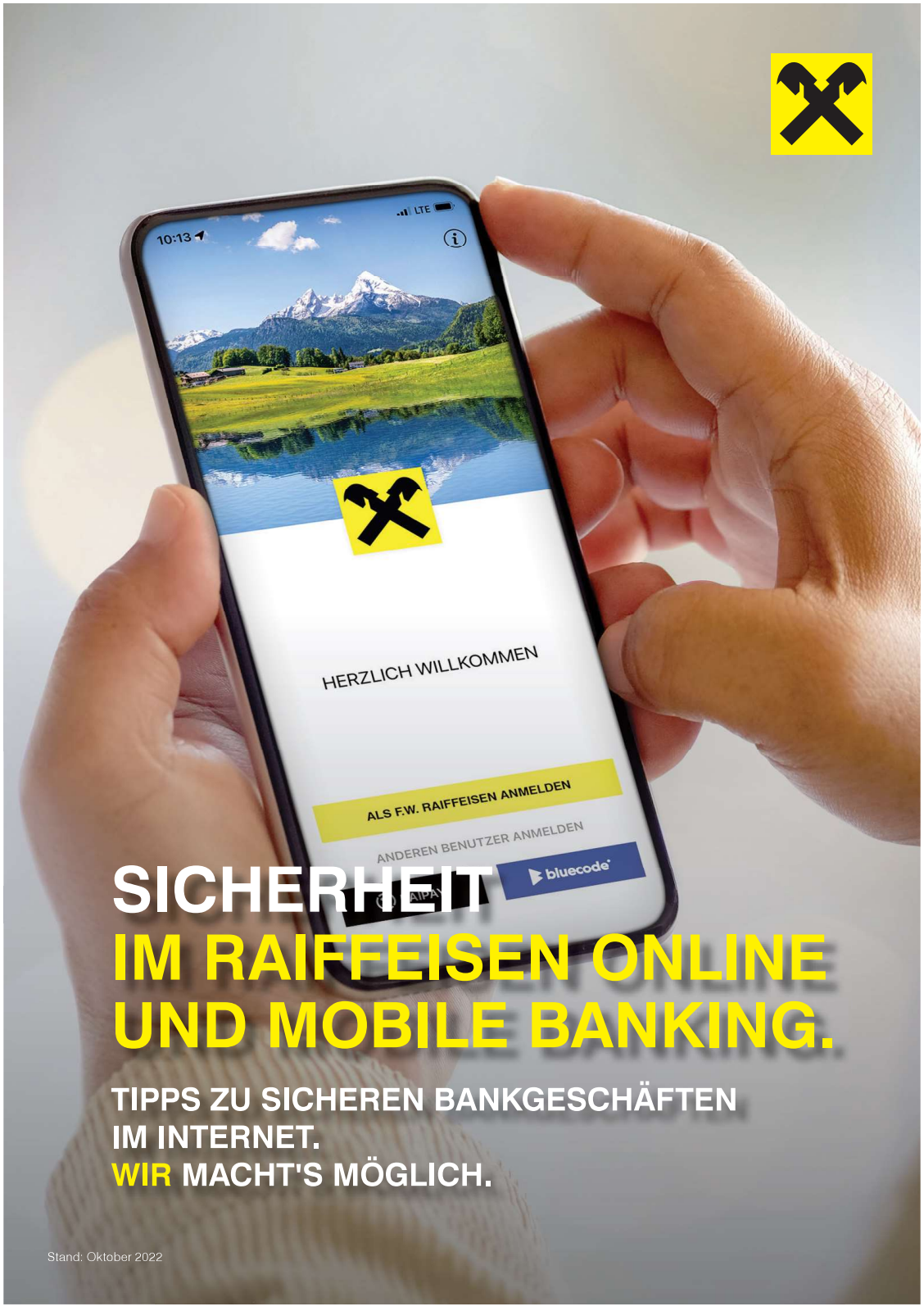


SICHERHEIT IM RAIFFEISEN ONLINE UND MOBILE BANKING.

TIPPS ZU SICHEREN BANKGESCHÄFTEN IM INTERNET.
WIR MACHT'S MÖGLICH.

Stand: Oktober 2022

Das Wichtigste im Überblick:

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

Tipps zu sicheren Bankgeschäften im Internet

Der Zugriff auf Ihre Raiffeisen Konten 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.

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 Raiffeisenberater:in. Verwenden Sie dazu die Ihnen bereits bekannte Telefonnummer, E-Mail-Adresse oder Raiffeisen-Mailbox Ihrer Bank oder Ihres:Ihrer Raiffeisenberater:in. Kontaktdaten, die direkt im Phishing Mail enthalten sind, könnten gefälscht sein.

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, 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.

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

Ihre sichere Verbindung: die Raiffeisen Mailbox
Mit der Raiffeisen 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 Raiffeisenberater:in ausgetauscht werden.

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

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 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 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.

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!

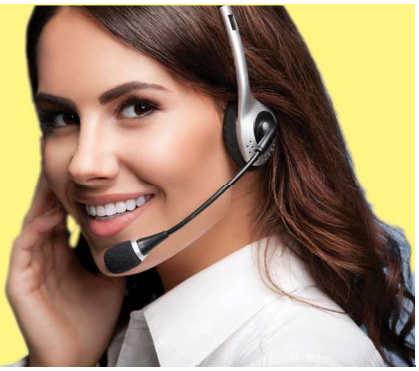
- Geben Sie Ihre Bank-/Zugangsdaten keinesfalls an unberechtigte Dritte weiter.
- Wählen Sie einen sicheren Aufbewahrungsort für Ihre schutzwürdigen Daten.
- Notieren Sie Bank-/Zugangsdaten (z.B. ELBA-/Karten-PIN, CVC Code, pushTAN Signaturcode, usw.) nicht, damit sie nicht in „falsche" Hände geraten.
- 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.).

Hinweis: Im Zweifel wenden Sie sich an die Sperr-Hotline oder ELBA-Hotline:
Bei Auffälligkeiten sofort reagieren!

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

Kontaktieren Sie bei Auffälligkeiten (z.B. unbekannte Online Banking-Seiten oder es kommt auf der Seite zu merkwürdigem Verhalten) umgehend Ihre:n Raiffeisenberater:in 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.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.

Verwendung aktueller Browser bzw. Betriebssysteme

VIRENSCHUTZ AKTUALISIEREN!

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

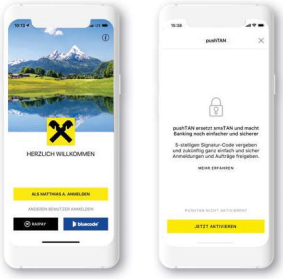
Abmeldung am Ende der Online oder Mobile (App) Sitzung.

NACH JEDER SITZUNG ABMELDEN!

Beenden Sie Ihre Mein ELBA Sitzung immer mit Klick auf „Abmelde-Icon".

Zeichnen Sie Ihre Aufträge mit unseren innovativen, komfortablen und sicheren Autorisierungsverfahren.

pushTAN – Der 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 Mein ELBA-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 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 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. 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: Oktober 2022