager e disattivate la funzione di salvataggio automatico delle password sul dispositivo mobile.

Proteggete il vostro dispositivo mobile dagli accessi non autorizzati!

- **Utilizzate le impostazioni di sicurezza offerte dal vostro dispositivo!** Attivate il blocco dello schermo con una password sicura, l'impronta digitale o il riconoscimento facciale. Non comunicate a nessuno i vostri dati d'accesso.
- **Bloccate immediatamente il vostro dispositivo mobile in caso di furto o smarrimento!** Varie app permettono di bloccare in remoto i dispositivi mobili persi o rubati. In questo modo, i vostri dati personali non saranno più consultabili. Chiedete inoltre al vostro provider di bloccare la scheda SIM.
- **Prima di vendere o smaltire il vostro dispositivo mobile, effettuate un ripristino delle impostazioni di fabbrica!** In questo modo i dati memorizzati sul dispositivo mobile non finiranno nelle mani sbagliate. Rimuovete e distruggete anche la scheda SIM, se non vi serve più.



Mobile Banking

Per “Mobile Banking” s’intende l’esecuzione di transazioni bancarie su un dispositivo mobile per mezzo di app o portali e-banking dei vari istituti finanziari. Il modo di accedere al Mobile Banking non cambia nulla a livello di sicurezza, purché si seguano i suggerimenti indicati sopra.

Se utilizzate il Mobile Banking, vi consigliamo di...

- **scegliere una connessione sicura.** Per le connessioni WLAN utilizzate uno standard WPA2 o WPA3, attivabile sul vostro router.
- **utilizzare un dispositivo separato per l’autenticazione a doppio fattore.** Con il Mobile Banking utilizzato sul dispositivo mobile in combinazione con la procedura mTAN o PhotoTAN manca il secondo canale di comunicazione indipendente. Utilizzate quindi un dispositivo diverso, come un telefonino vecchio o un dispositivo TAN della vostra banca.

Mobile Payment

Per "Mobile Payment" s'intende il pagamento senza contanti e contactless effettuato con dispositivi mobili. Spesso la sicurezza del Mobile Payment viene messa in dubbio: cosa succede ai miei dati? La connessione è sicura? Le transazioni sono crittografate? La cosa più importante è che i dati del cliente e i dati di pagamento siano mantenuti separati. Così il gestore dell'app (come Twint o Apple Pay) non dovrebbe mai sapere cosa ha acquistato il cliente e dove, e il commerciante non dovrebbe mai conoscere il saldo del conto del cliente. È difficile verificare se queste due condizioni sono rispettate, ma si possono chiedere delucidazioni al gestore dell'app.

Per securizzare al meglio i vostri pagamenti senza contanti e contactless, seguite i suggerimenti indicati sopra e...

- **inserite nell'app di Mobile Payment soltanto i dati davvero necessari.** Il rischio di un uso improprio dei dati risiede proprio nella possibilità di combinare i dati di pagamento e dell'acquisto con i dati di utilizzo e di geolocalizzazione per creare profili utente significativi.
- **proteggete l'accesso all'app di Mobile Payment.** Attivate le impostazioni di sicurezza dell'app. Configurate il blocco automatico tramite codice, password, impronta digitale o riconoscimento facciale.

Ulteriori informazioni su: **www.ebas.ch/mobilebanking**

Primavera 2019

SKPPSC

Prevenzione Svizzera della Criminalità
Casa dei Cantoni
Speichergasse 6
3001 Berna

www.skppsc.ch

Questo pieghevole è stato realizzato in collaborazione con la **Scuola Universitaria Professionale di Lucerna** e **«eBanking – ma sicuro!».**

www.ebas.ch | www.ebankingmasicuro.ch

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

eBanking ma sicuro!