PRIVAT BANK
der Raiffeisenlandesbank OÖ

SICHERHEIT IM ONLINE UND MOBILE BANKING

Tipps zu sicheren Bankgeschäften im Internet

Der Zugriff auf Ihre Konten über Ihr Online und Mobile Banking ist technisch mit den besten verfügbaren Systemen abgesichert. Damit diese Wirkung zeigen können, sollten auch Sie als Nutzer:in entsprechende Vorkehrungen für Ihr Online Banking auf Ihrem Rechner und am Smartphone treffen. Lesen Sie hier unsere Sicherheitstipps.

Das Wichtigste im Überblick:

- Geben Sie Ihre Zugangsdaten (PIN, Signatur-Code, TAN) niemals an Dritte weiter! Die Bank wird Sie NIEMALS dazu auffordern, Zugangsdaten bekannt zu geben.
- Achten Sie auf Sicherheitsmerkmale und nutzen Sie unsere sicheren Autorisierungsverfahren.
- Erkennen Sie Phishing-Versuche! Rufen Sie Mein ELBA nur direkt über https://mein.elba.raiffeisen.at auf.
- Vorsicht vor Schadprogrammen! Halten Sie Ihre Systeme aktuell und installieren Sie nur Software aus vertrauenswürdigen Quellen.
- Nutzen Sie die Mailbox für die sichere Kommunikation mit der Bank.
- Auffälligkeiten? Kontaktieren Sie sofort die ELBA-Hotline oder Ihre:n Berater:in.

Schutz Ihrer Bank-/Zugangsdaten

Schützen Sie Ihre persönlichen Daten (IBAN, Verfügernummer, PIN, Signaturcode, TAN, Debit-/Kreditkartennummer inklusive zugehörigem CVC Code, usw.) auch im digitalen Bereich und halten Sie diese geheim!

- Geben Sie Ihre Bank-/Zugangsdaten keinesfalls an unberechtigte Dritte weiter.
- Wählen Sie einen sicheren Aufbewahrungsort für Ihre schutzwürdigen Daten.
- Notieren Sie Bank-/Zugangsdaten (z.B. ELBA-/Karten-PIN , CVC Code, pushTAN Signaturcode, usw.) nicht, damit sie nicht in „falsche“ Hände geraten.
- Speichern Sie PIN/Signaturcode niemals auf dem Computer, Smartphone oder Tablet oder als getarnte Telefonnummer. Apps haben teilweise Zugriff auf Ihre Kontaktdaten und könnten so an die Daten gelangen.
- Achten Sie darauf, dass Sie niemand bei der Eingabe Ihrer Zugangsdaten beobachtet.
- Benutzen Sie beim Online Banking niemals fremde, offene WLAN-Hotspots bzw. öffentlich zugängliche Endgeräte (Computer, Smartphones oder Tablets, usw.).

SICHERHEITSTIPPS UND SICHERHEITSMERKMALE BEIM ONLINE BANKING

Achten Sie auf die Verschlüsselung und das Sicherheitszertifikat! Geben Sie zur Anmeldung die Adresse https://mein.elba.raiffeisen.at immer manuell im Browser ein oder hinterlegen Sie ein Lesezeichen im Browser. Kontrollieren Sie, ob auf der Anmeldeseite die Adresse https://sso.raiffeisen.at/ angezeigt wird und das Sicherheitsschloss links daneben in der Adressleiste geschlossen ist.

VIRENSCHUTZ AKTUALISIEREN!

Verwendung aktueller Browser bzw. Betriebssysteme
Achten Sie darauf, dass Ihr Internet-Browser bzw. Betriebssystem immer auf dem neuesten Sicherheitsstand gehalten wird. Installieren Sie dazu die vom Hersteller empfohlenen Updates.

Abmeldung am Ende der Online oder Mobile (App) Sitzung.
Beenden Sie Ihre Mein ELBA-Sitzung immer mit Klick auf den „Abmelde-Icon".

NACH JEDER SITZUNG ABMELDEN!

ZEICHNEN SIE IHRE AUFTRÄGE MIT UNSEREN INNOVATIVEN, KOMFORTABLEN UND SICHEREN AUTORISIERUNGSVERFAHREN

pushTAN – Der neue Sicherheitsstandard für Login und Autorisierung
Die pushTAN ist die kundenfreundliche und sichere Lösung zum Signieren von Transaktionen und die Autorisierung der Anmeldung in mobile und Desktop-Anwendungen.

Die Aktivierung der pushTAN erfolgt entweder über die PRIVAT BANK-App am Mobilgerät oder die pushTAN Desktop (Windows, MacOS). Bei der Aktivierung erfolgt eine Kopplung an das jeweilige Mobilgerät oder Desktop PC. Die pushTAN wird über einen eigenen sicheren Kanal in die PRIVAT BANK-App bzw. pushTAN Desktop-Anwendung geschickt und automatisch erkannt. Daher ist kein Eintippen notwendig. Sie ist auftragsgebunden und nur 5 Minuten gültig. Kontrollieren Sie vor dem Bestätigungsvorgang die in der jeweiligen Anwendung angezeigten Transaktionsdaten! Das Verfahren entspricht den neuesten gesetzlichen Anforderungen der 2-Faktor-Authentifizierung bzw. -Autorisierung.

cardTAN – Unterschreiben mit Debitkarte und cardTAN-Generator
Für dieses moderne Autorisierungsverfahren benötigen Sie Ihre cardTAN-fähige Karte und einen cardTAN-Generator. Der cardTAN-Generator funktioniert völlig verbindungslos. Sie müssen keinerlei zusätzliche Software auf Ihrem PC oder Smartphone installieren.

Zur Berechnung der TAN werden die Auftragsdaten Ihrer Überweisung mit einbezogen. Die TAN ist damit unlösbar mit den von Ihnen erfassten Aufträgen verbunden. Vergleichen Sie die angezeigten Daten am cardTAN-Generator auch immer mit dem Originalbeleg!

smsTAN – die TAN per SMS auf Ihr Mobiltelefon
Bei der smsTAN erhalten Sie eine SMS mit Ihrer TAN an die von Ihnen bei der Registrierung angegebene Mobilfunknummer. Zu Ihrer Sicherheit enthält die SMS eine Kurzinformation zur Transaktion. Vergleichen Sie die angeführten Daten auch noch einmal mit Ihrem Originalbeleg. Die smsTAN ist nur einmal verwendbar und insgesamt für 5 Minuten gültig. Ein Signaturvorgang mittels smsTAN muss zusätzlich mit Eingabe der ELBA-PIN bestätigt werden.

ERKENNEN SIE PHISHING-VERSUCHE!

Phishing bezeichnet eine betrügerische Methode, um mittels unverlangt zugesandter gefälschter E-Mails, SMS, Nachrichten in sozialen Netzwerken, Telefonaten oder Formularen auf Webseiten an vertrauliche Daten zu gelangen. Dabei werden Sie durch unterschiedliche Vorwände zur Eingabe Ihrer vertraulichen Daten verleitet (z.B. Konto-/Kartensperre, Verrechnung (hoher) Gebühren, usw.).

- Löschen Sie unverlangt zugesandte Nachrichten (E-Mails, SMS, Messenger und Soziale Dienste) bei Erhalt oder klären Sie im Zweifelsfall deren Echtheit mit Ihrer Bank oder der Hotline ab!
- Folgen Sie niemals darin enthaltenen Links bzw. öffnen Sie keine Anhänge!
- Antworten Sie keinesfalls auf solche Nachrichten!

Ihre Bank fordert Sie NIE per E-Mail, SMS oder telefonisch auf, Ihre Zugangsdaten oder Sicherheits-/Signatur-Codes bekannt zu geben! Halten Sie Ihre Zugangsdaten stets geheim!

Im Zweifelsfall kontaktieren Sie direkt Ihre:n Bankberater:in. Verwenden Sie dazu die Ihnen bereits bekannte Telefonnummer, E-Mail-Adresse oder Mailbox Ihrer Bank oder des:der Berater:in. Kontaktdaten, die direkt im Phishing Mail enthalten sind, könnten gefälscht sein.

Beispiele zu aktuellen Phishing-Mails finden Sie auch unter raiffeisen.at/sicherheit.

Vorsicht vor Schadprogrammen!
Schadprogramme (Viren, Trojaner, Remote Access Tools, usw.) fordern Sie z.B. über eine gefälschte Seite dazu auf, eine „Aktualisierung von Sicherheitszertifikaten oder -programmen/Apps“ durchzuführen, ein „Demokonto“ zu testen, eine „Testüberweisung“ oder Ähnliches auszuführen. Folgen Sie derartigen Aufforderungen auf keinen Fall und informieren Sie Ihre PRIVAT BANK bzw. die ELBA-Hotline!

Zum eigenen Schutz:

- Installieren Sie niemals bedenkenlos Programme/Apps auf Ihrem Computer/ Smartphone, insbesondere dann nicht, wenn Ihnen dies unaufgefordert empfohlen wird (z.B. Aufforderung per SMS, QR-Code, Telefon usw.).
- Beziehen Sie Programme/Apps nur aus vertrauenswürdigen offiziellen Quellen. Achten Sie insbesondere beim Download von Apps für Mobilgeräte (Smartphones, Tablets etc.) darauf, dass diese über offizielle Stores angeboten werden und prüfen Sie diese vorab (z.B. vor dem Download die Bewertungen anderer Benutzer lesen). Behalten Sie die Standardeinstellung bei, welche das Installieren von Apps aus unsicheren Quellen auf Ihrem Smartphone unterbindet.
- Nehmen Sie keine vom Hersteller/Verkäufer untersagten Systemänderungen vor (speziell bei Smartphones: „Jailbreak“, „Rooten“, „Unlocking“ usw.). Dies kann Sicherheitslücken verursachen und zu Datenmissbrauch führen.
- Reagieren Sie niemals unüberlegt auf (unaufgefordert) zugesandte Nachrichten (E-Mail, SMS, WhatsApp, Facebook/Meta, usw.). Dies gilt insbesondere für Nachrichten, die Sie zu Handlungen im Zusammenhang mit Ihrem Online oder Mobile Banking auffordern (Überweisung tätigen, Konto-/ Karteninformationen eingeben, usw.).
- Seien Sie vorsichtig bei Telefonanrufen und Nachrichten, wenn diese Sie zur Installation eines Fernwartungsprogrammes auffordern oder Sie auf anderen Wegen Dritten einen Zugriff auf Ihren Computer oder Ihr Smartphone/Tablet gewähren sollen.
- Bestätigen Sie pushTAN Signaturanforderungen nur dann, wenn diese aus einer bewusst von Ihnen zuvor gesetzten Aktion im Zusammenhang mit Online/Mobile Banking oder einer Debit-/Kreditkartentransaktion stammen.
- Prüfen Sie vor der Bestätigung einer pushTAN Signaturanforderung die darin enthaltenen Informationen auf Korrektheit (Vergleichswert für Anmeldung / Auftragsdaten für eine Überweisung / Händlerdaten für eine Kartentransaktion).
- Führen Sie laufend alle Systemupdates inkl. Sicherheitsupdates durch - speziell auch auf Smartphones und Tablets.

Ihre sichere Verbindung: die Mailbox
Mit der Mailbox ist die Kommunikation mit Ihrer Bank so sicher wie ein Vier-Augen-Gespräch. Auf diese Weise bleiben persönliche Daten und Informationen – im Gegensatz zum normalen E-Mail Verkehr – frei von unbefugten Zugriffen Dritter.
Über die Mailbox können auch Dokumentenanhänge (z.B. pdf-Dokument) gesichert zwischen Ihnen und Ihrem:Ihrer Berater:in ausgetauscht werden.

Aber auch hier gilt: Ihr:e Berater:in fragt Sie auf diesem Wege nicht nach Zugangs- oder Signaturdaten (PIN, Signatur-Code, TAN usw.)!

Sicher Online und Offline mit der Karte zahlen
Bei Kartenzahlungen – ob online oder im Geschäft und Restaurant – ist das Thema Sicherheit zentral. Hohe Sicherheitsstandards für sichere Kartenzahlungen sind bei HYPO Salzburg eine Selbstverständlichkeit.

Das Wichtigste im Überblick:

- Informieren Sie sich über die wichtigsten Sicherheitsvorkehrungen Ihrer Karte.
- Wenden Sie unsere Sicherheitstipps an und schützen Sie sich selbst.
- Nutzen Sie Geocontrol zum Schutz Ihrer Karte im Ausland.
- Auffälligkeiten? Kontaktieren Sie sofort die ELBA-Hotline oder Ihre:n Berater:in.

DIE WICHTIGSTEN SICHERHEITSVORKEHRUNGEN IHRER KARTE

Sicherheitskennzahl
Häufig wird bei der Bestellung im Internet die Eingabe/Bekanntgabe des CVV2 Code (steht für: Card Verification Value), einer KPN (Kartenprüfnummer) oder des „Sicherheitscodes" verlangt. Es handelt sich dabei immer um die letzten drei Stellen neben dem Unterschriftsfeld auf der Rückseite Ihrer Karte.

3D Secure
Mit der 3D-Secure-Technologie bietet Ihnen Raiffeisen zusätzlichen Schutz beim Online-Einkauf. Nach Ihrer Anmeldung wird jede Transaktion bei teilnehmenden Internet-Händler:innen zusätzlich mit diesem Code geschützt. Bei jeder Transaktion wird überprüft, ob sowohl der/die Karteninhaber:in als auch der/die Akzeptanzpartner:in jene Teilnehmer:innen am Zahlungsverkehr sind, für die sie sich ausgeben.

PIN (Personal Identification Number)
Jede Karte ist mit einer hochverschlüsselten 4-stelligen PIN ausgestattet.

SICHERHEITSTIPPS FÜR KARTENZAHLUNGEN IM IN-/AUSLAND UND ONLINE

Sichere Online-Zahlungen
Achten Sie bei Internet-Transaktionen stets darauf, dass eine sichere Internet- Verbindung (SSL-Verschlüsselung) zur Verfügung steht und geben Sie Ihre Kreditkarten- bzw. Debitkartendaten nur bei einem tatsächlichen Kauf an. Sie erkennen die SSL-Verschlüsselung durch eine optische Anzeige im Browser in Form eines Schlüssels (geteilt oder ganz) oder eines Vorhängeschlosses (offen oder geschlossen) bzw. durch das „https" in der URL. Sollte kein Verschlüsselungssystem angeboten werden, so bestellen Sie bitte auf einem anderen Weg.

Generelle Sicherheitstipps

- Bewahren Sie die Zahlungsbelege auf.
- Kontrollieren Sie Ihre Kreditkartenabrechnung regelmäßig.
- Lassen Sie beim Bezahlvorgang Ihre Karte nicht aus den Augen.

Tipps zur Bargeldzahlung/Kartenbehebung im In-/Ausland
Etwas Bargeld in der jeweiligen Landeswährung sollten Sie bei einer Auslandsreise mit sich führen, damit Sie kleine Einkäufe, Taxifahrten, Eintrittstickets etc. bar begleichen können. Aus Sicherheitsgründen sollten Sie jedoch Ihre Debit- und Kreditkarte mit sich führen, denn im Fall eines Diebstahls ist Bargeld unwiederbringlich verloren.

Überlegen Sie vor Antritt der Reise, welche Karten Sie mitnehmen wollen.
Lassen Sie sich dabei auch von Ihrer PRIVAT BANK beraten.

- Decken Sie beim Eingeben der PIN die Tastatur immer mit der freien Hand ab.
- Lassen Sie sich nicht ablenken.
- Lassen Sie sich nicht von Dritten „helfen".
- Geben Sie die Karte nicht aus der Hand.
- Tragen Sie die PIN nie bei sich.
- Melden Sie Auffälligkeiten direkt der Polizei oder dem Betreiber des Bankomaten.
- Lassen Sie die Karte bei Verdacht auf Missbrauch, Diebstahl, Verlust oder Einzug am Bankomaten umgehend sperren.

GEOCONTROL SCHÜTZT IHRE KARTE IM AUSLAND

Geld kann mit der PRIVAT BANK Debitkarte außerhalb Europas nur dann abgehoben werden, wenn das von Ihnen ausdrücklich autorisiert wurde.

Was macht GeoControl?
GeoControl ermöglicht Ihnen nach der Deaktivierung, Bargeldbehebungen mit Ihrer Debitkarte auch in Ländern außerhalb Europas durchzuführen.
Zudem schützt GeoControl Sie auch vor „Skimming", eine der häufigsten Missbrauchsformen, die stark im Steigen begriffen ist. Dabei wird an manipulierten Geldausgabeautomaten der Magnetstreifen der Karte kopiert und der PIN-Code ausgespäht.
Mit den gestohlenen Daten wird außerhalb Europas Bargeld abgehoben.

Ihre Vorteile von GeoControl

- Ihr Risiko, Opfer einer Skimming-Attacke zu werden, wird erheblich verringert.
- Der Karteneinsatz ist weltweit rund um die Uhr freischaltbar.
- Der Einsatzzeitraum der Karte außerhalb Europas ist frei wählbar.
- Automatische Reaktivierung von GeoControl

HÄUFIGE FRAGEN ZU GEOCONTROL

Was kostet GeoControl?
Diese Dienstleistung, die die sichere Nutzung Ihrer PRIVAT BANK Debitkarte erhöht, wird Ihnen von den österreichischen Banken kostenlos zur Verfügung gestellt.

Wie kann ich GeoControl deaktivieren?
Sie haben folgende Möglichkeiten zur Deaktivierung:

- über Ihren Online Banking-Zugang Mein ELBA unter „Services“ - „Self Service“ oder im Modul „Karten“ unter „Karten verwalten“
- über Ihre:n Berater:in
- über die Hotline +43 1 204 8800 / im Ausland über die SperrHotline

Wo sehe ich, ob GeoControl deaktiviert ist?
In Ihrem Online Banking Mein ELBA finden Sie den jeweils aktuellen Status für die geografischen Einsatzmöglichkeiten Ihrer PRIVAT BANK Debitkarte.

Wie lange kann ich GeoControl deaktivieren?
Der Deaktivierungszeitraum sollte zu Ihrer eigenen Sicherheit drei Monate nicht überschreiten. Bei längerem Auslandsaufenthalt kontaktieren Sie bitte Ihre:n Berater:in bei Ihrer Hausbank.

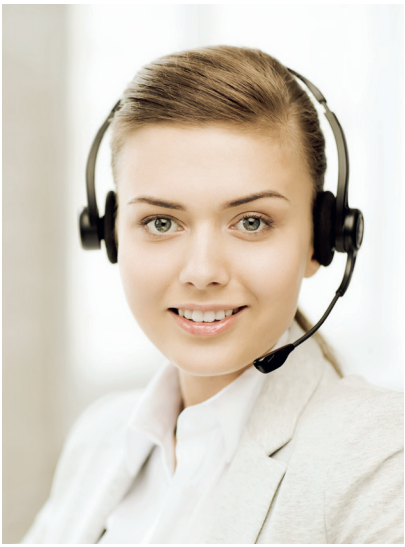
Wie kann ich GeoControl wieder aktivieren?
GeoControl wird automatisch ab dem bei der Deaktivierung bekanntgegebenen Datum reaktiviert.

PRIVAT BANK
der Raiffeisenlandesbank OÖ

AUFFÄLLIGKEITEN? KONTAKTIEREN SIE SOFORT DIE ELBA-HOTLINE ODER IHRE:N BERATER:IN

ELBA-Hotline

Niederösterreich, Wien	+43 1 33701 4800
Burgenland	+43 1 33701 4803
Oberösterreich	+43 599 Bankleitzahl 992
Salzburg	+43 662 8886 13333
Tirol	+43 599 Bankleitzahl 992
Vorarlberg	+43 5574 405 557
Steiermark	+43 316 4002 990
Kärnten	+43 599 Bankleitzahl 992



Sperr-Hotline für alle Raiffeisenkarten

Niederösterreich, Wien	+43 599 320 32
Burgenland	+43 599 331 23
Oberösterreich	+43 599 340 34
Salzburg	+43 599 355 99
Tirol	+43 599 360 36
Vorarlberg	+43 599 370 37
Steiermark	+43 599 380 38
Kärnten	+43 599 390 39

Umfassende und aktuelle Informationen zum sicheren Online Banking finden Sie auf:
raiffeisen.at/sicherheit

Medieninhaber, Herausgeber und Hersteller: Raiffeisenlandesbank Oberösterreich Aktiengesellschaft, Europaplatz 1a, 4020 Linz. Stand 07/2023