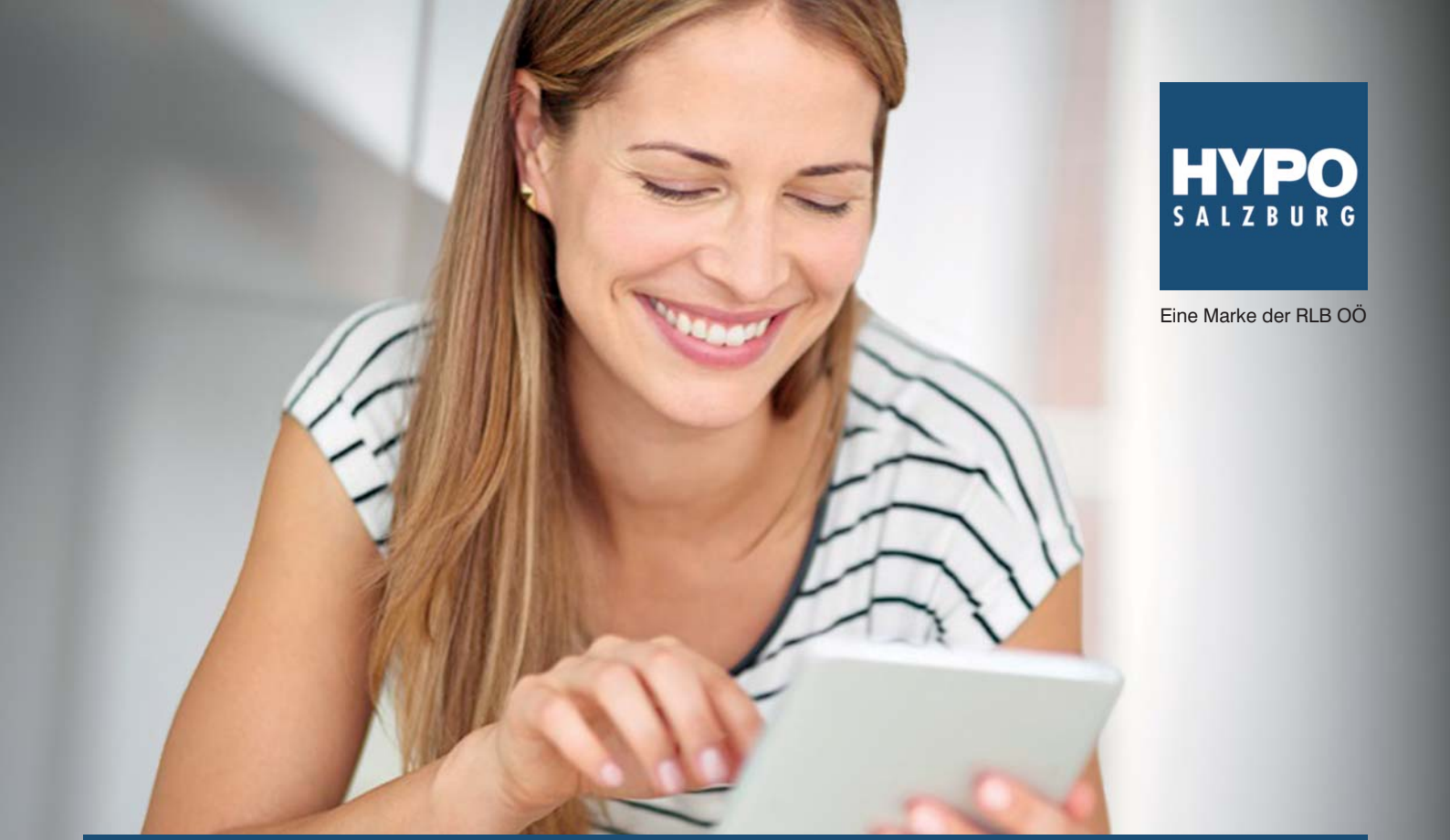

HYPO SALZBURG

Eine Marke der RLB OÖ

SICHERHEIT IM ONLINE UND MOBILE BANKING

Tipps zu sicheren Bankgeschäften im Internet

DIE GESUNDE PORTION MISSTRAUEN

Der Zugriff auf Ihre HYPO Konten über Mein ELBA, 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 Sicherheitscodes bekannt zu geben! Halten Sie Ihre Zugangsdaten stets geheim! Im Zweifelsfall kontaktieren Sie direkt Ihren Kundenberater.

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 Aufforderungen auf keinen Fall und informieren Sie Ihre HYPO Salzburg bzw. die ELBA-Hotline!

SICHERHEIT IM ONLINE UND MOBILE BANKING

Tipps zu sicheren Bankgeschäften im Internet.

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.

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 HYPO Mailbox

Mit der HYPO Mailbox ist die Kommunikation mit Ihrem Kundenberater 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 Kundenberater ausgetauscht werden.

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

Im Zweifel wenden Sie sich an die Sperrhotline für Karten oder ELBA-Sperrhotline:

HYPO Sperrhotline für Karten
und
HYPO ELBA-Sperrhotline
+43 599 34 0 34

WEITERE SICHERHEITSTIPPS

Achten Sie auf die Verschlüsselung und das Sicherheitszertifikat!

Geben Sie zur Anmeldung die Adresse https://mein.elba.hypo.at immer manuell im Browser ein oder nutzen Sie ausschließlich Direktverlinkungen von Ihrer HYPO 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.

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 Debitkarte und cardTAN-Generator

Für dieses moderne Autorisierungsverfahren benötigen Sie Ihre card-TAN-fähige Karte (z.B. Debitkarte) 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 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.

Medieninhaber und Hersteller: Raiffeisenlandesbank Oberösterreich Aktiengesellschaft, Europaplatz 1a, 4020 Linz. Stand 09/2021