Zürcher Kantonalbank

Security in digital banking

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 security as well as valuable tips on using your PC or smartphone for digital banking.

1 Digital banking

Means of authentication

You need three identification features to log in:
– your username
– your chosen password
– the ZKB Access App or a ZKB Access reader

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. That is why:
– 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

In digital banking we use the ZKB Access authentication procedure. Dividing the authentication procedure into two channels (smartphone or reader) makes digital banking significantly more secure.

Using digital banking

You do not need to install a program to use digital banking. Simply log in using your browser. Only use the login function on our website. You can find a summary of Zürcher Kantonalbank login portals at zkb.ch/logins. Do not log in to digital banking via search engines such as Google or other websites.

Security certificates

The 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" › "Sicherheitszertifikat überprüfen" to find the latest fingerprint version.

Transaction confirmations (e.g. payment transactions)

Transaction confirmation enhances the security of payment transactions. After entering and verifying a payment, the payment details (payee's account number, currency and amount) are displayed on your ZKB Access device. Only approve the payment if the details match those on the original invoice. If they do not match, cancel the action and contact Support immediately.

2 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. Prevent fraudulent access with the following basic measures, which are very easy to put in place.

General

– 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
– Enable the automatic update function

3 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 password, 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.

4 Code of Conduct

Under no circumstances will we ask you for confidential information (e.g. account number, mobile phone number, user name, passwords, code) by e-mail. Therefore, be critical of e-mails with Zürcher Kantonalbank as the sender: Zürcher Kantonalbank will only communicate with you by e-mail if you expressly wish to do so, for example if you have subscribed to our newsletter. We will also never send you software for you to install by e-mail.

5 Further information

You can find more information on "Security in digital banking" at zkb.ch/sicherheit.

6 Support

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

As a precaution, you can block access 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	0844 840 140
E-mail	online@zkb.ch
Postal address	Zürcher Kantonalbank eBanking Support P.O. Box, 8010 Zurich