Mobile banking and mobile payments

How to securely use your mobile device for payment transactions

Police and Swiss Crime Prevention –
an office supported by the cantonal
ministries of justice and police,
in co-operation with the University of
Lucerne and “eBanking – but secure!”

You conduct banking transactions on your tablet, and prefer cashless payments via your smartphone at the checkout?

Mobile banking and mobile payments are currently two of the most widely used applications on mobile devices. But what should you look out for with regard to security, and can you avoid financial losses?

Mobile devices such as smartphones and tablets offer some obvious advantages: they are compact, always to hand and connected to the Internet. Yet similar to your home computer, using your mobile devices every day entails certain risks and dangers. The following tips advise you on how to best protect your mobile device.

Keep your mobile device up-to-date and clean.

- **Only ever install apps from the official store.** You should never download any apps from providers other than the Apple App or Google Play Store. And be wary of any apps with no reviews. If you have never heard of the provider, find out more about them before installing any apps.
- **Regularly run updates.** Activate the automatic update feature on your mobile device, and install any updates available for your operating system and apps as soon as you can. To avoid any further security risks, remove all old apps or those you no longer need.
- **Always be wary of opening messages from anyone you don't know.** Don't click on any links, and never download any attachments in any e-mails, short messages (e.g. WhatsApp) or MMS from unknown senders. These could conceal malware. You should also install an antivirus app on your Android device. With iOS devices, this is not possible, but not necessary either.
- **Only permit trustworthy connections you actually need.** Your mobile device can connect to the Internet or other devices via WiFi, NFC, Bluetooth, Infrared, 3G/4G/5G, USB, etc. Only ever activate the type of connection you would actually like to use at the time, and don't accept any connection requests from unknown devices.

Follow certain basic rules with regard to your mobile device settings.

- **Restrict access rights for each app.** Check whether an app actually needs these access rights to function, and deactivate any rights not required. Extensive rights, for instance to access your location data, camera or address book, are not always necessary for every app.
- **Be cautious about passing on your location details.** Use localisation services with caution, and don't save any location details in any photos you might upload to social media.
- **Don't store any confidential data on your mobile device or in the cloud.** Access details such PIN, TAN and passwords used in your browser or for any store should never be stored on your mobile device or in the cloud. Use a password manager, and deactivate automatic storage of passwords on your mobile device.

Protect your mobile device against unauthorised access.

- **Use the security settings available on your device.** Activate your screen lock with a strong password, fingerprint or facial recognition feature. Don't pass on your access details to anyone.
- **Immediately lock your mobile device in case of theft or loss.** With the help of various apps, lost or stolen mobile devices can be locked remotely. That way, your personal details can no longer be accessed. You should also ask your provider to block your SIM card.
- **Before selling or disposing of your mobile device, reset it to factory settings.** This ensures any data stored on your mobile device don't end up in the wrong hands. Unless you still need it, you should also remove and destroy your SIM card.

Mobile banking

Mobile banking means conducting your banking business with the help of a mobile device. To this end, you can use either an app provided by your financial institution, or their portal via your browser. As long as you follow the above tips, security is not affected by the method you use for mobile banking.

When mobile banking, you should also...

- **choose a secure connection.** For WiFi, use WPA2 or WPA3 encryption (with a strong password), which you can activate in your WiFi router.
- **use a separate device for two-factor authentication.** When mobile banking on a mobile device via the mTAN or PhotoTAN process, there is no second independent communication channel. You should therefore use another device for this purpose, for instance an old mobile phone or your bank's TAN device.

Mobile payment

Mobile payment means cashless and contactless payments via mobile devices. Mobile payment security often raises a few questions: what happens to my data? Is there a secure connection? Are the transactions encrypted? The most important thing is that customer and payment data are separate. The app provider (e. g. Twint or Apple Pay) should therefore not be able to find out what a customer has bought where. Retailers should not be able to establish what their customers' bank balance is. Whether this is actually the case is very difficult to check, but can be established with the app provider.

Pay cashless and contactless securely by following the above tips, and by...

- **only ever actually divulging data which are absolutely necessary to the mobile payment app.** Potentially linking payment and purchase data with usage and location details could lead to data misuse to create meaningful user profiles.
- **protecting access to your mobile payment app.** Activate your app's security settings. Set up an automatic lock using a code, password, fingerprint or facial recognition.

Further information: **www.ebas.ch/mobilebanking**

August 2022

SKPPSC

Swiss Crime Prevention (SCP)
House of Cantons
Speichergasse 6
CH-3001 Bern

www.skppsc.ch

This leaflet was created in co-operation with the University of Lucerne and "eBanking – but secure!"

www.ebas.ch | www.ebankingbutsecure.ch

HSLU Lucerne University of Applied Sciences and Arts

eBanking but secure!