



Ihr PC-Sicherheits-Berater

So schützen Sie Ihre Privatsphäre und sensiblen Daten

2 Installieren Sie diesen sicheren Browser

Setzen Sie einen speziellen Browser nur für Online-Banking ein: Chip BankingBrowser 2019 – Ihr bester Schutz!

4 Vorsicht: Feind liest Ihre Eingaben mit

Fiese Betrüger fangen Ihre Eingaben über die PC-Tastatur ab. Verwenden Sie ab sofort die sicherere Bildschirmtastatur.

6 Vertrauen Sie der App-Empfehlung nicht

Lassen Sie sich von Ihrer Bank nicht zu einer Smartphone-Lösung überreden. Setzen Sie ein sichereres Verfahren ein.

8 Checkliste: Ist Ihr Banking jetzt sicher?

Mein Sicherheits-Check zeigt, ob Sie an alle Schutzschilder gedacht haben und beim Online-Banking sicher sind.

Stoppen Sie die aktuelle Online-Banking-Gefahr: 7 Schutzschilder schützen Ihr Bankkonto vor Online-Bankräubern

Das Ende der TAN-Listen naht – und das ist gut so!

Verwenden Sie für Ihr Online-Banking eine gedruckte Liste mit nummerierten sechsstelligen Zahlen, kommt 2019 eine große Umstellung auf Sie zu.

Ihre iTANs (indizierte Transaktionsnummern, die sechsstelligen Zahlen) dürfen Sie nur noch bis zum 14. September 2019 verwenden. So will es die Europäische Union aus Sicherheitsgründen. Die Gefahr ist zu groß, dass Kriminelle über Betrugs-Mails, gefälschte Bankseiten und Banking-Trojaner in den unbefugten Besitz von iTANs gelangen und Ihr Konto leer räumen.

Doch was die meisten Banken Ihnen empfehlen ist noch gefährlicher als iTAN: Sie sollen ein oder zwei Apps (Programme) auf einem Smartphone (Mobiltelefon) installieren. Das jedoch kann gefährlich sein: Ein Banking-Trojaner und Ihr Geld ist weg!

Meine Empfehlung: Die Banken verschweigen oft, dass Sie Ihren PC weiter nutzen und sichere TAN-Generatoren statt eines Smartphones verwenden können. Lesen Sie in diesem Leitfaden, wie Sie Ihre Online-Bankgeschäfte sicher erledigen.



Viele Grüße, Ihr

Michael-Alexander
Beisecker,
Deutschlands

PC-Sicherheitsexperte Nr. 1

7 Schutzschilder, damit Sie kein Geld verlieren

Online-Banking 2019: So erreichen Sie das höchste Sicherheitsniveau

57.809,30 € verlor Ehepaar A. aus Westerhausen im Oktober 2018 durch einen **einzigsten Banking-Trojaner**. Sie hatten sich auf die Empfehlung Ihrer Bank verlassen und tätigten Ihre Geldgeschäfte per Online-Banking mit dem Smartphone. **Damit Ihnen so etwas nicht passiert, habe ich einen sicheren Online-Banking-Schutz auf PC-Basis für Sie entwickelt, den Sie mit den Anleitungen auf den nächsten Seiten einrichten.**

Das Wichtigste zuerst: Nutzen Sie zum Online-Banking niemals ein Smartphone mit Android-Betriebssystem, denn immer wieder werden im Google Play Store getarnte Bank-Trojaner entdeckt. Sie installieren beispielsweise ein vermeintlich harmloses Horoskop-Programm und schon ist Ihr Geld weg.

Doch auch bei Ihrem PC bleiben Sie nicht vor Angriffen durch Banking-Trojaner wie dem neuen DanaBot verschont. Die Gefahr geht dabei hauptsächlich von E-Mail-Anhängen aus. Sie öffnen zum Beispiel ein infiziertes Word-Dokument und geben damit Kriminellen freien Zugriff auf Ihren PC.

Meine 7 Schutzschilder berücksichtigen diese Bedrohungen und alle weiteren bisher bekannten Tricks der Betrüger. Halten Sie alle meine Empfehlungen ein, werden Sie nicht einen Cent an einen Online-Bankräuber verlieren.

Ihr Maßnahmen-Katalog für sicheres Online-Banking

Schutzschild 1: Sichern Sie Ihren PC ab und schließen Sie alle Schwachstellen (siehe Seite 2).

Schutzschild 2: Verwenden Sie einen sicheren Online-Banking-Browser (siehe Seite 2).

Schutzschild 3: Verhindern Sie das Auslesen Ihrer Anmeldedaten und PINs durch Tastaturspione (siehe Seite 4).

Schutzschild 4: So erkennen Sie einen Trojaner, bevor er zuschlägt (siehe Seite 4).

Schutzschild 5: Verwenden Sie kein Mobiltelefon für das Online-Banking (siehe Seite 5).

Schutzschild 6: Verwenden Sie ein Online-Banking-Verfahren mit sehr hoher Sicherheit (siehe Seite 6).

Schutzschild 7: So verhalten Sie sich richtig beim Online-Banking (siehe Seite 8).

Zu jedem Angriff ein Schutzschild: Diese 7 Schutzschilder bewahren Sie vor Banking-Trojanern.

>>> Lesen Sie bitte weiter auf Seite 2

Schutzschild 1: Sichern Sie Ihren PC ab und schließen Sie alle Schwachstellen

Online-Banking ist nur so sicher wie Ihr PC. Lassen Sie Sicherheitslücken in Ihrem Windows und Ihren Anwendungen zu, öffnen Sie damit Ihr System für Hacker und Banking-Trojaner. Mit meiner 3-Punkte-Sicherheits-Checkliste überprüfen Sie Ihr Windows-System auf Schwachstellen und beseitigen erkannte Sicherheitsrisiken.

1. Haben Sie auf Ihrem PC und jedem PC im Netzwerk Windows 10 oder 7 installiert?

☐ Ja

☐ **Nein:** Verwenden Sie keinen PC mit einem veralteten Windows für Online-Banking, da Microsoft keine Sicherheits-Updates mehr dafür liefert. Die höchste Sicherheit haben Sie mit Windows 10. Verbinden Sie auch keinen PC mit veraltetem Windows mehr mit Ihrem Netzwerk oder dem Internet.

2. Sind auf Ihrem PC ausschließlich aktuelle Programme mit allen Sicherheits-Updates installiert?

☐ Ja

☐ **Nein/Nicht bekannt:** Überprüfen Sie bei allen installierten Programmen, ob die Version aktuell ist. Deinstallieren Sie veraltete Programme über die **Einstellungen** und **Apps** (Windows 10) bzw. die **Systemsteuerung** und **Programme und Funktionen** (Windows 7) oder führen Sie ein Update auf eine aktuelle Version durch.

3. Überprüfen Sie, ob alle Ihre Treiber auf dem aktuellen Stand sind?

☐ Ja

☐ **Nein/Nicht bekannt:** Rufen Sie die Support-Seite Ihres PC-Herstellers auf (zum Beispiel Medion) und sehen Sie nach, ob für das installierte Windows neue Treiber für Ihren PC angeboten werden. Haben Sie oder Ihr Händler den PC selbst aus einzelnen Komponenten zusammengestellt, dann schauen Sie auf den Support-Seiten der Hersteller dieser Komponenten nach.

Fazit: Haben Sie alle Fragen mit **Ja** beantwortet, ist Ihr PC-System auf dem aktuellen Sicherheitsstand. Bei Ihnen ist die Grundvoraussetzung für sicheres Online-Banking erfüllt. Wurde von Ihnen eine Frage mit **Nein** beantwortet, führen Sie zunächst meine angegebenen Anleitungen aus, bevor Sie im nächsten Schritt Schutzschild 2 einrichten.

Schutzschild 2: Verwenden Sie einen sicheren Online-Banking-Browser

Online-Banking über die Internetseite Ihrer Bank ist einfach und bequem – aber auch gefährlich. Banking-Trojaner wie EMOTET greifen Ihren Browser an und nutzen Sicherheitslücken in Erweiterungen oder im Browser selbst. Die Internetseite Ihrer Bank kann über Skripte (Programme) von anderen geöffneten Internetseiten manipuliert werden. Der beste Schutz vor solchen Angriffen ist ein spezieller sicherer Browser, den Sie nur für Online-Banking und Online-Shopping verwenden.

Ich empfehle Ihnen als sicheren Browser den CHIP BankingBrowser 2019, denn er ist einzeln ohne Antiviren-Programm verfügbar und wird kostenlos angeboten.

Maßnahme 1: Installieren Sie den CHIP Banking Browser 2019 und registrieren Sie sich

1. Laden Sie den **CHIP BankingBrowser 2019** über den Link https://www.chip.de/downloads/CHIP-Banking-Browser-2019_29733912.html herunter. Sie gelangen darüber auf die Anbieterseite. Klicken Sie dort zum Herunterladen auf **Manuelle Installation**.

2. Wird Ihnen das Programm nicht angezeigt, öffnen Sie mit **(Strg)+[J]** die Download-Liste Ihres Browsers und starten das Programm **ChipBankingBrowser2019.exe**.

3. Bestätigen Sie das Ausführen des Programms mit **Ja** und folgen Sie dem Assistenten mit **Weiter** sowie **Installieren**. Zum Abschluss klicken Sie auf **Fertigstellen**.

4. Installieren Sie den CHIP BankingBrowser 2019 zum ersten Mal, erscheint vor dem Browser-Start ein Registrierungsformular. Füllen Sie zum Freischalten des CHIP Banking-Browsers 2019 die Felder **Vorname** **a**, **Nachname** **b** und **E-Mail-Adresse** **c** aus. Danach klicken Sie auf die Schaltfläche **Kostenlose Freischaltung per E-Mail anfordern** **d**.

Der **CHIP BankingBrowser 2019** fragt bei der ersten Installation nach einer Registrierung.

5. Suchen Sie in Ihrem E-Mail-Postfach nach der Freischaltungs-Mail und klicken Sie auf den Link darin. Der Absender ist die Firma Abelssoft, die den Browser entwickelt hat. Finden Sie die E-Mail nicht, ist diese möglicherweise in Ihrem Spam-Ordner gelandet. Schauen Sie einfach dort nach. Erhalten Sie keine E-Mail, haben Sie sich womöglich bei der Eingabe der E-Mail-Adresse vertippt. Sobald Sie den Link angeklickt haben und die Freischaltung erfolgt ist, startet der CHIP BankingBrowser 2019.

Maßnahme 2: Wählen Sie Ihre Bankseite für die Startseite aus

1. Starten Sie den CHIP BankingBrowser 2019 und klicken Sie auf **Sicheres Surfen aktivieren**. Es erscheint die Willkommensseite mit einer Übersicht der gespeicherten Bankseiten.
2. Klicken Sie hinter der Seite Ihrer Bank auf **Hinzufügen**. Finden Sie Ihre Bank oder die örtliche Filiale nicht, suchen Sie die betreffende Bankseite mit dem folgenden Schritt.
3. Geben Sie im Feld **Hier suchen** den Namen der Bankfiliale ein, wie zum Beispiel **Stadtsparkasse Oberhausen**. Dann klicken Sie auf **Suchen**. Die Bankseite wird mit der Suchmaschine Google gesucht. Klicken Sie im Suchergebnis auf den Eintrag für die Internetseite Ihrer Bank und bestätigen Sie, dass die betreffende Seite sicher ist.

Maßnahme 3: Überprüfen Sie die Einstellungen



1. Klicken Sie oben rechts auf das **Menü-Symbol** ≡ des CHIP BankingBrowsers 2019 und wählen Sie **Einstellungen**.
2. Setzen Sie einen Haken bei der Option **Bei Programmstart auf Updates prüfen**, falls diese noch nicht aktiviert ist. Ihr Banking-Browser muss wie Ihre anderen Browser auch regelmäßig aktualisiert werden, um sicher zu bleiben.
3. Setzen Sie einen Haken bei der Option **Breche das Laden einer Seite nach zu langer Wartezeit ab**. Das spart bei einer fehlerhaften Internetseite Zeit.
4. Setzen Sie einen Haken bei der Option **Blockiere Popups**, damit Werbeeinblendungen unterdrückt werden.
5. Die Option **Unsichere Zertifikate zulassen** sollten Sie dagegen aus Sicherheitsgründen niemals aktivieren, sonst besteht die Gefahr, dass gefälschte Bankseiten geladen werden.

6. Setzen Sie einen Haken bei der Option **Immer nachfragen, wo Downloads gespeichert werden sollen**. Diese Abfragen sind zwar lästig, machen Sie dafür aber auf jeden Download aufmerksam. Lassen Sie keinen Download zu, den Sie nicht selbst angefordert haben.




Mein Tipp: Sollte beim CHIP BankingBrowser 2019 einmal ein Fehler auftreten, den Sie nicht beheben können, rufen Sie die **Einstellungen** auf und klicken Sie auf **Systeminformationen auf dem Desktop speichern**. Hängen Sie diese Datei an Ihre Support-Anfrage im Computerwissen Club an, dann können meine Redaktionskollegen und ich meist daraus direkt die Fehlerursache ablesen und Ihnen schneller helfen: <https://club.computerwissen.de>.

Maßnahme 4: Führen Sie Ihre erste Überweisung mit dem sicheren CHIP BankingBrowser 2019 durch

1. Starten Sie den CHIP BankingBrowser 2019 über das Symbol  auf dem Desktop oder über das **Start**-Menü.
2. Wechseln Sie zum Register **Startseite**. Dort werden die von Ihnen hinzugefügten Bankseiten angezeigt. Weitere Seiten lassen sich über die Pfeile links und rechts  auswählen.



Die Startseite des CHIP-Browsers zeigt die von Ihnen genutzten Bankseiten; sehen Sie sie nicht, fügen Sie sie mit der Anleitung von Maßnahme 2 hinzu.

3. Klicken Sie auf das Bild der gewünschten Bankseite und die Seite wird aufgerufen.
4. Melden Sie sich auf der Bankseite über die Bildschirmtastatur an. Die Tastatur rufen Sie über das Symbol  auf. Verwenden Sie diese Bildschirmtastatur auch zur Eingabe der Transaktionsnummern (TAN), mit denen Sie Ihre Überweisungen bestätigen.

Meine Empfehlung: Schließen Sie vor dem Aufruf des CHIP BankingBrowsers 2019 alle anderen Browser. Sie verhindern dadurch, dass einer dieser Browser für Angriffe auf Ihr Online-Banking oder Online-Shopping missbraucht werden kann. Schließen Sie den CHIP BankingBrowser 2019 nach dem Online-Banking, damit sichergestellt ist, dass die verwendeten Seiten oder deren Token (Zugangskennungen) nicht mehr von Unbefugten oder von Schadprogrammen missbraucht werden können.

LESERSERVICE

Redaktionshilfe: Fragen Sie bei Sicherheitsbedenken immer zuerst Ihren persönlichen PC-Sicherheits-Berater Michael-Alexander Beisecker.

Melden Sie sich dazu einfach kostenlos unter <https://club.computerwissen.de> an und stellen Sie ihm dort Ihre Fragen.

Michael-Alexander Beisecker und seine Redaktionsmitarbeiter helfen Ihnen gern weiter. Sie erhalten werktags innerhalb von 48 Stunden eine Antwort auf Ihre Frage – garantiert.

Schutzschild 3: Verhindern Sie das Auslesen Ihrer Anmeldedaten und PINs durch Tastaturspione

Schützen Sie sich davor, dass Ihre Zugangsdaten zu Ihrer Bankseite sowie Ihre PINs durch Keylogger (Tastaturspione) ausspioniert werden. Diese Art von Schadprogramm kann alle Ihre Tastatureingaben mitlesen. Dagegen bleiben Eingaben über Bildschirmtastaturen vor den Keyloggern verborgen. Stellen Sie sich das so vor, als würden Sie bei der Eingabe einen Tarnmantel tragen: Ihre Eingaben sind für die Angreifer unsichtbar.

Finden Sie über die nachfolgende Checkliste heraus, ob Ihnen bereits eine Bildschirmtastatur oder eine andere sichere Eingabemethode zur Verfügung steht. In diesem Fall müssen Sie nichts weiter tun, als die sichere Eingabe über die Bildschirmtastatur oder ein entsprechend sicheres Verfahren konsequent zu nutzen.

1. Bietet Ihnen die Bankseite bei der TAN-Eingabe eine Bildschirmtastatur an?

- ☐ **Ja:** Verwenden Sie diese Bildschirmtastatur für Ihre TAN-Eingaben.
- ☐ **Nein:** Verwenden Sie zur Eingabe von TANs **a** die Bildschirmtastatur des CHIP BankingBrowsers 2019 (siehe Seite 3) oder die Bildschirmtastatur von Windows 10, die Sie über **Windows + R**, die Eingabe von **osk.exe** und das Drücken der Eingabetaste **Enter** aufrufen.

Geben Sie die TAN für Ihre Überweisung niemals direkt über die Tastatur in das Eingabefeld ein, sondern immer per Mausklick über die Bildschirmtastatur.



2. Haben Sie ein Antiviren- oder Sicherheitsprogramm mit integrierter Bildschirmtastatur installiert?

- ☐ **Ja:** Verwenden Sie die Bildschirmtastatur dieses Sicherheitsprogramms zum Anmelden bei Ihrer Bankseite und zur Eingabe von TANs, sofern die Bankseite dafür keine spezielle Bildschirmtastatur zur Verfügung stellt.
- ☐ **Nein:** Verwenden Sie die Bildschirmtastatur des CHIP BankingBrowsers 2019 (siehe Seite 3), die Bildschirmtastatur Ihres Windows oder eine nachträglich installierte Bildschirmtastatur zur Eingabe der Anmelde-

daten. TANs geben Sie, sofern möglich, über die spezielle Bildschirmtastatur der Bankseite ein.

3. Verwenden Sie zur Eingabe der PIN beim HBCI-Banking mit Kartenlesegerät immer die Tastatur auf dem Kartenlesegerät?

- ☐ **Ja**
- ☐ **Nein:** Verwenden Sie zur Eingabe der Karten-PIN immer die Tastatur des Lesegeräts **b**. Informieren Sie sich bei Ihrer Bank, ob Ihr Lesegerät (Secoder) noch auf dem aktuellen Stand ist. Tauschen Sie es ansonsten um. Bei Secodern kann die PIN-Eingabe nur über die Tastatur des Geräts erfolgen. Durch diese Geräte sind Sie deshalb besser abgesichert gegen Banking-Trojaner-Angriffe.

Die Sicherheit eines solchen Kartenlesers ist nur dann gewährleistet, wenn Sie für Eingaben ausschließlich die integrierte Tastatur verwenden.



Meine Empfehlung: Stellen Sie über die Checkliste fest, dass Ihnen eine Bildschirmtastatur fehlt, installieren Sie den CHIP BankingBrowser 2019. Haben Sie auf Ihrem PC Windows 10 installiert, steht Ihnen außerdem eine Bildschirmtastatur über die Taskleiste zur Verfügung. Wird sie Ihnen auf Ihrer Taskleiste nicht angezeigt, klicken Sie mit der rechten Maustaste auf die Taskleiste und im sich öffnenden Kontextmenü auf **Bildschirmtastatur anzeigen**.

Schutzschild 4: So erkennen Sie einen Trojaner, bevor er zuschlägt

Sie haben als Schutzschild 2 einen kostenlosen Banking-Browser installiert und verwenden für das Eingeben Ihrer TANs eine Bildschirmtastatur (Schutzschild 3). Das reicht bei Ihrem PC als Schutz vor Angriffen über gefährliche Internetseiten aus. Gelangt jedoch ein Banking-Trojaner trotz all Ihrer Sicherheitsvorkehrungen auf Ihren PC oder Ihr Smartphone, kann dieser womöglich trotzdem unbemerkt Ihre Überweisungen manipulieren. Ich empfehle

Ihnen daher ein Antiviren-Programm mit Banking-Trojaner-Schutz. Dieses Antiviren-Programm sollten Sie unbedingt auch auf Ihrem Smartphone installieren, wenn Sie das Smartphone mit dem PC verbinden oder es zum Online-Banking oder Online-Shopping verwenden.

Empfehlung 1: Bitdefender Antiviren-Programm

Die Antiviren-Programme von Bitdefender, einem europäischen Sicherheitsunternehmen, sind regelmäßig Testsieger bei Antiviren-Programm-Tests. Verwenden Sie ein solches Antiviren-Programm, brauchen Sie den CHIP Banking-Browser 2019 nicht. Es ist mit SafePay ein spezieller Banking-Browser enthalten. Benötigen Sie ein Antiviren-Programm für Ihr Android-Smartphone oder iPhone mit iOS-Betriebssystem, empfehle ich Ihnen Bitdefender Total Security Multi-Device 2019, ansonsten Bitdefender Internet Security 2019.

Empfehlung 2: G DATA mit BankGuard

Einen anderen Ansatz geht das deutsche Sicherheitsunternehmen G DATA mit der Browser-Erweiterung BankGuard. Diese Erweiterung schützt vor Mann-in-der-Mitte-Angriffen durch Banking-Trojaner wie ReTeFe, SpyEye und Zeus. Dabei wird auf dem vorhandenen Browser aufgesetzt. Es gibt keinen speziellen sicheren Browser wie bei Bitdefender oder

Kaspersky. Alle Programme beinhalten den BankGuard-Schutz.

Empfehlung 3: Sicherer Zahlungsverkehr von Kaspersky

Meine dritte Empfehlung ist das Antiviren-Programm Internet Security 2019 von Kaspersky mit dem Schutz „Sicherer Zahlungsverkehr“. Er soll Mann-in-der-Mitte-Angriffe und das Abfangen Ihrer Eingaben durch Tastaturspione verhindern.

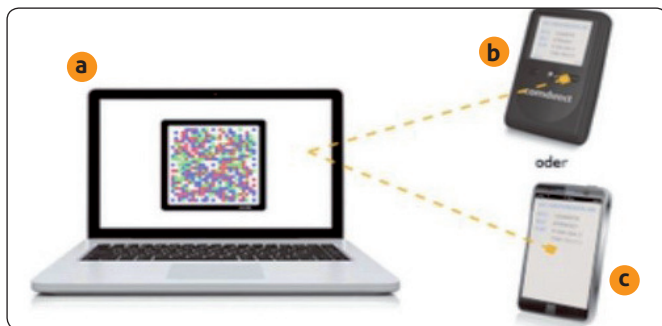
Meine Empfehlung: Für welches dieser Programme Sie sich auch entscheiden, Sie treffen immer eine gute Wahl. Die Vergleichsübersichten der Programme finden Sie auf unserer sicheren Service-Webseite www.pc-sicherheitsberater.de. Zusätzlich sollten Sie jedoch immer ein sehr sicheres Online-Banking-Verfahren verwenden (siehe Schutzschild 6, Seite 6).

Schutzschild 5: Verwenden Sie kein Mobiltelefon für das Online-Banking

Verwenden Sie aktuell eines der Online-Banking-Verfahren chipTAN, eTAN, mTAN, photoTAN, QR-TAN, sm@rt-TAN oder SmartTAN optic mit einem Mobiltelefon oder Smartphone, riskieren Sie hohe Geldverluste. Infiziert ein Banking-Trojaner Ihr Smartphone, kann das Schadprogramm wie beim PC Ihre Tastatureingaben erkennen und die Bankseite oder auch das Banking-Programm manipulieren. Sie merken es erst, wenn Sie den nächsten Kontoauszug erhalten und sich über den niedrigen Kontostand erschrecken. Die Lösung ist ganz einfach: Verlagern Sie das Online-Banking auf den PC, wo es sicher ist, oder ersetzen Sie das Smartphone je nach Verfahren durch einen TAN-Generator oder ein Karten-Lesegerät.

Ersetzen Sie das Smartphone durch einen Decoder oder Generator

Für Ihre Sicherheit ist unabhängig von Ihrem Online-Banking-Verfahren nur eines wichtig: Verwenden Sie auf keinen Fall Ihr Mobiltelefon für den Empfang der TANs per SMS



Bei dem heute oft von Banken empfohlenen photo-TAN-Verfahren erscheint auf dem PC-Bildschirm eine bunte Grafik (a), die durch einen Generator (b) (sicher) oder ein Smartphone (c) (nicht zu empfehlen) in eine TAN für Ihre Überweisung umgewandelt wird.

oder zum Anzeigen von TANs, die über einen Code auf der Bankseite erzeugt werden. Kriminelle könnten die SMS abfangen oder Banking-Trojaner das Generieren der TANs manipulieren.

Ihre sichere Lösung: Bestellen Sie bei Ihrer Bank als Ersatz für Ihr Mobiltelefon oder Smartphone (c) ein Lesegerät bzw. den zu Ihrem Verfahren passenden Generator (b). Da die Generatoren kein WLAN benötigen und nicht mit dem Internet verbunden sind, sind sie im Vergleich zu Smartphones auch nicht angreifbar. Diese Generatoren sind für das Online-Banking zertifiziert und daher wesentlich sicherer als ein Mobiltelefon. Die Kosten betragen rund 10 bis 15 €; das ist wenig für die dadurch gewonnene Sicherheit.

Meine Empfehlung: Lassen Sie sich bei Ihrer Bankfiliale beraten, wie Sie das Mobiltelefon oder Smartphone am besten und sichersten ersetzen. Entscheiden Sie jedoch nicht sofort, sondern fragen Sie mich zunächst über den Computerwissen Club, ob die angebotene Lösung die sicherste ist: <https://club.computerwissen.de>.

Schutzschild 6: Verwenden Sie ein Online-Banking-Verfahren mit sehr hoher Sicherheit

Welche Online-Banking-Verfahren aktuell sicher sind, hat die Stiftung Warentest im Herbst 2019 mit den gängigsten Verfahren getestet und die Sicherheit in allen Fällen mit mindestens „hoch“ bewertet. Das gilt auch für das SMS-TAN-Verfahren (mTAN), auf das Ehepaar A. aus Westerhausen vertraute – ein teurer Fehler (siehe Seite 1). Stiftung Warentest warnt bei diesem Verfahren vor Betrügern und Trojanern auf dem Smartphone. Alle getesteten Verfahren können zudem „unter Laborbedingungen“ mithilfe eines Schadprogramms auf dem PC überlistet werden. Sie können aber das Risiko fast ausschalten, statt mit der falschen Wahl Ihre gesamten Ersparnisse zu verlieren.

Der Umstieg von iTAN auf ein anderes Verfahren ist nicht schwer

Das iTAN-Verfahren ist ein sehr einfaches Online-Banking-Verfahren. Sie suchen aus Ihrer TAN-Liste die angeforderte Zahl heraus und geben sie ein. Doch keine Sorge, auch die anderen Verfahren sind nicht schwer anzuwenden.

Statt vom Papier lesen Sie die benötigte TAN von einem Kartenlesegerät, einem Programm auf Ihrem Smartphone oder von einem TAN-Generator ab. Die Kartenleser und TAN-Generatoren sind einfach zu bedienen.

Von einer Smartphone-Lösung rate ich Ihnen allerdings aus Sicherheitsgründen ab. Die Gefahr von Schadprogrammen ist zu groß. Zudem ist ein Smartphone ähnlich komplex zu bedienen wie ein PC und erfordert daher entsprechende Kenntnisse.

Kann ich das FinTS-Verfahren mit HBCI-Karte und Secoder weiter nutzen?

Haben Sie den Test von Stiftung Warentest gelesen, werden Sie sich als sicherheitsbewusster PC-Anwender fragen: „Was ist mit dem FinTS-Verfahren mit HBCI-Karte? Ist das noch sicher?“ Die Stiftung Warentest hat dieses Verfahren nämlich nicht getestet.

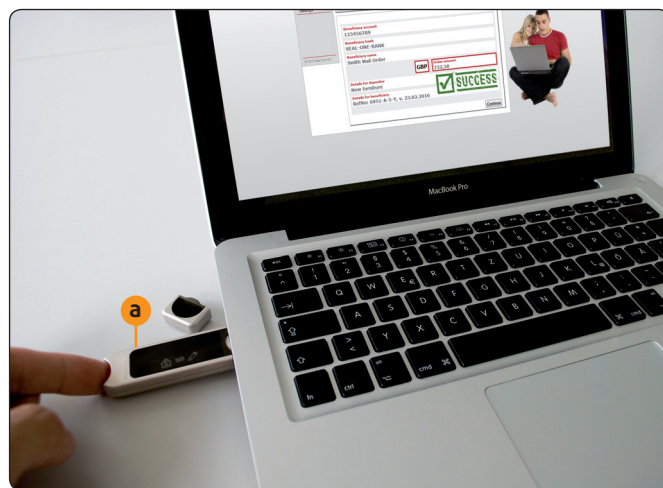
Nutzen Sie das FinTS-Verfahren mit einer Karte Ihrer Bank und einem Secoder (sicherer Kartenleser, siehe Bild auf Seite 4), dann machen Sie das ruhig weiter so. Dieses Verfahren ist immer noch das sicherste Online-Banking-Verfahren, solange Sie die HBCI-Karte nicht zusammen mit der PIN neben Ihrem PC aufbewahren.

Brandneu, bequem und sehr hohe Sicherheit: BestSign, auch bekannt als signdirect

Zum Online-Banking müssen Sie aber jetzt keine TAN mehr ablesen und eingeben oder eine Karte Ihrer Bank in einen Kartenleser einlegen und einen PIN-Code eingeben. Bei BestSign der Postbank funktioniert das Online-Banking super-einfach und ohne sichtbare TAN:

1. Sie stecken ein spezielles sicheres Gerät (Seal One Secure Hardware, sichere Hardware der Firma Seal One) an die USB-Buchse Ihres Desktop-PCs oder Notebooks oder verbinden es per Bluetooth mit Ihrem Tablet-PC oder Smartphone.

2. Sie vergleichen die Überweisungsdaten von der Anzeige auf dem Bildschirm mit denen auf dem Display des kleinen USB-Geräts.
3. Stimmen die Daten überein, geben Sie die Überweisung per Knopfdruck frei **a**.



*Einfacher und sicherer geht Online-Banking nicht mehr:
Per Knopfdruck geben Sie die Überweisung frei.*

In Verbindung mit einer App auf Ihrem Smartphone können Sie eine Überweisung auch per Fingerabdruck oder Gesichtserkennung freigeben. Das sichere Gerät ist dann nicht erforderlich. Dafür besteht die Gefahr, dass das Verfahren durch ein Schadprogramm auf dem Smartphone ausgehebelt wird.



Mein Tipp: Sind Sie sehr viel unterwegs und brauchen daher das Online-Banking auf dem Smartphone, sollten Sie statt eines Android-Smartphones ein aktuelles iPhone der Firma Apple verwenden. Das ist zwar deutlich teurer, aber das Betriebssystem iOS hat weniger Sicherheitslücken und es gibt im AppStore von Apple keine Banking-Trojaner.

Stiftung Warentest hat dem BestSign-Verfahren eine sehr hohe Sicherheit bescheinigt und ich kann es Ihnen auch uneingeschränkt empfehlen. Der Pferdefuß: Bisher wird BestSign nur von der Postbank angeboten. Weitere Banken bezeichnen das Verfahren als signdirect, bieten es aber nicht aktiv an. Fragen Sie bei Ihrer Bank daher bei Interesse nach.

Keine sichere Lösung, auch wenn die Banken es ständig empfehlen: Verwenden Sie kein mTAN!

Eine ebenfalls sehr einfache Methode des Online-Bankings ist MobileTAN oder kurz mTAN, bei der Ihnen Ihre Bank die benötigte TAN für eine Überweisung per Kurznachricht (SMS) schickt.

Stiftung Warentest bewertet die Sicherheit von mTAN mit „hoch“. Trotzdem sollten Sie auf keinen Fall mTAN verwenden, denn Kriminelle kennen zahlreiche Methoden, um das angeblich sichere Verfahren auszutricksen.

Dazu werden entweder Schadprogramme auf dem PC und Smartphone installiert oder die Kriminellen beschaffen sich eine zweite SIM-Karte und fangen die SMS damit ab.

Einfach und sehr hohe Sicherheit: chipTAN und photoTAN mit speziellem Lesegerät

Stattdessen rate ich Ihnen zu den Verfahren chipTAN und photoTAN mit Kartenleser bzw. photoTAN-Leser, deren Sicherheit von der Stiftung Warentest als sehr hoch eingestuft wurde. Da das photoTAN-Verfahren ohne Bankkarte auskommt, ist es einfacher anzuwenden als chipTAN.

chipTAN: Sie erhalten von Ihrer Bank einen TAN-Generator mit Anzeige und Tastatur oder kaufen diesen im Fachhandel (rund 10 €). Die für Ihre Überweisungen benötigte TAN wird nach Einlegen Ihrer EC-Karte oder nach dem Scannen eines Codes aus schwarz-weißen Balken erzeugt (Flickercode). Die Weiterentwicklung dieses Verfahrens ist photoTAN.

photoTAN: Sie erhalten von Ihrer Bank ein spezielles Lesegerät zum Preis von rund 30 €. Mit dem Lesegerät scannen Sie eine farbige Grafik auf der Seite Ihrer Bank ein und erhalten die Daten Ihrer Überweisung und die TAN angezeigt. Nach dem Überprüfen der Überweisungsdaten geben Sie die TAN ein.

Statt des Lesegeräts kann auch eine App auf einem Smartphone verwendet werden. Hier ist die Sicherheit jedoch weit aus geringer und ich rate Ihnen daher von der Smartphone-Lösung ab.

Gehen Sie kein Risiko ein: Von diesen Verfahren auf Smartphone-Basis rate ich Ihnen ab

Ein Smartphone ist kein sicheres Gerät wie das SealOne-Gerät, ein Kartenleser bzw. Secoder oder ein TAN-Decoder, da

Smartphones über Schadprogramme manipuliert werden können. Daher rate ich Ihnen von den folgenden Online-Banking-Verfahren ab, bei denen eine TAN über eine App auf einem Smartphone erzeugt wird:

- **appTAN, pushTAN, S-pushTAN, SpardaSecure, TAN-2go, VR-SecureGo:** Eine passwortgeschützte App auf dem Smartphone zeigt die benötigte TAN und die Überweisungsdaten an. Nach dem Abgleich der Daten mit der Überweisung auf dem PC-Bildschirm geben Sie die TAN auf der Bankseite ein. Es ist auch möglich, über eine App auf dem Smartphone eine Überweisung auszufüllen und über eine zweite App die TAN abzurufen. Das wird zum Beispiel von den Sparkassen beworben.

Sicherheitsforscher weisen jedoch darauf hin, dass aus Sicherheitsgründen immer zwei Geräte zum Online-Banking verwendet werden sollten, also zum Beispiel PC und Smartphone oder TAN-Generator kombiniert werden sollen. Die Verwendung einer App statt eines speziellen sicheren Geräts (also einer Software statt einer Hardware) ist der zweite Schwachpunkt dieses Verfahrens. Der Chaos Computer Club demonstrierte bereits 2015, wie leicht sich die Sparkassen-App überlisten lässt.

- **QR-TAN, QR-TAN+:** Sie scannen einen QR-Code (Grafik aus schwarzen Rechtecken) auf der Bankseite über eine App auf Ihrem Smartphone und erhalten die Daten Ihrer Überweisung und die dazugehörige TAN angezeigt. Nach dem Überprüfen der Überweisungsdaten geben Sie die TAN am PC auf der Bankseite ein. Stiftung Warentest hat die Sicherheit des QR-Tan-Verfahrens als sehr hoch eingestuft. Ich rate dennoch davon ab. Das Scannen über ein Smartphone ist ein Sicherheitsrisiko.

Meine Empfehlung: Sofern Ihre Bank das Verfahren anbietet, ist das BestSign-Verfahren derzeit die einfachste, schnellste und bequemste Methode zum Bestätigen Ihrer Online-Banking-Transaktionen. Allerdings rate ich Ihnen von der Nutzung auf einem Smartphone ab, zumindest auf einem Android-Smartphone.

Ebenfalls empfehlenswert ist das photoTAN-Verfahren mit TAN-Generator. Das weiterhin sicherste Verfahren FinTS mit HBCI-Karte wird leider mittlerweile überhaupt nicht mehr oder nur noch für Firmenkunden angeboten. Sie sollten es aber, solange es Ihre Bank weiter unterstützt, nutzen, sofern Sie nicht aus Mobilitätsgründen zu BestSign oder photoTAN wechseln möchten.

Impressum

Ihr PC-Sicherheits-Berater, ISSN 2196-9299
Dieses monothematische Supplement
„Ihr Leitfaden für sicheres Online-Banking
gehört zu dem Titel „Ihr PC-Sicherheits-Berater“.
Computerwissen, ein Verlagsbereich der
VNR Verlag für die Deutsche Wirtschaft AG

Vorstand: Richard Rentrop

Chefredakteur: Michael-Alexander Beisecker
(V.i.S.d.P.), Oberhausen

Herausgeberin: Patricia Sparacio

Adresse: Verlag für die Deutsche Wirtschaft AG,
Theodor-Heuss-Str. 2-4, 53177 Bonn

Telefon: 0228/9550190, Fax: 0228/3696350

Eingetragen: Amtsgericht Bonn HRB 8165

Die Beiträge in „Ihr PC-Sicherheits-Berater“ wurden mit Sorgfalt recherchiert und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Daher ist eine Haftung, auch für telefonische Auskünfte, ausgeschlossen. Vervielfältigungen jeder Art sind nur mit Genehmigung des Verlags gestattet.

© Copyright 2019 by Verlag für die Deutsche Wirtschaft AG;
Bonn, Bukarest, Manchester, Warschau



Schutzschild 7: So verhalten Sie sich richtig beim Online-Banking

Sie selbst sind der wichtigste, der siebte Schutzschild. Alle Online-Banking-Verfahren sind auf dem PC grundsätzlich sicher. Lassen Sie sich durch keinen Trick der Kriminellen hereinlegen, haben Sie nichts zu befürchten. Überprüfen Sie mit meiner nachfolgenden Checkliste, ob Sie immer richtig reagieren. Nur so sind Sie immer auf der sicheren Seite.

1. Haben Sie einen aktuellen PC mit Windows 10 oder 7 und ausschließlich aktuelle und noch von den Herstellern gepflegte Programme?

- ☐ Ja
- ☐ **Nein:** Sehen Sie sich noch einmal Schutzschild 1 auf Seite 2 an und aktualisieren Sie Ihr Windows und Ihre Anwendungen, damit Schadprogramme keine Sicherheitslücken finden.

2. Löschen Sie E-Mails unbekannter Absender mit Anhang sofort und überprüfen Sie jeden Anhang und jeden Download mit dem Online-Antiviren-Programm VirusTotal?

- ☐ Ja
- ☐ **Nein:** Über 90 Prozent aller Online-Banking-Schadensfälle entstehen dadurch, dass die Anwender den Banking-Trojaner selbst installieren. Seien Sie daher äußerst vorsichtig mit E-Mail-Anhängen und Downloads. Überprüfen Sie jeden Anhang und jede heruntergeladene Datei mit VirusTotal, das Sie an der Adresse <https://www.virustotal.com/gui/home/upload> aufrufen.

3. Löschen Sie E-Mails sofort, in denen Sie zur Eingabe von Kontodaten und/oder TANs aufgefordert werden?

- ☐ Ja
- ☐ **Nein:** Löschen Sie alle E-Mails mit dem Absender einer Bank am besten sofort ungeöffnet, denn es sind meist Fälschungen. Sofern Ihre Bank Ihnen etwas Wichtiges mitzuteilen hat, wird sie das in Briefform tun.

4. Informieren Sie bei jeder verdächtigen Bildschirmanzeige sofort Ihre Bank und fragen nach, ob diese in Ordnung ist?

- ☐ Ja
- ☐ **Nein:** Seien Sie beim Online-Banking bei jeder ungewöhnlichen Meldung äußerst misstrauisch, denn sie kann von einem Banking-Trojaner stammen. Der häufigste Trick: Sie erhalten eine Meldung, dass Ihnen angeblich versehentlich mehrere Tausend Euro auf Ihr Konto überwiesen wurden, die Sie zurücküberweisen sollen. Machen Sie das auf keinen Fall!
Der zweithäufigste Trick: Sie erhalten eine Meldung, dass Sie für eine Testbuchung eine TAN eingeben sollen oder dass eine Überweisung nicht geklappt hätte.

Geben Sie auf gar keinen Fall eine neue TAN ein. Informieren Sie Ihre Bank in solchen Fällen und untersuchen Sie Ihren PC mit dem ESET-Online-Scanner auf Schadprogramme. Den ESET-Online-Scanner erreichen Sie am Link

<https://www.eset.com/de/home/online-scanner/>.

5. Verwenden Sie ausschließlich Ihren PC und einen TAN-Generator oder Kartenleser für das Online-Banking und kein Smartphone?

- ☐ Ja
- ☐ **Nein:** Sehen Sie sich noch einmal Schutzschild 6 auf Seite 6 an und sprechen Sie mit Ihrem Bankberater, damit Sie einen passenden TAN-Generator oder ein Kartenlesegerät erhalten.

6. Vergleichen Sie bei Verwendung eines TAN-Generators immer die Kontodaten auf dem Display des Generators mit denen auf Ihrem Bildschirm?

- ☐ Ja
- ☐ **Nein:** Nehmen Sie diese wichtige Prüfung unbedingt vor. Nur so erkennen Sie, wenn ein Banking-Trojaner die Überweisungsdaten auf dem PC-Bildschirm verändert hat.

7. Schließen Sie Aufzeichnungen über Ihre Zugangsdaten, TAN-Listen, Bankkarten und Lesegeräte oder TAN-Generatoren immer weg?

- ☐ Ja
- ☐ **Nein:** Das sicherste Online-Banking-Verfahren schützt Sie nicht, wenn alle dafür erforderlichen Informationen, Karten und Geräte direkt griffbereit am PC liegen und so von Unbefugten missbraucht werden können. Legen Sie die Bankkarte und Zugangsdaten nach der Benutzung in Ihren Tresor oder ein sicheres Versteck.

Auswertung: Haben Sie als sicherheitsbewusster PC-Anwender alle Fragen mit **Ja** beantwortet, betreiben Sie Online-Banking auf dem höchsten Sicherheitsniveau, das im privaten Bereich möglich ist. Sie haben nichts zu befürchten. Sofern Sie eine Frage mit **Nein** beantwortet haben, folgen Sie einfach meiner Empfehlung und Sie sind auch sicher.

Haben Sie eine Fragen zum Online-Banking? Meine Redaktionskollegen und ich helfen Ihnen gerne über den Computerwissen Club, die Sicherheit bei Ihrem Online-Banking zu optimieren: <https://club.computerwissen.de>.