Mobile Banking App

More than half of all e-banking transactions are carried out via a smartphone or tablet. Usually, a specific app provided by the financial institution is used for this purpose. Mobile banking offers many advantages, but also holds quite a few risks.

This is how you use your mobile banking app in a secure manner:

- Protect your mobile device with our "5 steps for your digital security" (https://www.ebas.ch/en/5-steps-for-your-digital-security/) . Only a clean and secure device will ensure mobile banking is secure.
- Do not use the send function to remit larger sums of money via your mobile banking app, but only ever the request function. In case of a typing error, this means only the request, but no money is received by the wrong recipient.
- Only ever install your mobile banking app and all your other apps from the official store.
- Only ever install apps you actually need, and de-install any apps you don't need (any longer).
- Restrict access rights for each respective app to the absolute minimum.
- Only connect your device to trustworthy networks when on the go.
- Immediate lock your device in case of loss, and reset it properly before selling or disposing of it.

Risks and advantages of mobile banking apps

Smartphones and tablets are (small) computers and therefore prone to similar risks as classic computers: Data loss or theft, malware infection, unauthorised access, etc. There are additional risks of mobile use such as loss or theft, too.

On the other hand, there are advantages such as mobility and reduced space requirements. When using a mobile banking app, there is another decisive advantage: **Unlike with classic e-banking using a browser, customers receive a ready-made bit of software which is specifically adapted to electronic banking by their financial institution and is thus effectively secured.**

This relieves security-conscious users of such onerous tasks as manual entry of the bank's address in their browser, and the need to check whether a connection is secure, since unlike browsers, banking apps take care of such tasks automatically and in the background. This minimises the risk of typical application errors, such as typing mistakes and phishing - always provided users observe some basic rules.

Using mobile banking apps securely

Establish a basic level of protection

The first step is to minimise those general risks the use of a mobile device poses. You should therefore follow our "5 steps for your digital security" (https://www.ebas.ch/en/5-steps-for-your-digital-security/) for your mobile devices, too. In particular, you should make sure that you have switched on your automatic screen lock using a code, password, fingerprint or face recognition feature.

The need to remain alert is particularly vital with smartphones and tablets: Never leave your device unattended. Make sure that you don't let anyone else know your log-in information such as PIN, TAN and passwords, always conceal them when logging in, and ensure that no-one looks over your shoulder while you do so. Always be wary of opening e-mails, attachments, Messenger notifications (for instance WhatsApp) and MSS. WhatsApp and MMS can be abused for spreading malware, too. Don't click on any unknown links, and immediately delete any messages by unknown senders. Before calling anyone back, please check out any unfamiliar numbers.

Check app origins

Only install apps you actually need, and ensure that they originate from reputable sources, i.e. directly from an official store (e. g. Apple App Store or Google Play Store).

Remain wary towards apps with a low reputation or with recommendations by persons unknown. If you have never heard of the provider, find out more about them before installing any app.

You should also check periodically which of your apps you are actually still using. De-install any obsolete apps and those you no longer need - every additional app is an inherent vulnerability.

Notify your financial institution (https://www.ebas.ch/en/partners/) immediately in case of error messages and unusual events.

Restrict access rights

Many mobile apps grant themselves extensive access rights with no apparent justification. It is for instance not necessary for any old app to access data such as location, address book or telephone status. You should therefore critically check whether an app actually needs these access rights to function, and deactivate any rights not required if possible.

Check network provider

Your smartphone or tablet can establish a connection to your financial institution in several ways. On the go, your device will connect with various networks. If you use a WiFi connection, you should ensure it offers confidentiality: Dubious providers of "free" WiFi networks can refer your banking app to the wrong server and capture any access data you enter.

With Android devices, you can set up an additional firewall app to monitor and secure active connections. With iOS devices (iPhone/iPad), this is neither possible nor necessary.

Handle loss, sale or disposal correctly

If your smartphone or tablet ends up in the wrong hands, data or access data stored there might just be captured and abused.

With the help of various apps, lost or stolen mobile devices can be locked remotely. This will ensure your personal data on your device are erased and can no longer be retrieved. Once you have locked your device, you should also have your SIM card provider lock the card.

If you don't want your stored data to end up in the wrong hands when selling or disposing of your device, you should remember that data traces can remain if you haven't securely erased all data storage media beforehand. How to do so is for instance described on the Apple website (https://support.apple.com/de-de/HT201274) and on SRF (https://www.srf.ch/sendungen/kassensturz-espresso/services/handy-daten-sicher-loeschen-so-funktioniert-s) . As long as you no longer wish to use it, you should of course also remove the SIM card and destroy it.

The term "mobile banking" denotes the processing of banking transactions via mobile devices, such as a smartphone or tablet.

Next to the option to access your e-banking facility via your browser, specific apps are also increasingly used for this purpose.

Info sheet: *Download (PDF) (https://www.ebas.ch/wp-content/uploads/2019/10/mobilebankingSKP_en.pdf)*