

Sicherheit und Diskretion im Internet

5 Schritte für Ihre IT-Sicherheit

- 1. Sichern** Regelmässig Backup erstellen
- 2. Schützen** Virenschutz installieren und regelmässig aktualisieren
- 3. Überwachen** Firewall einsetzen (überprüft den eingehenden und ausgehenden Datenverkehr)
- 4. Vorbeugen** Software-Updates bei allen installierten Programmen ausführen (täglich werden Sicherheitslücken und Schwachstellen gefunden und optimiert)
- 5. Aufpassen** Persönliches Verhalten, Eigenverantwortung wahrnehmen

E-Mails

Öffnen Sie keine E-Mail unbekannter Herkunft oder mit nicht erwarteten Anhängen. Seien Sie vorsichtig beim Anklicken von Links. Misstrauen Sie einer E-Mail lieber einmal zu viel als zu wenig.

E-Banking

Anmeldung im E-Banking

Beenden Sie sämtliche Aktivitäten im Internet, bevor Sie sich im E-Banking der Bank EKI anmelden. Melden Sie sich bitte immer über den dafür vorgesehenen Link auf der [Webseite der Bank EKI \(www.bankeki.ch\)](http://www.bankeki.ch) an. Wenden Sie sich bei Unregelmässigkeiten und ungewohnten Vorgängen bei Ihrer E-Banking Sitzung sofort an Ihre Bank.

9 Regeln für ein sicheres Passwort

1. Mindestens 10 (maximal 50) Zeichen lang
2. Muss eine Kombination aus Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen sein. Zum Beispiel einen Satz definieren und die ersten Buchstaben der Wörter als Passwort merken: [Der Winter im Jahr 2018 war durchgezogen!](#) = DWij2018wd!
3. Keine Leerzeichen verwenden
4. Keine Tastaturfolgen wie z. B. «asdfgh» oder «45678»
5. Kein Wort einer bekannten Sprache, d. h. das Passwort sollte keinen Sinn machen
6. Nicht überall das gleiche Passwort
7. Passwort nirgends aufschreiben oder unverschlüsselt abspeichern
8. Darf kein bereits verwendetes Passwort sein
9. Verwenden Sie keine 3-fachen Wiederholungen von Zahlen, Sonderzeichen oder Buchstaben wie z. B. «111» oder «???»

Zahlungen

Überprüfen Sie nach der Erfassung von Zahlungsdaten nochmals deren Korrektheit online im Menü «Zahlungen/pendent Zahlungen».

Transaktionssignierung

Die Transaktionssignierung schützt Sie vor unbeabsichtigten Zahlungen an Dritte. Hierbei findet für bestimmte Zahlungsempfänger eine Datenüberprüfung statt. Sobald Sie eine entsprechende Zahlung erfassen und ausführen, müssen Sie die Daten mittels Bank EKI Mobile App überprüfen und bestätigen. Erst nach Eingabe des Bestätigungscode wird Ihre Zahlung zur Ausführung freigegeben. Die Transaktionssignierung erfolgt nach Kriterien, die aus Sicherheitsgründen nicht kommuniziert werden.

Abmelden

Melden Sie sich immer mit «Logout» ab, wenn Sie Ihren E-Banking Account verlassen wollen. Leeren Sie den Cache des Browsers nach dem «Logout». In den gängigsten Browsern finden Sie die Option zum Löschen des Browserverlaufs zum Beispiel unter dem Menü: Extras > Browserverlauf löschen > Temporäre Internet- und Websitedateien markieren > Cookies und Websitedaten markieren > löschen. Mehr Informationen und Anleitungen für die Löschung des Verlaufs finden Sie im Internet.

«E-Banking – aber sicher. Sicherheit und Diskretion haben höchste Priorität.»

Christine Bärtschi
Stv. Leiterin Zahlungsverkehr

Sparen	mehr Zins
+ Zahlen	spesenfrei zahlen
+ Anlegen	mehr Ertrag
+ Finanzieren	Bonus für Sie
+ Vorsorgen	Ruhestand geniessen
+ Versichern	optimal versichert
= 6 Vorteile	= Ihr Gesamtnutzen



Phishing

Was ist Phishing (Phishing-Mails) und wie schütze ich mich davor?

Beim klassischen Phishing versuchen Angreifer, potentielle Opfer mithilfe von gefälschten E-Mails auf gefälschte Webseiten zu locken und auf diese Weise dazu zu bringen, auf den gefälschten Webseiten ihre Anmeldeinformationen (z.B. Vertragsnummer, Passwort) einzugeben. Mit den ausspionierten Anmeldeinformationen versuchen sich die Angreifer auf Kosten der Opfer (Kunden der angegriffenen Online-Dienstleister) zu bereichern.

Prävention durch richtiges Surfverhalten

- Nie einen Link verwenden, der per E-Mail zugeschickt wurde, um sich bei einem Finanzinstitut anzumelden. Ebenso wenig dürfen Felder in Formularen, die per E-Mail zugestellt wurden und zur Eingabe von Anmeldeinformationen auffordern, ausgefüllt werden. [Die Bank EKI Genossenschaft verschickt nie solche E-Mails.](#)
- Die sichere Navigation zur E-Banking Login-Seite der Bank EKI Genossenschaft erfolgt über den dafür vorgesehenen Link auf der Webseite der Bank EKI (www.bankeki.ch).

Social Engineering

Wie sehen mögliche Social Engineering Angriffe aus?

- Eine Person gibt sich als Techniker aus (z.B. Telefongesellschaft, Elektrizitätswerk etc.) und versucht so Zugang in Ihr Haus oder ins Unternehmen zu erlangen.
- Eine Person ruft Sie an und gibt vor eine Umfrage durchzuführen, um an sensitive Informationen (z.B. zum Einkommen, zu Sicherheitsmassnahmen usw.) zu gelangen.
- Zu Ihrem Arbeitsplatz kommt eine Person, die sich als Informatiker ausgibt und Ihnen vorgaukelt, an Ihrem PC Wartungsarbeiten verrichten zu müssen.

Alle Angriffe haben zum Ziel Ihnen persönliche oder vertrauliche Informationen (z. B. Zugangsdaten, Passwörter usw.) zu entlocken, um diese dann unbefugt einzusetzen.

Tipps zu Ihrem Schutz:

- Geben Sie möglichst wenig persönliche Informationen über sich preis. Insbesondere in sozialen Netzwerken wie Facebook usw. sollten Sie sparsam damit umgehen.
- Geben Sie Ihre Passwörter grundsätzlich **nie** einer anderen Person bekannt. Auch nicht einem Systemadministrator oder Vorgesetzten. Ein Passwort gehört **nur** Ihnen!
- Beurteilen Sie Anfragen per E-Mail kritisch. Auch E-Mails von bekannten Absendern können gefälscht sein und Ihnen sensitive Daten entlocken.
- Öffnen Sie Attachements in E-Mails nur dann, wenn Ihnen der Absender persönlich bekannt ist.
- Wenn Sie mit der Maus über einen Link fahren (**nicht klicken!**), können Sie die Webseite sehen, auf die Sie beim Klicken gelangen würden.

Die wichtigsten Tipps in Kürze

- **Sichere Passwörter wählen** (Nutzen Sie keine naheliegenden Wörter und verwenden Sie Sonderzeichen)
- **Vorsicht bei unbekanntem Nachrichten** (Öffnen Sie keine unbekanntem 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 Unbekanntem konsequent ab)

Weitere Informationen zur Sicherheit im E-Banking finden Sie unter:

E-Banking – aber sicher! www.ebankingabersicher.ch

BANK EKI Genossenschaft	Geschäftsstellen
Rosenstrasse 1 3800 Interlaken	Grindelwald T 033 853 29 70
T 033 826 17 71 F 033 826 17 79	Lauterbrunnen T 033 855 36 55
info@bankeki.ch www.bankeki.ch	Wilderswil T 033 823 10 70