BSI - Online Banking

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/onlinebanking_node.html

Inhaltsverzeichnis

1. So funktioniert Online Banking

1.01 Grundlagenwissen

In diesem Kapitel erfahren Sie, wie Online-Banking grundlegend funktioniert und welchen Nutzen es bietet. Auch wird hier beschrieben, welche technischen Voraussetzungen Sie mitbringen müssen, um Online-Banking nutzen zu können. Im Kapitel über die TAN-Verfahren erfahren Sie, welche Sicherheitsstandards es derzeit gibt.

1.02 Kapitelübersicht:

Nutzen von Online-Banking: Die Dienstleistungen der Banken, von einfacher Umsatzabfrage bis hin zu Daueraufträgen und Depotverwaltung.

1.1 Welchen Nutzen hat Online-Banking?

Online-Banking soll Bankgeschäfte einfacher machen: Statt etwa handschriftlich Überweisungsträger auszufüllen und in einer Bank-Filiale abzugeben, können Sie Überweisungen und andere Transaktionen zu Hause an Ihrem Computer erledigen.

Dazu gehört beispielsweise:

- Kontostände sowie Ein- und Ausgänge abfragen
- Kreditkartenumsätze einsehen
- Geld ins In- und Ausland überweisen
- Terminüberweisungen einrichten
- Daueraufträge einrichten und stornieren

Mithilfe von Online-Banking können Sie nicht nur ihr Giro-Konto verwalten. Je nach Bank ist es auch möglich auf Wertpapier-Depots zuzugreifen, um Aktien zu kaufen und zu verkaufen. Auch Spar-, Bauspar-, Tagesgeld- oder Festgeldkonten lassen sich online verwalten.

Die Vorzüge des Online-Banking überzeugen immer mehr Bankkunden: Laut dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) erledigten 2012 über 28 Millionen Deutsche ihre Bankgeschäfte online. Damit nutzen derzeit 45 Prozent aller Bundesbürger im Alter von 16 bis 74 Jahren Online-Banking.

Vorraussetzungen für Ihr Online-Banking: Sie brauchen nicht viel, um Online-Banking nutzen zu können.

1.2 Was brauchen Sie für Online-Banking?

Die Hürden für den Einstieg ins Online-Banking sind vergleichsweise niedrig. Um Bankgeschäfte online erledigen zu können, brauchen Sie einen handelsüblichen Computer oder ein anderes internetfähiges Gerät, wie zum Beispiel ein Smartphone. Weil keine hohe Rechenleistung vonnöten ist, können dabei auch ältere Modelle zum Einsatz kommen. Auch das Betriebssystem spielt keine Rolle: Online-Banking ist sowohl unter Windows als auch unter MacOS und Linux möglich.

In jedem Fall muss das verwendete Gerät über eine Internet-Anbindung verfügen. Weil das Datenaufkommen beim Online-Banking gering ist, funktioniert Online-Banking auch mit langsamen Internetverbindungen per Modem oder UMTS. Eine schnelle Breitband-Anbindung – etwa per DSL – erhöht lediglich die Geschwindigkeit, mit der sich die Seiten aufbauen.

Die einzige Software, die zur Nutzung der Online-Dienste der Banken erforderlich ist, ist ein Internet-Browser. Grundlegende Kenntnisse bei der Bedienung der Internet-Software genügen, um damit Bankgeschäfte abwickeln zu können. Bei der Auswahl der Browser gilt: Sie können mit allen gängigen Programmen wie Microsoft Internet Explorer, Apple Safari, Mozilla Firefox oder Google Chrome die Online-Banking-Websites besuchen. Aus Sicherheitsgründen sollten aber sowohl Browser als auch Betriebssystem und alle installierten Softwareprodukte per Updates stets auf dem neuesten Entwicklungsstand gebracht werden (siehe auch Artikel "Wie Sie Ihren Computer sicher einrichten").

1.2.1 Wie Sie Ihren Computer sicher einrichten

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungComputer/EinrichtungComputer_node.html

Wieviel Aufwand Sie zum Schutz Ihres PC und einem ungetrübten Surf-Vergnügen – und somit natürlich auch zum Schutz Ihrer Privatsphäre – betreiben müssen, hängt in erster Linie von Ihren persönlichen Anforderungen ab.

Für die private Nutzung von PCs unter Windows und Ubuntu, sowie Macs unter Apple OS X hat das BSI konkrete Hilfestellungen für eine sichere Konfiguration erstellt. Dabei wird der komplette Lebenszyklus vom Kauf des Systems über die Installation und Inbetriebnahme, den regelmäßigen Betrieb bis hin zur Entsorgung betrachtet.

- PCs unter Microsoft Windows 7 - Privatanwender V1.5 (PDF, 278KB)
- Sichere Nutzung von PCs unter Ubuntu V1.1 (PDF, 209KB)
- Sichere Nutzung von Macs unter Apple OS X Mountain Lion V1.1 (PDF, 219KB)

1.2.2 Grundlegender Schutz leicht gemacht!

Viele Computer von Privatanwendern, die zum Internetsurfen verwendet werden, sind nicht ausreichend gegen die Risiken der Online-Welt geschützt. Kriminelle nutzen dies, indem sie solche Rechner zum Beispiel mit Schadprogrammen infizieren und für ihre Zwecke missbrauchen. Dadurch können Ihnen erhebliche Schäden entstehen. Zum Beispiel können die Kriminellen Ihre Daten löschen oder ausspionieren, in Online-Shops Waren in Ihrem Namen und auf Ihre Kosten bestellen, Transaktionen beim Online-Banking manipulieren oder Ihnen den Zugang zu Ihrem Bankkonto sperren. Die Kriminellen können Ihren Rechner außerdem zum Teil eines Botnetzes machen und ihn so für Cyber-Angriffe auf Unternehmen oder andere Institutionen sowie zum Versand von Spam-E-Mails einsetzen.
Einen hundertprozentigen Schutz gegen diese Gefährdungen gibt es leider nicht. Um die Risiken jedoch weitgehend einzuschränken, können Sie selbst etwas tun.

Zwölf Maßnahmen zur Absicherung gegen Angriffe aus dem Internet

Die **wichtigsten Tipps,** die Sie auf jeden Fall beherzigen sollten, haben wir in einer Übersicht zusammengestellt.

1.2.3 Zwölf Maßnahmen zur Absicherung gegen Angriffe aus dem Internet

Einen hundertprozentigen Schutz gegen diese Gefährdungen gibt es leider nicht. Um die Risiken jedoch weitgehend einzuschränken, können Sie selbst etwas tun. Wenn Sie die folgenden Maßnahmen umsetzen, dann erhöhen Sie die Sicherheit Ihres Rechners und Ihre Sicherheit im Internet bereits erheblich. Die ersten fünf Empfehlungen (**"Kernmaßnahmen"**) sollten Sie dabei in jedem Fall umsetzen. Die weiteren Empfehlungen sind **ergänzende Maßnahmen**, mit deren Umsetzung Sie Cyber-Kriminellen weniger Angriffsfläche bieten und präventiv dafür sorgen können, Ihre Internet-Sicherheit zu verbessern und mögliche negative Folgen zu mindern.

Alle Maßnahmen sind in der Regel auch für Laien einfach umzusetzen. Wenn Sie sich dies dennoch nicht zutrauen, dann sollten Sie einen Internet-Profi oder den Hersteller Ihres IT-Systems zur Rate ziehen, der Sie dabei unterstützen kann.
Hilfestellung bietet auch das Service-Center des BSI.

Telefon 0800 2741000
Kostenlos aus dem deutschen Fest- und Mobilfunknetz
Erreichbarkeit: Montag bis Freitag von 8:00 bis 18:00 Uhr
Oder schicken Sie eine E-Mail an: mail@bsi-fuer-buerger.de

Kernmaßnahmen

- Installieren Sie regelmäßig von den jeweiligen Herstellern bereitgestellte **Sicherheitsupdates** für Ihr Betriebssystem und die von Ihnen installierten Programme (zum Beispiel Internet-Browser, Office, Flash Player, Adobe Reader) – idealerweise über die Funktion "Automatische Updates". Diese Funktion können Sie in der Regel im jeweiligen Programm einstellen, meist unter dem Menüpunkt "Optionen" oder "Einstellungen".
- Setzen Sie ein **Virenschutzprogramm** ein und aktualisieren Sie dieses regelmäßig, idealerweise über die Funktion "Automatische Updates"

- Verwenden Sie eine **Personal Firewall**. Diese ist in den meisten modernen Betriebssystemen bereits integriert und soll Ihren Rechner vor Angriffen von außen schützen. Dazu kontrolliert sie alle Verbindungen des Rechners in andere Netzwerke und überprüft sowohl die Anfragen ins Internet als auch die Daten, die aus dem Internet an Ihren Rechner gesendet werden.
- Nutzen Sie für den **Zugriff auf das Internet** ausschließlich ein **Benutzerkonto mit eingeschränkten Rechten**, keinesfalls ein Administrator-Konto. Alle gängigen Betriebssysteme bieten die Möglichkeit, sich als Nutzer mit eingeschränkten Rechten anzumelden. Wie Sie ein einfaches Benutzerkonto einrichten, ist hier erklärt: Microsoft Windows, Mac OS X, Linux, Linux Ubuntu
- **Seien Sie zurückhaltend mit der Weitergabe persönlicher Informationen. Seien Sie misstrauisch.** Klicken Sie nicht automatisch auf jeden Link oder jeden Dateianhang, der Ihnen per E-Mail gesendet wird. Überprüfen Sie gegebenenfalls telefonisch, ob der Absender der Mail authentisch ist. Wenn Sie Software herunterladen möchten, dann sollten Sie dies möglichst ausschließlich von der Webseite des jeweiligen Herstellers tun.

Ergänzende Maßnahmen

- Verwenden Sie einen modernen **Internet-Browser mit fortschrittlichen Sicherheitsmechanismen** wie etwa einer Sandbox. Konsequent umgesetzt wird dieser Schutz gegenwärtig zum Beispiel von Google Chrome. Zudem sollte der Browser über einen Filtermechanismus verfügen, der Sie vor schädlichen Webseiten warnt, bevor Sie diese ansurfen. Beispiele solcher Filtermechanismen sind der Smart Screen Filter beim Internet Explorer sowie der Phishing- und Malwareschutz bei Google Chrome und Mozilla Firefox. Darüber hinaus sollten Sie nur solche Browser-Zusatzprogramme "Plugins" verwenden, die Sie unbedingt benötigen. Weitere Empfehlungen zur sicheren Konfiguration Ihres Browsers hat das BSI hier für Sie zusammengestellt.
- Nutzen Sie möglichst **sichere Passwörter**. Verwenden Sie für jeden genutzten Online-Dienst – zum Beispiel E-Mail, Online Shops, Online Banking, Foren, Soziale Netzwerke – ein anderes, sicheres Passwort. Ändern Sie diese Passwörter regelmäßig. Vom Anbieter oder Hersteller voreingestellte Passwörter sollten Sie sofort ändern. Wie Sie ein sicheres Passwort erstellen können, haben wir hier für Sie beschrieben.
- Wenn Sie im Internet persönliche Daten übertragen wollen, etwa beim Online Banking oder beim Online Shopping, dann sollten Sie dies ausschließlich über eine **verschlüsselte Verbindung** tun. Jeder seriöse Online-Dienst bietet eine solche Möglichkeit an, beispielsweise durch die Nutzung des sicheren Kommunikationsprotokolls "HTTPS". Sie erkennen dies an der von Ihnen aufgerufenen Internetadresse, die stets mit "**https://**" beginnt und an dem kleinen Schloss-Symbol in Ihrem Browserfenster.
- **Deinstallieren Sie nicht benötigte Programme.** Je weniger Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche Ihres gesamten Systems.
- Erstellen Sie **regelmäßig Sicherheitskopien "Backups"** Ihrer Daten, um vor Verlust geschützt zu sein. Hierzu können Sie beispielsweise eine externe Festplatte nutzen.
- Wenn Sie ein WLAN ("Wireless LAN", drahtloses Netzwerk) nutzen, dann sollte dies stets mittels des **Verschlüsselungsstandards WPA2** verschlüsselt sein. Wie Sie ein sicheres WLAN einrichten können, erfahren Sie hier.
- Überprüfen Sie in regelmäßigen Abständen den **Sicherheitsstatus Ihres Computers**. Eine schnelle Testmöglichkeit bietet die Initiative botfrei des eco-Verbands.

Weitere Informationen:

- Zu Fragen der IT-Sicherheit finden Sie Hinweise in unseren Tipps und Checklisten.
- Der Avira PC-Cleaner eignet sich für einen zusätzlichen **Schnelltest** auf Schadsoftwarebefall, ersetzt jedoch kein vollwertiges Virenschutzprogramm.

Hinweis:

Ein Programm will sich plötzlich installieren.

Wenn plötzlich, scheinbar ohne Grund während des Surfens im Internet ein Fenster aufgeht und Ihnen mitteilt, dass sich ein Programm installieren möchte und dazu nach Ihrem Passwort fragt, ist höchste Vorsicht geboten. Wenn Sie Zweifel am Zweck des Programms haben, brechen Sie den Vorgang ab ohne ein Passwort einzugeben.

1.3 Sicherheit im Online-Banking

Inhalt des Dossiers

Die PIN-/TAN-Verfahren und andere Schutzmaßnahmen

Um sicherzustellen, dass nur Sie auf Ihr Konto zugreifen können, setzen die Anbieter schon seit vielen Jahren das PIN/TAN-Verfahren ein. Um etwa eine Überweisung durchzuführen, müssen Sie sowohl eine persönliche Identifikations-Nummer (PIN) als auch eine Transaktionsnummer (TAN) eingeben.

Die Transaktionsnummer ist eine Nummer, die nur einmalig für eine Transaktion gilt. Es gibt viele verschiedene Wege, die Transaktionsnummer dem Bankkunden zu übermitteln, sodass er eine Überweisung oder ähnliches tätigen kann. Welche TAN-Verfahren es gibt und welche sicherer sind als andere, erfahren Sie hier.

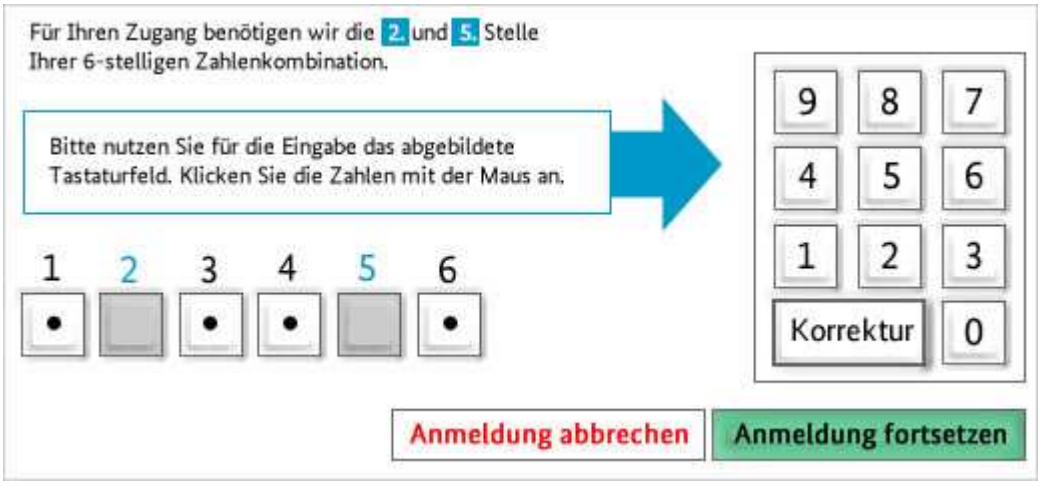
1.3.1 PIN-/TAN-Verfahren allgemein erklärt

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/SoFunktioniertDasOnlineBanking/Sicherheit/PIN-TAN-Schutzverfahren.html;jsessionid=A65307F08CADDBEC31C2213E9C3440C6.1_cid360?cms_pos=1

Um sicherzustellen, dass nur Sie auf Ihr Konto zugreifen können, setzen die Banken schon seit vielen Jahren das PIN/TAN-Verfahren ein. Um etwa eine Überweisung durchzuführen, müssen Sie sowohl eine persönliche Identifikations-Nummer (PIN) als auch eine Transaktionsnummer (TAN) eingeben.

Die PIN ist das Passwort, das Sie jedes Mal eingeben müssen, um auf Ihr Benutzerkonto und alle Funktionen zugreifen zu können. Mit den Zugangsdaten zum Online-Banking erhalten Anwender ihre PIN. Dabei muss es sich nicht zwangsläufig um eine Zahl handeln. Inzwischen können Nutzer in der Regel nach dem erstmaligen Einloggen ins Banking-System eine neue PIN aus beliebigen Zeichenkombinationen selbst bestimmen (siehe auch Artikel "Passwörter").

Manche Banken verlangen von ihren Kunden neben der PIN, eine zusätzliche Zahlen- oder Buchstabenkombination, die nur per Mausklick, nicht jedoch mit der Tastatur eingegeben werden kann.



Die Eingabe einer Zahlenkombination per Mausklick sichert den Zugang zum Online-Banking zusätzlich ab.

So entsteht eine zusätzliche Sicherheitsbarriere. Hat ein Krimineller etwa durch das Aufzeichnen der Tastatureingaben die PIN erhalten, hat er noch keinen Zugriff auf das Konto, da das zusätzliche Passwort fehlt. Das könnte er nur erhalten, wenn er auch die Bildschirmbewegungen aufzeichnet.

Haben Sie sich mithilfe der PIN (plus eventuell zusätzlichem Passwort) eingeloggt, können Sie auf alle Funktionen des Online-Bankings zugreifen. Aber egal, ob Sie eine Überweisung tätigen oder einen Dauerauftrag einrichten wollen – um Transaktionen auszuführen, müssen Sie zusätzlich jeweils eine TAN, also eine Transaktionsnummer eingeben. Im Gegensatz zur immer gleichen PIN benötigen Sie für jede Transaktion eine neue TAN.

Wie sicher Online-Banking ist, hängt maßgeblich vom eingesetzten PIN/TAN-Verfahren ab. Sie sollten daher bei der Auswahl Ihrer Bank auch darauf achten, welche Angebote die Unternehmen beim Online-Banking machen: Nicht alle Kreditinstitute bieten sichere PIN/TAN-Verfahren an. Allerdings ist keines der TAN-Verfahren gegen alle Angriffe resistent, ein gewisses Risiko bleibt immer. Beachten Sie daher auch immer die Geschäftsbedingungen der Banken: Manche Banken bieten zwar beim Online-Banking Verfahren an, die technisch unsicherer sind als andere, aber übernehmen dafür eine sogenannte "Risikogarantie". Durch die Geschäftsbedingungen beziehungsweise Sicherheitsvorgaben der Banken werden Ihnen auch besondere Sorgfaltspflichten auferlegt. Diese sollten Sie kennen und wahrnehmen.

1.3.2 PIN-/TAN-Verfahren mit TAN-Liste

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/SoFunktioniertDasOnlineBanking/Sicherheit/PIN-TAN-Schutzverfahren.html;jsessionid=A65307F08CADDBEC31C2213E9C3440C6.1_cid360?cms_pos=2

Um sicherzustellen, dass nur Sie auf Ihr Konto zugreifen können, setzen die Banken schon seit vielen Jahren das PIN/TAN-Verfahren ein. Die unterschiedlichen PIN/TAN-Verfahren bieten einen unterschiedlichen Schutz.

1.3.2.1 Das klassische PIN/TAN-Verfahren

Beim klassischen PIN/TAN-Verfahren verschickt die Bank eine auf Papier gedruckte TAN-Liste per Post. Wenn Online-Banking-Nutzer eine Transaktion durchführen wollen, können Sie eine beliebige TAN aus der Liste verwenden. Dabei kann jede TAN nur einmal verwendet werden.

Dieses klassische Verfahren bietet nur einen eingeschränkten Schutz vor Phishing-Angriffen (siehe auch Artikel "Online-Banking: Sicherheitsrisiken" Phishing. Wenn Kriminelle Kontodaten, PIN und TANs ausspioniert haben, können sie ungehindert Geld abheben und auf ihre Konten überweisen.

1.3.2.2 iTAN-Verfahren

Mehr Sicherheit bietet das iTAN-Verfahren: Auch hier verschickt die Bank eine TAN-Liste auf Papier – die Transaktionsnummern sind aber zusätzlich durchnummeriert. Wenn Sie eine Überweisung durchführen wollen, werden Sie von der Bank aufgefordert, eine bestimmte TAN (zum Beispiel Nummer 17) einzugeben. Die angeforderte TAN ist an diesen bestimmten Auftrag gebunden und kann nicht beliebig verwendet werden. Der Vorteil des iTAN-Verfahrens gegenüber dem normalen TAN-Verfahren liegt darin, dass es im Falle eines erfolgreichen Phishing-Angriffs eine zusätzliche Sicherheitshürde gibt: Ausspionierte Transaktionsnummern nutzen den Online-Kriminellen nichts, wenn sie nicht die dazugehörige laufende Positionsnummer kennen.

Diese zusätzliche Sicherheitshürde führte dazu, dass die Zahl der bekannt gewordenen Phishing-Attacken nach der Einführung des iTAN-Verfahrens bei vielen Banken deutlich sank . Die Kriminellen reagierten aber schnell und entwickelten neue Methoden. Schon 2009 wies das BKA daher darauf hin, dass das iTAN-Verfahren nicht mehr als sicher einzustufen sei [Bundeskriminalamt: Bundeslagebild Cybercrime 2009]. Das liegt daran, dass das iTAN-Verfahren nicht vor so genannten Man-In-The-Middle-Angriffen (siehe auch Artikel "Schadprogramme beim Online-Banking") schützt, bei denen Schadprogramme zum Beispiel die Kontonummer des Empfängers verändern.

1.3.2.3 iTANplus

Eine Weiterentwicklung des iTAN-Verfahrens ist das sogenannte iTANplus-Verfahren. Bei diesem Verfahren wird nach Übermittlung der Transaktionsdaten auf dem Bildschirm ein Kontrollbild eingeblendet. Dieses sogenannte Captcha zeigt bei einer Überweisung Betrag, Bankleitzahl und Kontonummer des Empfängers, das Geburtsdatum des Kunden sowie die Positionsnummer der

angeforderten TAN an. Weil der Nutzer die Transaktionsdaten vor der Überweisung noch einmal überprüfen kann, werden Man-In-The-Middle-Angriffe erschwert.

1.3.3 Das mTAN-Verfahren – TAN-Versand per SMS

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/SoFunktioniertDasOnlineBanking/Sicherheit/PIN-TAN-Schutzverfahren.html?nn=6596940&cms_pos=3

Das mTAN-Verfahren (auch "mobileTAN" oder "smsTAN" genannt) ist eine Alternative zu klassischen TAN-Verfahren für alle Anwender, die ein Mobiltelefon besitzen. Nutzer dieses Verfahrens bekommen keine TAN-Liste auf Papier zugeschickt. Stattdessen verschickt die Bank nach Aufforderung durch den Anwender bei jeder Überweisung eine "mobile TAN" per SMS auf das vorher registrierte Mobilgerät des Kunden.

Das mTan-Verfahren ist zwar praktisch und benutzerfreundlich, birgt aber leider auch einige Risiken. Unter Umständen können Kriminelle die zur Authentifizierung verschickten SMS-Nachrichten abfangen oder umleiten. So besteht die Gefahr, dass die in der SMS enthaltene TAN missbraucht wird.

Erschwert wird ein solcher Angriff durch das sogenannte Dynamic Linking. Dabei fließen in die Erzeugung der TAN auch die Überweisungsdaten ein, so dass weder der Betrag noch das Ziel-Konto nachträglich verändert werden können. Das dadurch tatsächlich erreichte Schutzniveau ist allerdings von der Qualität der TAN-Erzeugung abhängig.

Das BSI empfiehlt daher, auf den Einsatz von mTAN-Verfahren zu verzichten.

1.3.3.1 Vorsichtsmaßnahmen beim Einsatz von mTAN-Verfahren

Sollten Sie mTAN dennoch nutzen wollen, beachten Sie folgende Sicherheitsempfehlungen:

In der SMS sollten neben der TAN auch die Kontonummer des Empfängers sowie der Überweisungsbetrag stehen. Diese sollten Sie vor Eingabe der TAN prüfen. Sollten hier Unstimmigkeiten bestehen, brechen Sie die Transaktion im Zweifel ab und setzen Sie sich mit Ihrer Bank in Verbindung.

Online-Banking und die Übermittlung der TAN erfolgen auf verschiedenen Übertragungswegen. Hat ein Angreifer den PC infiltriert, kann er keine Transaktionen ausführen, solange er nicht auch gleichzeitig Zugriff auf das Mobiltelefon hat. Beachten Sie aber, dass dieser Sicherheitsvorteil beim Online-Banking mit dem Smartphone nicht gegeben ist. Außerdem greifen Internet-Kriminelle das mTAN-Verfahren verstärkt an. Dass sowohl das mobile Gerät als auch der PC mit Schadsoftware infiziert sind, ist also inzwischen nicht mehr auszuschließen. Siehe hierzu Pressemitteilung des BSI aus 2011. Mittlerweile tauchen immer mehr Trojaner für Smartphones auf. Zusätzlich versuchen Internet-Kriminelle, das System der verschiedenen Übertragungswege zu überlisten: Zunächst wird dabei der Rechner infiziert, um den Nutzer dann im Anschluss aufzufordern ein angebliches Zertifikat oder Update für das mTAN-Verfahren auf seinem Mobilgerät zu installieren. Wer diesen Aufforderungen folgt, installiert sich ein Schadprogramm, welches den Angreifern Tür und Tor öffnet. Gehen Sie auf solche Forderungen nicht ein und wenden Sie sich im Zweifel zunächst an Ihre Bank.

Sie sollten zudem beachten: Bei einigen Banken sind die TAN-SMS nicht kostenlos.

1.3.4 TAN-Generatoren: Individuelle TAN für jeden Auftrag

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/SoFunktioniertDasOnlineBanking/Sicherheit/PIN-TAN-Schutzverfahren.html?nn=6596940&cms_pos=4

Um das PIN/TAN-Verfahren sicherer zu machen, geben immer mehr Banken sogenannte TAN-Generatoren aus. Diese Geräte generieren auf Knopfdruck die Transaktionsnummern und zeigen sie auf einem eingebauten Bildschirm an. Ein Nachteil des Verfahrens ist, dass der TAN-Generator griffbereit sein muss, um Online-Banking zu nutzen. Zudem müssen die Kunden einiger Banken den TAN-Generator selbst bezahlen. Zu beachten ist auch, dass die Banken unterschiedliche TAN-Generator-Verfahren anbieten, die zudem je nach Anbieter verschiedene Namen tragen.

1.3.4.1 eTAN-Verfahren

Der TAN-Generator beim eTAN-Verfahren verfügt über ein Display und ein Ziffernfeld. Um eine Transaktion durchführen zu können, wird Ihnen auf der Banken-Webseite zunächst eine Kontrollnummer angezeigt, die Sie in den TAN-Generator eingeben müssen. Dieser erzeugt dann – unter anderem

abhängig von der Uhrzeit und der Empfängernummer – eine TAN, die nur für diese Kontrollnummer und für kurze Zeit gültig ist. Den TAN-Generator erhalten Sie von Ihrer Bank. Je nach Institut können damit Mehrkosten für Sie verbunden sein. Außerdem bieten nicht alle Banken das eTAN-Verfahren an.
Durch die Nutzung dieses Verfahrens sind Sie besser gegen Phishing-Angriffe geschützt, weil eine generierte TAN nur für die passende Kontrollnummer gültig ist – und das auch nur für einen kurzen Zeitraum. Erhöht wird die Sicherheit dadurch, dass anstatt einer Kontrollnummer die Empfängerkontonummer in den Generator eingegeben werden muss. Man-In-The-Middle-Angriffe werden so erschwert.

1.3.4.2 sm@rtTAN-Verfahren

Beim sm@rtTAN-Verfahren erhalten Sie einen TAN-Generator ohne Ziffernfeld. Damit eine TAN erzeugt wird, müssen Sie Ihre Bankkarte in den Generator schieben. Die generierten TANs sind nicht an eine bestimmte Transaktion gebunden und auch nicht zeitlich eingeschränkt. Sie müssen sich bei Eingabe der TANs lediglich an die Reihenfolge halten, in der Sie die TANs erzeugt haben. Dadurch bietet das Verfahren keinen besonderen Schutz vor Phishing-Angriffen. Auch Man-In-The-Middle-Angriffe werden nicht erschwert, da die TAN nicht auftragsbezogen generiert wird. Das sm@rtTAN-Verfahren ist nicht sehr weit verbreitet.

1.3.4.3 sm@rtTAN plus / chipTAN manuell

Bei den Verfahren mit den Namen "sm@rtTAN plus" bzw. "chipTAN manuell" erhalten Kunden einen TAN-Generator mit Ziffernfeld und Einschubmöglichkeit für die Bank-/EC-Karte – sie sind also quasi eine Kombination aus eTAN- und sm@artTAN-Verfahren. Wenn Sie am PC oder Smartphone eine Online-Transaktion durchführen, müssen Sie die Bankkarte in den Generator schieben und eine Kontrollnummer eingeben, die das Online-Banking am Bildschirm anzeigt. Zudem müssen Sie die Transaktionsdaten teilweise oder vollständig eingeben – zum Beispiel die Kontonummer und Bankleitzahl des Empfängers sowie den zu überweisenden Betrag.
Aus diesen Informationen erzeugt der Generator nun die TAN. Diese ist nur für den speziellen Auftrag gültig – Betrüger können es nicht für Überweisungen auf andere Konten nutzen. Daher ist dieses Verfahren relativ sicher vor Angriffen durch Phishing- und Man-In-The-Middle-Attacken.

1.3.4.4 sm@rtTAN optic / chipTAN comfort

Die Eingabe der Kontrollnummer und der Transaktionsdaten ist vergleichsweise umständlich. Um das Verfahren zu vereinfachen, bieten einige Banken TAN-Generatoren an, die die nötigen Daten mithilfe von optischen Sensoren vom Computer-Bildschirm ablesen. Nach Eingabe der Transaktionsdaten erscheint auf dem Bildschirm eine Grafik mit flackernden, schwarzweißen Flächen. Kunden stecken nun ihre Bankkarte in den Generator und halten diesen vor die Grafik auf dem Monitor. Von dort aus werden die Informationen als Lichtsignale an den Generator übertragen, der in seinem Display danach die Kontonummer des Empfängers und den Überweisungsbetrag anzeigt – diese Daten müssen die Nutzer also nicht mehr manuell eingeben.

Nachdem der Kunde die Zahlen kontrolliert und bestätigt hat, errechnet der Generator eine TAN. Dieses Verfahren bietet einen guten Schutz vor Phishing- und Man-In-The-Middle-Angriffen, da Sie die Transaktionsdaten vor der Bestätigung überprüfen können. Wenn Sie beim Blick auf das Display feststellen, dass ein anderes als das gewünschte Empfängerkonto angezeigt wird, können Sie die Übermittlung abbrechen.

1.3.4.5 photoTAN

Das Verfahren photoTAN funktioniert ähnlich wie sm@rtTAN optic. Auch hier wird dem Kunden das mühsame Abtippen der Transaktionsdaten dadurch erspart, dass diese Informationen optisch vom Bildschirm eingelesen werden. Bei photoTAN flackert hierzu aber nicht der Bildschirm, sondern es wird ein farbiger Barcode angezeigt, der die Daten enthält. Der Kunde benutzt die Kamera seines Smartphones, um diesen Barcode aufzunehmen und sich die Transaktionsdaten auf seinem Smartphone anzeigen zu lassen. Wenn die Transaktionsdaten korrekt sind, gibt der Kunde die vom Smartphone ebenfalls angezeigte TAN in den PC ein und bestätigt damit die Transaktion.

Für die Nutzung mittels Smartphone muss eine kostenlose App auf dem Smartphone installiert werden. Die Stammdaten des Kunden werden bei photoTAN nicht von der Bankkarte eingelesen, sondern einmalig von einem Initialisierungsbrief, den die Bank im Zuge der Anmeldung des Kunden an ihn versendet. Als Alternative zum Smartphone können Kunden auch ein spezielles, von der Bank bereitgestelltes Lesegerät für photoTAN verwenden.

1.3.5 Signaturverfahren: Karte statt TAN

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/SoFunktioniertDasOnlineBanking/Sicherheit/PIN-TAN-Schutzverfahren.html?nn=6596940&cms_pos=5

Bei allen PIN/TAN-Verfahren besteht die größte Gefahr darin, dass Angreifer PIN und TAN (bzw. Möglichkeiten der Generierung von TAN) in ihren Besitz bringen und damit Geld vom Konto des Bankkunden entwenden. Eine Alternative ist die Absicherung des Online-Bankings mit dem Verfahren HBCI mit Chipkarte (HBCI steht für: Homebanking Computer Interface).

Dabei bestätigen die Anwender eine Transaktion nicht mit einer TAN, sondern mithilfe eines digitalen Schlüssels, der auf einer Chipkarte gespeichert ist. Selbst wenn Angreifer die Zugangspasswörter erbeutet haben, fehlt ihnen für einen Kontenzugriff die Signaturkarte.
Anwender benötigen für dieses Verfahren eine Finanzsoftware und ein Signaturkarten-Lesegerät – dafür fallen zusätzliche Kosten an. Das Lesegerät muss mit dem Rechner direkt verbunden sein.

Eine Transaktion mit Signaturverfahren läuft folgendermaßen ab: Sie geben die Daten – etwa für eine Überweisung – in einer Finanzsoftware ein. Danach stecken Sie die Signaturkarte in das Lesegerät und geben eine festgelegte PIN ein. Die Signaturkarte "unterschreibt" und verschlüsselt die Transaktion. Danach wird Ihr Auftrag an die Bank übermittelt. Diese entschlüsselt die Daten und prüft die digitale Unterschrift. Erst wenn diese bestätigt wurde, wird Ihr Auftrag ausgeführt.

Es erhöht die Sicherheit, wenn Anwender ein Kartenlesegerät kaufen, das über eine eigene Tastatur verfügt. Sonst erfolgt die Eingabe der PIN über die PC-Tastatur; Schadprogramme können dann die Eingabe aufzeichnen und für unerwünschte Überweisungen missbrauchen.
HBCI ist ein offener Standard im Bereich des Online-Bankings. Er wurde von verschiedenen deutschen Bankengruppen entwickelt. Inzwischen ist bereits ein Nachfolge-Standard mit höherer Sicherheit entwickelt worden: Bei dem HBCI-Nachfolger Secoder ist die Tastatur am Lesegerät Standard. Zudem zeigen Secoder-Karten-Lesegeräte die Transaktionsdaten zusätzlich auf einem Display an. Dies erhöht noch einmal die Sicherheit, weil Benutzer die Überweisung abbrechen können, wenn eine Schadsoftware etwa die Kontonummer des Empfängers manipuliert hat. Moderne Kartenleser gemäß Secoder-Standard können übrigens in der Regel auch den neuen Personalausweis auslesen, mit dem Sie sich online identifizieren können.

1.4 Online-Banking: Gefahren und Sicherheitsrisiken

Inhalt des Dossiers

Wer Online-Banking nutzt, spart sich zwar Zeit und Mühe, weil er viele Bankgeschäfte von zu Hause aus erledigen kann – der Anwender setzt sich aber auch Sicherheitsrisiken aus. Gerade Online-Banking ist für viele Kriminelle ein beliebtes Angriffsziel, denn es lassen sich nicht selten direkt hohe Geldbeträge erbeuten.

In diesem Kapitel erfahren Sie, welche Gefahren und Sicherheitsrisiken mit Online-Banking verbunden sind.

1.4.1 E-Mail-Phishing: Passwortdiebstahl mit manipulierten E-Mails

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/GefahrenUndSicherheitsrisiken/Gefahren_Sicherheitsrisiken.html?cms_pos=1

Beim Online-Banking weisen Kunden mit PIN beziehungsweise Passwort und TAN ihre Identität nach. Diese Daten versuchen Internet-Kriminelle daher auszuspähen und mit ihrer Hilfe an das Geld der Bankkunden zu kommen. Der Fachbegriff für dieses illegale Vorgehen heißt Phishing.

Das sogenannte E-Mail-Phishing war viele Jahre die beliebteste Methode der Internet-Kriminellen, um an Kundendaten zu gelangen. Ein Beispiel: Die Datendiebe verschicken E-Mails, die optisch wie inhaltlich offiziellen E-Mails von Bankhäusern nachempfunden sind. Darin werden die Kunden unter Angabe verschiedenster Vorwände aufgefordert, auf einen Link zu klicken, der angeblich auf die Webseite der Bank verweist. In Wahrheit führt ein Klick die Nutzer aber auf eine dem Internetauftritt der Bank nachempfundene gefälschte Webseite. Dort werden die Anwender aufgefordert, ihre Kontonummer, die PIN und einige TANs einzugeben. Mit diesen Daten können die Kriminellen dann abhängig vom verwendeten TAN-Verfahren illegal Transaktionen durchführen.

Beispiel einer gefälschten Banken-Website, die auffordert alle unbenutzten Transaktionsnummern einzugeben.

Die ersten Phishing E-Mails waren häufig leicht zu erkennen, da sie oft viele Rechtschreibfehler enthielten und ihr Erscheinungsbild von dem der Original-Nachrichten von Banken stark abwich. Da viele Internetnutzer heute weitaus skeptischer auf E-Mails reagieren, die nicht persönlich an sie adressiert

sind und unseriös wirken, gehen Kriminelle nun geschickter vor. So wird immer häufiger das sogenannte Spear-Phishing betrieben: Dabei beschaffen sich Kriminelle auf illegalen Wegen persönliche Daten und E-Mail-Adressen von einer bestimmten Nutzergruppe und schreiben diese gezielt mit auf sie zugeschnittenen Nachrichten an. Es hat sich gezeigt, dass die persönliche Ansprache bei Internetnutzern zu mangelnder Vorsicht führt.

Diese Tatsache machen sich Angreifer auch zunutze, indem sie zunehmend Instant-Messaging-Dienste und soziale Netzwerke zur Verbreitung von Phishing-Nachrichten nutzen. Dabei verschicken Sie die gefälschten Nachrichten über manipulierte Zugänge im Namen von ahnungslosen Nutzern. Da das "Opfer" dem Freund vertraut, steigt die Wahrscheinlichkeit, auf solche Nachrichten hereinzufallen und Anhänge zu öffnen oder Links zu folgen.

1.4.1.2 Phishing

Gefährliche Umleitung für Ihre Passwörter

1.4.1.2.1 Schnell zum Abschnitt

Schlimm genug, dass Spammer Ihre Mailbox zumüllen, andere auf Ihrem PC oder den mobilen Geräten herumschnüffeln wollen oder Schadprogramme einem die Lust am Internet verderben. Phishing: Das klingt nach fischen gehen – und genau so ist es auch. Das Wort setzt sich aus "Password" und "fishing" zusammen, zu Deutsch "nach Passwörtern angeln". Immer öfter fälschen Phishing-Betrüger E-Mails und Internetseiten und haben damit einen Weg gefunden, um an vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern heran zu kommen – die Nutzer geben ihre Daten einfach freiwillig preis.

Als seriöse Bank oder andere Firma getarnt fordern die Betrüger den Empfänger in der E-Mail auf, seine Daten zu aktualisieren. Entweder weil zum Beispiel die Kreditkarte ablaufe, das Passwort erneuert werden müsse, die Zugangsdaten verloren gegangen seien oder aus Sicherheitsgründen Kontoinformationen bestätigt werden müssten. Angreifer spekulieren dabei darauf, dass der Empfänger der massenweise verschickten Nachrichten auch tatsächlich Kunde der vorgegebenen Firmen ist. Der Inhalt der so genannten Phishing-Mails wirkt dabei täuschend echt. Diese E-Mails im HTML-Format zeigen dann einen "offiziellen" Link an, hinter dem sich jedoch tatsächlich ein ganz anderer Link verbirgt. Um diesen Link zu entdecken, muss man den Quelltext der HTML-Mail lesen. Das funktioniert über einen Klick mit der rechten Maus-Taste im Nachrichtenfeld und der Auswahl des Menüpunktes "Quelltext anzeigen".

1.4.1.2.2 Trügerische Links und Webseiten

Der Empfänger wird für die Dateneingabe über einen Link auf eine Internetseite geführt, die zum Beispiel der Banken-Homepage ähnlich sieht. Auf den ersten Blick scheint alles ganz normal, selbst die Eingabeformulare sehen gleich aus. Die Phishing-Betrüger nutzen darüber hinaus entweder Internetadressen, die sich nur geringfügig von denen der renommierten Firmen unterscheiden. Oder aber sie fälschen die Adressleiste des Browsers mit einem JavaScript. Man glaubt also, man sei auf einer seriösen Seite, ist es aber nicht. Wer einer solchen Seite seine EC-Geheimnummer, Passwörter oder andere Daten anvertraut, der beschert dem Angler fette Beute und kann sich selbst jede Menge Ärger einhandeln.

Formal gesehen passiert ein solcher Phishing-Angriff also in zwei Etappen, die manchmal auch einzeln auftreten:

1. Da ist zum einen die E-Mail, die ein Vertrauensverhältnis ausnutzt und entweder auf eine bösartige Internetseite lockt oder Computerschädlinge im Schlepptau hat. Diese Mails sind heute übrigens oft perfekt formuliert, während sie zu Beginn der Phishing-Angriffe zumeist in sehr schlechtem Deutsch verfasst waren. Das lag daran, dass sie oft aus dem fremdsprachigen Ausland stammten und mit automatischen Übersetzungsprogrammen oder von Laien ins Deutsche übertragen wurden.

2. Zum anderen gibt es die Nachahmung von Teilen oder einer gesamten vertrauten Webseite, auch "Spoofing" ("Verschleierung") genannt. Hier geschieht der eigentliche Betrug, indem die Angreifer einen getäuschten Nutzer zur Preisgabe vertraulicher Daten verleiten, die dann missbraucht werden.

1.4.1.2.3 Woran kann man Phishing-E-Mails erkennen?

- Die Absenderadressen sind zumeist gefälscht. Die Erkennung des gefälschten Absenders ist nur über die Header-Auswertung möglich.
- Die Anrede ist unpersönlich gehalten ("Lieber Kunde der x-Bank!")
- Dringender Handlungsbedarf wird signalisiert ("Wenn Sie nicht sofort Ihre Daten aktualisieren, gehen diese verloren…")
- Drohungen kommen zum Einsatz ("Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren…")
- Vertrauliche Daten (wie zum Beispiel PINs und TANs) werden abgefragt, etwa in einem Formular innerhalb der E-Mail.
- Die Mails enthalten Links oder Formulare, die vom Empfänger verfolgt beziehungsweise geöffnet werden sollen.
- Die Nachrichten sind manchmal (aber nicht immer!) in schlechtem Deutsch verfasst. Die Gründe dafür: Sie werden manchmal von Computerprogrammen aus anderen Sprachen automatisch übersetzt.
- Die E-Mails enthalten kyrillische Buchstaben oder falsch aufgelöste bzw. fehlende Umlaute (z. B. nur "a" statt "ä" beziehungsweise "ae").

1.4.1.2.4 Woran kann man Phishing-Webseiten erkennen?

- Oft fehlt in der Adresszeile des Browsers das Kürzel "https://", das eine gesicherte Verbindung signalisiert. Allerdings kann in manchen Fällen auch das gefälscht werden.
- In der Adresszeile erscheinen Internetadressen, die den echten ähnlich sind, aber unübliche Zusätze enthalten (zum Beispiel Zahlen: www.135x-bank.com oder www.x-bank.servicestelle.de)
- Auf der Login-Seite werden TAN-Codes abgefragt.
- Das Sicherheitszertifikat, erkennbar durch das Schlosssymbol in der Stautsleiste, fehlt oder ist gefälscht.

1.4.2 Schadsoftware: Trojanische Pferde sammeln unbemerkt Daten

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/GefahrenUndSicherheitsrisiken/Gefahren_Sicherheitsrisiken.html?cms_pos=2

Vorsicht und ein gesundes Misstrauen sind gute Mittel gegen E-Mail-Phishing-Attacken. Da Anwender sensibler für diese Bedrohung geworden sind, nutzen Kriminelle beim Erbeuten von Passwörtern zunehmend Schadprogramme. Dabei handelt es sich um sogenannte Trojanische Pferde.

Diese schleusen Angreifer auf den unterschiedlichsten Wegen auf die Rechner der Online-Banking-Anwender ein, häufig ohne dass diese die Bedrohung auf ihrem Rechner bemerken. Beim sogenannten Man-In-The-Middle-Angriff überwachen und manipulieren diese Schadprogramme als "Mann in der Mitte" den Datenverkehr zwischen dem Browser des Anwenders und dem Rechner der Bank. Wenn der Benutzer eine Überweisung durchführt, fängt das Schadprogramm die Auftragsdaten ab, verändert Betrag und Kontonummer des Empfängers und leitet die manipulierten Daten an die Bank weiter. Kriminelle überweisen sich auf diese Weise, also mithilfe des Schadprogrammes das Geld, das Sie eigentlich jemandem anderen zukommen lassen wollten. Sie merken davon zunächst nichts, weil das Trojanische Pferd die Anzeige im Browserfenster verändert und so eine ordnungsgemäß durchgeführte Transaktion vortäuscht. Erst beim nächsten Blick auf einen Kontoauszug wird der Schaden sichtbar.

Bei sogenannten "Man-In-The-Browser"-Attacken greifen die Schadprogramme nicht in den Datenverkehr zwischen Ihrem Rechner und dem Bank-Computer ein, sondern manipulieren nur die Darstellung der Online-Banking-Webseite im Browser. Wenn Sie bei einem infizierten Rechner die Adresse der Online-Banking-Webseite eingeben, wird eine normale Verbindung hergestellt. Öffnet sich die Anmelde-Webseite des Bankportals, sorgt die Schadsoftware aber dafür, dass zwar die korrekte Webseite aufgerufen, dort aber manipulierte Inhalte angezeigt werden. Unter Vorspiegelung falscher Tatsachen wird der Nutzer zum Beispiel über eine gefälschte Eingabemaske dazu gebracht, bestimmte Daten preiszugeben – zum Beispiel TANs oder die Kreditkartendaten. Gleichzeitig deutet aber die korrekte Adresse in der Adressleiste des Browsers darauf hin, dass alles seine Richtigkeit hat. Mit derartigen Manipulationen ist es Angreifern schon gelungen, die als relativ sicher geltenden chipTAN-Verfahren auszuhebeln.

1.4.3 Mobile Banking: Unterwegs lauern Gefahren

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/GefahrenUndSicherheitsrisiken/Gefahren_Sicherheitsrisiken.html;jsessionid=CF526D6622EC75AA4F078AEB9BFDCD4D.1_cid351?nn=6596934&cms_pos=3

Der entscheidende Vorteil des Online-Bankings ist, dass Sie nicht länger eine Filiale Ihrer Bank aufsuchen müssen, um ihre Bankgeschäfte zu erledigen. Im Prinzip können Sie Ihren Kontostand mithilfe jedes internetfähigen Computers weltweit einsehen. Aus dieser Freiheit resultieren aber Gefahren.

Es ist beispielsweise riskant, fremde Rechner fürs Online-Banking zu nutzen. Denn Browser speichern Daten der letzten Verbindungen in einem Zwischenspeicher ab – dem sogenannten Cache. Wer Bankgeschäfte etwa im Internetcafé abwickelt, riskiert, dass Kriminelle später diese Informationen im Cache auslesen. Können Sie nicht vermeiden, fremde Rechner zu nutzen, sollten Sie den Cache des Browsers in jedem Fall im Anschluss an Ihre Sitzung löschen. Wenn sie häufiger von unterwegs Online Banking nutzen möchten, sollten Sie in Erwägung ziehen, sicherere Systeme zu nutzen: Es gibt Online Banking Plattformen, die über USB-Sticks oder CD-Roms gebootet werden. Nähere Informationen und eine Anleitung bietet zum Beispiel die Fachzeitschrift c't.

Ein weiteres Risiko unterwegs ist der Internetzugang über öffentliche WLANs (Wireless Local Area Network). Mithilfe eines solchen drahtlosen Netzwerkes können Sie mit Ihrem Computer ohne störende Kabelverbindungen auf das World Wide Web und somit auch auf das Online-Banking-Angebot Ihrer Bank zugreifen. Die Funkverbindung ist allerdings nur dann sicher, wenn der Datenverkehr ausreichend verschlüsselt ist, was bei einem öffentlichen WLAN schwer zu überprüfen ist (siehe auch Artikel WLAN).

1.4.3.1 Gefahr für Smartphone-Anwender

Die Gefahren beim Online-Banking beschränken sich nicht nur auf PCs. Inzwischen nehmen die Angreifer auch Handys, Smartphones und Tablet-Computer ins Visier – auch weil viele Nutzer den Schutzbedarf mobiler Geräte noch unterschätzen. Obwohl heute fast jeder Vierte ein Smartphone oder Handy mit Internetzugang besitzt (24 Prozent), ist über einem Drittel der Nutzer (36 Prozent) nicht bekannt, dass ein Smartphone dieselben Sicherheitsvorkehrungen und Schutzmaßnahmen wie ein PC benötigt. Diese Schutzlücke nutzen Angreifer aus, um beispielsweise per SMS einen Link zu einem angeblichen Sicherheitszertifikat für das Smartphone des Anwenders zu versenden. Tatsächlich verbirgt sich hinter dem Link jedoch eine Schadsoftware, die mTANs ausspäht und es den Angreifern ermöglicht, Überweisungen zu manipulieren.

Grundsätzlich bestehen alle Gefahren, die Sie vom Online-Banking mit dem Heim-Computer kennen, auch beim Mobile Banking. So ist es beispielsweise auch bei Smartphones nötig, regelmäßig Updates einzuspielen, um eventuelle Sicherheitslücken zu schließen. Hinzu kommen aber die spezifischen Sicherheitsrisiken mobiler Geräte. So können beim Diebstahl des Gerätes die darauf gespeicherten Informationen in den Besitz von Kriminellen gelangen; darum sollten Sie dort niemals PIN oder TANs abspeichern. Unbemerkten Zugriff auf Ihr Mobiltelefon verhindern Sie unter anderem dadurch, dass Sie die Tastensperre mit Passwortschutz aktivieren. Weitere wichtige Hinweise zum Schutz beim mobilen Surfen können Sie hier nachlesen. Um Kunden das mobile Banking mithilfe von Smartphones zu erleichtern, können Anwender inzwischen sogenannte Mobile-Banking-Apps über die App-Stores auf ihren Mobiltelefonen installieren. Bei diesen Apps handelt es sich um Programme, die den Zugriff auf die Funktionen des Online-Bankings ohne Browser erlauben. Dies soll nicht nur den Komfort, sondern auch die Sicherheit des Mobile-Bankings erhöhen. Allerdings hat sich in der Vergangenheit gezeigt, dass auch diese Programme nicht frei von Sicherheitslücken sind.

Mehr Informationen zu Mobile Banking finden Sie auch hier.

1.4.3.2 Online-Banking mit mobilen Internet-Geräten

Wer mit einem mobilen Gerät Online-Banking betreiben will (etwa per Smartphone oder Tablet), kann dafür auch einen Browser nutzen – es besteht grundsätzlich kein Unterschied zum Online-Banking mit einem stationären PC. Bequemer ist Online-Banking jedoch mit einer passenden Anwendung/App, die auf dem Smartphone installiert werden kann. Viele Banken bieten inzwischen Online-Banking-Apps für Ihre Kunden kostenlos an. Welche Sicherheitsmaßnahmen beim Mobile Banking zu beachten sind, erfahren Sie im Kapitel "Mobile Banking". Außerdem sollten Sie den Empfehlungen im Kapitel "Apps auf mobilen Geräten" folgen.

1.4.3.2.1 Mobile Banking

Mit mobilen, internetfähigen Geräten können Sie auch Ihre Bankgeschäfte unterwegs erledigen. Doch aufgepasst: Alle Gefahren, die Sie vom Online-Banking mit dem Computer kennen, bestehen auch beim Mobile Banking. Hinzu kommen die speziellen Sicherheitsrisiken mobiler Geräte. Mit welchen Maßnahmen Sie sich vor den Gefahren schützen können, erfahren Sie hier

1.4.3.2.2 Gefahren: Phishing

Die größte Gefahr beim Mobile Banking besteht, wie beim Online-Banking vom heimischen PC, im Ausspionieren der Zugangsdaten, dem sogenannten Phishing. War ein Betrüger mit einem Phishing-Angriff erfolgreich, hat er Zugriff auf das Konto und kann es für Finanztransaktionen missbrauchen. Phishing-Angriffe können zum Beispiel über E-Mails, Trojanische Pferde oder Spyware ausgeführt werden.

1.4.3.2.3 So können Sie sich schützen

- Gehen Sie sorgfältig mit den Zugangsdaten für Ihr Konto wie Benutzername und Passwort bzw. PIN und TANs um. In jedem Fall sollten Sie moderne TAN-Verfahren wie ChipTAN nutzen.
- Klicken Sie niemals auf Links in E-Mails, Facebook-Nachrichten etc., in denen Sie dazu aufgefordert werden, Ihre Kontodaten abzugleichen. Auch wenn die Nachricht täuschend echt aussieht, solche E-Mails sind Phishing-Versuche. Ihre Bank fordert Sie niemals per E-Mail dazu auf, vertrauliche Daten wie PIN oder TAN bekannt zu geben. Geben Sie die Internetadresse Ihrer Bank bei jedem Aufruf erneut über das Tastenfeld oder den Touchscreen ein beziehungsweise wählen Sie die Adresse über Ihre Favoriten oder Bookmarks an.
- Seien Sie vorsichtig beim Öffnen von MMS. Über MMS können Programme versendet werden, die Schadcode enthalten. So kann sich zum Beispiel ein Trojaner auf Ihrem Handy einnisten und Ihre Daten ausspionieren. Löschen Sie MMS von unbekannten Absendern am besten sofort.
- Setzen Sie – so weit aus vertrauenswürdiger Quelle für Ihr Betriebssystem verfügbar – eine aktuelle Virenschutzsoftware ein und halten Sie diese auf dem aktuellen Stand. So können Sie Sypware und Trojanische Pferde, die Bankdaten ausspähen könnten, von Ihrem Mobilfunkgerät fernhalten. Informieren Sie sich bei Ihrem Geräte- und Betriebssystemhersteller, welche Schutzprogramme für Ihr Gerät verfügbar sind. Eine Übersicht, der zurzeit verfügbaren Virenschutzprogramme für Smartphones ist auch auf der Website des Heise-Verlages zu finden. Bei Verwendung eines iPhones oder iPads ist das Installieren von Virenschutzprogrammen nicht möglich. Dies ist derzeit allerdings auch nicht erforderlich, da für diese Geräte bislang keine Schadprogramme existieren und die technischen Schutzmaßnahmen des Betriebssystems ausreichen.
- Überprüfen Sie regelmäßig Ihre Kontobewegungen und informieren Sie Ihre Bank, wenn Ihnen etwas unschlüssig erscheint. Außerdem sollten Sie mit Ihrer Bank ein Limit für tägliche Geldbewegungen beim Online-Banking vereinbaren.
- Verwenden Sie für das Online-Banking nach Möglichkeit eine von Ihrem Geldinstitut bereitgestellte und autorisierte App.
- Beachten Sie die Geschäftsbedingungen und Haftungsregelungen Ihres Geldinstitutes bei der Verwendung eines Smartphones für das Online-Banking.

Weitere Informationen über alle notwendigen Schutzmaßnahmen können Sie in unseren Schwerpunkt-Themen Online-Banking und Phishing nachlesen.

1.5 Online-Banking - Was tun im Ernstfall?

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/WasTunImErnstfall/ernstfall_node.html

Woran erkennen Sie, dass Sie Opfer eines Phishing-Angriffs geworden sind? Es gibt eine Reihe von Anzeichen, bei deren Auftreten Sie misstrauisch werden sollten:

- Nach der Eingabe von Anmeldename oder Legitimations-ID und -PIN zur Anmeldung werden Sie zum Beispiel auf einer manipulierten Folgeseite zur Eingabe von mehreren unbenutzten TANs und den dazugehörigen laufenden Nummern aufgefordert. Achten Sie bitte grundsätzlich bei der TAN-Eingabe darauf, dass diese in Verbindung zu Ihrem Auftrag (zum Beispiel einer Überweisung) steht.
- Während des Online-Banking-Vorgangs öffnet sich ein neues Browser-Fenster. Sie werden aufgefordert, Ihre Bankleitzahl, PIN und/oder eine oder mehrere TANs einzugeben.

- Sie werden während oder nach Abschluss einer Transaktion aufgefordert, eine oder mehrere TANs einzugeben. Oft erscheint die Meldung, dass die vorher eingegebene TAN bereits verbraucht oder falsch sei.
- Ihre gesicherte Verbindung zum Online-Banking wird nach Eingabe von PIN und TAN unterbrochen.
- Ihr Internet-Browser wird ohne ersichtlichen Grund geschlossen. Eventuell wird eine entsprechende Fehlermeldung angezeigt.
- Nach dem Abschluss einer Transaktion durch Eingabe einer TAN zeigt Ihr Internet-Browser die Fehlermeldung an, dass das Online-Banking nicht mehr erreichbar ist. Die Meldung wird Ihnen wiederholt angezeigt, wenn Sie zu einem späteren Zeitpunkt das Online-Banking starten möchten.

Wenn eine der oben genannten Auffälligkeiten auftritt oder Sie aus einem anderen Grund den Eindruck oder den Verdacht haben, dass etwas nicht stimmt, sollten Sie sofort aktiv werden:

1. Sperren Sie unverzüglich Ihr Bankkonto und Ihren Zugang zum Online-Banking. Am schnellsten geht das, indem Sie zum Beispiel die Anmeldemaske zum Online-Banking aufrufen und dreimal hintereinander die falsche PIN eingeben. Oder rufen Sie den zentralen Sperr-Notruf 116 116 (aus dem Ausland +49 116 116) an und lassen Sie Ihren Zugang telefonisch sperren.
2. Danach wenden Sie sich sofort an Ihre Bank und melden die Auffälligkeiten. Gegebenenfalls besteht die Möglichkeit, Kontobewegungen rückgängig zu machen.
3. Prüfen Sie umgehend die Kontoumsätze anhand des Papierauszuges.
4. Sollten Sie Opfer eines Phishing-Angriffs mittels eines Trojaners geworden sein, müssen Sie Ihren PC fachgerecht von der Schadsoftware befreien.