Onlinebanking -
So sind Sie rundum sicher.

Sicheres Onlinebanking -

45 wichtige Tipps von Ihrer VR Bank

Sicherheitsvorkehrungen am eigenen PC

1 Versuchen Sie, so wenig Personen wie möglich an dem PC arbeiten zu lassen, den Sie für das Onlinebanking 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 Softwareprogramme, von denen Sie genau wissen, welche Funktion sie haben und wer ihr Hersteller ist. Installieren Sie niemals Software aus dubiosen Quellen.

5 Vermeiden Sie das Installieren unnötiger Softwareprogramme, damit Sie einen besseren Überblick haben. Vermeiden Sie ebenso häufige Installationen von Demoprogrammen.

6 Führen Sie eine regelmäßige Aktualisierung Ihres Betriebssystems durch – am besten automatisch im Hintergrund. So ist sichergestellt, dass eventuell vorhandene Sicherheitslöcher gestopft werden.

7 Informieren Sie sich möglichst regelmäßig über verfügbare Aktualisierungen, z.B. auf www.microsoft.de.

8 Überprüfen Sie Ihren PC regelmäßig anhand der Firewallsoftware auf mögliche ungewollte Besucher auf Ihrem Rechner.

9 Speichern Sie Ihre Daten regelmäßig als Sicherheitskopien auf CD/DVD/Blu-ray oder auf externen Laufwerken. 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 auf Mailadressen, um Ihr Onlinebanking aufzurufen. Nutzen Sie Bookmarks, die Sie selbst angelegt haben und die auf die Einstiegsseite Ihrer Bank verweisen.

12 Öffnen Sie keine Mailanhänge, die Sie nicht erwarten. Erhalten Sie Ihre Telefonrechnung üblicherweise auf dem Postweg, ist es nicht sehr wahrscheinlich, dass Ihre Telefongesellschaft Ihre Mailadresse kennt und Ihnen die Rechnung neuerdings auf diesem Weg zustellt.

13 Versuchen Sie nicht durch Deaktivierung oder Abschaltung von Sicherheitsvorkehrungen Ihren Internetzugang zu beschleunigen. Durch diese Deaktivierung ist einem Angreifer oder Schädling Tür und Tor geöffnet.

Besonderes Augenmerk auf den Internetbrowser

14 Verwenden Sie keinesfalls Testversionen von Internetbrowsern. Diese so genannten Betaversionen können Sicherheitslücken enthalten oder Fehlfunktionen aufweisen.

15 Nutzen Sie nicht die „Autovervollständigung“-Funktion Ihres Browsers. Benutzernamen und Passwörter werden hierbei schwach geschützt auf der Festplatte gespeichert.

16 Aktualisieren Sie regelmäßig Ihren Internetbroser. Die einzelnen Anbieter stellen auf Ihren Webseiten regelmäßig Aktualisierungen (so genannte Updates/Patches) bereit, die neu erkannte Sicherheitslücken schließen.

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

18 Verwenden Sie nach Möglichkeit keine Erweiterungen (Plug-Ins) für Ihren Browser, da sie ein zusätzliches Risiko darstellen. Wenn Sie diese Plug-Ins unbedingt nutzen möchten, so halten Sie diese Erweiterungen auch immer auf dem aktuellen Stand (z.B. Adobe Flash Player, Java,...).

19 Löschen Sie den Zwischenspeicher (Cache) des Browsers nach jeder Onlinebanking-Sitzung oder am besten deaktivieren Sie die automatische Cache-Speicherung.

20 Sorgen Sie dafür, dass nur Sie allein Kenntnis von Ihrer VR-NetKey-Nummer und Ihrer PIN haben.

21 Notieren Sie die PIN niemals auf Zetteln am Computer, der Schreibtischunterlage usw.

22 Speichern Sie Ihre PIN nicht in ungeschützten Dateien wie Word oder Excel.

23 Speichern Sie die PIN nicht ab, auch wenn z.B. der Browser eine Speicherung Ihres Benutzernamens und Passwortes anbietet.

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

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

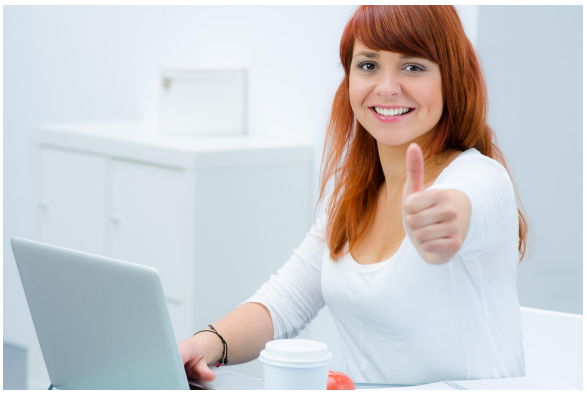
26 Stellen Sie Ihre Passwörter aus Groß- und Kleinbuchstaben, Zahlen und wenn möglich auch unter Nutzung von Sonderzeichen wie „$“ oder „&“ zusammen. Dies macht es für Dritte fast unmöglich, Ihr Passwort herauszufinden.

27 Ändern Sie Ihre Passwörter regelmäßig.

28 Verwenden Sie nach Möglichkeit für verschiedene Funktionen wie die Einwahl ins Internet, Onlinebanking etc. unterschiedliche Passwörter.

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

30 Sperren Sie Ihren Zugang zum Onlinebanking, sobald Sie den Verdacht haben, dass ein Dritter im Besitz Ihrer Zugangsdaten ist. Haben Sie bereits einen VR-NetKey? Dann nutzen Sie die Möglichkeit, den VR-NetKey direkt in Ihrer eBanking-Anwendung über den Menüpunkt „Service“ und „Onlinezugang sperren“ zu sperren. Auch durch die dreifache Falscheingabe Ihrer PIN ist Ihr Onlinebanking gesperrt. Falls Sie keinen VR-NetKey besitzen, lassen Sie Ihr Onlinebanking umgehend über Ihren Bankberater sperren.



Sichere Handhabung beim Onlinebanking

31 Vereinbaren Sie mit Ihrer Bank ein Tageslimit für Onlineüberweisungen. So kann ein möglicher Schaden von vornherein auf eine bestimmte Summe begrenzt werden.

32 Verwenden Sie nach Möglichkeit nicht das Angebot verschiedener Onlinebanking-Programme, die PIN einmalig einzugeben und zu speichern.

33 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 Webseite, damit Sie sicher sein können, dass eine verschlüsselte Verbindung zur Bank aufgebaut wurde.

34 Beachten Sie die Warnhinweise Ihres Browsers. Geben Sie keine PIN auf einer Seite ein, vor der Sie Ihr Webbrowser durch eine Sicherheitsmeldung gewarnt hat.

35 Brechen Sie Onlinebanking-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 Onlinebanking gehören.

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

37 Kontrollieren Sie alle eingegebenen Daten genauestens, denn die einmal getätigte Überweisung ist verbindlich!

38 Überprüfen Sie die Angaben Ihrer Überweisung: bei allen TAN-Verfahrenden wird Ihnen die IBAN des Empfängers und der Betrag angezeigt. Geben Sie die TAN erst nach Überprüfung Ihrer Daten ein.

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 könnten unter Umständen zwei Überweisungen erfolgen, da die Computer der Bank nicht auf die Korrektur einer vorherigen Überweisung ausgelegt sind.

40 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.

Gefahren beim Onlinebanking an fremden Computern

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

42 Kontrollieren Sie Sicherheitsfunktionen wie Zertifikate von Webseiten oder die verschlüsselte Verbindung sehr genau, um das Risiko zu reduzieren.

43 Nutzen Sie möglichst nie Internet-Cafés für das Onlinebanking. 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 Onlinebankings 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.

Stand 02/2019