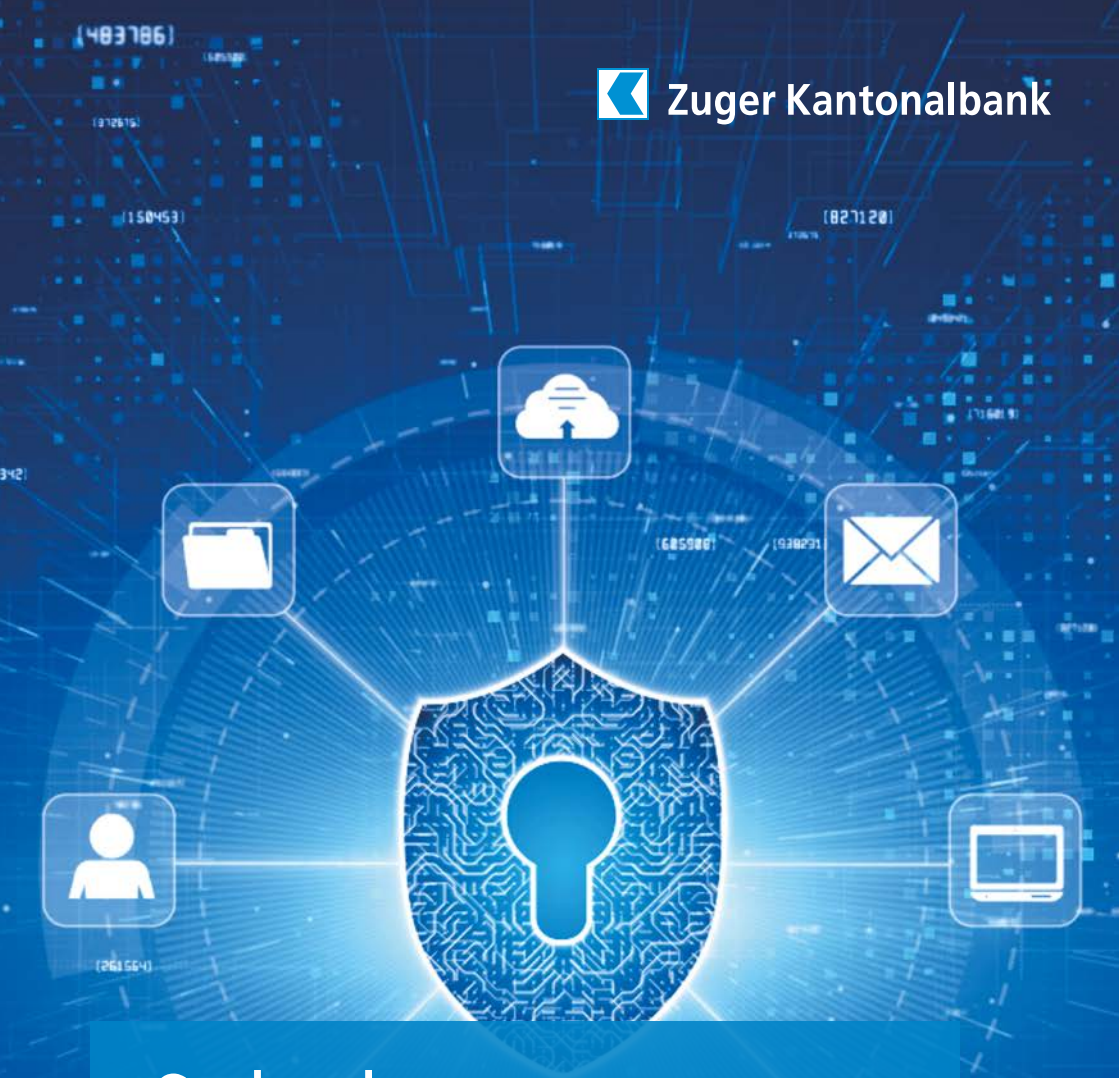
Zuger Kantonalbank



Sicherheit im Digital Banking

Unsere Empfehlungen

Wir begleiten Sie im Leben.

Gemeinsam sicher im digitalen Banking

Bankgeschäfte im Mobile Banking und im E-Banking sind heute sehr gut geschützt. Die Zuger Kantonalbank verwendet modernste Sicherheitslösungen, setzt auf hohe Standards und lässt diese regelmässig extern überprüfen. Betrug zielt jedoch meist nicht auf die Systeme der Bank ab, sondern auf die mangelnde Achtsamkeit der Nutzerinnen und Nutzer. Deshalb ist Ihr wachsames und umsichtiges Verhalten entscheidend.

Unsere Verantwortung

- Moderne Sicherheits- und Verschlüsselungstechnologien
- Mehrstufige Login- und Freigabeverfahren
- Regelmässige externe Sensibilisierungen und Prüfungen

Ihr Beitrag zur Sicherheit

- Zugangsdaten sorgfältig schützen
- Verdächtige Nachrichten und Aufforderungen erkennen
- Ungewöhnliche Vorgänge sofort melden

Die häufigsten Betrugsmaschen und unsere Empfehlungen

Betrügerinnen und Betrüger versuchen über verschiedene Wege, an Ihre Daten zu gelangen.

Phishing-Mail
Absender und Anhänge prüfen

Telefonanruf
Keine Passwörter am Telefon nennen

Unbekannte Links
Links nicht anklicken

Werbelinks
E-Banking nicht über Suchmaschinen aufrufen

Soziale Manipulation
Betrüger geben sich als Bekannte aus. Misstrauisch bleiben.

SMS-Falle
Keine Codes weitergeben oder auf Rückrufwünsche eingehen

Fake-App
Nur offizielle App Stores nutzen

WLAN
Nur sichere Internetverbindungen verwenden

QR-Codes
Links aus QR-Codes kritisch prüfen

Fernzugriff
Keine Fernwartungssoftware (wie AnyDesk oder TeamViewer) nutzen

Die Zuger Kantonalbank wird Sie zu keinem Zeitpunkt per E-Mail, SMS oder Telefon dazu auffordern, Ihre Zugangsdaten bekannt zu geben.

Sicherheitsregeln – das Wichtigste auf einen Blick

Ob Computer, Tablet oder Smartphone: Folgende Sicherheitsregeln gelten unabhängig vom Gerät oder Betriebssystem. Mit den folgenden einfachen Tipps schützen Sie Ihre Daten und Ihr Geld wirksam im Alltag.

1 Zugangsdaten immer vertraulich behandeln

Bewahren Sie Ihre Vertragsnummern und Passwörter sorgfältig auf. Nutzen Sie für unterschiedliche Zugänge jeweils verschiedene, möglichst komplexe Passwörter und geben Sie diese niemals an Dritte weiter.

2 Verdächtige Nachrichten und Anrufe kritisch prüfen

Seien Sie aufmerksam bei unerwarteten Nachrichten und Anrufen. Öffnen Sie keine unbekannten Dateianhänge und klicken Sie nicht auf verdächtige Links. Die ZugerKB wird Sie niemals auffordern, Zugangsdaten preiszugeben oder Software zu installieren.

3 Nur offizielle Login-Seiten und Apps nutzen

Melden Sie sich ausschliesslich über die offizielle E-Banking-Website oder die offizielle App an. Starten Sie Ihre E-Banking-Session niemals über einen Link. Geben Sie die E-Banking-Adresse (URL) immer manuell im Browser ein. Installieren Sie Apps ausschliesslich aus den offiziellen App Stores von Apple und Android.

4 Geräte und Software aktuell halten

Installieren Sie regelmässig Updates für Betriebssystem, Browser und Apps. Verwenden Sie wo möglich aktuelle Virenschutz- und Sicherheitsprogramme.

5 Sichere Netzwerkverbindungen

Erledigen Sie E-Banking-Geschäfte nicht an öffentlich zugänglichen Computern. Verbinden Sie Ihr Smartphone, Tablet oder Notebook unterwegs nur mit sicheren und vertrauenswürdigen Netzwerken.

6 Bei Unsicherheit sofort reagieren

Beenden Sie die Sitzung oder das Gespräch, wenn Ihnen etwas ungewöhnlich erscheint. Seien Sie besonders wachsam, wenn Ihnen die Rufnummer unbekannt ist. Melden Sie den Verdacht oder den Betrug – wir unterstützen Sie gerne.

7 Jede Zwei-Faktor-Authentifizierung genau prüfen

Prüfen Sie jede Aufforderung zur Zwei-Faktor-Authentifizierung sorgfältig und geben Sie ausschliesslich Aktionen frei, die Sie selbst initiiert haben.

Verhalten im Notfall

Was tun bei Betrugsverdacht?

E-Banking/Mobile Banking
Kontaktieren Sie sofort unsere Hotline unter +41 41 709 11 11.
Ausserhalb der Servicezeiten können Sie den E-Banking-Zugang selbst sperren, indem Sie dreimal bewusst ein falsches Passwort eingeben.

ZugerKB Debitkarte und Kreditkarte
Sperren Sie Ihre Karte sofort im ZugerKB E-Banking, im Mobile Banking, in der One App oder telefonisch (24/7) unter +41 41 709 11 11.

TWINT
Kontaktieren Sie sofort unsere Hotline (24/7) unter +41 41 709 11 11.

Wenden Sie sich für die Erstattung einer Anzeige an die Polizei.

Wir sind für Sie da

Gemeinsam für Ihre digitale Sicherheit

- Wir begleiten Sie partnerschaftlich bei allen Fragen zum digitalen Banking
- Nutzen Sie unsere App und die Website (www.zugerkb.ch/sicherheit) für aktuelle Sicherheitshinweise
- Weiterführende Informationen finden Sie auf «eBanking – aber sicher!» (www.ebas.ch), beim Bundesamt für Cybersicherheit (www.ncsc.admin.ch) oder auf www.cybercrimepolice.ch
- Bei Fragen oder Unsicherheiten kontaktieren Sie unsere Hotline – wir helfen Ihnen gerne

Wir begleiten Sie im Leben.

Zuger Kantonalbank

Die Zuger Kantonalbank leistet für die Produktion dieser Broschüre einen finanziellen Klimabeitrag. 8537-0526