Informationen Ihrer PSD Bank

# PSD OnlineBanking

## Mit Sicherheit ins Internet

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

August 2016

# Mit Sicherheit ins Internet

Mit dem PSD OnlineBanking können Sie Ihre Konten bequem rund um die Uhr verwalten - egal, ob Sie den Kontostand abfragen oder eine Überweisung tätigen möchten. Dabei geht es um Ihr Geld und immer, wenn das der Fall ist, ist Sicherheit natürlich oberstes Gebot - in der realen Welt genauso wie im Internet. Es gilt bestimmte Verhaltensregeln einzuhalten, so wie Sie unterwegs besonders auf Bargeld und BankCard Acht geben.

Diese Verhaltensregeln beziehen sich dabei nicht nur auf das OnlineBanking im Besonderen. Vielmehr verhelfen wir Ihnen zu einem sicheren Umgang mit dem Internet allgemein. In dieser Broschüre haben wir die wichtigsten Regeln zusammengestellt, damit die Benutzung des Internets und des OnlineBankings für Sie zum sicheren Vergnügen wird.

# So schützen wir Ihre Daten

Um beim OnlineBanking die größtmögliche Sicherheit zu erreichen, müssen beide daran beteiligten Seiten - also die Bank und der Kunde - für eine Absicherung der vertraulichen Daten sorgen. Dabei haben wir als PSD Bank die Aufgabe, die Kundendaten auf dem Bankrechner vor unbefugtem Zugriff zu schützen sowie eine sichere Kommunikation zwischen dem Kunden und dem Bankrechner zu gewährleisten.

Die PSD Banken setzen für die Übertragung von Kundendaten im OnlineBanking immer die so genannte TLS-Verschlüsselung ein, auch bekannt unter der Vorgängerbezeichnung SSL.

TLS steht für Transport Layer Security (zu Deutsch Transportschichtsicherheit) und ist die Weiterentwicklung der SSL-Verschlüsselung. Es handelt sich dabei um ein hybrides Sicherheitsprotokoll, das die zwischen Kunde und Bank ausgetauschten Daten verschlüsselt. Das PSD OnlineBanking verwendet die als absolut sicher eingestufte Verschlüsselungstiefe von 256 Bit. Dies setzt voraus, dass der von Ihnen verwendete Web-Browser diese Technik ebenfalls unterstützt.

Nutzer älterer Browser, bei denen dies nicht der Fall ist, können daher aus Sicherheitsgründen nicht am PSD OnlineBanking teilnehmen.

Das PSD OnlineBanking verfügt über ein TLS-Zertifikat, das gegenüber Ihrem Browser als eine Art „elektronischer Ausweis“ fungiert und anzeigt, dass Ihre Daten ausschließlich vom PSD OnlineBanking entschlüsselt werden können.

Durch das Extended Validation (kurz: EV) TLS-Zertifikat (deutsch etwa: Zertifikat mit erweiterter Überprüfung) wird dies schnell und einfach angezeigt: Beim Aufruf unseres sicheren OnlineBankings färbt sich je nach Browser die URL oder die komplette Adresszeile grün und ein Schloss-Symbol wird eingeblendet.


## Sicherheit mit TÜV-Siegel

Der TÜV-Rheinland bestätigte erneut die Sicherheit des PSD OnlineBankings und der von den PSD Banken angebotenen PIN- und TAN-Verfahren zur Autorisierung von Transaktionen.

### InfoBox: 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 Zertifikats können Sie 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.



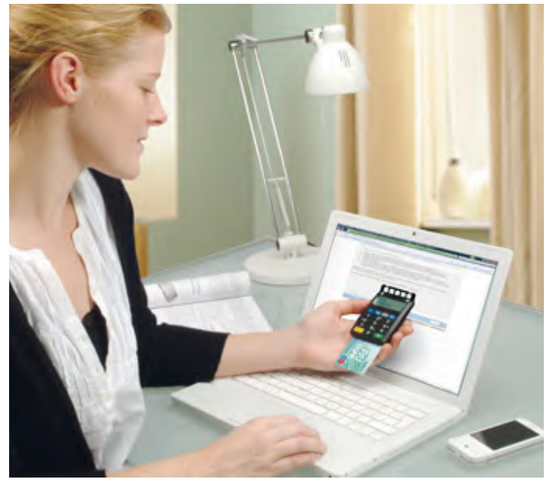
Sicherer ist sicher

# Unsere TAN-Verfahren

Moderne TAN-Verfahren bieten effektiven Schutz im OnlineBanking. Mit den Verfahren mobileTAN, Sm@rt-TAN plus und SecureGo bieten wir Ihnen drei mobile und flexible TAN-Verfahren, mit denen Ihr PSD OnlineBanking zukunftssicher ist.

Mit dem **mobileTAN**-Verfahren kommt die TAN per SMS auf Ihr mobiles Endgerät. Zu jedem Auftrag, den Sie im PSD OnlineBanking einstellen, wird eine spezielle Transaktionsnummer (TAN) erstellt, die nur für diesen speziellen Auftrag und für wenige Minuten gültig ist. Weitere in der SMS enthaltene Daten wie z.B. Empfänger-IBAN und Betrag bieten Ihnen dabei die optimale Möglichkeit zur Überprüfung Ihres Auftrags.

**Smart-TAN-plus** ist ein innovatives flexibles Verfahren zur Ermittlung von Transaktionsnummern (TAN) im OnlineBanking. Mit einem handlichen kabellosen TAN-Generator und Ihrer BankCard können Sie jederzeit und überall Ihre Bankgeschäfte sicher erledigen - unabhängig davon, ob Sie diese per OnlineBanking auf einem PC, einem Notebook, einem Tablet-Computer oder per Banking-App auf Ihrem Smartphone tätigen. Hierbei wird unterhalb Ihres Auftrags eine blinkende Grafik, der sog. Flicker-Code, eingeblendet. Stecken Sie nun Ihre BankCard in den TAN-Generator und halten Sie diesen vor die Grafik an den Bildschirm. Über die Lichtsensoren auf der Rückseite werden Ihre Auftragsdaten auf den TAN-Generator übertragen. Im Display des TAN-Generators können Sie nun die Auftragsdaten (z.B. Empfänger-IBAN und Betrag) überprüfen, bevor auf dem Chip Ihrer BankCard die speziell für diesen Auftrag gültige TAN errechnet wird.



**SecureGo** ist das modernste der drei TAN-Verfahren der PSD Banken und eine Weiterentwicklung der mobileTAN. Jedoch werden bei SecureGo die TAN-Benachrichtigungen nicht per SMS versandt, sondern in der SecureGo-App angezeigt. Diese ist erhältlich für Android und iOS. Sie benötigen lediglich ein Smartphone oder Tablet, auf dem diese App installiert ist, sowie eine Registrierung in der App und im PSD OnlineBanking.

Geben Sie im PSD OnineBanking einen Auftrag ein, z.B. eine Überweisung, klicken Sie dort zum Bestätigen des Auftrags auf den Button „Eingaben prüfen“. Dann melden Sie sich in der SecureGo-App an und prüfen die Auftragsdaten (z.B. Betrag und Empfänger-IBAN) auf Korrektheit. Sind die Daten korrekt, wird Ihnen die TAN angezeigt, die Sie im PSD OnlineBanking eingeben. Bei Nutzung der Banking-App können Sie die TAN auch ganz einfach per Klick übertragen. Das geht natürlich nur, wenn beide Apps auf dem gleichen Gerät installiert sind.

### InfoBox: Warum sind die TAN-Verfahren des PSD OnlineBankings besonders sicher?

- Optimale Kontrollmöglichkeiten zur Abwehr von Manipulationsversuchen durch Anzeige der Auftragsdaten wie Empfänger-IBAN oder Betrag
- Die jeweilige TAN ist nur für den aktuellen Auftrag gültig und kann von Dritten nicht für andere Aufträge missbraucht werden.
- Die TAN wird jeweils neu erzeugt und ist nur wenige Minuten gültig.
- Erhöhte Sicherheit durch die Nutzung zweier unterschiedlicher Kommunikationsgeräte (z.B. Smartphone und PC) bzw. Kommunikationskanäle (Banking-App und SecureGo-App)

# Auch Sie müssen mithelfen!

Die Maßnahmen der PSD Bank sichern zwar den Datentransport effektiv, können aber Ihren Computer nicht pauschal gegen Angriffen von außen schützen. Da jedes Endgerät individuell von seinem Benutzer konfiguriert wird, können und müssen Sie selbst für eine ausreichende Absicherung Ihres Systems sorgen. Viele Angriffe zielen auf OnlineBanking-Kunden, um vertrauliche Daten 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.

Ungeziefer auf Ihrem Rechner

# Von Viren, Würmern, Pferden & Bots

Gefahren lauern überall - auch und gerade im Internet. Diverse Arten von Schadprogrammen machen das Netz unsicher - bösartige Programme, die auf von ihnen befallenen Rechnern unerwünschte Funktionen auführen. Viele Exemplare haben dabei eine unangenehme Eigenschaft gemeinsam: Sie versuchen, andere Rechner ebenfalls zu infizieren und sind zudem so raffiniert, dass Sie über das Internet automatisch neue Funktionen nachladen und sich ständig verändern können.

**Viren** im Computer funktionieren ähnlich 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 oder - und das ist ein gravierendes Sicherheitsproblem - vertrauliche Daten werden unbemerkt weitergeleitet oder ausspioniert.

E-Mails können das Eingangstor von Viren zu Ihrem Rechner sein, z.B. ein schneller Klick auf einen Anhang der Ihr Interesse geweckt hat. Aber auch über USB-Stick, CD-Rom oder aus nicht-offiziellen Download-Quellen können Viren in Ihr System gelangen. In jeder ausführbaren Datei (z.B. *.exe, *.com) kann sich ein Virus verstecken. Aber auch Text-Dokumente (*.docx) oder Tabellen (*.xlsx) können virenverseucht sein.

**Würmer** nutzen undichte Stellen Ihrer Computerprogramme. Sie können eindringen, sobald Sie mit dem Internet verbunden sind. Sind sie erst einmal im System können Sie sich durch die Sicherheitslücken in einigen E-Mail-Programmen besonders schnell verbreiten. Bei einigen Programmen ist es sogar möglich, dass sich die verseuchten E-Mails ohne Wissen des Benutzers an Personen aus dem Adressbuch versenden - die dann natürlich den Versender kennen und als vertrauensvoll einstufen können. Ein Klick und schon pflanzt sich der Wurm weiter fort.

**Trojanische Pferde** haben ihren Namen nach der Kriegslist der Griechen aus dem Trojanischen Krieg. Unter dem Deckmantel nützlicher Funktionen nistet sich ein Programm auf Ihrem Computer ein und kann im Hintergrund Schaden anrichten. So können sensible Daten wie Passwörter, Kreditkartennummern und IBAN ausspioniert, kopiert und unbemerkt weitergeleitet werden. Außerdem können alle Aktivitäten am Computer überwacht und dadurch über die Tastatur eingegebene Daten abgefangen und an unberechtigte Empfänger übermittelt werden. Schließlich können durch sogenannte Hintertüren Angreifer aus dem Internet auf Ihren Computer zugreifen.

**Bots** installieren sich selbstständig, oft mit Hilfe von Viren und Würmern. Sind Sie erst einmal in den Computer eingedrungen, übernehmen Sie die Herrschaft darüber. Ist der Rechner mit dem Internet verbunden, kann er so Teil eines Botnetzes werden. Dabei handelt es sich um ein Netzwerk von Rechnern, die mit Bots verseucht sind, die durch den Verursacher der Schadprogramme aktiviert werden können. Botnetze werden von Cyber-Kriminellen genutzt, um beispielsweise mit gezielten Angriffen große Internetseiten lahmzulegen oder unerkannt Spam zu versenden. Die Folge: Ihr Rechner ist nicht mehr nur Opfer sondern wird gleichzeitig auch zum Täter.



## InfoBox: So schützen Sie sich vor Schadprogrammen

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.

Viele Schadprogramme nutzen Sicherheitslücken von Betriebssystemen und Browsern aus. Darum sollten Sie Ihr Betriebssystem und Ihre Anwendungen regelmäßig aktualisieren. Vor allem für weit verbreitete Betriebssysteme wie Windows oder Android sollten alle wichtigen Service-Packs und Updates regelmäßig installiert werden.

Bei der Benutzung von Antivirenprogrammen ist es wichtig, regelmäßig (am besten täglich) die von den Herstellern bereitgestellten aktuellen Virensignaturen einzuspielen. Mit der meist vorhandenen Update-Funktion geschieht dies automatisch und Sie müssen sich nicht aktiv darum kümmern.

Eine Firewall stellt eine sinnvolle Ergänzung zu Antivierenprogrammen dar. Hier wird der Datenverkehr von und zu Ihrem Rechner kontrolliert. Dadurch wird zwar die Infektion des Computers nicht verhindert, der Datentransfer wird jedoch überwacht und wenn nötig auch unterbunden.

Nicht zuletzt können Sie mit den TAN-Verfahren der PSD Bank Echtzeitangriffe auf Ihre OnlineBanking-Sitzung (sog. Man-in-the-middle-Angriffe) durch die Kontrolle der Auftragsdaten schnell und einfach erkennen und somit zeitnah abwehren. Weichen die Daten von den von Ihnen eingegebenen ab, bestätigen Sie die Transaktion auf keinen Fall sondern brechen den Vorgang ab, sperren Ihren OnlineBanking-Zugang und melden dies Ihrer PSD-Bank.

Auch unterwegs online

# Mobile Besonderheiten

Immer mehr OnlineBanking-Nutzer tätigen ihre Bankgeschäfte inzwischen per Smartphone oder Tablet. Viele von ihnen fragen nur ihren Kontostand ab, doch die Zahl der mobilen Überweisungen steigt von Tag zu Tag. Hierbei sollten Sie einige Sicherheitshinweise beachten.

Durch die Nutzung einer offiziellen Banking-App umgehen Sie die Gefahr, auf gefälschte Seiten hereinzufallen. Externe Apps wie StarMoney oder OutBank werben mit größerer Bedienerfreundlichkeit, sind aber oft kostenpflichtig. Dagegen ist die multibankfähige PSD Banking-App kostenfrei.

Besondere Vorsicht ist beim Zugang zum Konto geboten. Der Automatische Login bei Banking-Apps oder auf dem mobilen Gerät gespeicherte Zugangsdaten machen es einem Dieb oder Finder leicht, auf Ihr Konto zuzugreifen. Vermeiden Sie dies und nutzen Sie die automatische Bildschirmsperre mit PIN-Abfrage!

In öffentlichen WLAN-Netzen ist ihr Datenfluss nicht sicher und kann angezapft werden. Darum ist hier besondere Vorsicht geboten, genauso wie bei Banking-Apps oder Links die nicht offiziell anmuten. Auch hier gilt: Nutzen Sie die Angebote nicht!

Und schließlich: Was für den PC gilt, ist auch bei mobilen Geräten wichtig. Dazu gehören Virenschutz und Firewall genauso wie aktuelle Versionen von Gerätesoftware und Apps.

## InfoBox: Schutz für Smartphone & Co.

- Gesunder Menschenverstand: Prüfen Sie kritisch, ob die Zugriffsrechte einer App wirklich für ihren Betrieb nötig sind oder ob Sie unter diesen Bedingungen lieber auf diese App verzichten.
- Installieren Sie Apps nur aus vertrauenswürdigen Quellen.
- Deaktivieren Sie drahtlose Schnittstellen (WLAN, Bluetooth), wenn Sie diese nicht nutzen und koppeln Sie externe Geräte mit Ihrem Smartphone nur in gesicherter Ungebung
- Führen Sie regelmäßig Sicherheitsupdates durch, und zwar für die Firmware Ihres Gerätes, das Betriebssystem und sonstige Software und Apps. Auch hier gilt: nur aus gesicherter Quelle.
- Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht und wenn möglich nur über eine gesicherte Verbindung (https://). Vermeiden Sie OnlineBanking in offenen Netzwerken.
- Halten Sie mobile Geräte stets unter Aufsicht.
- Lassen Sie bei Verlust Ihres mobilen Gerätes die SIM-Karte sofort sperren.

Das sollten Sie beachten

# Allgemeine Hinweise

Die eingebauten Schutzfunktionen Ihres Betriebssystems sollten grundsätzlich genutzt werden. Dazu zählt zum Beispiel, 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. Wenn Sie sich dann als User unvorsichtig verhalten, ermöglicht dies Trojanischen Pferden, Viren, Würmern und Bots, sich im System festzusetzen und ungehindert Schaden anzurichten.

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

## Die wichtigsten Schutzmaßnahmen auf einen Blick

### Allgemeine Maßnahmen

- Arbeiten Sie mit dem aktuellsten Betriebssystem und installieren Sie regelmäßig die verfügbaren Updates.
- Benutzen Sie ein aktuelles Antivirenprogramm. Nutzen Sie die Update-Funktion für regelmäßige (möglichst tägliche) Updates. Durchsuchen Sie mit Hilfe eines Antivirenprogramms Ihren Rechner regelmäßig nach Viren.
- Aktivieren Sie stets eine Firewall und aktualisieren Sie diese regelmäßig!
- Arbeiten Sie mit einem aktuellen Browser und halten Sie diesen auf dem neuesten Stand.
- Nutzen Sie für den Zugriff auf das Internet ein Benutzerkonto mit eingeschränken Rechten.
- Seien Sie misstrauisch, wenn sich Ihr Computer anders als gewohnt verhält.


### Maßnahmen für sicheres OnlineBanking

- Geben Sie Ihre Online-PIN niemals an Dritte weiter.
- Speichern Sie Ihre PIN nicht auf Ihrem Rechner ab.
- Achten Sie darauf, dass die Kommunikation verschlüsselt erfolgt. Überprüfen Sie das Zertifikat.
- Vermeiden Sie es, Ihre Bankgeschäfte an fremden Computern (z. B. Internet-Cafe) zu tätigen, da es dort einfacher ist, Ihre persönlichen Daten auszuspionieren.
- Reagieren Sie nicht auf Phishing-Mails. Ihre Bank wird Sie nie auffordern, Daten wie PIN oder IBAN bekannt zu geben.
- 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“ im OnlineBanking unter „Service“ und dort „Sicherheit im OnlineBanking“
  - Dreimalige Eingabe einer falschen PIN im OnlineBanking
  - Anruf beim Sperr-Notruf 116 116

### 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 Trojaner und Viren etc. zu informieren. Viele Hintergrundinformationen finden Sie beim „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) auf https://www.bsi-fuer-buerger.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.



# Glossar

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

## Fachbegriffe verständlich erklärt

**Antivirenprogramm**

Ein Antivirenprogramm (oder Virenscanner) schützt den Computer vor Viren, Würmern oder Trojanischen Pferden. Das Programm überwacht zum einen den Rechner vor gefährlichen Aktivitäten und kann zum anderen genutzt werden, um die Speichermedien (Festplatten, CDs, DVDs, USB-Sticks etc.) nach vorhandenen Schadprogrammen zu durchsuchen.

**App**

Eine App (kurz für „application“) ist ein Anwendungsprogramm u.a. für mobile Endgeräte wie Smartphones oder Tablet-Computer. Diese werden direkt auf dem entsprechenden Gerät installiert. Die PSD Banking-Apps ermöglichen Ihnen zum Beispiel den mobilen Zugriff auf die wichtigsten Zahlungsverkehrsfunktionen.

**Browser**

Ein Browser ist ein Programm, um Seiten aus dem Internet anzuzeigen. Bekannte Browser sind z. B. der Internet Explorer, Firefox, Chrome, Edge, Safari und Opera.

**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. So werden Angriffe von außen und die unbemerkte Weitergabe von Informationen verhindert.

**Homepage**

Als Homepage wird i. d. R. die Startseite eines Internetauftrittes bezeichnet, d. h. die Seite, welche Ihnen nach der Eingabe der neuen Adresse in Ihren Browser zuerst angezeigt wird.

**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 Dokument oder eine andere Internetseite. Mit einem Klick auf die Markierung wird z.B. automatisch die mit dem Link verknüpfte Adresse in Ihrem Browser aufgerufen.

**Man-in-the-middle-Angriff**

Beim Man-in-the-middle-Angriff (kurz MITM-Angriff) klinkt sich ein Dritter in die Kommunikation zwischen zwei Partnern ein. Wenn sich zum Beispiel ein Kunde mit dem OnlineBanking verbinden will, schaltet sich der Angreifer dazwischen und kann die Informationen, die ausgetauscht werden, lesen und auch manipulieren. Und da der „Mann in der Mitte“ beiden Beteiligten vorgaukelt, der jeweils andere zu sein, geschieht das Ganze meist unbemerkt.

**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.

**Patch**

Ein so genanntes Patch (von englisch „Flicken“) ist eine Korrektur für Software oder Daten und schließt meist vorhandene Sicherheitslücken.

**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 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. Aktivieren Sie den Spam-Filter Ihrer E-Mail-Software.

**TLS**

Die Abkürzung steht für Transport Layer Security. Es handelt sich hierbei um eine zusätzliche Versicherungstechnik für Datenübertragungen im Internet (z.B. HTTPS statt HTTP).

**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 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 eingegeben werden muss, um eine Seite aufzurufen. (Beispiel: https://www.psd-bank.de)

**Virensignatur**

Jedes Antivirenprogramm nutzt so genannte Virensignaturen (auch Virendefinitionen genannt), um die charakteristischen Merkmale der Viren zu kennen. Da täglich neue Viren auftauchen, ist es sehr wichtig, diese Erkennungslisten regelmäßig – möglichst täglich – zu aktualisieren.

Impressum

Herausgeber:
Servicegesellschaft der PSD Banken mbH,
Dreizehnmorgenweg 36, 53175 Bonn
Redaktion: Mark Schulz
Verantwortlich i.S.d.P.: Markus Berkenkopf

Bildnachweis

S. 1, 2: © stokkete/fotolia.com,
S. 2 unten, 8: © WavebreakmediaMicro/fotolia.com,
S. 3 unten: © Rido/fotolia.com,
S. 4 oben: © Simon Greig/fotolia.com,
S. 4 unten: © flucas/fotolia.com,
S. 5 oben: © ristaumedia.de/fotolia.com,
S. 5 unten: © Tanusha/fotolia.com,
S. 6 oben: © Andrey Popov/fotolia.com,
S. 7: © trinaestipo/fotolia.com

# Checkliste

Sie wissen jetzt: OnlineBanking kann nur so sicher sein wie die von Ihnen genutzten Geräte! 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!

## Das Wichtigste auf einen Blick

### ☐ Ja, ich nutze ein aktuelles Betriebssystem!

Nutzer von älteren Systemen sollten unbedingt auf die aktuelle Version aktualisieren! Verfügbare Sicherheitspatches und Service-Packs sollten regelmäßig installiert werden.

### ☐ Ja, ich benutze einen aktuellen Browser!

Nutzer von älteren Browsern sollten unbedingt auf die aktuellste Version wechseln! Verfügbare Sicherheitspatches und Service-Packs sollten regelmäßig installiert werden.

### ☐ Ja, ich benutze eine Firewall!

Nutzer von Windows-Betriebssystemen sollten überprüfen, ob die integrierte Firewall aktiviert ist, oder eine andere Firewall eines namhaften Herstellers installieren. Nutzen Sie die automatische Update-Funktion, 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 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 auf die Aufforderung aus einer E-Mail hin weiter.

### ☐ Ja, ich verwende keine Downloads aus zwielichtigen 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. Schließen 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 Ihrer OnlineBanking-PIN fragen, weder am Telefon noch per E-Mail. Speichern Sie niemals Ihre PIN auf Ihrem Rechner ab.

### ☐ Ja, ich starte das OnlineBanking nur über die Homepage meiner Bank oder per App!

Starten Sie das OnlineBanking immer nur über die jeweilige Homepage oder per App. Legen Sie keine Favoriten (bzw. Bookmarks) an, denn diese könnten manipuliert werden. 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.