

## Unsere Tipps für sicheres Online Banking:

1. **Aktualisieren Sie Ihr Betriebssystem und Ihren Browser regelmäßig.**  
Die meisten Programmanbieter stellen regelmäßige Aktualisierungen bereit, die neu erkannte Sicherheitslücken schließen.
2. **Schützen Sie Ihren PC mit Sicherheitsprogrammen wie Antivirensoftware und Firewall.**  
Vergessen Sie bitte vor allem bei der Antivirensoftware nicht, diese regelmäßig zu aktualisieren.
  - § **Achten Sie auf eine sichere Verbindung beim Internet Banking.**  
Die Daten, die zwischen Ihrem PC und der Bank übertragen werden, sind so verschlüsselt, dass Dritte die Daten weder lesen noch manipulieren können. Sie erkennen die Verschlüsselung daran, dass in der unteren Statusleiste des Browsers am rechten Rand ein gelbes geschlossenes Vorhängeschloss angezeigt wird.  
Fehlt dieses Vorhängeschloss oder wird ein geöffnetes Schloss angezeigt, dann werden die Daten nicht verschlüsselt.  
  
So können Sie das Sicherheitszertifikat überprüfen und herausfinden, dass Sie sich wirklich auf der Seite der Bank befinden:
3. **Deaktivieren Sie kritische Funktionen in Ihrem Browser.**  
Die Einstellungen betreffen den Microsoft Internet Explorer sowie alle darauf basierenden Browser (z.B. T-Online Browser oder AOL-Browser).  
Öffnen Sie den Einstellungs-Dialog über: **Start | Systemsteuerung | Internetoptionen | Sicherheit.**  
Klicken Sie hier auf die Schaltfläche **[Stufe anpassen]** und führen folgende Änderungen durch:
  - § **ActiveX**  
Stellen Sie alle Einträge, die sich auf ActiveX beziehen, auf Deaktivieren.  
*Hinweis: Es gibt nur wenige Seiten, die ActiveX voraussetzen und nach dessen Deaktivierung nicht mehr funktionieren. Hierzu zählt unter anderem die Updateseite von Microsoft. Umgehen können Sie das Problem, indem Sie die betreffenden Seiten zur Liste der 'vertrauenswürdigen Sites' hinzufügen.*
  - § **IFRAME**  
Programme und Dateien in einem IFRAME starten: Deaktivieren.
  - § **Subframes**  
Subframes zwischen verschiedenen Domänen bewegen: Deaktivieren.
4. **Behalten Sie PIN und TAN geheim.**  
Beachten Sie, dass Volks- und Raiffeisenbanken niemals Ihre persönlichen Informationen oder vertraulichen Daten per eMail abfragen.  
Seien Sie insbesondere misstrauisch, falls Sie per eMail aufgefordert werden, per Link eine Bankseite zu besuchen auf der PIN und TAN abgefragt werden. Es handelt sich hierbei um gefälschte Seiten.
5. **Seien Sie misstrauisch bei fremden PCs.**  
Fremde PCs (z.B. in Internet-Cafés) bergen ein deutlich höheres Sicherheitsrisiko, da die Zuverlässigkeit der Datenverbindung nicht eingeschätzt werden kann.
6. **Sperren Sie Ihr Konto, sobald Sie glauben, dass ein Dritter Ihre PIN oder TAN erlangt hat.**  
Dies geht direkt über Ihre Bank oder im Notfall über dreimalige falsche Eingabe der PIN beim Online-Banking.
7. **Höchste Sicherheit bietet das HBCI-Chipkartenverfahren in Verbindung mit einem Zahlungsverkehrsprogramm.**  
Wir beraten Sie in dieser Hinsicht gerne.

**Tel. 0781 -800258**