Tips for secure online banking and protection against phishing

If something seems dubious to you during online banking, you'd better cancel the action immediately.

With this checklist, you can carry out banking transactions more securely.

Use trustworthy equipment

For online banking, use devices you know and whose software is up to date. Regular updates close security gaps in the system software and applications. Therefore, avoid using devices in public places for online banking.

Banking with separate devices

The securest way to carry out banking is on two separate devices. Access your bank's banking website from your desktop or notebook at home. You receive or generate the key code IDs for confirming transfers on your mobile phone or with a key code generator. A hacker would have to compromise both devices, which would be quite difficult.

Manually access the bank’s website

Go to your bank's website and use the online banking link there.

Do not use a search engine or create a bookmark that a virus could manipulate.

Make sure the address is correct: it must start with "**https**". You can see from the lock symbol in the address bar of your browser that the data is transferred securely.

Never click on given links

Never click on online banking links in emails - no matter what threat, promise or resourceful argument they try to get you to do so.

Do not open links in messengers

Likewise, do not follow any banking links in text messages (SMS) or messages in messengers like Whatsapp.

Tips for secure online banking and protection against phishing

Check with the bank

Banks don't send emails with clickable links or requests to download or install anything. Should you nevertheless have received such a message and doubt whether it could possibly be genuine, call your bank's hotline and ask explicitly. You can find the hotline number on your bank's website.

Pay attention to grammar

Hackers are creative when it comes to using fake messages to get access data.

Often you can recognize the fake on closer inspection by the missing direct salutation, clumsily formulated sentences, contradictory information or attached files - then just delete.

Never pass on access data

Do not pass on any access data on the phone, by email or via a messenger.

If a caller or an email - supposedly from your bank - asks for the activation of the account after alleged technical problems, hang up. Inform your bank by phone - but only under the official telephone number from the bank's homepage.