

# Online und Mobile Banking

## Sicherheitsrichtlinien

### Die gesunde Portion Misstrauen

Der Zugriff auf Ihre bankdirekt.at-Konten über bankdirekt.at-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 gefälschter E-Mails, Nachrichten in sozialen Netzwerken oder Formularen auf Websites an vertrauliche Daten zu gelangen. Dabei werden Sie durch unterschiedliche Vorwände zur Eingabe Ihrer vertraulichen Daten verleitet (z.B. „Ihr Konto wurde gesperrt“ oder es würde bei Nichtbefolgung eine Gebühr verrechnet werden).

- >> Löschen Sie derartige E-Mails sofort bei Erhalt!
- >> Folgen Sie niemals darin enthaltenen Links bzw. öffnen Sie keine Anhänge!
- >> Antworten Sie keinesfalls auf solche E-Mails!



**Ihre Bank fordert Sie NIE per E-Mail oder telefonisch auf, Ihre Zugangsdaten oder vermeintliche Sicherheits-codes bekannt zu geben! Halten Sie Ihre Zugangsdaten stets geheim! Im Zweifelsfall kontaktieren Sie direkt Ihren Bankberater.**

#### 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 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 Anforderungen auf keinen Fall und informieren Sie Ihre bankdirekt.at bzw. die ELBA-Hotline!**



## Schutz Ihrer Zugangsdaten - Passwort/PIN regelmäßig ändern

Schützen Sie daher Ihre persönlichen Zugangsdaten (Verfügernummer, Kontonummer, PIN, TAN, Benutzername/Passwort 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/Passwort 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 oder unbekannte Computer, Smartphones oder Tablets.

Ihr Zugangspasswort bzw. Ihre PIN zum Online Banking sollte in regelmäßigen Intervallen geändert werden.

Hinweis: Im Notfall können Sie Ihren ELBA-Zugang selbst sperren, indem Sie bewusst 4-mal eine falsche PIN im Sperrfenster eingeben (aufrufbar im Bereich „Sicherheit“ unter <https://banking.raiffeisen.at>).

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

### SperrHotline für alle Karten

Oberösterreich +43 599 340 34

### ELBA-Hotline

Oberösterreich +43 599 34000 900 - 4

## 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!

## Ihre sichere Verbindung: die bankdirekt.at Mailbox

Mit der bankdirekt.at Mailbox ist die Kommunikation mit Ihrem Berater 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 Berater ausgetauscht werden.

## Weitere Sicherheitstipps

### Achten Sie auf die Verschlüsselung und das Sicherheitszertifikat!

Geben Sie zur Anmeldung die Adresse <https://banking.raiffeisen.at> immer manuell im Browser ein oder nutzen Sie ausschließlich Direktverlinkungen von Ihrer bankdirekt.at-Homepage. 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.

Eine Beschreibung zur Überprüfung des Sicherheitszertifikats von bankdirekt.at für die unterschiedlichen Internet-Browser erhalten Sie unter <https://banking.raiffeisen.at> im Bereich „Browserkonfiguration“.



### 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. Im Bereich „Browserkonfiguration“ unter <https://banking.raiffeisen.at> werden die aktuell getesteten Browser angeführt, die den gesamten Funktionsumfang von bankdirekt.at unterstützen.

### 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 ELBA-internet/ELBA-mobil bzw. ELBA-App Sitzung.

Beenden Sie Ihre Sitzung immer mit Klick auf „Abmelden“.

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

### **cardTAN – Unterschreiben mit Maestro-Karte und cardTAN-Generator**

Für dieses moderne Autorisierungsverfahren benötigen Sie Ihre card-TAN-fähige Karte (z.B. bankdirekt.at-Bankomat-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 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 Kurzzinformation 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.

### **Die digitale Signatur**

Sie können Ihre elektronischen Bankgeschäfte in ELBA-internet auch mit der digitalen Signatur autorisieren.

Umfassende und aktuelle Informationen zum sicheren Online Banking finden Sie auf **[www.bankdirekt.at/sicherheit](http://www.bankdirekt.at/sicherheit)**.