Online-Banking

45 Tipps für das sichere Online-Banking

Notwendige Sicherheits-vorkehrungen am PC

1 Versuchen Sie, möglichst wenige Personen an dem PC arbeiten zu lassen, an dem Sie auch das Online-Banking nutzen. Dadurch werden die Risiken reduziert, die durch andere Personen entstehen können.

2 Setzen Sie Sicherheitsprogramme wie Anti-Viren-Software oder Firewalls ein, um Ihren PC gegen Schadprogramme wie Viren, Trojaner usw. zu schützen.

3 Installieren Sie nur Softwareprogramme, von denen Sie genau wissen, wer der Hersteller ist und welche Funktion diese haben.

4 Vermeiden Sie das Installieren unnötiger Softwareprogramme, damit Sie einen besseren Überblick haben.

5 Führen Sie eine regelmäßige Aktualisierung Ihres Betriebssystems wie Windows XP oder ME durch – am Besten automatisch im Hintergrund. So ist sichergestellt, dass eventuell vorhandene Sicherheitslöcher gestopft werden.

6 Informieren Sie sich regelmäßig z.B. auf www.microsoft.de über verfügbare Aktualisierungen.

7 Überprüfen Sie Ihren PC regelmäßig anhand der Firewall-Software auf mögliche ungewollte Besucher auf Ihrem Rechner.

8 Speichern Sie regelmäßig Ihre Daten als Sicherheitskopien auf CD oder Diskette. So begrenzen Sie einen möglichen Datenverlust durch Viren oder eine Beschädigung des Betriebssystems.

9 Nutzen Sie nur Funktastaturen mit eingebauter Verschlüsselung für das Online-Banking. Denn ohne Verschlüsselung können je nach Modell mit Funkempfängern im Umkreis mehrerer Meter – auch durch Wände – alle eingegebenen Daten direkt empfangen und mitgelesen werden.

10 Verwenden Sie keine Links aus Mailadressen, um ihr Online-Banking aufzurufen. Nutzen Sie Bookmarks, die Sie selber angelegt haben und die entweder auf die Einstiegsseite ihrer Bank oder auf direkt auf das Online-Banking verweisen.

Großes Augenmerk für den Internet-Browser

11 Verwenden Sie keine Test-Versionen von Internet-Browsern. Diese so genannten Beta-Versionen können Sicherheitslücken enthalten oder Fehlfunktionen aufweisen.

12 Nutzen Sie nicht die „Autovervollständigung“-Funktion Ihres Browsers. Benutzernamen und Passwörter werden hierbei relativ ungesichert auf der Festplatte gespeichert.

13 Aktualisieren Sie regelmäßig Ihren Internet-Browser. Die einzelnen Anbieter stellen auf ihren Webseiten regelmäßig Aktualisierungen (so genannte Updates und Patches) bereit, die neu erkannte Sicherheitslücken schließen.

14 Deaktivieren Sie die Zusatzfunktion „ActiveX“ in Ihrem Browser. Hierüber können Dritte über das Internet unter Umständen unkontrolliert Programme installieren.

15 Verwenden Sie nach Möglichkeit keine Erweiterungen (Plug-Ins) für Ihren Browser, da sie ein zusätzliches Risiko darstellen.

16 Löschen Sie den Zwischenspeicher (Cache) des Browsers nach jeder Online-Banking-Sitzung.

Vorsichtiger Umgang mit den Geheimzahlen

17 Sorgen Sie dafür, dass nur Sie alleine Kenntnis von PIN und TAN haben.

18 Bewahren Sie PIN und TAN grundsätzlich getrennt voneinander auf.

19 Legen Sie den TAN-Bogen möglichst an einer nicht mit dem PC in Verbindung stehenden Stelle ab.

20 Notieren sie PIN oder TAN nicht auf Zetteln am Computer, der Schreibtischunterlage etc.

21 Speichern Sie Ihre PIN oder TAN nicht in ungeschützten Dateien wie z.B. Word oder Excel.

22 Verwenden Sie nach Möglichkeit nicht das Angebot verschiedener Online-Banking-Programme, die komplette TAN-Liste und die PIN einmalig einzugeben und zu speichern.

23 Nutzen Sie die mögliche Anzahl von Zahlen und Buchstaben, die Ihre Bank ermöglicht, weitestgehend aus. Dies macht ein Erraten oder Herausfinden Ihrer PIN viel schwieriger.

24 Verwenden Sie auf keinen Fall Geburtstage oder Namen von Kindern oder Haustieren als PIN, da Sie zu leicht erraten werden können.

25 Stellen Sie Ihre Passwörter aus Groß- und Kleinbuchstaben, Zahlen und wenn möglich auch unter Nutzung von Sonderzeichen wie „$“ oder „&“ zusammen. Dies macht es für Dritte fast unmöglich, Ihr Passwort herauszufinden.

26 Ändern Sie Ihre Passwörter regelmäßig.

27 Verwenden Sie nach Möglichkeit für verschiedene Funktionen wie die Einwahl ins Internet, Online-Banking etc. unterschiedliche Passwörter.

28 Antworten Sie grundsätzlich nicht auf E-Mails oder Anrufe, bei denen nach PIN und TAN gefragt wird. Denn Banken fragen Sie nie nach Ihren persönlichen Daten, demzufolge müssen sich dahinter Dritte mit risikobehafteten Absichten befinden.

29 Sperren Sie Ihr Konto, sobald sie glauben, dass ein Dritter Ihre PIN oder TAN erlangt hat. Z.B. bei Überweisungen, die sie nicht getätigt haben und die in den Kontobewegungen aufgeführt werden. Dies geht direkt über Ihre Bank oder im Notfall über dreimalige falsche Eingabe der PIN beim Online-Banking.

Sichere Benutzung des Online-Banking-Programms

30 Vereinbaren Sie mit Ihrer Bank ein Limit für Online-Überweisungen pro Tag. So kann ein möglicher Schaden von vornherein auf eine bestimmte Summe begrenzt werden.

31 Speichern Sie PIN und TAN nach Möglichkeit nicht ab, auch wenn z.B. der Browser eine Speicherung Ihres Benutzernamens und Passwortes anbietet.

32 Stellen Sie grundsätzlich vor Eingabe Ihrer PIN sicher, dass eine geschützte Verbindung (128bit SSL) aufgebaut wurde. Dies ist an dem geschlossenen Schloss-Symbol unten rechts im Browser zu erkennen. Überprüfen Sie zusätzlich das Zertifikat (s.u.) der Webseite, damit Sie sicher sein können, dass eine verschlüsselte Verbindung zur Bank aufgebaut wurde.

33 Überprüfen Sie, ob die im Browser angezeigte Internet-Adresse mit der zertifizierten Adresse Ihrer Bank übereinstimmt. Die Informationen erhalten Sie über einen Doppelklick auf das Schloss-Symbol im Browser.

34 Brechen Sie Online-Banking-Sitzungen grundsätzlich sofort ab, wenn Sie irgendwelche Sachverhalte während des Vorgangs auffällig finden. Fragen Sie im Zweifelsfall erst bei Ihrer Bank nach, ob diese Auffälligkeiten zum regulären Ablauf beim Online-Banking gehören.

35 Stellen Sie sicher, dass Sie niemand bei der Eingabe von PIN und TAN beobachten kann.

36 Kontrollieren Sie alle eingegebenen Daten genauestens. Denn die einmal getätigte Überweisung ist verbindlich!

37 Sollten Sie nicht sicher sein, ob Ihre Überweisung die Bank erreicht hat, warten Sie lieber bis zum nächsten Tag oder rufen Sie Ihre Bank an, bevor Sie den Überweisungsvorgang wiederholen. Sonst erfolgen unter Umständen zwei Überweisungen, da die Computer der Bank keine Korrektur einer vorherigen Überweisung erkennen können.

38 Verlassen Sie die Webseite Ihrer Bank nach Überweisungen grundsätzlich über die „Logout“- oder „Beenden“-Funktion und schließen Sie alle Browserfenster. Dadurch kann ein Dritter nicht auf ihr Konto zugreifen, wenn Sie ihren PC verlassen haben.

Besondere Gefahren beim Online-Banking an anderen Orten

39 Seien Sie sich grundsätzlich bewusst, dass ein fremder Rechner deutlich höhere Sicherheitsrisiken birgt.

40 Kontrollieren Sie Sicherheitsfunktionen wie Zertifikate von Webseiten oder die verschlüsselte Verbindung genauestens, um das Risiko zu reduzieren.

41 Nutzen Sie möglichst nie Internet-Cafés für das Online-Banking. Hier hat jeder teilweise völlig unkontrollierten Zugang, was das Sicherheitsrisiko drastisch erhöhen kann.

42 Meiden Sie auch andere private PCs oder den Firmen-PC, da sie hier nicht wissen, wie sicher der Rechner ist und ob Viren etc. auf der Festplatte schlummern.

43 Löschen Sie bei einem fremden Rechner grundsätzlich den Zwischenspeicher (Cache) nach Beendigung des Online-Banking und melden Sie sich auf jeden Fall über die „Abmelden"-Funktion Ihrer Bank ab. So kann niemand herausfinden, auf welchen Seiten Sie sich aufgehalten haben.

44 Vermeiden Sie Online-Banking über öffentliche Hotspots, da hierbei Funkverbindungen (Wireless-LAN) in das Internet bestehen, deren Abhörsicherheit von Ihnen nicht genau eingeschätzt werden kann.

45 Nutzen Sie keine Rechner für das Online-Banking, die sich nicht direkt in das Internet einwählen, sondern sich einen gemeinsamen Internetzugang teilen. Hier ist ein Router zwischen Ihrem Rechner und der Bank geschaltet, was das Risiko erhöhen kann. Dies trifft auf Internet-Cafés, Hotspots oder auch Firmennetzwerke zu.

FIDUCIA IT AG

Fiduciastraße 20
76227 Karlsruhe
Telefon (07 21) 40 04 - 43 21

info@fiducia.de
www.fiducia.de