



Mit Sicherheit ins Internet

Die wichtigsten Grundregeln
für den sicheren Umgang
mit Internet und
PSD OnlineBanking

- 2 Sicherer ist sicher
Das iTANplus-Verfahren
- 3 Vom Angeln nach Passwörtern
Phishing
- 4 Der Lauschangriff auf Ihren Rechner
Trojanische Pferde
- 5 Mehr als nur lästiges Ungeziefer
Viren und Würmer
- 6 Das sollten Sie beachten
Allgemeine Hinweise
- 7 Fachbegriffe verständlich erklärt
Glossar
- 8 Das Wichtigste
auf einen Blick
Checkliste

Mit dem PSD OnlineBanking haben Sie die Möglichkeit, Ihre Konten bequem rund um die Uhr zu verwalten. Egal, ob Sie nur den Kontostand abfragen oder eine Überweisung beauftragen möchten. Doch gerade, wenn es um Geld geht, ist die Sicherheit natürlich besonders wichtig – in der realen Welt wie im Internet. Und genau so, wie Sie auf Ihre Geldbörse oder BankCard aufpassen müssen, gilt es auch bei der Benutzung des Internets bestimmte Vorsichtsregeln einzuhalten. Diese Sicherheitsmaßnahmen beziehen sich dabei nicht nur auf das OnlineBanking im Besonderen, sondern verhelfen Ihnen zu einem sicheren Umgang mit dem Internet allgemein.

In dieser Broschüre stellen wir Ihnen diese wichtigen Regeln vor, damit die Benutzung des Internets und des OnlineBankings für Sie zum sicheren Vergnügen wird.

So schützen wir Ihre Daten!

Um beim OnlineBanking eine größtmögliche Sicherheit zu erreichen, müssen grundsätzlich beide daran beteiligten Seiten – sowohl die Bank als auch der Kunde – für eine Absicherung vertraulicher Daten sorgen. Hierbei ist es die Aufgabe der PSD Bank, die Kundendaten auf dem Bankrechner vor unbefugten Zugriffen zu schützen sowie eine sichere Kommunikation zwischen dem Kunden- und dem Bankrechner zu gewährleisten.



Die Übertragung vertraulicher Daten erfolgt bei der PSD Bank grundsätzlich über eine **256 Bit SSL-Verschlüsselung** (→ „SSL“ steht dabei für „Secure Socket Layer“), dem allgemein als sicher anerkannten Standard. Dabei werden die Daten verschlüsselt über-

tragen, ohne dass Außenstehende diese Übertragung mitverfolgen können.

Für die Datenkommunikation im PSD OnlineBanking verwenden wir eine solche gesicherte Verbindung. Dies können Sie jederzeit daran erkennen, dass die Adresse der von Ihnen aufgerufenen Seite mit → „https://“ beginnt. Darüber hinaus zeigt Ihnen der → Browser ein entsprechendes Sicherheitssymbol (beispielsweise ein Schloss in der Statusleiste) an.

Wichtig: Aktueller → Browser

Diese gesicherte Verbindung kann nur aufgebaut werden, wenn der von Ihnen verwendete → Browser eine 128 Bit starke Verschlüsselung auch unterstützt. Mit älteren

bzw. nicht mehr aktuellen Programmen, die nur eine geringere Verschlüsselung aufweisen, können Sie das PSD OnlineBanking daher nicht nutzen!

! MERKMALE EINER SICHEREN ÜBERTRAGUNG

- Es wird eine geschützte Verbindung aufgebaut, in der die Daten ausschließlich verschlüsselt übertragen werden.
- Der Rechner des Anbieters (z. B. der Bankrechner) kann eindeutig anhand des hinterlegten Zertifikates identifiziert werden. Die Echtheit des Zertifikates, welches von der Firma VeriSign für uns ausgestellt wurde, können Sie jederzeit direkt auf der Anmeldeseite durch einen Klick auf das Schloss-Symbol prüfen.
- Es handelt sich um eine zuverlässige Verbindung, bei der die übermittelten Daten nicht manipuliert werden können.

Sicherer ist sicher

Das iTANplus-Verfahren

Das iTANplus-Verfahren, das im neuen PSD OnlineBanking Anwendung findet, ist eine Erweiterung des bisher angewendeten iTAN-Verfahrens. iTANplus vermindert die Möglichkeit eines Missbrauchs nochmals deutlich. Basis sind auch hier die "indizierten Transaktionsnummern" (iTAN), die durch den so genannten Index auf Ihrem TAN-Bogen eindeutig bestimmt sind.

Im verbesserten iTANplus-Verfahren sind alle TANs auf einer TAN-Liste mit einem so genannten Index durchnummeriert.

Das OnlineBanking fordert Sie weiterhin auf, eine Transaktion (z.B. eine Überweisung) durch Eingabe einer ganz bestimmten TAN zu bestätigen. Diese ist durch die angegebene Index-Nummer, die Sie auf Ihrer TAN-Liste finden, eindeutig bestimmt.

Soweit also kein Unterschied zum Ihnen bekannten iTAN-Verfahren. iTANplus bietet Ihnen jedoch dank eines speziellen Kontrollbilds die Möglichkeit, zu prüfen, ob Ihre Eingaben auch wirklich im PSD OnlineBanking angekommen sind.

So funktioniert das iTANplus-Verfahren:

Das PSD OnlineBanking fordert Sie beispielsweise zur Eingabe der TAN mit der Index-Nummer 57 auf. Suchen Sie bitte die zur Index-Nummer 57 gehörende 6-stellige TAN auf Ihrer TAN-Liste und geben Sie diese anschließend ein. Nur wenn die TAN tatsächlich die zur angeforderten Index-Nummer gehörende TAN ist, wird sie vom Bankrechner akzeptiert. Andere TANs, auch wenn diese tatsächlich auf Ihrer TAN-Liste vorhanden sind, lehnt das System als falsch ab.

Über dem TAN-Eingabefeld finden Sie nun zusätzlich noch das iTANplus-Kontrollbild: Dort werden Ihnen nun die Transaktionsdaten (z.B. Betrag, Kontonummer etc.) ange-

zeigt. Als Wasserzeichen wird Ihnen außerdem Ihr Geburtsdatum eingeblendet. Dieses ist einem möglichen Angreifer nicht bekannt. Das richtig angezeigte Geburtsdatum erhöht daher die Sicherheit, dass Sie direkt mit dem PSD OnlineBanking kommunizieren.

Nutzen Sie daher unbedingt diese zusätzlichen Kontrollmöglichkeiten, bevor Sie die angeforderte TAN eingeben und mit "OK" bestätigen.

So werden mit dem neuen iTANplus-Verfahren Missbrauchsversuche, z.B. durch Phishing oder Trojaner, effektiv erschwert.

Auch Sie müssen mithelfen!



Die Maßnahmen der PSD Bank sichern zwar den Datentransport effektiv, können aber Ihren Computer nicht pauschal gegen Angriffe von außen schützen. Da jeder PC individuell von seinem Benutzer konfiguriert wird, können und müssen Sie selbst für eine ausreichende Absicherung Ihres Systems sorgen.

Viele Angriffe zielen derzeit auf die PCs von OnlineBanking-Kunden, um vertrauliche Daten (z. B. PIN und TANs) auszuspähen und damit finanziellen Schaden anzurichten.

Mit den richtigen Maßnahmen können Sie solche Angriffe verhindern und dafür

sorgen, dass auch weiterhin nur Sie selbst Zugriff auf Ihr Konto haben!

Im Folgenden informieren wir Sie über die momentan größten Gefahren für OnlineBanking-Kunden und geben Ihnen Ratschläge, wie Sie sich ausreichend schützen können.

Vom Angeln nach Passwörtern

Phishing

Dieses Kunstwort wurde aus den Begriffen „Passwort“ und „Fishing“ zusammengesetzt und bedeutet übersetzt soviel wie „nach Passwörtern angeln“. Beim so genannten „Phishing“ fälschen Betrüger →E-Mails und Internetseiten, um an Ihre vertraulichen Daten (z. B. PIN und TANs) zu gelangen.

Als Bank getarnt fordern die Betrüger Sie in einer →E-Mail (unter einem mehr oder weniger plausiblen Vorwand) auf, Ihre wertvollen Daten auf einer Internetseite einzugeben, z. B., weil das Passwort erneuert werden müsse oder um angeblich einen besseren Schutz gegen Betrüger zu erreichen. Diese so genannten Phishing-Mails werden dabei als Massenmail (sog. →Spam-Mail) wahllos an Tausende von Empfängern versandt.

Der Inhalt dieser →E-Mails wirkt meist täuschend echt. Der Empfänger wird für die Dateneingabe über einen →Link auf eine Internetseite geführt, die z. B. der →Banken-Homepage ähnlich sieht. Auf den ersten Blick scheint alles ganz normal, selbst die Eingabeformulare sehen gleich aus.

Die Phishing-Betrüger nutzen hierfür entweder Internetadressen, die sich kaum wahrnehmbar von denen der Bank unterscheiden. Oder aber sie fälschen die Adressleiste des →Browsers, indem Dateien auf Ihrem Rechner ausgetauscht oder umprogrammiert werden. Ergebnis: Sie glauben, Sie wären auf einer seriösen Seite,



sind es aber nicht! Sobald Sie auf der gefälschten Seite Ihre vertraulichen Daten (z. B. PIN oder TAN) eingegeben haben, nutzt ein Betrüger diese Daten selbst, um sich beim OnlineBanking anzumelden und in Ihrem Namen eine Überweisung auf z. B. sein eigenes Konto zu veranlassen.

Hierbei kann für Sie ein finanzieller Schaden entstehen, da es meist sehr schwierig ist, überwiesene Beträge, die bereits beim Empfänger gutgeschrieben sind, zurückzufordern.

! SO KÖNNEN SIE SICH VOR „PHISHING“ SCHÜTZEN

- Sie werden von uns niemals eine →E-Mail erhalten, in der Sie aufgefordert werden, Ihre Zugangsdaten (insbesondere PIN und TAN) preiszugeben! Wir werden Sie auf keinen Fall darum bitten, dass Sie uns solche Angaben per →E-Mail, Post oder auf einem anderen Weg (z. B. Eingabeformular auf Internetseiten) zukommen lassen.
- Öffnen Sie niemals →E-Mails und insbesondere deren Dateianhänge, wenn Ihnen die Absender unbekannt sind oder die →E-Mail unverlangt zugesandt wurde.
- Folgen Sie nicht blind Anweisungen, welche aus einer →E-Mail hervorgehen. Rufen Sie vor allem niemals unsere Login- bzw. Anmeldeseiten über einen →Link aus einer unaufgefordert zugesandten →E-Mail auf.
- Starten Sie das PSD OnlineBanking nur über die →Homepage der PSD Bank.
- Prüfen Sie die Adresse der von Ihnen aufgerufenen Internetseite in der Adresszeile Ihres →Browsers. Die →URL des PSD OnlineBankings beginnt immer mit **<https://onlinebanking.psd-bank.de/>**
- Fragen Sie sich, ob die auf der Internetseite geforderten Eingaben im Zusammenhang mit der von Ihnen gewünschten Aktion Sinn ergeben.

Für Sie als Internetnutzer heißt es grundsätzlich: Aufpassen! Schauen Sie gerade bei Internet-Angeboten, welche die Eingabe von vertraulichen Daten von Ihnen verlangen, zweimal hin und überlegen Sie genau, wem Sie Ihre Daten anvertrauen.



Der Lauschgriff auf Ihren Rechner

Trojanische Pferde

Dieser Computervirus wurde nach dem historischen Vorbild benannt: Unter dem Deckmantel scheinbar nützlicher Funktionen nistet sich hierbei ein Programm auf Ihrem Computer ein und kann – meist von Ihnen unbemerkt – im Hintergrund Schaden anrichten.

Viele Trojanische Pferde sorgen sogar dafür, dass sie bei jedem Start des Computers automatisch wieder aktiviert werden. Hierdurch ist das schädliche Programm permanent im Einsatz. Die durchgeführten Veränderungen im System lassen sich dann auch durch das Löschen des Ursprungsprogramms (also dem Trojanischen Pferd selbst) nicht mehr rückgängig machen, da dieses ja nur als Übertragungsmedium diente.

Wenn ein Computer von einem Trojanischen Pferd befallen ist, können unterschiedlichste Schäden die Folge sein. Die folgenden Beispiele sollen Ihnen als OnlineBanking-Nutzer die möglichen Gefahren verdeutlichen:

- Es können sensible Daten, die auf dem PC gespeichert sind, ausspioniert, kopiert und unbemerkt weitergeleitet werden. Für den

Urheber des Trojanischen Pferdes sind insbesondere Passwörter, Kreditkartennummern und Kontonummern interessant.

- Alle Aktivitäten am Computer können überwacht werden. Dadurch ist es möglich, auch die über die Tastatur eingegebenen Daten abzufangen und an einen unberechtigten Empfänger zu übermitteln – unabhängig von einer gesicherten Verbindung!
- Es werden so genannte „Hintertüren“ auf Ihrem PC eingerichtet. Hierdurch können Angreifer aus dem Internet auf Ihren Computer zugreifen und unbemerkt weitere Programme installieren oder Daten ausspähen.

Der „Datendiebstahl“ bleibt häufig unbemerkt, weil Daten auf dem PC weder geändert noch gelöscht werden.

! SO SCHÜTZEN SIE SICH VOR TROJANISCHEN PFERDEN

Am effektivsten schützen Sie sich vor Trojanischen Pferden, indem Sie keine Programme aus unbekanntem oder unsicheren Quellen ausführen, insbesondere, wenn diese einen unseriösen oder gar illegalen Eindruck machen.

Viele Trojanische Pferde versenden Kopien von sich selbstständig und ohne Zutun des Benutzers per →E-Mail, meist werden als Empfänger kurzerhand die Einträge des Adressbuchs eingesetzt. Der Text der →E-Mail ist dabei stets so gestaltet, dass der Empfänger dazu verleitet wird, den Anhang zu öffnen und dadurch eine weitere Infektion auszulösen.

Der Schutz gegen diese Verbreitungsform ist sehr einfach: **Öffnen Sie keine →E-Mail-Anhänge mit unverlangt zugesandten Dateien!** Auch wenn Sie den Absender kennen, ist dieses keine Gewährleistung, dass Sie den Dateianhang bedenkenlos öffnen können! Die Absenderadresse derartiger →E-Mails ist nämlich meist gefälscht. Außerdem können auch Ihnen bekannte Absender Opfer eines Trojanischen Pferdes geworden sein.

Aktuelle →Antivirenprogramme schützen in der Regel vor bekannten Trojanischen Pferden. **Nutzen Sie daher unbedingt ein →Antivirenprogramm und halten Sie die →Virensignaturen immer auf dem neusten Stand!**

Einen anderen Weg geht die so genannte „Personal →Firewall“: Hier wird der Datenverkehr von und zu Ihrem Rechner nach Ihren Vorgaben kontrolliert. Dadurch kann zwar die Infektion des Computers nicht verhindert werden, aber der unerwünschte Datentransfer wird dadurch überwacht bzw. unterbunden. **Eine →Firewall stellt daher eine sinnvolle Ergänzung zu den →Antivirenprogrammen dar und sollte stets von Ihnen aktiviert sein. Auch hier sind regelmäßige →Updates wichtig, um die Software aktuell zu halten.**

Mehr als nur lästiges Ungeziefer

Viren und Würmer

Fast wie ein „richtiger“ Virus infiziert die elektronische Variante den Computer und nimmt dabei keine Rücksicht auf dessen „Wohlergehen“. Auch ein Computervirus vermehrt sich unkontrolliert und meist sehr schnell. Viren können nach der Infektion eines Computers unterschiedliche Schäden verursachen, die häufig auch zu Datenverlust oder -veränderung führen.

Ein Computervirus benötigt zur Infektion eines Rechners eine Möglichkeit, um den PC zu gelangen. Hierzu dient meistens eine Netzwerk- oder Internet-Verbindung oder das Einlegen eines Datenträgers.

Viren im Computer funktionieren dabei genauso wie Krankheitsviren im menschlichen Körper: Sie können sich selbst vermehren und richten überall, wo sie sich festgesetzt haben, Schaden an. Wenn Sie sich einen harmloseren Virus eingefangen haben, gibt Ihr Computer vielleicht seltsame Texte aus; oft werden aber Dateien und auch schon mal die ganze Festplatte gelöscht.

Computer-Viren stellen aber auch ein gravierendes Sicherheitsproblem dar, wenn vertrauliche Daten unbemerkt weitergeleitet oder ausspioniert werden.

Infiziert werden kann Ihr Rechner immer dann, wenn Sie Dateien aus dem Internet herunterladen oder Sie Anhänge von →E-Mails öffnen. Viren können aber auch über CD-ROMs, DVDs oder z. B. USB-Sticks auf Ihren Computer gelangen. In jeder ausführbaren Datei, wie z. B. mit den Dateiendungen *.exe oder *.bat, kann sich ein Virus verstecken. Aber auch Dateien mit anderen Endungen können virenverseucht sein.

Häufig werden auch Dateien mit doppelten Endungen verwendet (z. B. „dateiname.doc.pif“), um den eigentlichen Dateityp zu verschleiern.

So genannte Würmer sind eine Variante der Viren. Die Infektion eines Computers mit einem Wurm erfolgt oftmals über eine verseuchte →E-Mail. Startet man eine angehängte Datei, wird der Virus aktiviert und verbreitet sich anschließend von selbst weiter.

Durch Sicherheitslücken in einigen E-Mail-Programmen können sich die Würmer besonders schnell verbreiten. Bei einigen E-Mail-Programmen ist es sogar möglich, dass sich die verseuchten →E-Mails ohne Wissen des Benutzers an Personen aus dem Adressbuch versenden. Weil die Empfänger den Absender der →E-Mail kennen, geraten sie in Versuchung, den Anhang zu öffnen, und der Wurm pflanzt sich dadurch weiter fort.

! SO SCHÜTZEN SIE SICH VOR VIREN UND WÜRMERN

Grundsätzlich sollten Sie niemals unbekannte Programme aus unsicherer Quelle ausführen und generell beim Öffnen von Dateien sehr vorsichtig sein.

Das gilt insbesondere für Dateien, die Ihnen per →E-Mail zugesandt wurden. Solche Dateien sollten, wenn überhaupt, erst nach Überprüfung mit einem aktuellen →Antivirenprogramm geöffnet werden.

Da viele Würmer Sicherheitslücken von Betriebssystem und →Browser ausnutzen, sollten Ihr Betriebssystem und Ihre Anwendungen regelmäßig aktualisiert werden. Für das weit verbreitete Betriebssystem Windows sollten alle wichtigen →Service-Packs und →Updates regelmäßig installiert werden. Andernfalls sind Ihre Verbindungen auf Dauer unsicher.

Aktuelle →Antivirenprogramme schützen vor bekannten Viren. Daher ist es bei der Benutzung eines solchen Programms wichtig, regelmäßig die von den Herstellern bereitgestellten aktuellen →Virensignaturen einzuspielen. Dies sollte möglichst täglich erfolgen, am besten nutzen Sie die meist vorhandene →Update-Funktion, dann geschieht dies automatisch.





Das sollten Sie beachten

Allgemeine Hinweise

Die eingebauten Schutzfunktionen Ihres Betriebssystems sollten zusätzlich ausgenutzt werden. Dazu zählt insbesondere, nicht als Administrator mit allen Rechten, sondern nur als Nutzer mit eingeschränkten Rechten zu arbeiten, der z. B. keine Software installieren darf. Denn was Sie selbst nicht an Ihrem PC verändern dürfen, kann auch ein Virus nicht verändern.

Das automatische Öffnen von Dateien aus dem Internet sowie das automatische Anzeigen von Dateianhängen sollte deaktiviert werden, um auch hier unkontrollierte Installationen zu verhindern. Alle Angriffsversuche durch schädliche Programme

haben eines gemeinsam: sie müssen auf Ihren Rechner gelangen und dort die Möglichkeit haben, sich durch unvorsichtiges Verhalten im System festzusetzen. Nur so können Trojaner, Viren und Würmer ungehindert Schaden anrichten.

Seien Sie daher dem virtuellen Ungeziefer immer einen Schritt voraus und entwickeln Sie ein gesundes Misstrauen vor vermeintlich nützlichen Programmen und Downloads.

! DIE WICHTIGSTEN SCHUTZMASSNAHMEN AUF EINEN BLICK

Allgemeine Maßnahmen

- Benutzen Sie unbedingt ein aktuelles → Antivirenprogramm. Nutzen Sie regelmäßig (möglichst täglich) die → Update-Funktion!
- Durchsuchen Sie mit Hilfe eines → Antivirenprogramms Ihren Rechner regelmäßig nach Viren.
- Aktivieren Sie stets eine → Firewall und aktualisieren Sie diese regelmäßig!
- Arbeiten Sie mit dem aktuellsten Betriebssystem und installieren Sie regelmäßig die verfügbaren → Updates.
- Arbeiten Sie mit einem aktuellen → Browser und halten Sie diesen auf dem neuesten Stand.
- Installieren Sie keine Software auf Ihrem Rechner, deren Hersteller nicht vertrauenswürdig erscheint.
- Seien Sie misstrauisch, wenn sich Ihr Computer plötzlich ungewohnt verhält.

Maßnahmen für sicheres OnlineBanking

- Geben Sie Ihre Online-PIN niemals an Dritte weiter.
- Bewahren Sie Ihre TAN-Liste getrennt von Ihrer PIN auf und sorgen Sie dafür, dass kein Dritter diese einsehen kann.
- Speichern Sie weder die PIN noch TANs auf Ihrem Rechner ab.
- Bei einem Verbindungsabbruch starten Sie den → Browser neu.
- Wenn Sie Hinweise oder Verdachtsmomente auf einen möglichen Missbrauch haben, ändern Sie sofort Ihre PIN oder sperren Sie das Konto.
- Vermeiden Sie es, Ihre Bankgeschäfte an fremden Computern (z. B. Internet-Cafe) zu tätigen, da es dort einfacher ist, Ihre persönlichen Daten auszuspionieren.
- Ändern Sie häufiger Ihr Passwort und achten Sie darauf, dass es kompliziert genug ist (keinesfalls z. B. Namen oder Geburtsdaten verwenden!).
- Kontrollieren Sie regelmäßig Ihre Kontoauszüge.
- Sollten Ihnen Unregelmäßigkeiten auf Ihrem Konto auffallen, sperren Sie den Zugang zu Ihrem Konto sofort.

- Zur raschen Sperrung des Online-Zugangs zu Ihrem Konto stehen Ihnen verschiedene Wege zur Verfügung:
 - Anruf bei Ihrer PSD Bank
 - „Online-Zugang sperren“ unter „Service“ im OnlineBanking
 - dreimalige Eingabe einer falschen PIN im PSD OnlineBanking

Sie möchten mehr erfahren?

Gerade im Kampf gegen die Gefahren aus dem Internet ist es wichtig, sich stets auf dem Laufenden zu halten. Wir empfehlen Ihnen daher, sich regelmäßig über aktuelle Bedrohungen durch Phishing, Trojaner, Viren etc. zu informieren.

Viele Hintergrundinformationen finden Sie beim „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) auf den Seiten

<http://www.bsi-fuer-buerger.de>

<http://www.bsi.de/>



oder auch unter der Adresse

<https://www.sicher-im-netz.de>

– einer Initiative namhafter Firmen unter der Schirmherrschaft des Bundesministeriums für Wirtschaft und Arbeit.

Natürlich haben wir auch auf unseren Internetseiten im Kapitel OnlineBanking/Sicherheit viele Tipps und ausführliche Informationen rund ums Thema Sicherheit zusammengestellt.

Fachbegriffe verständlich erklärt

Glossar

Ihnen ist ein Begriff unbekannt? Kein Problem! Diese Erläuterungen helfen Ihnen, die Bedeutung komplizierter Fremd- oder Fachworte zu verstehen.



Antivirenprogramm	Ein Antivirenprogramm (oder Virenschanner) schützt den Computer vor bekannten Viren, Würmern oder Trojanischen Pferden. Das Programm überwacht dabei zum einen den Rechner vor gefährlichen Aktivitäten und kann zum anderen genutzt werden, um die Speichermedien (Festplatten, Disketten, CDs, DVDs, USB-Sticks etc.) nach vorhandenen Viren und Schadprogrammen zu durchsuchen.
Browser	Ein „Browser“ ist ein Computerprogramm, um Seiten aus dem Internet anzuzeigen. Bekannte Browser sind z. B. der Internet Explorer, Mozilla Firefox und Opera.
E-Mail	„E-Mails“ sind elektronische Nachrichten, die von einem Sender an einen oder mehrere Empfänger verschickt werden. Diese Nachrichten können auch unterschiedliche Dateien (z. B. Word-Dokumente oder Bilder) als Anhang enthalten.
Firewall	Eine „Firewall“ kontrolliert den Datenverkehr in einem Computernetz. Eine „Personal Firewall“ wird genutzt, um den Datenaustausch zwischen einem PC und dem Internet zu kontrollieren und zu steuern und damit Angriffe von außen oder die unbemerkte Weitergabe von Informationen zu verhindern.
Homepage	Als „Homepage“ wird i.d.R. die Startseite eines Internetauftrittes bezeichnet, d.h. die Seite, welche Ihnen zuerst angezeigt wird, nachdem Sie eine neue Adresse in Ihren →Browser eingegeben haben.
HTTPS	Mit „HTTPS“ wird ein Netzwerkprotokoll bezeichnet („Hypertext Transfer Protocol Secure“), das eine gesicherte Verbindung zwischen zwei Rechnern ermöglicht.
Link	Ein „Link“ ist die Kurzbezeichnung für den so genannten „Hyperlink“. Dies ist ein entsprechend markierter Verweis auf ein anderes Dokument oder eine andere Internetseite. Mit einem Mausklick auf die Markierung wird z. B. automatisch die mit dem Link verknüpfte Adresse in Ihrem →Browser aufgerufen.
Sicherheitspatch	Ein so genanntes „Patch“ (von englisch „Flicken“) ist eine Korrektur für Software oder Daten und schließt meist vorhandene Sicherheitslücken. (→Update)
Service-Pack	Ein „Service Pack“ ist die Zusammenstellung mehrerer →Patches zur Aktualisierung einer Software. →Patches korrigieren in der Regel nur einen Fehler. Service Packs bieten den Vorteil, dass sehr viele dieser →Patches mit einer einzigen Installation ausgeführt werden können.
Spam	Unter Spam versteht man unverlangt zugestellte →E-Mails, die massenhaft und wahllos an sehr viele Empfänger versendet werden. Der Inhalt ist dabei meist fragwürdig und kann von unseriöser Werbung (Medikamente, Software, etc.) über rassistische Parolen bis hin zum versuchten Betrug gehen. Spam-Mails können auch mit Viren verseucht sein und sich bei Aktivierung selbsttätig an weitere Benutzer (z. B. aus dem Adressbuch) versenden. Fragen Sie bei Ihrem Provider nach sog. Spam-Filtern oder aktivieren Sie den Spam-Filter Ihrer E-Mail-Software (falls vorhanden), um diese unerwünschten →Mails nicht mehr zu erhalten.
SSL	Übersetzt bedeutet dies „Secure Socket Layer“. Es handelt sich hierbei um ein Verschlüsselungsprotokoll für Datenübertragungen im Internet (→HTTPS).
Update	Als „Update“ wird ein Aktualisierungsprogramm bezeichnet, das installiert wird, um ein Programm oder ein ganzes System zu verbessern, auf eine neuere Version zu bringen und/oder um Fehler zu bereinigen. Die wichtigsten Updates sind die so genannten →Sicherheitspatches.
URL	Mit „URL“ wird häufig die Internetadresse bezeichnet, die in der Adresszeile des →Browsers zum Aufrufen der Seite eingegeben werden muss, um die Seite aufzurufen. (Beispiel: www.psd-bank.de)
Virensignatur	Jedes →Antivirenprogramm nutzt so genannte „Virensignaturen“ (oder auch „Virendefinitionen“), um die charakteristischen Merkmale der Viren zu kennen. Da täglich neue Viren auftauchen, ist es sehr wichtig, diese Erkennungslisten regelmäßig – möglichst täglich – zu aktualisieren.



Das Wichtigste auf einen Blick

Checkliste

Sie wissen jetzt: OnlineBanking kann nur so sicher sein wie Ihr eigener Computer! Um Ihnen die Überprüfung Ihres Systems zu erleichtern, haben wir hier die Inhalte der Broschüre zu einer einfachen Checkliste zusammengefasst. Gehen Sie einfach die Punkte Schritt für Schritt durch. Wenn Sie alle Themen abgehakt haben, sind Sie gegen mögliche Angriffsversuche optimal geschützt!

! CHECKLISTE

- Ja, ich nutze ein aktuelles → Betriebssystem!**
Nutzer von älteren Systemen (z. B. Windows 95) sollten unbedingt auf die aktuelle Version (z. B. Windows Vista) aktualisieren! Verfügbare → Sicherheitspatches und → Service-Packs sollten regelmäßig installiert werden.
- Ja, ich benutze einen aktuellen → Browser!**
Nutzer von älteren → Browsern (z. B. Internet Explorer 5.0 oder Netscape 4.7) sollten unbedingt auf die aktuellste Version aktualisieren! Verfügbare → Sicherheitspatches und → Service-Packs sollten regelmäßig installiert werden.
- Ja, ich benutze eine → Firewall!**
Nutzer von Windows XP und Vista sollten überprüfen, ob die integrierte → Firewall aktiviert ist, oder eine andere → Firewall eines namhaften Herstellers installieren. Nutzen Sie die automatische → Updatefunktion, um das Programm aktuell zu halten!
- Ja, ich benutze ein aktuelles → Antivirenprogramm!**
Installieren Sie ein → Antivirenprogramm eines namhaften Herstellers und aktivieren Sie den andauernden Schutz Ihres Systems. Durchsuchen Sie Ihre Festplatte regelmäßig nach bekannten Viren und aktualisieren Sie die Virenliste (so genannte → Virensignaturen) regelmäßig, am besten bei jeder Verbindung ins Internet. Nutzen Sie hierfür die Auto-→ Update-Funktion, die viele Programme anbieten.
- Ja, ich gehe sehr sorgfältig mit eingehenden → E-Mails um!**
Löschen Sie → E-Mails von Ihnen nicht bekannten Nutzern, öffnen Sie keinesfalls deren Anhänge. Seien Sie auch bei bekannten Absendern sehr kritisch und vorsichtig. Folgen Sie niemals blind Anweisungen, die in einer → E-Mail stehen. Rufen Sie niemals die OnlineBanking-Seiten über einen → Link in einer → E-Mail auf. Geben Sie niemals vertrauliche Daten (z. B. PIN oder TANs) auf die Aufforderung aus einer → E-Mail hin weiter.
- Ja, ich verwende keine Downloads aus zweifelhaften Quellen!**
Laden Sie keine Programme von dubiosen Internetseiten, die Ihnen nicht vertrauenswürdig erscheinen. Seien Sie vorsichtig bei angeblichen Schnäppchen und auffallend günstigen Angeboten, gehen Sie im Zweifel zu namhaften Anbietern. Überprüfen Sie die heruntergeladenen Programme vor der Ausführung in jedem Fall mit einem → Antivirenprogramm.
- Ja, ich bewege mich im Internet vorsichtig und verantwortungsbewusst!**
Verwenden Sie zum Surfen im Internet nicht den Administrator-Zugang, sondern einen Zugang mit eingeschränkten Rechten. Meiden Sie Internetseiten, deren Inhalt zweifelhaft erscheint. Beenden Sie bei verdächtigen Aktivitäten (z. B. plötzliche Installationshinweise, Fenster sollen mit OK bestätigt werden, Hinweis zum Ausführen eines Skripts etc.) sofort alle → Browserfenster.
- Ja, ich benutze meinen Computer aufmerksam und kritisch!**
Überprüfen Sie Ihren Rechner regelmäßig auf Viren. Seien Sie misstrauisch, wenn sich Ihr Computer plötzlich ungewohnt verhält (z. B. unvermittelte Abstürze, unaufgeforderte Aktivitäten etc.).
- Ja, ich gebe meine vertraulichen Daten nicht an Dritte weiter!**
Mitarbeiter der PSD Bank werden Sie niemals nach PIN oder TANs fragen, weder am Telefon noch per → E-Mail. Bewahren Sie Ihre TAN-Liste an einem sicheren Ort auf, den niemand einsehen kann. Speichern Sie niemals PIN oder TANs auf Ihrem Rechner ab.
- Ja, ich starte das OnlineBanking nur über die → Homepage meiner Bank**
Starten Sie das OnlineBanking immer nur über die jeweilige → Homepage, legen Sie keine Favoriten (bzw. Bookmarks) an. Starten Sie die Anmeldeseiten niemals über per → E-Mail zugesandte → Links. Beachten Sie aktuelle Sicherheitshinweise auf der → Homepage. Überprüfen Sie die Richtigkeit des aktuellen Zertifikates durch Klick auf das Schloss-Symbol. Prüfen Sie, ob die im OnlineBanking angezeigte → URL mit **https://onlinebanking.psd-bank.de/** beginnt.