

Sicherheit im Internet

Ihre Sicherheit steht bei uns an erster Stelle.

In dringenden Fällen, Missbrauch oder Verdacht rufen Sie uns bitte an.

Unsere Service Center Nummer:

+49 (0) 69 / 29 90 11 99

Unsere Online Banking Nummer:

+49 (0) 1802 / 472 265

Wichtige Hinweise zu ihrer Sicherheit im Internet

Die İsbank AG wird von Ihnen niemals vertrauliche Daten wie Ihre PIN / TAN oder Ihr Passwort per E-Mail, Telefon oder SMS abfragen bzw. um Rücksendung oder Angabe dieser Daten bitten.

Unsere Leistungen für Ihre Sicherheit

Alle İsbank AG Karten verfügen über die aktuellste Chip- und PIN-Technologie.

Unsere Systeme werden täglich geprüft und gescannt.

Für eine sichere Verbindung wird als Kommunikationsprotokoll HTTPS (sicheres Hypertext-Übertragungsprotokoll) angewendet.

Für den sicheren Datentransfer mit Ihnen wird eine TLS-Verschlüsselung benutzt.

Bei dreimaliger falscher Eingabe Ihrer PIN erfolgt eine automatische Sperrung Ihres Zugangs zum Online-Banking. Diese Vorgehensweise gilt auch für die Bankkarten.

Für das Online-Banking wird ein TAN-Verfahren angewendet:

- **AppTAN:** Mit unserer İSBANK TAN App können Sie ihre Aufträge im Onlinebanking einfach, direkt und sicher freigeben. Die İSBANK TAN App ist als Download für Apple- und Android-Geräte erhältlich.

Sie werden automatisch aus dem Online-Banking ausgeloggt, wenn Sie inaktiv sind.

Allgemeine Hinweise für Ihre Sicherheit

Installieren Sie keine Programme, die Sie ungefragt von Bekannten oder Unbekannten per E-Mail erhalten haben. Installieren Sie nur Programme aus einer vertrauenswürdigen Quelle.

Benutzen Sie ein Anti-Virus Programm auf Ihrem PC und lassen sie durch das Programm regelmäßig alle Daten auf Viren überprüfen. Vergessen Sie nicht, Ihr Anti-Virus Programm aktuell zu halten.

Beginnt eine Internetverbindung mit Https, dann bedeutet dies, dass eine sichere Verbindung vorliegt. Ein weiteres Merkmal ist das geschlossene Schloss in der Adressleiste. **Bitte beachten Sie, dass Ihre Verbindung aus einer Https Verbindung besteht.**

Prüfen Sie Ihre Browser-Einstellungen (unter Einstellungen/Sicherheit).

Geben Sie niemals Ihre PIN und TAN-Daten weiter. Kein Mitarbeiter der İŞbank AG wird Sie weder am Telefon noch per E-Mail danach fragen.

Allgemeine Informationen

Phishing

Hierbei wird versucht, über gefälschte E-Mails, Webseiten oder auch Kurznachrichten an Ihre persönlichen Datenzugelangen.

Pharming

Beim Pharming wird mithilfe von sogenannten Trojanern oder Viren Ihr Betriebssystem so manipuliert, dass sie automatisch auf gefälschte Webseiten umgeleitet werden, obwohl Sie die Internetadresse richtig eingegeben haben.

Spam

Spam steht für unerwünschte E-Mails.

Spyware

Spyware spioniert unbemerkt die Daten aus und leitet diese an Dritte weiter.

Trojan

Trojaner sind Schadprogramme, die unbemerkt Aktionen auf dem Computer des Benutzers ausführen.