

Raiffeisen ELBA-internet / ELBA-mobil

Sicherheitsrichtlinien

Der Zugriff auf Ihre Bankkonten über Raiffeisen ELBA-internet bzw. Raiffeisen ELBA-mobil ist technisch mit den besten verfügbaren Systemen abgesichert. Damit diese Sicherheitsmechanismen wirken können, müssen auch Sie als Anwender entsprechende Vorkehrungen treffen. Dazu gehören:

- die Einrichtung eines aktuellen Virenschutzes auf Ihrem Computer/Smartphone,
- die Abschirmung des Computers/Smartphones durch eine „Firewall“,
- der Einsatz eines aktuellen Betriebssystems,
- die Nutzung eines getesteten Browsers,
- die Verwendung von Benutzerkonten mit eingeschränkten Rechten und einem sicheren Passwort,
- die Verschlüsselung Ihrer WLAN-Verbindung,
- die Geheimhaltung und sichere Verwahrung Ihrer persönlichen Zugangsdaten,
- die Verwendung moderner Autorisierungsverfahren (cardTAN, Raiffeisen mobile TAN, digitale Signatur),
- das Erkennen von „Phishing“ und
- das Prüfen des Sicherheitszertifikats.

Schutz vor Schadprogrammen (Trojaner, Viren usw.)

Installieren Sie auf Ihrem Computer/Smartphone ein Virenschutz-Programm und halten Sie dieses laufend auf dem aktuellsten Stand! Üblicherweise bieten diese Programme ein automatisches Update an, das Sie nutzen sollten. Nur ein aktueller Virenschutz ist wirklich wirksam gegen Schadprogramme (Trojaner usw.)!

Hinweis:

- Öffnen Sie keine Anhänge/Links aus Nachrichten (E-Mail, SMS, soziale Netzwerke wie zB. Facebook, ...), deren Absender Sie nicht kennen.
- Installieren Sie nicht bedenkenlos Programme auf Ihrem Computer/Smartphone. Prüfen Sie diese vorab (zB indem Sie vor dem Download die Bewertungen anderer Benutzer im Downloadbereich/ App-Store lesen).

Firewall

Verwenden Sie unbedingt auch eine Firewall, bevor Sie die Verbindung mit dem Internet herstellen! Diese Hard- oder Software verhindert den Zugriff von Hackern auf Ihren Computer/Smartphone.

Update des Betriebssystems

Die Hersteller von Betriebssystemen veröffentlichen regelmäßig sicherheitsrelevante Updates, die Sie auf Ihrem Computer/Smartphone installieren sollten. Nutzen Sie die automatische Updatefunktion Ihres Betriebssystems!

Nutzung eines getesteten Browsers

Die auf der PIN-Eingabeseite bzw. unter „Browserkonfiguration“ angeführten getesteten Browser unterstützen den vollen Funktionsumfang von Raiffeisen ELBA-internet. Bei Verwendung eines anderen Browsers steht Ihnen unter Umständen nicht der gesamte Funktionsumfang zur Verfügung. Mit sicherheitstechnisch veralteten Browserversionen (Microsoft IE5 bzw. IE6, Mozilla Firefox 3.5) ist der Zugriff auf Raiffeisen ELBA-internet nicht möglich.

Benutzer mit eingeschränkten Rechten

Für jeden Benutzer eines Computer/Smartphone ist die Anlage eines eigenen Benutzerkontos mit eingeschränkten Rechten inklusive einem sicheren Passwort dringend empfohlen. Oftmals werden stattdessen „Administratorrechte“ eingestellt, oder es wird überhaupt nur ein einziges Benutzerkonto mit vollen Zugriffsrechten ohne Passwort verwendet. Mit einer „Administratorberechtigung“ kann der Benutzer zwar komfortabel arbeiten (zB Programme installieren, Systemeinstellungen ändern usw.), allerdings können sich dadurch auch Schadprogramme unbemerkt installieren (zB beim Surfen im Internet, bei Installation neuer Software aus unbekanntenen Quellen usw.).

Verschlüsselung Ihrer WLAN-Verbindung

Standard ist heutzutage die WPA2-Verschlüsselung (Wi-Fi Protected Access 2). Das Passwort sollte dabei mindestens 20 Zeichen lang sein. Ältere Verfahren wie zB WEP (Wired Equivalent Privacy) gelten als unsicher.

Schützen Sie Ihre Zugangsdaten (PIN, Passwort usw.)

Würden Sie Ihren Hausschlüssel oder Ihr Spargbuch-Losungswort an fremde Dritte weitergeben oder diese frei zugänglich liegen lassen? **NEIN - viel zu gefährlich!**

Schützen Sie daher Ihre persönlichen Zugangsdaten (Verfügernummer, Kontonummer, PIN, TAN, Benutzername/Passwort usw.) auch im digitalen Bereich und halten Sie diese geheim!

Wenn Sie diese Daten auf Internetseiten von anderen Anbietern eingeben, sind Sie nicht in Kontakt mit Ihrer Bank (auch wenn dieser Anbieter die Daten dann weitersendet). Sie haben keine Kontrolle über die weitere Verwendung Ihrer Daten!

Hinweis:

Bei den Adressen www.sofortueberweisung.de, www.sofortueberweisung.at und www.payment-network.com handelt es sich nicht um Raiffeisen-Adressen. Auf diesen Seiten dürfen Sie keinesfalls Ihre ELBA-Zugangsdaten eingeben!

- Geben Sie Ihre Zugangsdaten keinesfalls an Dritte weiter (Familienangehörige, Kollegen, Internetseiten/Bezahldienste außerhalb von Raiffeisen usw.).
- Wählen Sie einen sicheren Aufbewahrungsort für Ihr PIN-Kuvert.
- Notieren Sie Zugangsdaten nicht, damit sie nicht in „falsche“ Hände kommen.
- Speichern Sie PIN/Passwort niemals auf dem Computer/Smartphone.
- Achten Sie darauf, dass Sie niemand bei der Eingabe Ihrer Zugangsdaten beobachtet.

Sie können Ihre PIN jederzeit via ELBA-internet ändern, wenn Sie den Verdacht haben, dass diese nicht mehr sicher ist („Einstellungen“ >> „ELBA-services“ >> „PIN ändern“).

Tipp: Ändern Sie PIN und Passwort in regelmäßigen Intervallen (mindestens alle 2 Monate).

Im Notfall können Sie Ihren ELBA-Zugang selbst sperren, indem Sie beim Login bewusst 4-mal eine falsche PIN eingeben. Folgender Hinweis wird nach der vierten PIN-Falscheingabe angezeigt:

*PIN wurde mehr als 3-mal falsch eingegeben. Der Verfüger wurde gesperrt.
Bitte wenden Sie sich an Ihre kontoführende Bank.*

Sie können sich zwecks Sperre Ihres ELBA-Verfügers auch an die ELBA-SperrHotline wenden.
Rufnummer: +43 599 34034.

cardTAN – Unterschreiben mit Maestro-Karte und cardTAN-Generator

Für dieses moderne Autorisierungsverfahren benötigen Sie Ihre cardTAN-fähige Karte (Maestro-Karte oder Firmenkarte) und einen cardTAN-Generator. Der cardTAN Generator ist klein, handlich, funktioniert völlig verbindungslos und verschafft Ihnen Unabhängigkeit vom Handynet (Ausland, Zug, etc.). Die Überweisungsdaten werden beim Unterschreiben des Auftrags auf dem cardTAN-Generator angezeigt („Flickern“). Vergleichen Sie diese mit Ihrem Originalbeleg und bestätigen Sie die Korrektheit mit Drücken des „Ok“-Button. Damit wird eine neue und nur für diesen Auftrag gültige TAN erzeugt.

Raiffeisen mobile TAN – die TAN per SMS auf Ihr Mobiltelefon

Nach einmaliger Registrierung wird die mobile TAN beim Unterschreiben von Aufträgen auf Anforderung an Ihr Mobiltelefon gesandt und ist für fünf Minuten gültig. Kontrollieren Sie die Korrektheit der im SMS-Text übermittelten Auftragsdaten (Betrag, IBAN/BIC oder BLZ/Kontonummer, Empfänger usw.) mit Ihrem Originalbeleg. Unterschreiben Sie den/die Aufträge nur dann mit der am Ende des SMS-Textes angezeigten TAN, wenn diese Auftragsdaten übereinstimmen.

Die gleichzeitige Nutzung von Electronic Banking und der mobilen TAN auf demselben mobilen Endgerät ist aus Sicherheitsgründen nicht empfohlen. Ihr Schutz durch die 2-Wege-Autorisierung der mobilen TAN ist damit nicht gewährleistet. Verwenden Sie für Electronic Banking auf mobilen Endgeräten das Autorisierungsverfahren „cardTAN“.

Die digitale Signatur (ELU)

Zusätzlich haben Raiffeisenkunden auch die Möglichkeit, ihre elektronischen Bankgeschäfte in Raiffeisen ELBA-internet mit der digitalen Signatur durchzuführen. Nähere Informationen dazu (Erstregistrierung, Freischaltung in ELBA, Kartenleser usw.) erhalten Sie bei Ihrem Raiffeisenberater und auf <http://www.a-trust.at>.

Die Mailbox: Sichere Kommunikation mit Ihrem Berater

Mailbox-Nachrichten werden vor dem Versenden verschlüsselt. Sie sind daher so sicher wie das Vier-Augen-Gespräch mit Ihrem Berater. Trifft eine neue Nachricht in Ihrer Mailbox ein, erhalten Sie eine Mitteilung an Ihre angegebene E-Mail-Adresse bzw. eine Information in Raiffeisen ELBA-internet/ELBA-mobil, nicht jedoch die Nachricht selbst. Dadurch bleiben persönliche Daten und Informationen frei von unbefugten Zugriffsmöglichkeiten Dritter.

Phishing-Versuche erkennen

„Phishing“ – eine Kombination der Wörter „Password“ und „fishing“ – bezeichnet den Versuch, missbräuchlich in den Besitz fremder Zugangsdaten zu gelangen.

Eine Phishing-Attacke beginnt mit einer Nachricht (zB via E-Mail, SMS, sozialem Netzwerk, Telefonanruf usw), in der der Empfänger entweder aufgefordert wird, eine Website zu besuchen, oder aber direkt ein Formular innerhalb des Mails auszufüllen.

Mit unterschiedlichen Vorwänden wird der Empfänger zur Eingabe seiner vertraulichen Zugangsdaten verleitet (zB „Ihr Konto wurde gesperrt“, „Untersuchung von Unregelmäßigkeiten“, „Von Ihrem Konto wurden Euro 1500 abgebucht“ usw.).

- Bitte beachten Sie, dass Raiffeisen niemals Nachrichten (E-Mail, SMS usw.) versendet, in denen Kunden aufgefordert werden, geheime Bankdaten (Verfüger-/Kontonummer, PIN, TAN usw.) bekannt zu geben bzw. zu aktualisieren.
- Es werden auch keine Testaufträge versandt, die Sie autorisieren müssen.

Löschen Sie solche Nachrichten und klicken Sie keinesfalls auf darin enthaltene Links! Nutzen Sie zum Login ausschließlich die Adresse: <https://banking.raiffeisen.at>

Prüfung des Sicherheitszertifikats beim Login

Für den Windows Internet Explorer 9 gehen Sie wie folgt vor:

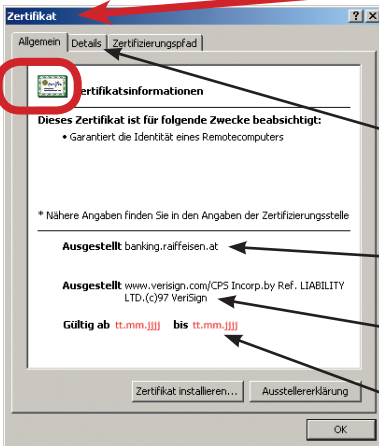
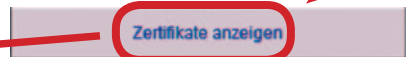
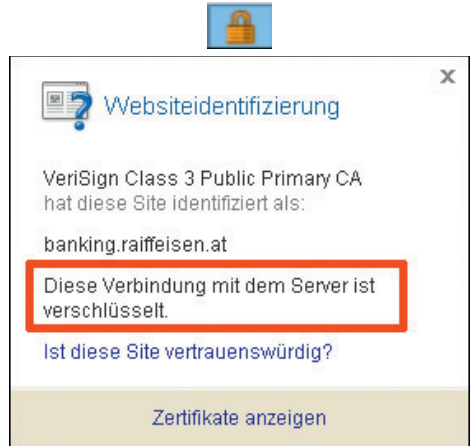
- Achten Sie darauf, dass Ihre Anmeldung stets auf der Startseite von ELBA-internet, <https://banking.raiffeisen.at>, erfolgt!
- Achten Sie darauf, dass das gelbe **Sicherheitsschloss** geschlossen ist.
- Überprüfen Sie unbedingt das Zertifikat und die aktive Verschlüsselung der Seite, indem Sie das Sicherheitsschloss anklicken. Im Fenster „Websiteidentifizierung“ sollte der Hinweis „Diese Verbindung mit dem Server ist verschlüsselt.“ angezeigt werden.

Nähere Details zum Zertifikat erhalten Sie mit einem Klick auf „Zertifikate anzeigen“.

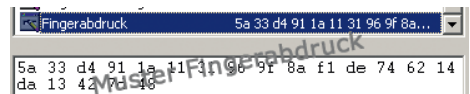
Bei diesem Zertifikat handelt es sich um den „digitalen Ausweis“ der Bank. Sie können mit dessen Hilfe überprüfen, ob Sie sich wirklich auf der richtigen Internet-Seite befinden.

Kontrollieren Sie folgende Elemente des Zertifikats:

- Für wen wurde das Zertifikat ausgestellt?
- Von wem wurde das Zertifikat ausgestellt?
- Ist das Zertifikat **gültig**?
- Wie lautet der **Fingerabdruck**?



Der Fingerabdruck steht als letzter Eintrag im Register „Details“. Nachstehend ein Muster wie dieser aufgebaut ist. Zur Überprüfung des aktuell gültigen Fingerabdrucks wenden Sie sich bitte an die ELBA-Hotline.



Das Zertifikat muss ausgestellt sein für: **banking.raiffeisen.at**

Das Zertifikat muss ausgestellt sein von: **www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign**

Die **Gültigkeit** des Zertifikats ist **zeitlich beschränkt**. Es ist **nur gültig**, wenn das **aktuelle Tagesdatum innerhalb des Zeitraums „Gültig ab/bis“** liegt.

Weiterführende Informationen zum Thema Sicherheit finden Sie

- auf der ELBA-internet Startseite <https://banking.raiffeisen.at> unter „Sicherheit“,
- in Raiffeisen ELBA-mobil unter dem Punkt „Sicherheitshinweise“ und
- der Raiffeisen-Internetseite www.raiffeisen-oe.at/sicherheit.