Security in Kathrein eBanking

November 2021

Online-Banking-Applikationen sind beliebte Ziele von Betrügern. Um die Sicherheitsmaßnahmen zu umgehen, versuchen sie zum Beispiel über täuschende E-Mails oder Schadsoftware an Nutzerdaten zu gelangen und so Zugang zum Online-Banking zu erhalten. Die Kathrein Privatbank empfiehlt Ihnen daher, stets aufmerksam zu sein und im Umgang mit Online-Banking die folgenden Sicherheitshinweise zu beachten. Verwenden Sie nur die Original-Website der Kathrein Privatbank.

! Grundsätzlich gilt: Die Kathrein Privatbank wird Sie nie per Telefon oder E-Mail auffordern, vertrauliche Daten bekanntzugeben oder Fernzugriff auf Ihr eBanking zu erteilen. Im Rahmen eines mit der Funktion CommuniKATE unterstützten Beratungsgespräches können Sie auch ein Screen-Sharing mit Ihrem Kathrein Kundenbetreuer durchführen.

Schützen Sie Ihre persönlichen Daten!

Bitte gehen Sie stets äußerst sorgsam mit Ihren Zugangsdaten (Verfügernummer, IBAN, PIN, Sicherheitscode, mTAN, usw.) um. Halten Sie diese Daten geheim!

- Geben Sie Ihre Zugangsdaten keinesfalls an unberechtigte Dritte weiter.
- Bewahren Sie diese Daten nicht frei zugänglich auf und wählen Sie einen sicheren Aufbewahrungsort für Ihre schutzwürdigen Daten.
- Notieren Sie Zugangsdaten nicht, damit sie nicht in „falsche“ Hände geraten, das heißt auch, machen davon keine Fotos, Kopien oder Scans.
- Speichern Sie PIN/Sicherheitscode niemals auf dem Computer, Smartphone oder Tablet 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.
- Wählen Sie keine leicht zu erratenden Passwörter und ändern Sie diese in regelmäßigen Intervallen bzw. sofort, wenn Sie einen Missbrauch befürchten.

Erkennen Sie Pishing-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 und klären Sie im Zweifelsfall deren Echtheit mit Ihrem Berater ab!
- Folgen Sie niemals darin enthaltenen Links bzw. öffnen Sie keine Anhänge!
- Antworten Sie keinesfalls auf solche Nachrichten!

! Die Kathrein Privatbank 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 persönlichen Berater. Verwenden Sie dazu die Ihnen bereits bekannte Telefonnummer oder Kathrein E-Mail-Adresse Ihres Kundenbetreuers. Kontaktdaten, die direkt im Pishing-Mail enthalten sind, könnten gefälscht sein.

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 derartige Aufforderungen auf keinen Fall und informieren Sie Ihren persönlichen Kathrein Berater!**

! **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 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).

Vorsicht bei unaufgeforderter Kontaktaufnahme durch Dritte (z.B. vermeintliche Techniker bekannter IT-Unternehmen) – speziell, wenn Sie hierbei Zugriff auf Ihren Computer/Smartphone gewähren sollen.

Sicherheitstipps

Achten Sie auf die Verschlüsselung und das Sicherheitszertifikat! 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 werden. Installieren Sie dazu die vom Hersteller empfohlenen Updates.

Einsatz von Virenschutz und Firewall

Verwenden Sie ein aktuell upgedatetes Virenschutzprogramm bzw. aktivieren Sie eine Personal Firewall zum Schutz Ihres PCs, Tablets bzw. Smartphones.

Abmeldung am Ende der Online eBanking Sitzung.
Beenden Sie Ihre eBanking bzw. eSecurities Trading Session immer mit dem Klick auf „LOGOUT“.

Unsere Kathrein Sicherheitsstandards für Login und Autorisierung

Der Zugriff auf Ihr Konto/Depot über das Internet ist nur mit einer gültigen Kombination aus Ihrem Benutzernamen und persönlichem Passwort möglich. Zusätzlich wird eine sichere, verschlüsselte Verbindung (SSL) beim Online-Zugriff auf Ihr Konto/Depot genutzt. Des Weiteren stellt eine Zwei-Faktor-Authentifizierung sicher, dass keine unbefugte Person Online-Dienste mit dem Konto des rechtmäßigen Nutzers tätigt. Für die zusätzliche Verifizierung dient ein einmaliger Sicherheitscode, welcher per SMS an das hinterlegte Mobiltelefon des Nutzers gesendet wird.

Des Weiteren sind Transaktionen über das Internet durch ein mTAN-Medium geschützt, welche auf Grund Ihrer zufälligen Zusammensetzungen Fishing vorbeugend abwehren soll. Sie erhalten diese mTAN als SMS an die von Ihnen bei der Registrierung angegebene Mobilfunknummer. Die mTAN ist unlösbar mit dem von Ihnen erfassten Auftrag verbunden und nur 5 Minuten gültig. Zu Ihrer Sicherheit enthält die SMS eine Kurzinformation zur Transaktion. Kontrollieren Sie immer vor dem Bestätigungsvorgang (Zeichnen) die in der SMS angezeigten Daten auf Übereinstimmung mit den online erfassten Transaktionsdaten.