Using remote support safely

Establishing a connection

- Only establish connections with trustworthy persons.
- They should only be able to establish such a connection after receiving your explicit invitation to do so.
- The person establishing a connection to your computer should also authenticate him- or herself via a meeting ID and/or a password.
- A connection should only be established once you have expressly agreed to this.
- Data transferred should be protected with the help of an adequate encryption process.

Remote support

Remote support software enables remote access to a third party system via a local network (LAN) or the Internet. This way, the remote machine's desktop will be displayed on a local machine and also allows for remote control of the remote machine. Many companies use remote support software to enable their support staff to have a quick look at a user's machine without the need of someone having to go and visit them on site in the first instance.

Remote support session

- Don't grant full access to your system. The person assisting you should basically only ever be a spectator and provide you with instructions on what to do.
- Enter as few passwords as possible during your session, and don't surf to any Internet sites which have nothing to do with your session.
- Anything appearing on your screen during this session can be viewed and captured by the other party.
- While the connection is being established, a remote support information screen should permanently display on your screen. This allows you to see whether the connection is still active, and someone else is able to view your screen.

Terminating a connection

- Please ensure that after obtaining assistance you disconnect the Remote Support connection to prevent any further access to your computer. To do so, please follow the instructions in the software documentation.

Further information: www.ebas.ch/remotesupport

«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