Sicheres Online-Banking

Mit Online-Banking erledigen Sie Ihre Bankgeschäfte schnell und komfortabel. Die Gefahren beim Online-Banking sind jedoch erheblich. Damit die Transaktionen auch sicher durchgeführt werden, beachten Sie unsere Sicherheitshinweise, denn Sie können mit wenigen Maßnahmen Langfingern den digitalen Zugriff auf Ihr Konto erheblich erschweren. Lesen Sie deshalb bitte die folgenden Sicherheitshinweise zur Internetsicherheit sorgfältig durch.

Bitte beachten Sie folgende Grundregeln für sicheres Online-Banking

1. Ihre Bank fragt beim Login zum Online-Banking niemals nach einer TAN!
2. Ihre Bank schickt Ihnen keine E-Mails, die einen Link zum Login des Online-Banking enthalten oder nach Zugangsdaten fragen!
3. Ihre Bank bittet grundsätzlich nicht um Rücksendung von Kreditkartennummern, Zugangsdaten, PIN oder TAN per E-Mail!
4. Geben Sie die URL zum Online-Banking (https://meine.bank.de/) immer direkt über die Tastatur ein und beachten Sie, dass Sie dabei lediglich ein Browserfenster bzw. ´Tab´ geöffnet haben!
5. Seien Sie vorsichtig auf Internetseiten, deren Adresse mit einer IP-Nummer statt eines Domain-Namens beginnt (z.B.: http://1232.456.789/...) oder deren Adresse die Bank nur als Sub-Domainnamen (z.B.: http://www.ihre-bank.domainname.com/...) bzw. Namensergänzungen oder Schreibvarianten enthält (z.B. http://www.ihre-bank-site.net/...)!
6. Handeln Sie umgehend, wenn Ihre Verbindung während des Online-Bankings nach Eingabe von PIN und TAN unterbrochen wird oder wenn ein Missbrauchsverdacht besteht. Sperren Sie sofort Ihren Online-Banking-Zugang und setzen Sie sich schnellstmöglich mit Ihrer Bank in Verbindung.

Wichtig beim Online-Banking

1. Loggen Sie sich möglichst nicht über einen Ihnen unbekannten Computer (z.B. Internetcafe) in Online-Banking ein.
2. Ändern Sie Ihre PIN regelmäßig und benutzen Sie dabei Kombinationen aus Buchstaben in Groß- und Kleinschreibung und Zahlen. Verwenden Sie dabei keine Kombinationen, die einen privaten Bezug haben wie beispielsweise Namen, Geburtsdatum, Telefonnummer, Postleitzahlen o.ä.
3. Führen Sie keine Online-Transaktionen aus, wenn Sie vermuten, dass Ihr PC von einem Trojanischen Pferd oder einem Virus befallen ist.

4. Nutzen Sie immer den Button 'Kunden-Logout', um Online-Banking zu verlassen.
5. Löschen Sie nach Verlassen vom Online-Banking immer den Zwischenspeicher (Cache), sofern nicht nur Sie an Ihrem Computer arbeiten.

Wichtig für Ihren PC

1. Spielen Sie immer die jeweils vom Hersteller empfohlenen aktuellen Sicherheitsupdates ein. Unser Service erledigt diese Aufgaben für Sie, fragen Sie uns, wir helfen Ihnen gerne.
2. Setzen Sie ein Virenschutzprogramm ein und aktualisieren Sie dieses regelmäßig - möglichst täglich. Wir sind Partner der führenden Anti-Virus Hersteller. Wir beraten Sie gerne.
3. Setzen Sie eine Personal Firewall ein, die Ihrem PC zusätzlichen Schutz bietet. Links zu Programmen bekannter Hersteller finden sie in unserem Shop oder fragen Sie uns persönlich.
4. Benutzen Sie beim Ausfüllen von Online-Formularen nie den 'Form-Manager' oder die 'Auto vervollständigen'-Funktion Ihres Browsers, da sonst eingetragene Daten auf Ihrem PC gespeichert und von Dritten gelesen werden können.
5. Deaktivieren Sie in den Sicherheitseinstellungen des Internet Explorer die Option ‚Subframes zwischen verschiedenen Domänen bewegen damit 'Phishing mit Frames' nicht funktioniert. Die aktuellen Versionen von Mozilla (ab 1.7.8), Firefox (ab 1.0.4) und Opera (ab 8.0) weisen das Problem nicht mehr auf.
6. Downloaden Sie Software nur aus vertrauenswürdigen Quellen.
7. Vorsicht bei der Datenübertragung über ein kabelloses lokales Funknetzwerk (WLAN). WLAN-Verschlüsselung aktivieren.
8. Wird Ihr alter PC verkauft bzw. entsorgt, vergewissern Sie sich das alle Daten auf der Festplatte nicht wieder rekonstruiert werden können.

Chipkartenbasiertes Online-Banking

Als Alternative haben Sie die Möglichkeit, das chipkartenbasierte Online-Banking (HBCI) zu nutzen. Hier ist Ihr Zugangscode hochsicher in einem Chip gespeichert. Lassen Sie sich von Ihrer Bank zu Ihrer Internetsicherheit beraten.

HBCI Banking

Homebanking Computer Interface (HBCI) ist ein offener Standard für den Bereich Electronic Banking und Kundenselbstbedienung.

Mit dieser chipkartenbasierten Lösung können Sie Ihre Bankgeschäfte direkt im Internet ohne PIN und TAN erledigen oder eine HBCI-fähige Banking Software nutzen.

Auf der Chipkarte sind die Zugangsdaten für Ihr Konto gespeichert. Beim Einloggen müssen Sie diese Daten nicht mehr eingeben, sondern nur noch die Karte ins Chipkartenlesegerät einlegen und Ihre Geheimzahl eingeben. Dabei bietet Ihnen die Chipkarte dank neuer Verschlüsselungstechniken und der sechsstelligen Geheimzahl größt mögliche Sicherheit.

Der Chipkartenleser

Mit dem Klasse 2-Chipkartenlesegerät runden Sie Ihr Sicherheitspaket ab – denn: Dieser Kartenleser ist vom Bundesamt für Sicherheit in der Informationstechnik zertifiziert. Die Geheimzahl wird über eine integrierte Tastatur (pinpad) direkt an die Chipkarte – und damit ohne Umweg über den PC – weitergegeben. Somit erfolgt die Verschlüsselung direkt im Chipkartenleser und nicht auf Ihrem PC.

Wir von Rösner-IT:

- ✓ Beraten Sie individuell
- ✓ Überprüfen ihren PC- und Netzwerk auf die geforderten Sicherheitsmechanismen
- ✓ Anti-Virus Lösungen für Privatanwender und Unternehmen
- ✓ Firewall Lösungen für Privatanwender und Unternehmen

Rösner-IT
EDV
IT-Security
Consulting & Service

Rösner-IT ♦ Lönsstr. 16 ♦ 48485 Neuenkirchen
Tel: +49 (0) 5973-90 06 52 ♦ Fax: +49 (0) 5973-90 07 98
E-Mail: info@roesner-it.com ♦ Web: www.roesner-it.com