«Mobile Banking» Information and Prevention

Risks when mobile banking

- **Phishing attack:** A fraudster captures your access data.
- **Man-in-the-Browser attack:** Your mobile phone is infected with malicious code which e.g. captures your access data.
- **Lost devices:** Attackers obtain access to your mTANs and any e-banking app installed.

Mobile Banking

«Mobile banking» means handling your banking from mobile devices, such as Smartphones (e.g. iPhone), notebooks or tablet PCs (e.g. iPad).

You can access your e-banking facility from a browser or a special app. But beware: All the risks you should already be aware of from your e-banking on stationary computers must also be considered when mobile banking. And mobile devices also carry additional security risks.

Protect yourself with the following 10 rules

- Only install apps you really need, and only from an official store
- Restrict access privileges
- Secure mobile devices against unauthorised access
- Don't store any confidential data on your device or in the Cloud
- Only permit connections which are necessary and trustworthy
- Keep device up-to-date and clean
- Use two-factor authentication
- Stay alert
- In case of loss, immediately block your device
- Ensure your device is correctly reset before disposal or sale

Notes on iPhone/iPad

- Make sure to also protect your computer or your notebook where iTunes is installed.
- Don't unlock your iPhone/iPad using Jailbreak.

Notes on Android

- Protect your Android with antivirus software which is always kept up-do-date.

Further information: www.ebas.ch/mobilebanking

«eBanking – but secure!» is offering helpful security hints for e-banking users

eBanking but secure!

You will find further practical information on measures and approaches required to ensure that e-banking applications are used securely under **www.ebankingbutsecure.ch**. The use of this website is free.

Hochschule Luzern – Informatik
Campus Zug-Rotkreuz, Suurstoffi 41b
CH-6343 Rotkreuz