Tipps für Ihre Sicherheit

Bankgeschäfte sicher erledigen

Schwyzer Kantonalbank

Der Umgang mit Debit- und Kreditkarten

Sicherer Umgang mit Debit- und Kreditkarten

- PIN am Bancomaten ändern. Keine leicht zu erratende Zahlenkombination wie Geburtsdatum, Autokennzeichen, Telefonnummer etc. wählen (mind. vier, besser sechs Zahlen).
- PIN nicht notieren.
- PIN nicht an Dritte weitergeben.
- Verlorene oder gestohlene Karte sofort sperren lassen.

Sichere Bargeldbezüge am Bancomaten

- Lassen Sie sich beim Bargeldbezug am Bancomaten nicht ablenken.
- Achten Sie darauf, dass Sie bei der Eingabe des PIN-Codes unbeobachtet sind und geben Sie die PIN geschützt ein (z.B. mit Hand abdecken).
- Stellen Sie eine äusserliche Veränderung am Bancomaten fest oder fallen Ihnen Personen während des Bancomatbezuges negativ auf, melden Sie dies unverzüglich der zuständigen Filiale (ausserhalb der Öffnungszeiten direkt der Polizei). Tätigen Sie keine Transaktionen an diesem Bancomaten.

Sichere Einkäufe mit der Karte

- Karte – wenn möglich – nicht aus der Hand geben.
- PIN geschützt eingeben (z.B. mit Hand abdecken).
- Sie können die Regionen selbstständig in Ihrem E-Banking/Mobile Banking festlegen

Kontaktloses Bezahlen mit der Debit- & Kreditkarte

- Die Karte direkt vor das Kontaktlos-Symbol am Bezahl-Terminal halten.
- Achten Sie auf das optische & akustische Signal zur Bestätigung Ihrer Zahlung.

Geoblocking für Visa Debitkarte

Mit dem Geoblocking können Sie den Einsatz Ihrer Visa Debitkarte geografisch einschränken. Aus Sicherheitsgründen empfehlen wir Ihnen, die Visa Debitkarte jeweils nur für die Regionen zu aktivieren, in welchen Sie die Karte einsetzen.

Karteneinsatz im Internet

Mit Ihrer Kredit- sowie Visa Debitkarte können Sie im Internet bezahlen. Achten Sie auf folgende Punkte, um sicher einzukaufen

- Laden Sie die One App (für Kreditkarte) / debiX+ App (für Visa Debitkarte) herunter und aktivieren die Push-Notification. So haben Sie jederzeit den Überblick über die getätigten Transaktionen. Zudem bietet Ihnen die 3D Secure-Technologie mehr Sicherheit, da Sie beim Einkauf aufgefordert werden, die Zahlung in der App zu kontrollieren und zu bestätigen.
- Kaufen Sie nur bei vertrauenswürdigen Händlern ein (auf SLL-Verschlüsselung achten)
- Klicken Sie nicht auf Links oder öffnen Anhänge, die Ihnen nicht bekannt sind
- Kontrollieren Sie Zahlungsaufforderung und gleichen diese mit Zahlungsempfänger ab
- Geben Sie persönliche Daten nie leichtfertig an Dritte/Unbekannte weiter

Wichtig

- Finanzinstitute informieren nie via E-Mail über ungewöhnliche Kontobewegungen, Karten-transaktionen usw. das sind Phishingmails
- Kontrollieren Sie Kreditkartenabrechnungen und Kontoauszüge regelmässig

Sicherheit E-Banking / Mobile Banking

Computer schützen und Schutz aktuell halten

- Installieren Sie einen Virenschutz und eine Firewall, die Ihren Computer vor Viren und Hackern schützen. Diese sind regelmässig zu aktualisieren.

Passwort

- Ändern Sie das Passwort nach Erhalt und wechseln Sie es alle paar Monate aus.
- Notieren Sie Ihr Passwort nicht, speichern Sie Ihre Zugangsdaten nicht auf Ihrem PC, Tablet oder Smartphone.
- Keine leicht nachvollziehbaren Passwörter wie Geburtsdatum, Autokennzeichen, Telefonnummer etc. wählen.
- Ein sicheres Passwort wählen.

Anmeldung

- Melden Sie sich mit den Zugangsdaten nur über die offizielle Anmelde-Seite der SZKB an.
- Mehr Sicherheit mit der SZKB Secure-App
- Klicken Sie auf keine Links zu Ihrem E-Banking, welche Sie via E-Mail erhalten.
- Die SZKB fordert Sie niemals via E-Mail auf, sich im E-Banking anzumelden. Löschen Sie die entsprechenden E-Mails (Phishing-Mails), ohne die angegebene Internetseite anzuklicken und informieren Sie Ihre SZKB-Filiale.

Abmeldung

- Verlassen Sie das E-Banking immer über den Button «Abmelden».
- Leeren Sie nach dem Verlassen des E-Bankings immer den Browser-Cache

Schutz vor Manipulation

- Schliessen Sie alle Browserfenster vor dem Einloggen auf unserer E-Banking-Startseite.
- Öffnen Sie während Ihrer E-Banking-Session keine zusätzlichen Webseiten.
- Während Sie im E-Banking arbeiten, sollte der Sicherheitsschlüssel in der Statusleiste immer geschlossen sein (verschlüsselte Verbindung).
- Reagieren Sie unter keinen Umständen auf Spam-/Junk-Mails. Denn damit würden Sie bestätigen, dass die E-Mail an eine korrekte Adresse gesandt wurde.
- Deaktivieren Sie die «E-Mail-Vorschau / Autovorschau». Sonst werden die E-Mails schon im Voraus geöffnet, so dass sich allenfalls schädliche Viren auf dem Computer verbreiten können.

Sicherheit im Mobile Banking

- Installieren Sie niemals Apps aus unbekannten oder nicht vertrauenswürdigen Quellen.
- Aktivieren Sie immer den Sperrcode Ihres mobilen Gerätes, so erschweren Sie Unbefugten den Zugriff auf Ihre Daten und Anwendungen.
- Führen Sie keinen «Jailbreak» auf Ihrem Smartphone durch.
- Verwenden Sie auf Ihrem mobilen Gerät immer die neuste verfügbare Systemversion.

Schützen Sie sich vor Phishing

Beim Phishing versuchen Cyberkriminelle durch Betrug, Täuschung oder Irreführung nach Ihren persönlichen Daten zu fischen, bzw. an diese zu gelangen. Der Angriff geschieht oftmals per E-Mail oder telefonisch. Auch SMS, Social Media oder Webseiten sind mögliche Kanäle.

- Kontrollieren Sie Absender und Inhalt von E-Mails auf deren Plausibilität
- Überprüfen Sie Links auf verdächtige Bezeichnungen (mit Maus über den Link fahren)
- Ignorieren Sie dringliche Anweisungen, bestimmte Handlungen auszuführen
- Verwenden Sie verschiedene Passwörter und wechseln Sie diese regelmässig
- Geben Sie persönliche Daten wie Karten-Nr., PIN-Code, Sicherheitscode und persönliche Passwörter oder auch Codes, welche auf Ihr Mobiletelefon gesendet werden, nie an Dritte/Unbekannte weiter

Mehr unter
www.szkb.ch/sicherheit
www.ebankingabersicher.ch

SZKB 11.2025

Schwyzer Kantonalbank
+41 58 800 20 20
kundenzentrum@szkb.ch
www.szkb.ch

Gut beraten, Schwyzer Art.

Schwyzer Kantonalbank