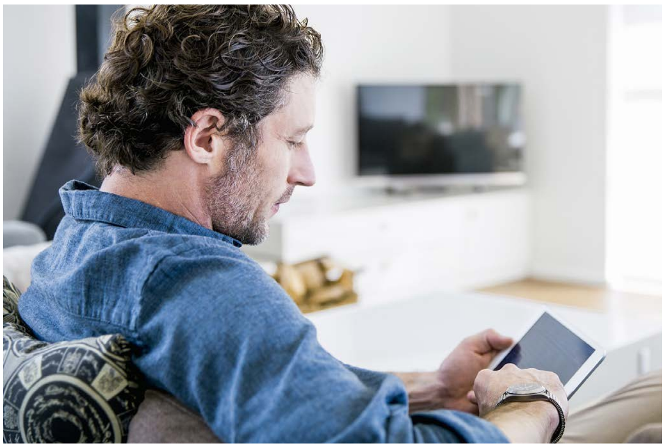
Security instructions for eBanking

Basic measures and rules

Our standards are continuously brought into line with the latest developments and comply with the stringent security standards in our industry. We provide you with some important information on "eBanking security" as well as valuable tips on how to get the best from your PC or smartphone for eBanking.



1 eBanking

Basics of eBanking:

Means of authentication

To log into eBanking, you need three identifying credentials:

- your personal user name
- your chosen password
- a changing transaction number

Password

You must replace the initial password you receive by post with a personal password of your own choosing during activation, i.e. when you log in for the first time. Choose a password that you can easily remember but that cannot be guessed by others. It must contain at least 8 characters. Combine letters, numbers, special characters and upper and lower case letters. Avoid names, phone numbers, dates of birth, car registration numbers, etc. Do not use the same password for different purposes, such as e-mail, social media, etc.

Safekeeping

You should be the only one who knows all three identifying credentials.

For this reason:

- never write down your password anywhere.
- keep any devices you use for authentication – your mobile phone with ZKB Access app or ZKB Access Reader – in a safe place.

Authentication procedure

eBanking uses the ZKB Access authentication procedure. The real-time generated transaction numbers (TAN) and the two-step authentication procedure (requiring a smartphone or reader) make eBanking significantly more secure.

Using eBanking

eBanking works on Windows or MacOS without any prior software installation. Simply log in using your browser. Select the login function on our website zkb.ch for direct access. Do not log in to eBanking on any other websites.

Security certificates

The eBanking login page is encrypted using the TLS protocol with at least 2048 bits. A closed lock in the browser indicates that the site is TLS encrypted. Certificates guarantee the authenticity of the web server. Zürcher Kantonalbank can be clearly identified as the website owner based on the fingerprint contained in the security certificate. To verify you are on the right site, go to the security certificate and check the fingerprint. Do not enter any identifying credentials on the login page until you have verified the security certificate.

Important: Visit zkb.ch/sicherheit – "Das können Sie tun" to find the latest fingerprint version.

Transaction confirmation

Transaction confirmation enhances the security of payment transactions. After entering and verifying a payment in eBanking, the payment information (the payee's account number, currency and the amount) will be displayed together with the TAN presented on your ZKB Access device. Only approve the payment if the details match those on the original invoice. If they do not match, click on "Cancel" in eBanking and contact eBanking Support immediately.

Tip: Decide whether you want to confirm all payments or only some of them. You can select this from the eBanking "Settings" menu under "TAN payment confirmation".

2 Mobile Banking

To log into the "ZKB Mobile Banking" app, you need to provide two identifying credentials:
- your personal user name
- your chosen password

Never write down or save your Mobile Banking password. As an additional layer of security, the app must be activated the first time you use it. You will receive the activation key for this when you activate the app in eBanking on your PC. To do this, go to your Profile "Name/Company" › "Settings" › "Security" and "ZKB Mobile Banking".

3 Protection for your computer

Threats abound everywhere – even on the Internet. You can significantly minimise the risk of an attack by actively protecting your data and your PC. The following basic measures, which are very easy to implement, can help keep intruders at bay.
- Read warnings and messages before clicking on them.

Software and apps

- Use a firewall
- Use a virus scanner
- Update your operating system and all software installed on your PC at regular intervals.
- Whenever possible, activate the automatic update function.

4 Protection for your smartphone

Smartphones are exposed to the dangers of the Internet just as much as computers. Observing a few basic rules can help prevent unwanted access to your device.

General

- Always activate the lock code on your mobile device.
- Do not save your credentials, such as user name and password, on your mobile device.
- When entering your PIN or TAN, make sure no one is looking over your shoulder.

Software

Always use the latest operating system version on your mobile device and update it regularly. Do not install apps from sources you do not know or trust.

5 Code of Conduct

Under no circumstances will we ask you for any confidential information whatsoever (e.g. account number, user name, passwords, code) by e-mail or ask you to click on a link in an e-mail and log in there. If you receive e-mails claiming to come from Zürcher Kantonalbank, be critical: Zürcher Kantonalbank communicates with you by e-mail only where you have expressly consented to this, for example, if you have subscribed to one of our newsletters.

In addition, we will never send you any software for you to install by e-mail.

6 Further information

Further information on eBanking and security can be found at zkb.ch/sicherheit.

7 eBanking Support

In the event of unexpected errors or error messages, in particular those relating to passwords, transaction numbers and being logged out, be sure to contact eBanking Support immediately.

As a precaution, you can block access to your eBanking by entering an incorrect password several times.

Monday to Friday	8 a.m. to 10 p.m.
Saturday and Sunday	9 a.m. to 6 p.m.
Public holidays	See branch for details

Telephone	
– from Switzerland	0844 840 140
– from outside Switzerland	+41 44 293 95 95

E-mail online@zkb.ch

Postal address

Zürcher Kantonalbank
eBanking Support
P.O. Box, 8010 Zurich

02/24 Printed in Switzerland on 100% recycled paper