Raiffeisen
Meine Bank

Sicherheit im Raiffeisen Online und Mobile Banking

Tipps zu sicheren Bankgeschäften im Internet
www.raiffeisen.at/sicherheit

Tipps zu sicheren Bankgeschäften im Internet

Der Zugriff auf Ihre Raiffeisenkonten über Raiffeisen Online und Mobile Banking vom PC, Tablet oder via Smartphone ist technisch mit den besten verfügbaren Systemen abgesichert. Damit diese Sicherheitsmechanismen wirken können, sollten auch Sie als Anwender entsprechende Vorkehrungen treffen.

Schützen Sie Ihre persönlichen Daten! Erkennen Sie Phishing-Versuche!

Phishing bezeichnet eine betrügerische Methode, 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, usw.) bei Erhalt oder klären Sie im Zweifelsfall deren Echtheit mit Ihrem Berater 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 Ihren Bankberater. Verwenden Sie dazu die Ihnen bereits bekannte Telefonnummer oder e-Mail Adresse Ihrer Bank oder des Beraters. Kontaktdaten, die direkt im Phishing Mail enthalten sind, könnten gefälscht sein.

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

Davon zu unterscheiden sind legitime Nachrichten (E-Mail) von Ihrem Bankberater an Ihre private E-Mail Adresse. Nachrichten mit Anhängen/Links werden Ihnen ausnahmslos auf Basis eines vorangehenden Beratergespräches übermittelt, z.B. um einen vereinbarten Vertrag digital zu signieren. Benachrichtigungen über Neuigkeiten

in Ihrer persönlichen Mailbox in Mein ELBA können auch ohne vorheriges Beratergespräch eintreffen. Diese enthalten allerdings niemals einen Dateianhang/Link. Aber auch hier gilt: Ihr Berater fragt Sie auf diesem Wege nicht nach Zugangs- oder Signaturdaten (PIN, Signatur-Code, TAN usw.)!

Vorsicht vor Schadprogrammen!

Schadprogramme, sogenannte Trojaner oder Viren, 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 Raiffeisenbank 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 (Google, Apple etc.) angeboten werden und prüfen Sie diese vorab (z.B. vor dem Download die Bewertungen anderer Benutzer lesen).
- Nehmen Sie keine vom Hersteller/Verkäufer untersagten Systemänderungen vor (speziell bei Smartphones: "Jailbreak", "Rooten", "Unlocking" usw.). Dies kann Sicherheitslücken verursachen und zu Datenmissbrauch führen.
- Vorsicht bei unaufgeforderter Kontaktaufnahme durch Dritte (z.B. vermeintliche Techniker bekannter IT-Unternehmen) – speziell wenn Sie hierbei Zugriff auf Ihren Computer/Smartphone gewähren sollen.

Schutz Ihrer Zugangsdaten – PIN regelmäßig ändern

Schützen Sie daher Ihre persönlichen Zugangsdaten (Verfügernummer, IBAN, PIN, Signaturcode, TAN, usw.) auch im digitalen Bereich und halten Sie diese geheim!

- Geben Sie Ihre Zugangsdaten keinesfalls an unberechtigte Dritte weiter.
- Wählen Sie einen sicheren Aufbewahrungsort für Ihre schutzwürdigen Daten.
- Notieren Sie Zugangsdaten 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.). Ihre Online Banking-PIN sollte in regelmäßigen Intervallen geändert werden.

Hinweis: Im Zweifel wenden Sie sich an die SperrHotline oder ELBA-Hotline:

SperrHotline 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

Ihre sichere Verbindung: die Raiffeisen Mailbox

Mit der Raiffeisen Mailbox ist die Kommunikation mit Ihrem Raiffeisenberater 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 Raiffeisenberater ausgetauscht werden.

Bei Auffälligkeiten sofort reagieren!

Kontaktieren Sie bei Auffälligkeiten (z.B. unbekannte Online Banking-Seiten oder es kommt auf der Seite zu merkwürdigem Verhalten) umgehend Ihren Berater oder die ELBA-Hotline!

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

Sicherheitstipps

Achten Sie auf die Verschlüsselung und das Sicherheitszertifikat!
Geben Sie zur Anmeldung die Adresse **https://mein.elba.at** immer manuell im Browser ein. Kontrollieren Sie, ob das Sicherheitsschloss im Browser geschlossen ist. Überprüfen Sie die aktive Verschlüsselung der Seite, indem Sie das Sicherheitsschloss anklicken. Im Fenster „Website-Identifizierung" sollte am Beispiel des Internet Explorers der Hinweis „Diese Verbindung mit dem Server ist verschlüsselt." angezeigt werden.

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.

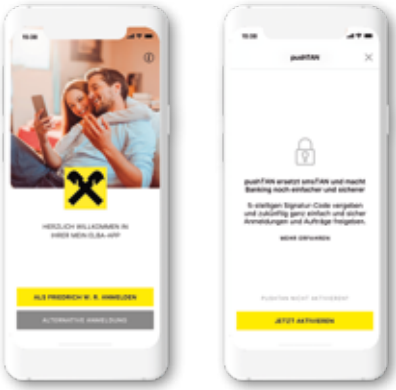
Einsatz von Virenschutz und Firewall
Verwenden Sie ein Virenschutzprogramm bzw. aktivieren Sie eine Personal Firewall zum Schutz Ihres PCs, Tablets bzw. Smartphones.

Achten Sie unbedingt darauf, Betriebssystem, Browser und Virenschutz- bzw. Firewall-Software auf Ihren Endgeräten laufend zu aktualisieren, da andernfalls kein zuverlässiger Schutz gewährleistet ist!

Abmeldung am Ende der Online oder Mobile (App) Sitzung.
Beenden Sie Ihre Mein ELBA Sitzung immer mit Klick auf „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 Generieren von Einmal-Passwörtern für das Login in mobile und Desktop-Anwendungen.

Die Aktivierung der pushTAN erfolgt entweder über die Mein ELBA-App am Mobilgerät (Android, iOS) oder die pushTAN Desktop (Windows, MacOS). Bei der Aktivierung erfolgt eine Kopplung an das jeweilige Mobilgerät oder Desktop PC. Die pushTAN wird im Hintergrund der Transaktion bzw. des Login über einen eigenen Kanal in die Mein ELBA-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 Maestro-Karte und cardTAN-Generator

Für dieses moderne Autorisierungsverfahren benötigen Sie Ihre cardTAN-fähige Karte (z.B. Raiffeisen Bankomatkarte) und einen cardTAN-Generator. Der cardTAN-Generator funktioniert völlig verbindungslos. Sie müssen keinerlei zusätzliche Software auf Ihrem PC oder Smartphone installieren.

Raiffeisen Meine Bank

Zur Berechnung der TAN werden die Auftragsdaten Ihrer Überweisung miteinbezogen. Die TAN ist damit unlösbar mit den von Ihnen erfassten Aufträgen verbunden. Kontrollieren 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. Kontrollieren 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.

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

Impressum:
Medieninhaber: Zentrale Raiffeisenwerbung, 1030 Wien
Hersteller: AV-Verlag Bankenbedarfsartikel GmbH Nfg KG, 1140 Wien
Verlagsort: Wien
Herstellungsort: Wien

Stand: Juli 2020

www.raiffeisen.at/sicherheit