



Sicherheit beim Online-Banking

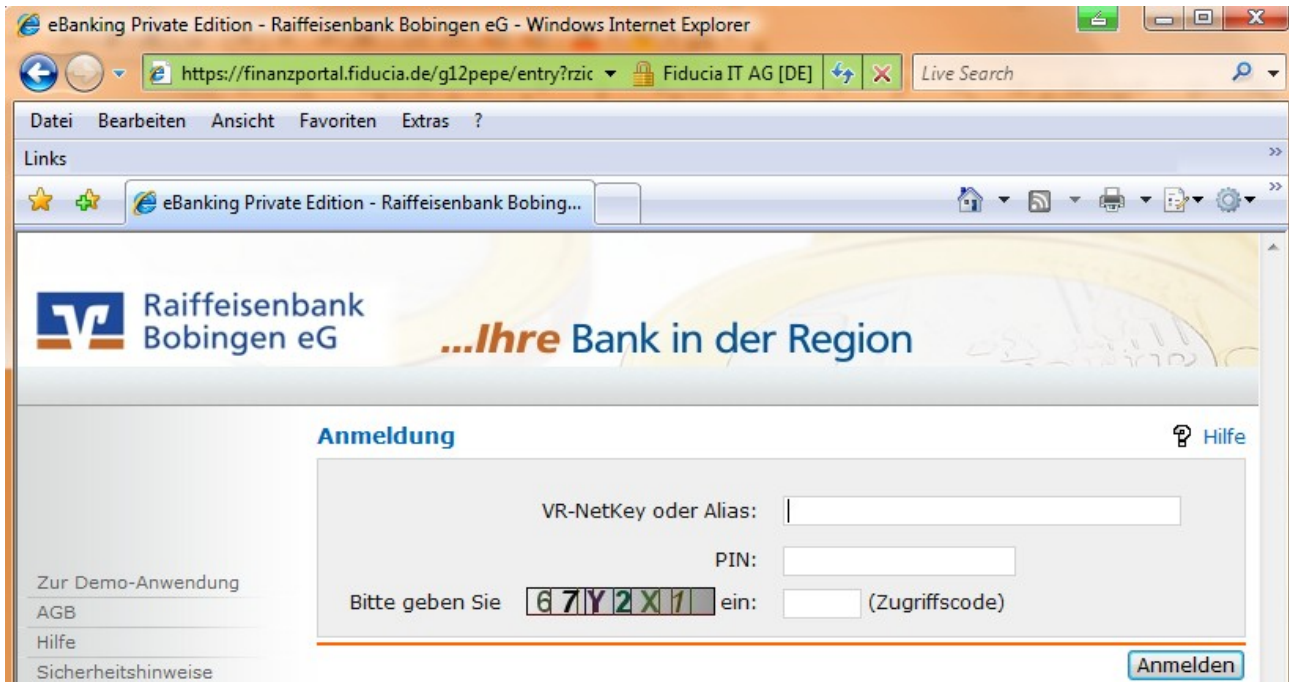
So schützen Sie sich vor "Phishing" & Co

Im Folgenden sind die wichtigsten Empfehlungen zusammengefasst, wie sich Nutzer des Online-Bankings vor unliebsamen Überraschungen aus dem Netz schützen können. Hält sich der Kunde daran, ist er beim Online-Banking auf der sicheren Seite.

- 1.) **Virenschutzlösung, Firewall und Antispy-Software:** Setzen Sie auf professionellen Virenschutz, Firewall und Antispy-Programme. Viele Hersteller verkaufen die drei Lösungen im Paket. Und vergessen Sie weder die regelmäßigen Updates noch die regelmäßigen Überprüfungen ihres Systems!
- 2.) **Regelmäßige Updates:** Immer wieder werden Fehler in den Betriebssystemen bekannt, die von Viren ausgenutzt werden, um in den Computer einzudringen. Hersteller wie Microsoft stellen regelmäßig Patches zum Download bereit, die diese Lücken schließen. Aktualisieren Sie Ihr Betriebssystem regelmäßig!
- 3.) **Anwendungen die regelmäßig mit dem Internet verbunden sind:** Anwendungen die regelmäßig auf das Internet zugreifen, wie etwa der Internetbrowser oder Adobe Reader, sollten ebenfalls stets aktuell sein!
- 4.) **Passwort:** Ein sicheres Passwort besteht aus mindestens acht Zeichen und enthält Sonderzeichen und Zahlen. Außerdem sollte es kein herkömmliches Wort einer Sprache sein. Besser ist beispielsweise ein Anagramm aus den Anfangsbuchstaben eines Kinderlieds. Wenn Sie dann noch Buchstaben durch ähnlich aussehende Zahlen und Sonderzeichen ersetzen, wird „Alle meine Entchen schwimmen auf dem See“ zu @mE5adS!“
- 5.) **Vorsicht bei E-Mail-Anfragen:** Ignorieren Sie Mails, in denen Sie nach Ihrer PIN oder einer TAN gefragt werden – Ihre Bank wird sie nie nach solch wichtigen Informationen fragen.
- 6.) **Vertrauenswürdige Seiten:** Bewegen Sie sich im Internet nur auf vertrauenswürdigen Webseiten und meiden Sie verdächtige Gegenden - ganz wie im richtigen Leben. Werden Sie misstrauisch, wenn in der Adressleiste nur die IP-Adresse statt einer richtigen Webadresse angezeigt wird!
- 7.) **Sichere Online-Banking-Verfahren:** Auch wenn Ihr PC rundum geschützt ist, verzichten Sie nicht auf den Einsatz eines sicheren Online-Banking-Verfahrens. Die mobileTAN und die SmartTANplus schützen beispielsweise gegen alle zur Zeit bekannten Betrugs-Szenarien. Darüber hinaus ermöglicht Ihnen die mobileTAN ihre Bankgeschäfte flexibel abzuwickeln – egal ob von Zuhause aus oder von unterwegs.
- 8.) **Anmeldung auf der Homebanking-Seite:** Starten Sie Ihren Internetbrowser (Firefox, Internet-Explorer, etc.) und **geben Sie die Internetadresse www.raiba-bobingen.de immer direkt in die Adressleiste ein.**



Achten Sie darauf, dass Sie sich auf einer sicheren Seite befinden (https), erkennbar an der farblichen Kennzeichnung, sowie an einem geschlossenen Sicherheitsschloss.



Wichtig:

Die Bankseite nicht in den Lesezeichen oder Favoriten speichern, da sich dort ein Virus oder Trojaner festsetzen könnte. Das Öffnen über die Google-Suche birgt außerdem die Gefahr auf eine Phishing-Seite zu gelangen. Das bedeutet, dass Sie dann auf einer gefälschten Internetseite Ihre Daten eingeben.

Optional können Sie noch folgende Tipps beachten:

- 1.) **Sicherheits-Check:** Die Initiative ‚Sicher im Netz‘ der Bundesregierung bietet einen kostenlosen Sicherheitscheck an. Testen Sie regelmäßig unter www.sicher-im-netz.de, wie sicher Ihr PC wirklich ist.
- 2.) **Benutzerrechte auf dem Rechner einschränken:** Um sicher zu surfen, sollte jeder PC-Besitzer ein zusätzliches Konto ohne Administrator-Rechte auf dem Rechner einrichten. So lässt sich verhindern, dass sich heimlich Schadprogramme auf dem Rechner einnisten, denn nur im Administratoren-Modus kann Software installiert und ausgeführt werden.
- 3.) **Virtuelle Tastatur:** Geben Sie Keyloggern keine Chance und nutzen Sie zur Eingabe von PIN und TAN eine virtuelle Tastatur. Die virtuelle Tastatur ist kein Hardwarebestandteil sondern eine Software, die eine Tastatur auf dem Bildschirm anzeigt. Die einzelnen Tasten werden mit der Maus angeklickt. Passwörter, TAN's und PIN's können so von Hardware-Keyloggern nicht ausgelesen werden.