BANK EKI

Interlaken 1852

E-Banking der Bank EKI

Anleitungen, Tipps und Informationen

Neuregistrierung für E-Banking

Voraussetzung für die Neuregistrierung für das E-Banking

- E-Banking Vertragsnummer
- E-Banking Passwort
- Airlock 2FA App (erhältlich in Ihrem Playstore oder App-Store)

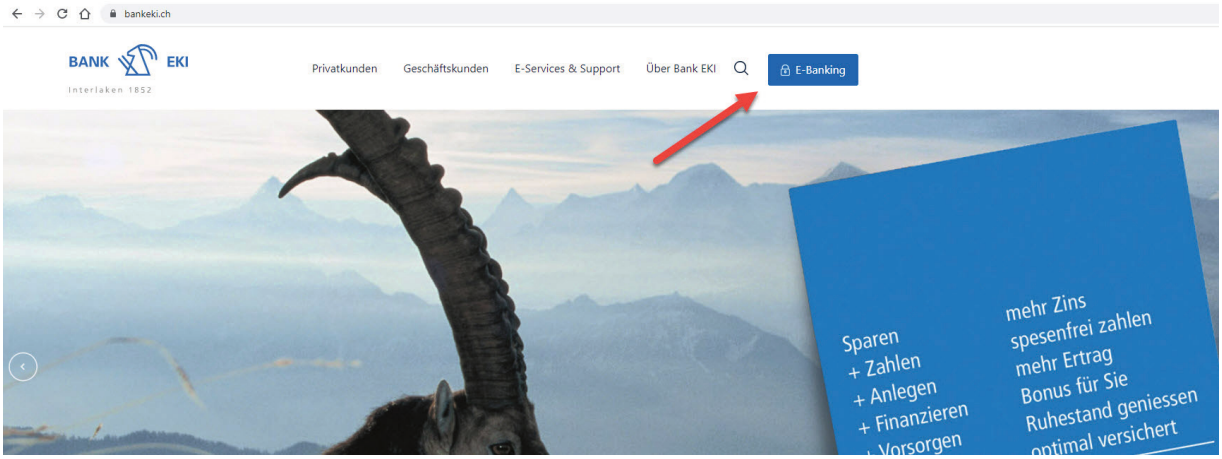
Available on the App Store

GET IT ON Google play

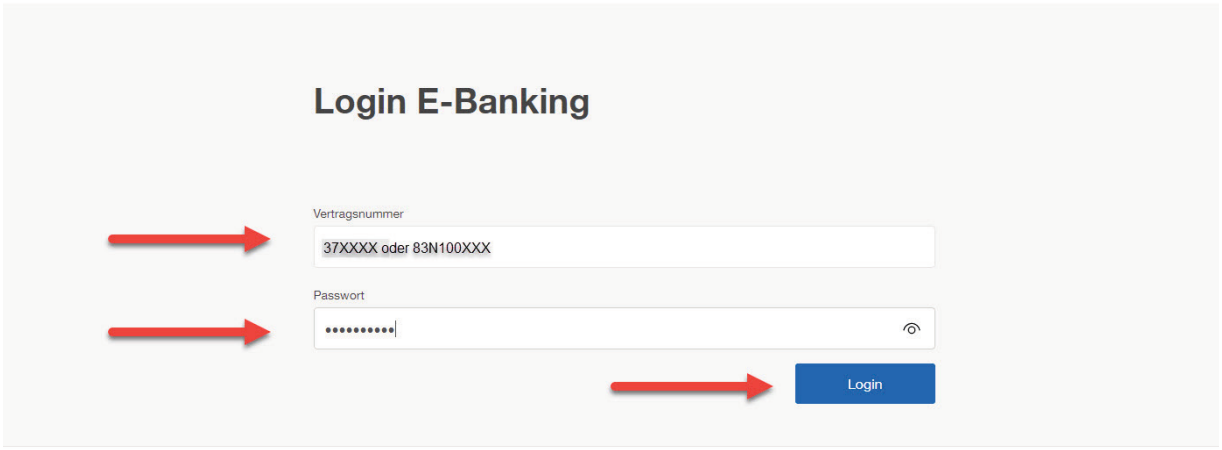
Download from Windows Phone Store

Aktivierung und Installation

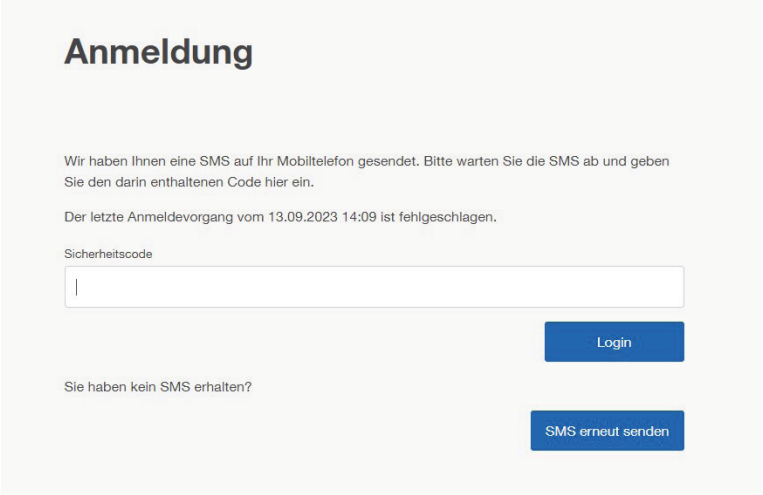
1. Einstieg ins E-Banking Portal auf der Webseite der Bank EKI (www.bankeki.ch)



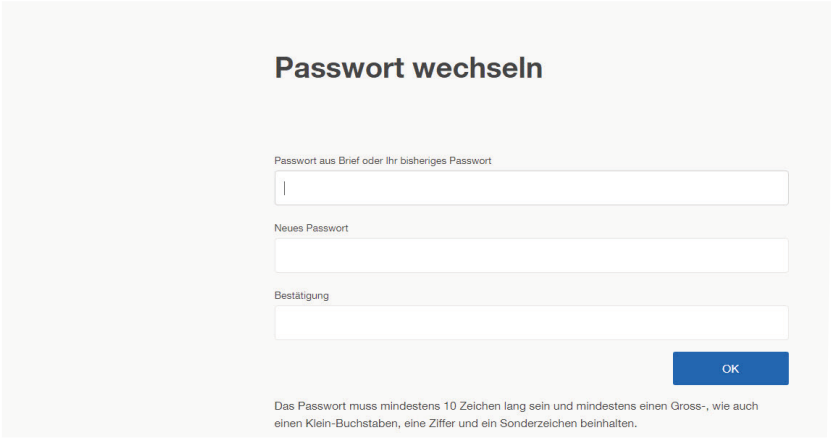
2. Eingabe Ihrer persönlichen Vertragsnummer und des Einstiegspassworts aus dem von uns zugestellten Passwortbrief.



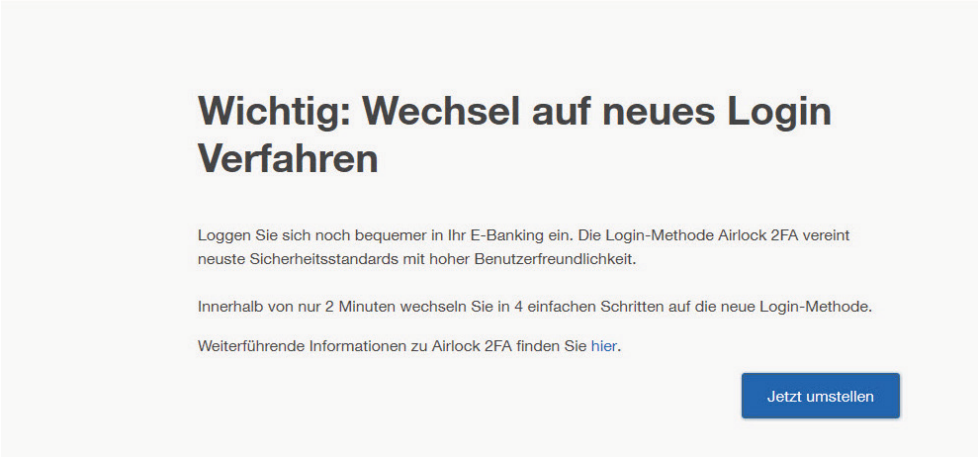
3. Sie erhalten einen SMS-Sicherheits-Code auf Ihr Smartphone, welchen Sie eingeben können.



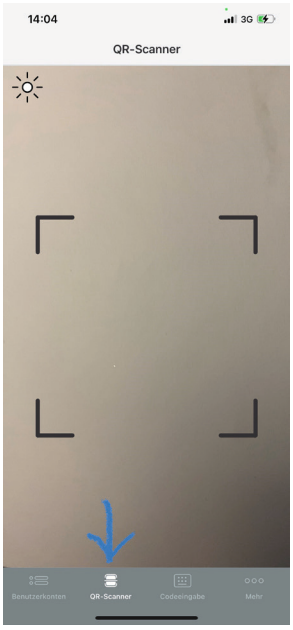
4. Sie werden nun aufgefordert, ein neues persönliches Passwort zu erstellen. Beachten Sie bitte die Standardanforderungen an das Passwort.

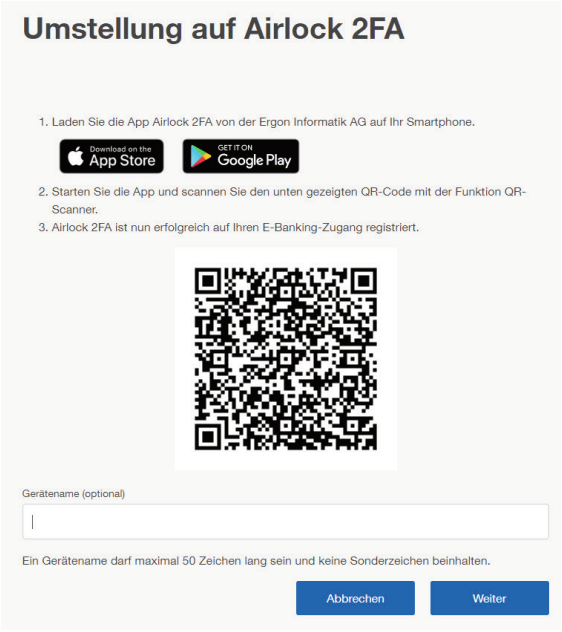


5. Sie werden nun vom System aufgefordert, auf das Loginverfahren Airlock2FA zu wechseln. Klicken Sie dazu auf «Jetzt umstellen».

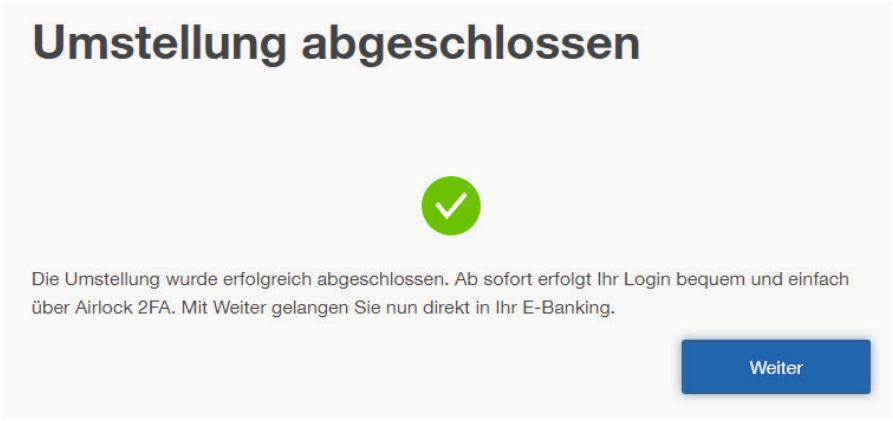


6. Öffnen Sie die Airlock2FA App auf Ihrem Smartphone und scannen Sie den QR-Code auf Ihrem PC-Bildschirm und bestätigen Sie auf dem Bildschirm mit «Weiter».





7. Nun erscheint die folgende Benachrichtigung auf Ihrem PC. Bestätigen Sie diese mit Klick auf «Weiter».



8. Gratulation! Sie haben die Aktivierung erfolgreich abgeschlossen und nutzen nun das E-Banking der Bank EKI Genossenschaft mit dem neuen Loginverfahren Airlock2FA! Beachten Sie bitte, dass Sie bei jedem Login dazu aufgefordert werden im Airlock2FA auf dem Smartphone Ihre Anmeldung mittels Face ID oder Handy Passwort zu bestätigen.

Übrigens:
Haben Sie ein neues Handy und können sich nicht mehr im E-Banking einloggen? Dann schreiben Sie uns eine E-Mail an info@bankeki.ch und geben Sie uns Ihre aktuelle Telefonnummer an.

Funktionen im E-Banking

Unter den Einstellungen im E-Banking finden Sie folgende Funktionen:

Monatlicher Freibetrag ohne Transaktionssignierung

Legen Sie einen Freibetrag fest, bis zu welchem Sie Zahlungen aus dem E-Banking nicht per Transaktionssignierung bestätigen möchten. Der Betrag gilt pro Vertrag und Monat für alle manuell erfassten Zahlungen an bisher unbekannte Empfänger. Sie können eine maximale monatliche Limite bis CHF 5'000 erfassen. Die Änderung des Freibetrags gilt automatisch für jeden Monat und liegt in Ihrer Verantwortung. Wenn Sie keinen Freibetrag einstellen, muss jede Zahlung an einen unbekannten Empfänger signiert werden.

Beispiel: Sie haben einen monatlichen Freibetrag von CHF 1'000 erfasst.

Datum	Betrag	Aktivität
1.03.	CHF 1'000	Erfassung monatlicher Freibetrag
2.03.	- CHF 600	**1. Zahlung:** Erfassung Zahlung an einen neuen Begünstigten Zahlung muss nicht signiert werden, da monatlicher Freibetrag ausreichend.
2.03.	**= CHF 400**	Verfügbarer monatlicher Freibetrag
10.03.	- CHF 600	**2. Zahlung:** selber Empfänger wie am 02.03. Zahlung muss nicht signiert werden, da gleicher Empfänger.
10.03.	**= CHF 400**	Verfügbarer monatlicher Freibetrag
11.03.	- CHF 150	**3. Zahlung:** Erfassung neue Zahlung an neuen Begünstigten. Zahlung muss nicht signiert werden, da monatlicher Freibetrag ausreichend.
11.03.	**= CHF 250**	Verfügbarer monatlicher Freibetrag
25.03.	- CHF 150	**4. Zahlung:** Selbe Zahlung wie am 11.03. Zahlung muss nicht signiert werden, da gleicher Empfänger.
25.03.	**= CHF 250**	Verfügbarer monatlicher Freibetrag
1.04.	CHF 1'000	Monatlicher Freibetrag wird zu Beginn des Monats wieder zurückgestellt.

Geografische Zulassung von Zahlungen

Legen Sie fest, in welche Ländergruppen Sie Auslandzahlungen erlauben wollen. Sie können bestimmte Regionen für Zahlungen sperren, befristet zulassen oder auf unbestimmte Zeit zulassen. Falls Sie ausnahmsweise eine Zahlung in eine gesperrte Region tätigen möchten, wird Ihnen nach dem Klick auf «Überweisen» eine Hinweismeldung angezeigt. Sie können via «Einstellungen anpassen» eine Änderung der zugelassenen Regionen vornehmen.

Automatische Sperrung von Regionen: Wenn eine Region (ausgenommen Schweiz und Europa) über ein Jahr ungenutzt freigeschaltet bleibt, wird diese automatisch durch die Bank gesperrt.

Geographische Zulassungen von Karten

Mit Geoblocking erhalten Sie automatisch einen wirksamen Schutz gegen Skimming. Ihre Debit-Mastercard der Bank EKI können Sie weltweit einsetzen. Zu Ihrer Sicherheit ist die Karte allerdings standardmässig nur in der Schweiz und in Europa freigeschaltet. Eine Änderung der entsprechenden Ländergruppen können Sie ebenfalls schnell und einfach direkt im E-Banking via «Einstellungen > Sicherheit > Karten > Geografische Zulassung von Karten» vornehmen.

Neuregistrierung für Mobile Banking

Voraussetzung für die Neuregistrierung für das Mobile Banking

- E-Banking Vertragsnummer
- E-Banking Passwort
- Bank EKI Mobile Banking App (Verfügbar in Ihrem Playstore oder App-Store)

Available on the App Store | GET IT ON Google play | Download from Windows Phone Store

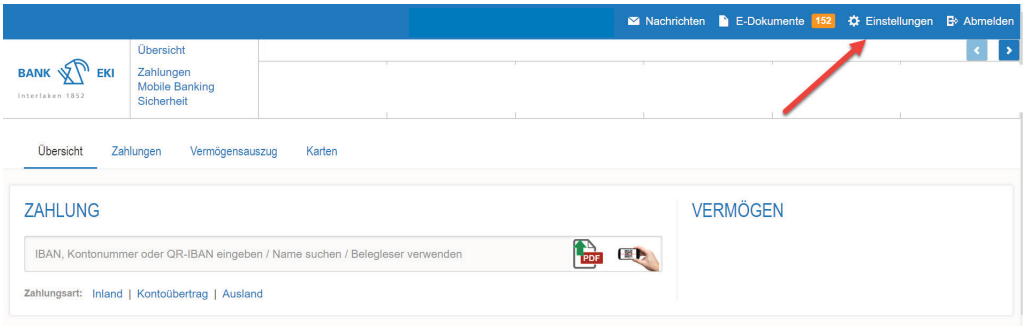
Wichtig

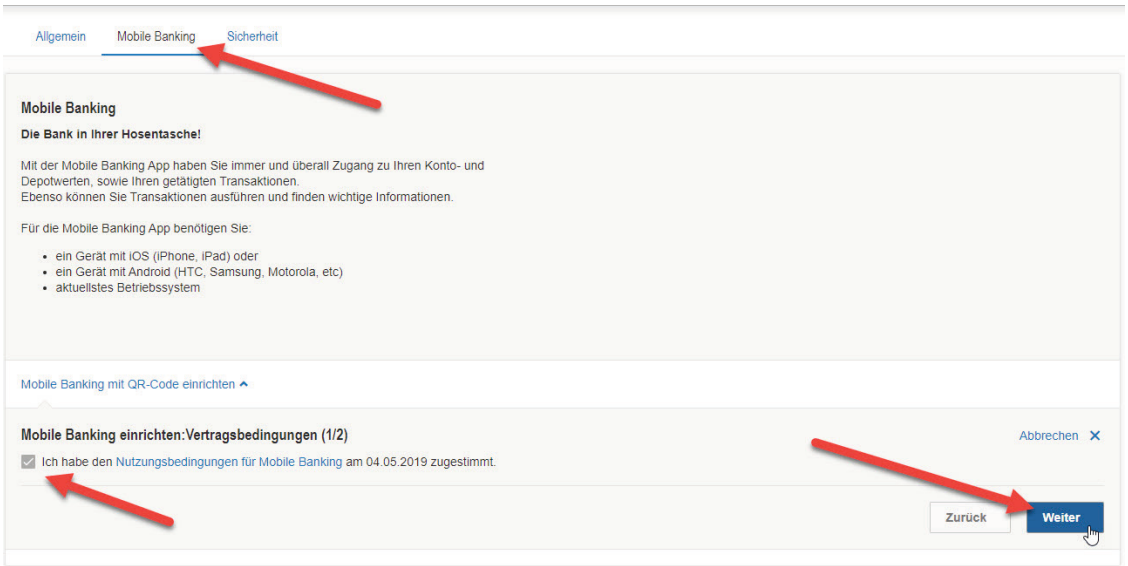
Die Registrierung für die Mobile Banking App kann erst nach erfolgreicher Registrierung im E-Banking vorgenommen werden!

Aktivierung und Installation

1. Loggen Sie sich am Computer mit Ihrer Vertragsnummer und Passwort im E-Banking der Bank EKI ein.

2. Begeben Sie sich zu den Einstellungen und anschliessend in die Rubrik «Mobile Banking».

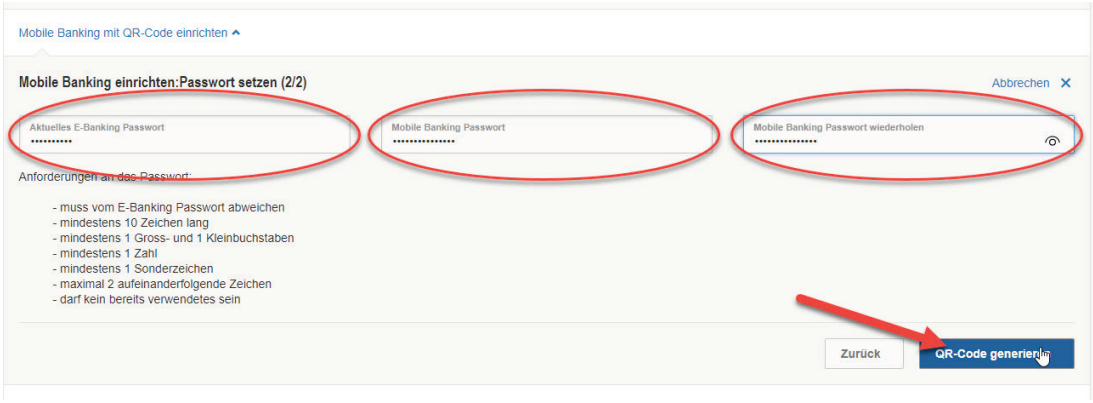




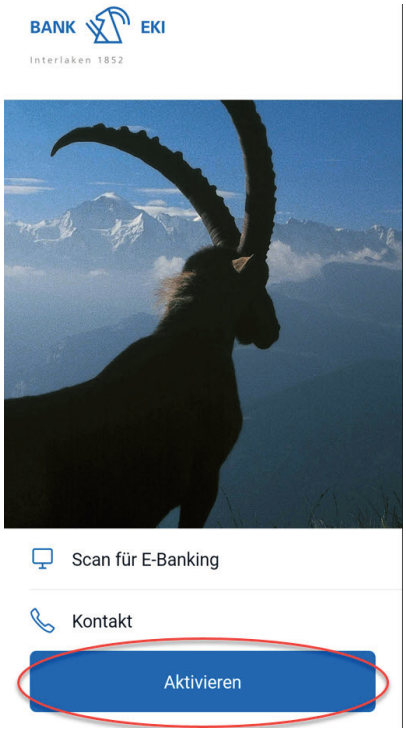
3. Klicken Sie auf «Mobile Banking mit QR-Code einrichten» und akzeptieren Sie unsere Nutzungs- und Vertragsbedingungen. Klicken Sie anschliessend auf «Weiter».

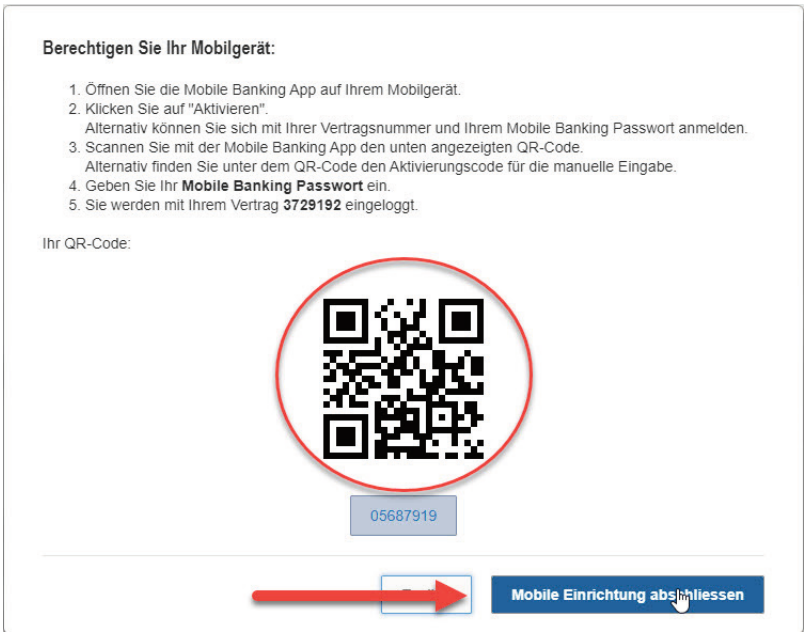
4. Erstellen Sie nun ein neues Passwort für das Login Ihres neuen Mobile Bankings. WICHTIG! Das Passwort für das Mobile Banking muss von Ihrem bestehenden E-Banking Passwort abweichen. Beachten Sie zudem die Standardanforderungen an das Passwort.

- Geben Sie zuerst Ihr bestehendes Passwort für Ihr Login ins E-Banking ein
- Geben Sie nun ein neues Passwort für das Mobile Banking ein
- Verwenden Sie keine 3-fachen Wiederholungen von Zahlen, Sonderzeichen oder Buchstaben wie «111»
- Bestätigen Sie das neue Mobile Banking Passwort mit der erneuten Eingabe und Klick auf «QR-Code generieren»



5. Nehmen Sie Ihr Smartphone zur Hand. Öffnen Sie die Bank EKI Mobile Banking App und scannen Sie den QR-Code mittels «Aktivieren» auf Ihrem PC-Bildschirm.





6. Die App fordert Sie nun dazu auf, Ihr neu erstelltes Passwort einzugeben.

7. Gratulation! Sie haben die Aktivierung erfolgreich abgeschlossen und nutzen nun das Mobile Banking der Bank EKI Genossenschaft.

Scanning QR-Rechnungen via Smartphone

Voraussetzung für das Scanning via Smartphone

- E-Banking Vertragsnummer
- E-Banking Passwort
- Bank EKI Mobile Banking App (Verfügbar in Ihrem Playstore oder App-Store)

Available on the App Store

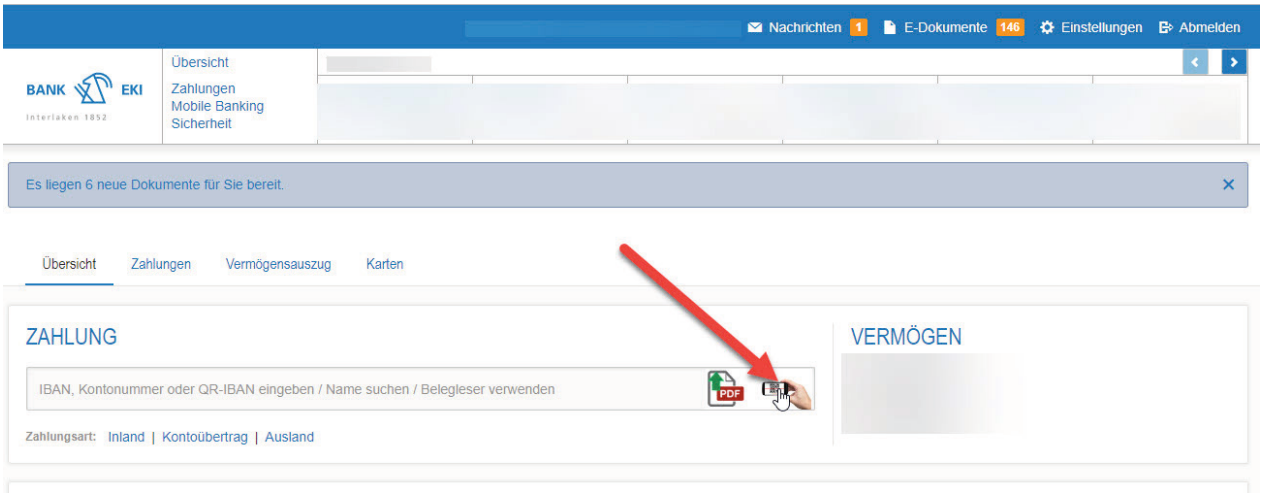
GET IT ON Google play

Download from Windows Phone Store

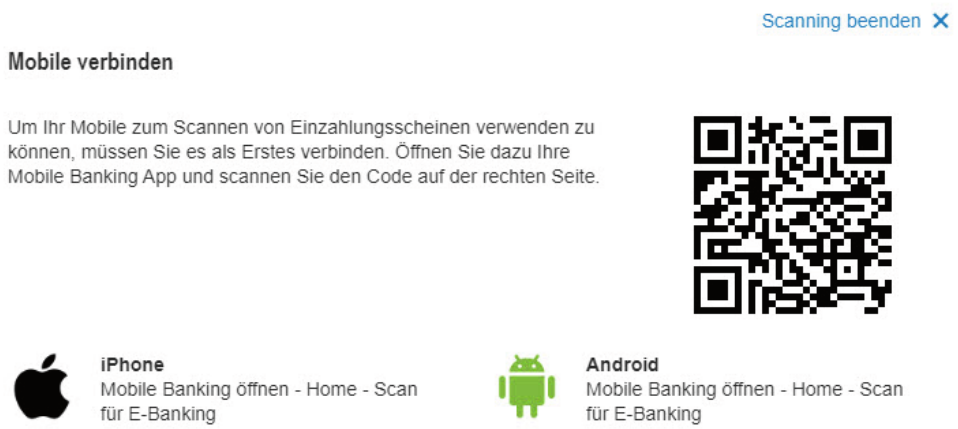
Ablauf

1. Loggen Sie sich am Computer mit Ihrer Vertragsnummer und Ihrem Passwort am Computer ins E-Banking der Bank EKI ein.

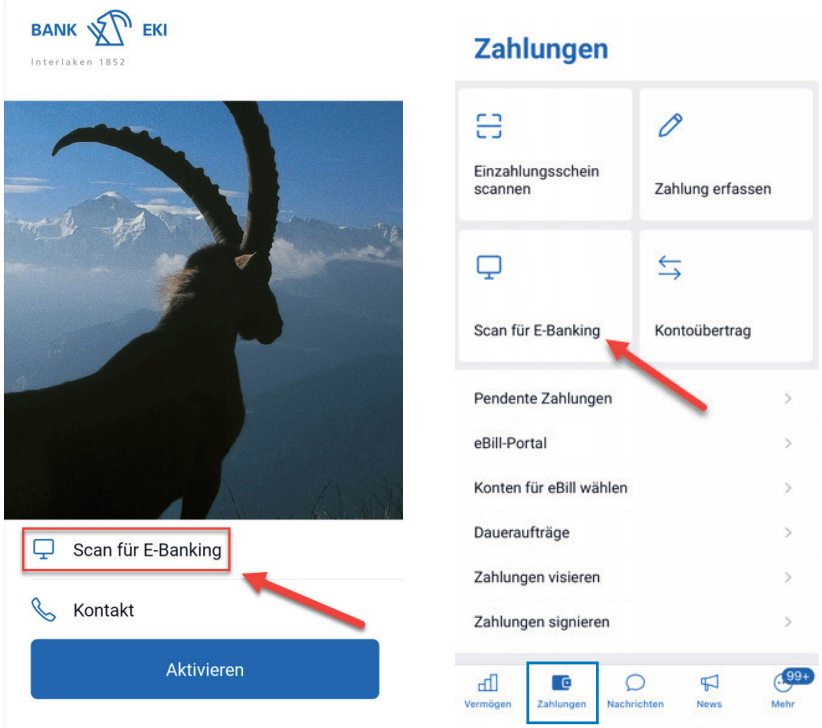
2. Anschliessend klicken Sie auf das Scanning-Symbol auf der Startseite.



3. Es erscheint Ihnen folgendes Fenster:



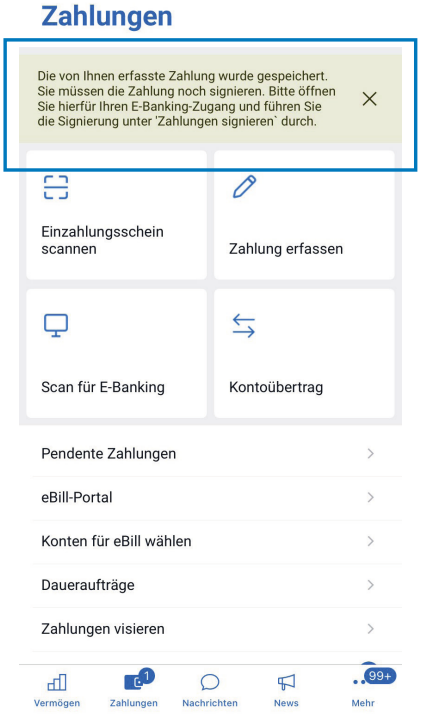
4. Nehmen Sie nun Ihr Smartphone zur Hand und öffnen Sie die Bank EKI Mobile Banking App. Klicken Sie auf die Taste «Scan für E-Banking» (Bild links) oder in der Menüleiste auf «Zahlungen» und danach auf «Scan für E-Banking» (Bild rechts) und scannen Sie den QR-Code auf Ihrem Computer-Bildschirm (siehe vorheriges Bild).



5. Gratulation! Ihr Smartphone ist jetzt mit Ihrem E-Banking verbunden und Sie können Ihre Einzahlungsscheine bequem einscannen. Am Computer können sie anschliessend die Zahlungen bearbeiten und abschliessen.

Übrigens:

Falls Sie das Mobile Banking App der Bank EKI bereits eingerichtet haben, können Sie die QR-Rechnungen direkt unter «Zahlungen > Einzahlungsscheine scannen» einscannen und bezahlen. Beachten Sie den Hinweis, ob die Zahlung signiert werden muss (siehe Bild) und vergessen Sie nicht diese im E-Banking am Computer unter «Zahlung freigeben» zu visieren.



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) 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 durchzogen! = 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».

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 Airlock2FA App überprüfen und bestätigen. Erst nach Eingabe des Bestätigungscodes 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». Beim Microsoft Internet Explorer (IE 11) finden Sie diesen zum Beispiel unter dem Menü: Extras > Browserverlauf löschen > Temporäre Internet- und Websitedateien markieren > Cookies und Websitedaten markieren > löschen. Verfügen Sie über einen anderen Browser? Mehr Informationen und Anleitungen für die Löschung des Verlaufs finden Sie im Internet.

Phishing

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

Beim klassischen Phishing versuchen Angreifer, potentielle Opfer mithilfe von gefälschten E-Mails aufgefälschte 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 Engeneering 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, Xing 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.

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

E-Banking – aber sicher! www.ebas.ch

BANK EKI

Interlaken 1852

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

gültig ab 1.1.2024