



Das **«** Wir machen den Weg frei **»** Prinzip

***Rundum sicher beim Online-Banking.
45 wichtige Tipps von Ihren
Volksbanken Raiffeisenbanken.***



Sicherheitsvorkehrungen am eigenen PC

- 1** Versuchen Sie, so wenig Personen wie möglich an dem PC arbeiten zu lassen, den Sie für das Online-Banking nutzen. Dadurch werden die Risiken reduziert, die durch andere Personen entstehen können.
- 2** Setzen Sie Sicherheitsprogramme wie Anti-Viren-/ Anti-Spyware-Software und Firewalls ein, um Ihren PC gegen Schadprogramme wie Viren, Trojaner usw. zu schützen. Nutzen Sie die automatische Aktualisierungsfunktion dieser Programme.
- 3** Arbeiten Sie an Ihrem PC mit niedrigen Berechtigungen. Richten Sie einen eigenen Benutzer mit administrativen Berechtigungen ein, den Sie ausschließlich für die Installation von Software benutzen. Dadurch haben viele Schädlinge keine Chance, sich auf Ihrem PC einzunisten.
- 4** Installieren Sie nur Software-Programme, von denen Sie genau wissen, welche Funktion sie haben und wer ihr Hersteller ist.
- 5** Vermeiden Sie das Installieren unnötiger Software-Programme, damit Sie einen besseren Überblick haben.
- 6** Führen Sie eine regelmäßige Aktualisierung Ihres Betriebssystems durch – am besten automatisch im Hintergrund. So ist sichergestellt, dass eventuell vorhandene Sicherheitslücken gestopft werden.
- 7** Informieren Sie sich regelmäßig, z.B. auf www.microsoft.de, über verfügbare Aktualisierungen.
- 8** Überprüfen Sie Ihren PC regelmäßig anhand der Firewall-Software auf mögliche ungewollte Besucher auf Ihrem Rechner.
- 9** Speichern Sie Ihre Daten regelmäßig als Sicherheitskopien auf CD oder Diskette. So begrenzen Sie einen möglichen Datenverlust durch Viren oder eine Beschädigung des Betriebssystems.
- 10** Benutzen Sie Funktastaturen nur, wenn sie mit einer eingebauten Verschlüsselung ausgestattet sind. Denn ohne Verschlüsselung können alle eingegebenen Daten je nach Modell im Umkreis mehrerer Meter – auch durch Wände – mit Funkempfängern direkt empfangen und mitgelesen werden.
- 11** Verwenden Sie keine Links aus Mail-Adressen, um Ihr Online-Banking aufzurufen. Nutzen Sie Bookmarks, die Sie selbst angelegt haben und die entweder auf die Einstiegsseite Ihrer Bank oder direkt auf das Online-Banking verweisen.
- 12** Öffnen Sie keine Mail-Anhänge, die Sie nicht erwarten. Wenn Sie Ihre Telefonrechnung üblicherweise auf dem Postweg erhalten, ist es nicht wahrscheinlich, dass Ihre Telefongesellschaft Ihre Mail-Adresse kennt und Ihnen die Rechnung neuerdings auf diesem Weg zustellt.

Besonderes Augenmerk auf den Internet-Browser

- 13** Verwenden Sie keine Test-Versionen von Internet-Browsern. Diese so genannten Beta-Versionen können Sicherheitslücken enthalten oder Fehlfunktionen aufweisen.
- 14** Nutzen Sie nicht die „Autovervollständigung“-Funktion Ihres Browsers. Benutzernamen und Passwörter werden hierbei schwach geschützt auf der Festplatte gespeichert.
- 15** Aktualisieren Sie regelmäßig Ihren Internet-Browser. Die einzelnen Anbieter stellen auf ihren Web-Seiten regelmäßig Aktualisierungen (so genannte Updates und Patches) bereit, die neu erkannte Sicherheitslücken schließen.
- 16** Deaktivieren Sie die Zusatzfunktion „ActiveX“ in Ihrem Browser. Hierüber können Dritte über das Internet unter Umständen unkontrolliert Programme installieren.
- 17** Verwenden Sie nach Möglichkeit keine Erweiterungen (Plug-Ins) für Ihren Browser, da sie ein zusätzliches Risiko darstellen.
- 18** Löschen Sie den Zwischenspeicher (Cache) des Browsers nach jeder Online-Banking-Sitzung.



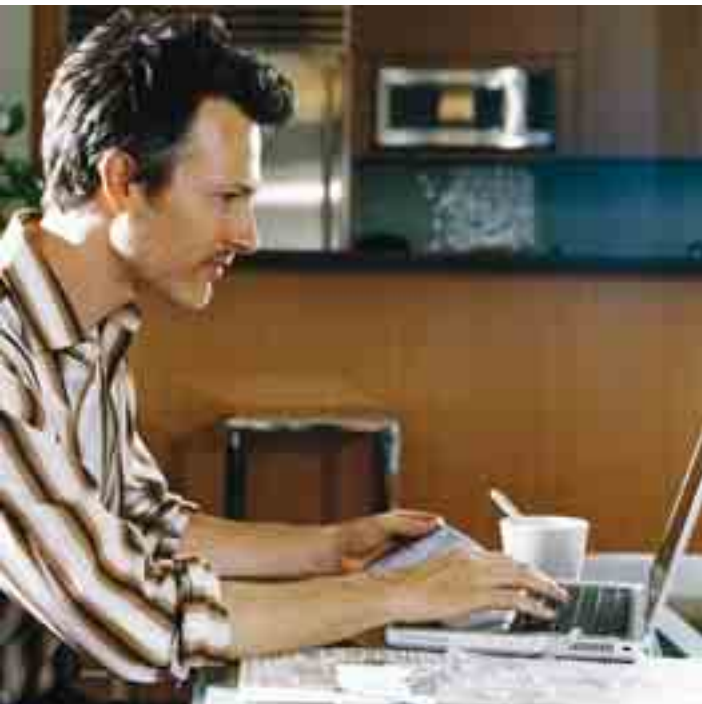


Vorsichtiger Umgang mit den Geheimzahlen

- 19 Sorgen Sie dafür, dass nur Sie allein Kenntnis von PIN und TAN haben.
- 20 Bewahren Sie PIN und TAN grundsätzlich getrennt voneinander auf.
- 21 Legen Sie den TAN-Bogen möglichst an einer nicht mit dem PC in Verbindung stehenden Stelle ab.
- 22 Notieren Sie PIN oder TAN nicht auf Zetteln am Computer, der Schreibtischunterlage etc.
- 23 Speichern Sie Ihre PIN oder TAN nicht in ungeschützten Dateien wie Word oder Excel.
- 24 Verwenden Sie nach Möglichkeit nicht das Angebot verschiedener Online-Banking-Programme, die komplette TAN-Liste und die PIN einmalig einzugeben und zu speichern.
- 25 Nutzen Sie die maximale Anzahl von Zahlen und Buchstaben, die Ihre Bank ermöglicht, weitestgehend aus. Dies macht ein Erraten oder Herausfinden Ihrer PIN viel schwieriger.
- 26 Verwenden Sie auf keinen Fall Geburtstage oder Namen von Kindern oder Haustieren als PIN, da sie zu leicht erraten werden können.
- 27 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.
- 28 Ändern Sie Ihre Passwörter regelmäßig.
- 29 Verwenden Sie nach Möglichkeit für verschiedene Funktionen wie die Einwahl ins Internet, Online-Banking etc. unterschiedliche Passwörter.
- 30 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.
- 31 Sperren Sie Ihren Zugang zum Online-Banking, sobald Sie den Verdacht haben, dass ein Dritter im Besitz Ihrer PIN oder TAN ist. Haben Sie bereits einen VR-NetKey? Dann nutzen Sie die Möglichkeit, den VR-NetKey direkt in Ihrer E-Banking-Anwendung über den Menüpunkt „VR-NetKey-Sperre“ zu sperren. Falls Sie keinen VR-NetKey besitzen, lassen Sie Ihr Online-Banking über Ihren Bankberater sperren.

Sichere Handhabung des Online-Banking-Programms

- 32** Vereinbaren Sie mit Ihrer Bank ein Tageslimit für Online-Überweisungen. So kann ein möglicher Schaden von vornherein auf eine bestimmte Summe begrenzt werden.
- 33** Speichern Sie PIN und TAN nach Möglichkeit nicht ab, auch wenn z. B. der Browser eine Speicherung Ihres Benutzernamens und Passwortes anbietet.
- 34** Stellen Sie grundsätzlich vor Eingabe Ihrer PIN sicher, dass eine geschützte Verbindung (mindestens 128 Bit SSL) aufgebaut wurde. Dies ist an dem geschlossenen Schloss-Symbol unten rechts im Browser zu erkennen. Überprüfen Sie zusätzlich das Zertifikat (s. u.) der Web-Seite, damit Sie sicher sein können, dass eine verschlüsselte Verbindung zur Bank aufgebaut wurde.
- 35** Beachten Sie die Warnhinweise Ihres Browsers. Geben Sie keine PIN auf einer Seite ein, vor der Sie Ihr Webbrowser durch eine Sicherheitsmeldung gewarnt hat.
- 36** 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.
- 37** Stellen Sie sicher, dass Sie niemand bei der Eingabe von PIN und TAN beobachten kann.
- 38** Kontrollieren Sie alle eingegebenen Daten genau. Denn die einmal getätigte Überweisung ist verbindlich!
- 39** 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 nicht auf die Korrektur einer vorherigen Überweisung ausgelegt sind.
- 40** Verlassen Sie die Web-Seite Ihrer Bank nach Überweisungen grundsätzlich über die „Logout“- oder die „Beenden“-Funktion und schließen Sie alle Browser-Fenster. Dadurch kann ein Dritter nicht auf Ihr Konto zugreifen, wenn Sie Ihren PC verlassen haben.





Gefahren beim Online-Banking an fremden Orten

- 41** Seien Sie sich grundsätzlich bewusst, dass ein fremder Rechner deutlich höhere Sicherheitsrisiken birgt.
- 42** Kontrollieren Sie Sicherheitsfunktionen wie Zertifikate von Web-Seiten oder die verschlüsselte Verbindung genauestens, um das Risiko zu reduzieren.
- 43** Nutzen Sie möglichst nie Internet-Cafés für das Online-Banking. Hier hat jeder teilweise völlig unkontrollierten Zugang, was das Sicherheitsrisiko drastisch erhöhen kann.
- 44** 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.
- 45** Löschen Sie bei einem fremden Rechner grundsätzlich den Zwischenspeicher (Cache) nach Beendigung des Online-Bankings 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.

Im Falle eines Falles:

Wenn Sie Unstimmigkeiten oder Sicherheitsrisiken bemerken – welcher Art auch immer – setzen Sie sich bitte mit unserer unten angegebenen 2CALL Security Line in Verbindung.

Sollten Sie Opfer einer Phishingmail geworden sein, informieren Sie bitte uns und die Kriminalpolizei. Alle Phishingmails verfolgen das gleiche Ziel: Sie zu einer Formularseite weiterzuleiten, auf der Sie Ihre Geheimzahlen eintragen sollen. Diese Seiten sind ebenfalls perfekt den offiziellen Web-Seiten nachgebaut. Auch wenn Sie die Link-Adresse als die richtige identifizieren, ist Vorsicht geboten – denn sie ist trotzdem gefälscht.

Allerdings: Ganz gleich wie geschickt die Trickbetrüger vorgehen – abwehren kann man sie mit relativ einfachen Maßnahmen.

Security Line: (01 80) 50 53 11 1
(12 Cent/Min. aus dem deutschen Festnetz)

