

# Sicherheit beim digitalen Banking

## Grundlegende Massnahmen und Regeln

Unsere Standards werden laufend an die neuesten Entwicklungen angepasst und entsprechen den strengen Sicherheitsnormen unserer Branche. Wir geben Ihnen wichtige Informationen zum Thema Sicherheit und wertvolle Tipps für den Einsatz von Computer und Smartphone beim digitalen Banking.



### 1 Digitales Banking

#### Legitimationsmittel

Zum Login ins eBanking benötigen Sie drei Identifikationsmerkmale:

- Ihren Benutzernamen
- Ihr selbst gewähltes Passwort
- die ZKB Access App oder ein ZKB Access Lesegerät

#### Passwort

Das Initialpasswort, das Sie per Post erhalten, muss bei der Aktivierung, also beim ersten Login, zwingend durch ein persönliches, selbst gewähltes Passwort ersetzt werden. Wählen Sie ein Passwort, das Sie sich leicht merken können, aber von anderen nicht erraten werden kann. Es muss mindestens 8 Zeichen umfassen. Kombinieren Sie dabei Buchstaben, Zahlen, Sonderzeichen sowie Gross- und Kleinschreibung. Vermeiden Sie Namen, Telefonnummern, Geburtsdaten, Autokennzeichen usw. Verwenden Sie nicht dasselbe Passwort für verschiedene Zwecke, wie beispielsweise E-Mail, Social Media etc.

#### Aufbewahrung

Niemand ausser Ihnen darf alle drei Identifikationsmerkmale kennen. Darum

- halten Sie Ihr Passwort nirgendwo schriftlich fest.
- bewahren Sie die Geräte für die Legitimation – Mobiltelefon mit ZKB Access App oder ZKB Access Lesegerät – an einem sicheren Ort auf.

#### Legitimationsverfahren

Beim digitalen Banking verwenden wir das Legitimationsverfahren ZKB Access. Die Aufteilung des Legitimationsverfahrens auf zwei Kanäle (Smartphone oder Lesegerät) machen das digitale Banking deutlich sicherer.

#### Digitales Banking nutzen

Für das digitale Banking müssen Sie kein Programm installieren. Sie loggen sich einfach über den Browser ein. Verwenden Sie nur die Login-Funktion auf unserer Webseite. Unter [zkb.ch/logins](https://zkb.ch/logins) finden Sie eine Übersicht über die Logins der Zürcher Kantonalbank. Loggen Sie sich nicht über Suchmaschinen wie Google oder andere Webseiten ins digitale Banking ein.

#### Sicherheitszertifikate

Die Login-Seiten werden durch das TLS-Verfahren mit mindestens 2048-Bit verschlüsselt. Die TLS-Verschlüsselung kennzeichnet der Browser durch ein geschlossenes Schloss. Die Echtheit des Webserver garantieren sogenannte Zertifikate. Die Zürcher Kantonalbank ist aufgrund des im Sicherheitszertifikat enthaltenen Fingerabdrucks eindeutig als Inhaberin der Webseite identifizierbar. Um sicherzustellen, dass Sie sich auf der richtigen Seite befinden, rufen Sie das Sicherheitszertifikat auf und überprüfen den Fingerabdruck. Geben Sie keine Identifikationsmerkmale auf der Login-Seite ein, bevor Sie das Sicherheitszertifikat nicht überprüft haben.

**Hinweis:** Unter [zkb.ch/sicherheit](https://zkb.ch/sicherheit) › [Das können Sie tun](#) › [Sicherheitszertifikat überprüfen](#) finden Sie die aktuelle Version des Fingerabdrucks.

#### Transaktionsbestätigung (z. B. Zahlungsverkehr)

Eine Transaktionsbestätigung erhöht die Sicherheit, zum Beispiel im Zahlungsverkehr. Nach Erfassung und Überprüfung einer Zahlung werden Ihnen die Zahlungsangaben (Kontonummer des Zahlungsempfängers, Währung

und Betrag) auf Ihrem ZKB Access Gerät angezeigt. Geben Sie die Zahlung nur frei, wenn die Angaben mit denjenigen auf der Originalrechnung übereinstimmen. Ist dies nicht der Fall, brechen Sie die Aktion ab und wenden Sie umgehend sich an den Support.



## 2 Schutz für Ihren Computer

Gefahren lauern überall – auch im Internet. Wer seine Daten und seinen Computer aktiv schützt, minimiert das Risiko eines Angriffes erheblich. Mit folgenden grundlegenden Massnahmen, die sehr einfach umzusetzen sind, beugen Sie missbräuchlichen Zugriffen vor.

### Allgemein

- Lesen Sie Warnungen und Meldungen, bevor Sie diese wegeklicken

### Software und Programme

- Benutzen Sie eine Firewall
- Verwenden Sie ein Virenschutzprogramm
- Aktualisieren Sie Ihr Betriebssystem sowie sämtliche auf Ihrem Computer installierte Software regelmässig
- Aktivieren Sie die automatische Update-Funktion



## 3 Schutz für Ihr Smartphone

Smartphones sind ebenso wie Computer den Gefahren des Internets ausgesetzt. Es ist also ratsam, auch hier ein paar grundlegende Massnahmen zu beachten und damit missbräuchlichen Zugriffen vorzubeugen.

### Allgemein

- Aktivieren Sie immer den Sperrcode Ihres mobilen Geräts
- Speichern Sie Ihre Zugangsdaten wie Benutzername und Passwort nicht auf Ihrem mobilen Gerät ab
- Achten Sie darauf, dass Ihnen bei der Eingabe von PIN und Passwort niemand über die Schulter blickt

### Software

Installieren Sie immer die aktuelle Version des Betriebssystems auf Ihrem mobilen Gerät und führen Sie regelmässig Updates durch. Installieren Sie keine Apps aus Ihnen unbekannten, nicht vertrauenswürdigen Quellen.



## 4 Verhaltensregeln

Wir werden von Ihnen unter keinen Umständen vertrauliche Informationen (z. B. Kontonummer, Handynummer, Benutzername, Passwörter, Code) per E-Mail erfragen. Begegnen Sie E-Mails mit dem Absender der Zürcher Kantonalbank deshalb kritisch: Die Zürcher Kantonalbank kommuniziert mit Ihnen nur mittels E-Mail, wenn Sie dies ausdrücklich wünschen, beispielsweise wenn Sie unseren «Eigenheim Newsletter» abonniert haben.

Zudem werden Sie von uns niemals Software zur Installation per E-Mail erhalten.



## 5 Weitere Informationen

Weitere Informationen zum Thema «Sicherheit beim digitalen Banking» finden Sie unter [zkb.ch/sicherheit](https://zkb.ch/sicherheit).



## 6 Support

Bei ungewöhnlichen Fehlern oder Fehlermeldungen, insbesondere im Zusammenhang mit Passwörtern und Codes sowie dem Logout, nehmen Sie bitte sofort Kontakt mit dem Support auf.

Sperren Sie vorsorglich Ihren Zugang durch mehrmalige Eingabe eines falschen Passworts.

|                     |                 |
|---------------------|-----------------|
| Montag bis Freitag  | 08.00–22.00 Uhr |
| Samstag bis Sonntag | 09.00–18.00 Uhr |
| Feiertage           | Sonderregelung  |

|               |                                                  |
|---------------|--------------------------------------------------|
| Telefonnummer | 0844 840 140                                     |
| E-Mail        | <a href="mailto:online@zkb.ch">online@zkb.ch</a> |

|              |                                                                     |
|--------------|---------------------------------------------------------------------|
| Briefadresse | Zürcher Kantonalbank,<br>eBanking Support,<br>Postfach, 8010 Zürich |
|--------------|---------------------------------------------------------------------|