Merkblatt

BANK EKI
Interlaken 1852

Sicher unterwegs im neuen Digital Banking

Cyberkriminelle entwickeln stetig neue Methoden, um an persönliche Daten und letztlich auch an Geld zu gelangen. Mit einigen einfachen, aber wirksamen Massnahmen können Sie Ihr E- und Mobile Banking schützen und Ihre Bankgeschäfte auch weiterhin sicher und flexibel erledigen.

Wir tun alles für Ihre Sicherheit

Die Bank EKI investiert viel in Sicherheitssysteme – von verschlüsselten Verbindungen über Firewalls bis hin zu automatisierten Betrugserkennungen. So auch mit der Einführung des neuen Digital Banking und der Zwei-Faktoren-Verifizierung via Mobile Banking App. Doch genauso wichtig ist Ihr eigenes Verhalten. Achten Sie stets auf ungewöhnliche Kontoaktivitäten, überprüfen Sie regelmässig Ihre Transaktionen und **melden Sie Auffälligkeiten sofort.** Gemeinsam lässt sich das Risiko auf ein Minimum reduzieren.

Typische Gefahren

Im Alltag begegnen Bankkundinnen und -kunden diverse Bedrohungen. Das Wissen um diese Risiken ist der erste Schritt zu mehr Sicherheit:

- **Phishing und gefälschte Webseiten**: Betrüger verschicken E-Mails oder SMS mit gefälschten Links, die auf täuschend echt aussehende Websites führen. Ziel ist es, an Ihre Zugangsdaten zu gelangen: Professionell nachgebaute Bank-Webseiten sollen Sie dazu verleiten, Ihre Log-in-Daten preiszugeben. Nutzen Sie für den Login in unser E-Banking jeweils nur unsere Seite www.bankeki.ch.

- **Malware wie Viren oder Trojaner:** Schadprogramme auf dem Computer oder dem Smartphone können Daten abfangen oder Tastatureingaben auslesen.

- **Social Engineering:** Kriminelle geben sich telefonisch oder online als Bankmitarbeitende aus, um Sie zur Herausgabe sensibler Informationen zu bewegen. **Die Bank EKI fordert Sie nie per Telefon oder E-Mail auf, Passwörter, Codes oder andere vertrauliche Angaben anzugeben**. Seien Sie daher besonders misstrauisch, wenn eine Nachricht Dringlichkeit signalisiert («Ihr Konto wird gesperrt, wenn …»). Öffnen Sie keine Links oder Anhänge aus verdächtigen Nachrichten. Im Zweifel: Löschen oder direkt bei Ihrem Kundenberater nachfragen.

Ihre Geräte aktuell halten

Eine der wichtigsten Schutzmassnahmen ist, Computer, Smartphone und Tablet stets auf dem neuesten Stand zu halten. Betriebssysteme, Virenschutz und Banking-App sollten regelmässig aktualisiert werden. Sicherheitslücken werden so geschlossen, bevor Angreifer sie ausnutzen können. Aktivieren Sie automatische Updates, wo immer möglich. Auch regelmässige Backups erhöhen die Sicherheit.

Die wichtigsten Tipps in Kürze

- **Sichere Passwörter wählen** (Nutzen Sie keine naheliegenden Wörter und verwenden Sie Sonderzeichen)
- **Vorsicht bei unbekannten Nachrichten** (Öffnen Sie keine unbekannten SMS, WhatsApp und E-Mails)
- **Aktueller Virenschutz** (Halten Sie Ihre Antivirenprogramme auf dem neuesten Stand)
- **Sorgfältige Prüfung von Zugriffsanfragen / Freigaben** (Seien Sie immer sehr kritisch)
- **Unbekannte Kontakte blockieren** (Lehnen Sie Kontaktversuche von Unbekannten konsequent ab)

Sie haben Zweifel?

Kontaktieren Sie uns umgehend über unsere Hauptnummer (033 826 17 71) und lassen Sie sich nie von Anrufern unter Druck setzen.

Weitere Informationen

Sind Sie gewappnet gegen die Gefahren aus dem Netz? «eBanking – aber sicher!» ist eine unabhängige Plattform der Hochschule Luzern – Informatik, die Sie dabei unterstützt, Ihre persönliche Informationssicherheit wahrzunehmen. Auf der Website **www.ebankingabersicher.ch** finden Interessierte praxisnahe Informationen zu notwendigen Massnahmen und Verhaltensregeln für eine sichere Anwendung von E-Banking-Applikationen.