Third party provider access to bank accounts

Impersonation as a security risk

- To access client bank accounts, third party providers usually request and use their clients' e-banking access data (impersonation).
- This gives third party providers unlimited access to these accounts.
- Technically speaking, this approach is the same as the one used for classic-style phishing attacks.
- Financial institutions will be practically unable to tell whether it is you (their clients), a third party provider instructed by you or a criminal intermediary they are communicating with.

Third party provider services

There are several third party providers who offer intra-bank payment and account information services for e-banking clients. Potential services include accessing bank accounts held with different financial institutions via just one platform.

Loss of control over bank client data

- Swiss financial institutions are subject to strict guidelines to protect their bank client data and the security of their systems.
- This is in contrast with third party providers, who can save and process large amounts of data in environments which are much less well regulated.
- These systems are sometimes neither owned nor controlled by such third party providers.
- And as a rule, Swiss bank client confidentiality does not apply to such systems either!

Protect yourself by:

- Not passing on your personal access data (password, PIN, ID number, etc.) for e-banking purposes to **anyone**, i.e. to no other person or any third party providers.

Further information: www.ebas.ch/impersonation

«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