



Stay safe when banking online

Our recommendations

Wir begleiten Sie im Leben.

Helping you stay safe when banking online

Banking transactions made via Mobile or E-Banking are highly secure. Zuger Kantonalbank uses state-of-the-art security solutions and adopts high standards which undergo regular external reviews. Even so, fraudsters usually seek to exploit a lack of vigilance by users rather than vulnerabilities in the bank's systems. That's why it's crucial for you to act in a prudent, careful manner.

Our responsibility

- State-of-the-art security and encryption technologies
- Multi-factor login and authorisation procedures
- Regular external awareness-raising and checks

How you can contribute to security

- Protect your access credentials
- Identify any suspicious messages and offers
- Report anything unusual straight away

Common scams and our recommendations

Fraudsters use various methods to access your data.



Phishing e-mails

Check sender and attachments



Phone calls

Never disclose passwords by phone



Unknown links

Don't click on links



Advertising links

Never use search engines to access E-Banking



Social manipulation

Fraudsters masquerade as acquaintances. Be on your guard.



SMS traps

Never pass on codes or respond to callback requests



Fake apps

Always use official app stores



WLAN

Always use secure internet connections



QR codes

Check any links from QR codes carefully



Remote access

Never use remote maintenance software (such as AnyDesk or TeamViewer)

Zuger Kantonalbank will never ask you to disclose your access details via e-mail, SMS or phone.

Security rules – key points at a glance

The following security rules apply regardless of the type of device or operating system – be it a computer, tablet or smartphone. The simple tips below will help you protect your data and money effectively on a day-to-day basis.

1 Always keep your access credentials confidential

Keep your agreement numbers and passwords safe. Always use different, complex passwords to access different services and never disclose them to third parties.

2 Watch out for any suspicious messages or phone calls

Be mindful if you receive unexpected messages or phone calls. Never open any attachments from unknown senders and never click on suspicious links. ZugerKB will never ask you to disclose your access details or ask you to install software.

3 Always use official login pages and apps

Always log in via the official E-Banking website or the official app. Never begin your E-Banking session via a link. Always enter the E-Banking address (URL) manually in your browser. Always install the apps via Apple or Android official app stores.

4 Keep your devices and software up to date

Install updates for your operating system, browser and apps on a regular basis. Always use the latest anti-virus and security programs if possible.

5 Secure network connections

Don't use publicly accessible computers for E-Banking transactions. When you're out and about, always connect your smartphone, tablet or notebook to secure, trustworthy networks.

6 Act immediately if unsure

End the session or conversation if something appears unusual to you. Be particularly cautious if you don't recognise the phone number. Report anything suspicious or fraudulent – we'll be happy to help.

7 Check any two-factor authentication carefully

Check any request for two-factor authentication carefully and only approve actions you have initiated yourself.

What to do in an emergency

What should you do if you suspect fraud?

E-Banking/Mobile Banking

Call our hotline immediately at +41 41 709 11 11.

Outside of office hours you can block E-Banking access yourself by deliberately entering an incorrect password three times.

ZugerKB debit card and credit card

Block your card immediately in ZugerKB E-Banking, Mobile Banking, in the one app or by phone (24/7) at +41 41 709 11 11.

TWINT

Call our hotline (24/7) immediately at +41 41 709 11 11.

Report the incident to the police.

We're here for you

Helping you stay safe online

- We're here to help if you have any questions about online banking.
- Please consult our app or website (www.zugerkb.ch/security) for the latest security information
- More in-depth information can be found at «eBanking but secure!» (www.ebas.ch), the National Cyber Security Centre (www.ncsc.admin.ch) or www.cybercrimepolice.ch
- Contact our hotline if you have any questions or are unsure about something – we'll be happy to help