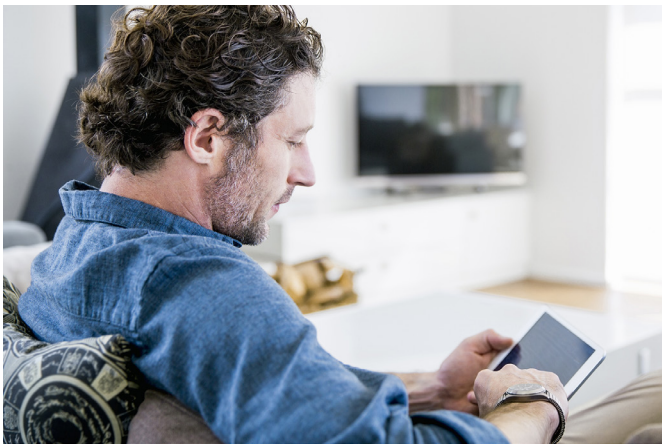
Zürcher Kantonalbank

Sicherheitshinweise für das eBanking

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 «eBanking Sicherheit» und wertvolle Tipps für den Einsatz von Computer und Smartphone beim eBanking.



1 eBanking

Grundlegendes zum eBanking:

Legitimationsmittel

Zum Login ins eBanking benötigen Sie drei Identifikationsmerkmale:
– Ihre persönliche Vertragsnummer
– Ihr selbst gewähltes Passwort
– eine jeweils ändernde Transaktionsnummer

Passwort

Das Initialpasswort, das Sie per Post erhalten, muss bei der Aktivierung, also beim ersten Login, zwingend durch ein persönliches, selbst gesetztes 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 photoTAN App, photoTAN Lesegerät, Mobiltelefon für mTAN an einem sicheren Ort auf.

Legitimationsverfahren

Das eBanking kennt zurzeit die Legitimationsverfahren photoTAN und mTAN. Die zeitnah generierten Transaktionsnummern (TAN) sowie die Aufteilung des Legitimationsverfahrens auf zwei Kanäle (Smartphone oder Lesegerät) machen das eBanking deutlich sicherer.

eBanking nutzen

Mit dem eBanking arbeiten Sie unter Windows oder MacOS ohne vorherige Programminstallation. Sie loggen sich einfach über den Browser ein. Wählen Sie für den direkten Einstieg die Login-Funktion auf unserer Webseite zkb.ch. Loggen Sie sich nicht über andere Webseiten ins eBanking ein.

Sicherheitszertifikate

Die Login-Seite des eBanking wird durch das SSL-Verfahren mit mindestens 248-Bit verschlüsselt. Die SSL-Verschlüsselung kennzeichnet der Browser durch eine Grünfärbung der Adresszeile sowie mit einem geschlossenen Schloss. Die Echtheit des Webservers 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 mit einem Klick auf den grünen Bereich der Adresszeile 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 – Ihr Beitrag finden Sie die aktuelle Version des Fingerabdrucks.

Transaktionsbestätigung

Die Transaktionsbestätigung erhöht die Sicherheit im Zahlungsverkehr. Nach Erfassung und Überprüfung einer Zahlung im eBanking, werden Ihnen die Zahlungsangaben (Teil der Kontonummer des Zahlungsempfängers, Währung und Betrag) je nach Legitimationsverfahren entweder zusammen mit der von Ihrem photoTAN Gerät berechneten TAN angezeigt oder zusammen mit einer TAN auf Ihr Mobiltelefon übermittelt. Geben Sie die Zahlung nur frei, wenn die Angaben mit denjenigen auf der Originalrechnung übereinstimmen. Ist dies nicht der Fall, klicken Sie auf «Abbrechen» und wenden Sie umgehend sich an den eBanking Support.

Tipp: Bestimmen Sie, ob Sie für alle oder nur für einen Teil der Zahlungen eine Transaktionsbestätigung anfordern möchten. Sie können diese Einstellung direkt im eBanking im Menü «Einstellungen» unter «Zahlungsbestätigung TAN» wählen.

2 eBanking Mobile

Zum Login in die App «eBanking Mobile» benötigen Sie zwei Identifikationsmerkmale:
– Ihre persönliche Vertragsnummer
– Ihr selbst gewähltes Passwort

Das Passwort für die Nutzung des eBanking Mobile sollte nicht aufgeschrieben oder abgespeichert werden. Zur zusätzlichen Sicherheit ist eine einmalige Aktivierung der App notwendig. Den dazu benötigten Aktivierungsschlüssel erhalten Sie, sobald Sie im eBanking am Computer im Menü «Service & Kontakt» unter «Zusatzfunktionen verwalten» «eBanking Mobile» die App aktivieren.

3 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.
– Rufen Sie während des Arbeitens mit dem eBanking keine fremden Internetseiten auf.
– Lesen Sie Warnungen und Meldungen bevor Sie diese wegklicken.

Software und Programme

– Installieren Sie eine Firewall
– Verwenden Sie ein Virenschutzprogramm
– Aktualisieren Sie Ihr Betriebssystem sowie sämtliche auf Ihrem Computer installierte Software regelmässig.
– Aktivieren Sie wann möglich immer die automatische Update-Funktion.

4 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.

Generell

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

Wenn Sie sich über den Browser eines Smartphones ins eBanking einloggen und dabei dasselbe Gerät für das mTAN Verfahren einsetzen, verlieren Sie den Sicherheitsvorteil der Nutzung zweier verschiedener Kommunikationskanäle. Benützen Sie daher ausschliesslich die App «eBanking Mobile» für das eBanking auf dem Smartphone.

Software

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

5 Verhaltensregeln

Wir werden von Ihnen unter keinen Umständen irgendwelche vertraulichen Informationen (z.B. Kontonummer, Vertragsnummer, Passwörter, Code) per E-Mail erfragen oder Sie per E-Mail dazu auffordern, einen Link anzuklicken und sich dort anzumelden. 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 irgendwelche Software zur Installation per E-Mail erhalten.

6 Weitere Informationen

Weitere Informationen zum eBanking und zum Thema Sicherheit finden Sie unter zkb.ch/sicherheit.

7 eBanking Support

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

Sperren Sie vorsorglich Ihren eBanking 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	online@zkb.ch
Briefadresse	Zürcher Kantonalbank, eBanking Support, Postfach, 8010 Zürich

06/20 219955 In der Schweiz gedruckt auf 100% Recyclingpapier.