Empfehlungen zur Sicherheit beim E-Banking

Mit der Berücksichtigung dieser Empfehlungen können Internetnutzer zur Steigerung der Sicherheit im E-Banking beitragen.

SYSTEMSICHERHEIT

1. NUTZUNG VERTRAUENSWÜRDIGER COMPUTER:

Vergewissern Sie sich, dass nur Personen Ihres Vertrauens das Computersystem nutzen oder administrieren. Wickeln Sie niemals Bankgeschäfte über nicht vertrauenswürdige Computer ab.

2. VERWENDUNG SICHERHEITSOPTIMIERTER BETRIEBSSYSTEME UND BROWSER:

Nur gepflegte und gewartete Computersysteme verwenden – das Betriebssystem sollte jedenfalls in regelmäßigen Abständen mit den neuesten Erweiterungen der Sicherheitssoftware versorgt werden. Gleiches gilt selbstverständlich für Ihren Browser. Aktivieren Sie die automatischen Updates und den Phishing-Filter im Internet-Browser. Nähere Informationen hierzu erhalten Sie bei Ihrem Software-Betreuer oder -Lieferanten.

3. EINSATZ VON VIRENSCHUTZ UND FIREWALL:

Verwenden Sie ein aktuelles Virenschutzprogramm mit regelmäßigen automatischen Updates gegen Spyware, Viren und Trojaner bzw. aktivieren Sie eine Personal Firewall zum Schutz Ihres Computersystems.

SICHERES VERHALTEN

4. VERTRAULICHKEIT VON PIN UND TAN:

Geben Sie Ihre persönlichen Zugriffs- und Autorisierungsdaten , wie die Login-Daten (PIN) und Geldtransferautorisierungsdaten (TAN), niemals an Dritte weiter und nur auf der überprüften Internet-Banking-Seite des Geldinstituts ein, zu dem eine Kontoverbindung besteht. Niemals dürfen diese vertraulichen Daten in E-Mails, Formularen oder unbekannten Internet-Banking-Systemen eingegeben werden.

5. INTERNET-BANKING-ADRESSE DER BANK (URL) NUR MANUELL EINGEBEN:

Folgen Sie niemals Links aus E-Mails oder von anderen Internet-Seiten zum (vermeintlichen) Internet-Banking-Portal der Hausbank. Auch die Verwendung von Bookmarks (Favoriten, Lesezeichen) birgt Gefahrenpotenzial, da sie von Hackern manipuliert werden können.

6. INTERNET-BANKING-SEITE PRÜFEN:

Die Internet-Banking-Adresse Ihrer Bank sollten Sie genau lesen und aufschreiben, damit Sie sie beim nächsten Einloggen sofort wiedererkennen. Achten Sie auf eine sichere, verschlüsselte Verbindung. Diese erkennen Sie am Schlosssymbol und daran, dass in der Adressleiste des Browsers „https://...“ angezeigt wird. Sollte Verdacht bestehen, dass es sich um eine nicht sichere Verbindung handelt, prüfen Sie auch, ob die Verschlüsselung mittels digitalem Sicherheitszertifikat aktiviert ist. Dazu genügt das Anklicken des Schloss-Symbols auf Ihrem Browsers. Sie können hier die Echtheit des Sicherheitszertifikates prüfen. Die Detaildaten erhalten Sie in den Sicherheitsinformationen Ihres Online-Banking Anbieters. Wird in der Adresszeile hingegen lediglich „http://...“ angezeigt, handelt es sich definitiv um keine legitime onlinebanking-Seite Ihrer Bank.

7. BENUTZER-PIN UND TAN GEHÖREN NICHT AM COMPUTER ABGELEGT:

Verwahren Sie Ihre vertraulichen Bankinformationen an einem sicheren Ort. Da die Daten auf einem PC ausgespäht werden können, raten wir von einer Speicherung auf dem PC dringend ab.

MÖGLICHE GEFAHREN BEACHTEN

8. VORSICHT BEI ANGEBLICHEN BANKEN E-MAILS:

Österreichische Bankinstitute versenden grundsätzlich keine E-Mails, in denen Kunden aufgefordert werden, vertrauliche Zugangs- und Transaktionsinformationen preiszugeben. Dazu zählen Verfügernummer, PIN und TAN. Bei dieser Art von E-Mails handelt es sich immer um Betrugsversuche.

9. BANKENINFOS BEACHTEN UND VORFÄLLE DER BANK-HOTLINE MELDEN:

Beachten Sie die Sicherheitshinweise Ihrer Hausbank auf der entsprechenden Internet-Homepage. Sobald der Verdacht auf Betrug entsteht, geben Sie keinerlei Daten Preis und melden Sie Ihren Verdacht der jeweiligen Bank-Hotline. Sie sollten auch die Nummer Ihrer Bank-Hotline in Ihrem Handy speichern. Bei sicherheitsrelevanten Vorfällen sollte der PIN schnellstmöglich über eine sichere Verbindung geändert werden.

10. KONTOAUSZÜGE REGELMÄSSIG PRÜFEN:

Überprüfen Sie in regelmäßigen Abständen Ihre Kontoauszüge auf Unregelmäßigkeiten.

Herausgegeben von der Bundessparte Bank und Versicherung der Wirtschaftskammer Österreich in Absprache mit der Konsumentenschutzsektion des BMSK.