Sicherheit beim Online-Banking

Es gibt keine absolute Sicherheit beim Online-Banking!
Die größte Unsicherheit ist der Mensch, deshalb muss er stets wieder informiert werden, wo Gefahren drohen.

Im Vortrag soll behandelt werden:
- Wie funktioniert das Online-Banking.
- Wo gibt es grosse Gefahren und was sollte man auf keinen Fall tun.
- Was sollte ich unbedingt machen.
- Wie kann ich den Vorgang möglichst sicher machen!

Wenn Sie einige wichtige Dinge einhalten, dann ist Online-Banking nicht unsicherer als Geld vom Geldautomaten abzuheben.

Bisherige Vorträge zum Thema Online-Banking

21. Mai 2003 — **Online-Banking** — **Birgit Bastian**

Was ist Onlinebanking? – Warum Onlinebanking? – Verbindungsmöglichkeiten – HBCI oder PIN & TAN – Sicherheit – Was brauche ich? – Börse, Wertpapiere, Depot

01. Juli 2003 — **Internet-Banking** — **R. Schmitt**

Internet-Banking am beispiel des Progr. „WISO Mein Geld 4“
Modern Cash (Postbank) – Internet (Advanced Bank) – „WISO Mein Geld“ (Buhl Data)
Bestandsabfrage - Konto Übersicht – Pseudo Konten – Darlehenskonten – Depot – Wertpapier Verwaltung – Spesenübersicht – Überweisungen

22. Dezember 2009 — **Sicherheit beim Onlinebanking** — **R. Schmitt**

Was ist Online Banking? - Wie funktioniert Online Banking? – Wo gibt es große Gefahren und was sollte man auf keinen Fall tun - Wie kann ich den Vorgang möglichst sicher machen? – 10 Sicherheitsregeln

25. Februar 2017 — **Zahlungssysteme** — **Günther Scheckeler**

Bezahlen im Internet – Amazon-pay – Kreditkarte – Lastschrift – Nachnahme – PayPal – Ratenkauf/Finanzierung – Sofortüberweisung Vorauskasse – Zahlung bei Abholung

04. April 2017 — **Sicherheit beim Onlinebanking** — **R. Schmitt**

Was ist Online Banking? - Wie funktioniert Online Banking? – Wo gibt es große Gefahren und was sollte man auf keinen Fall tun - Wie kann ich den Vorgang möglichst sicher machen? – Online Banking per Handy - Sicherheitsregeln

Welche Fragen haben Sie zu dem Thema „Sicherheit bein Online-Banking“?

1. **Kann ich Online-Banking auch mit dem Handy erledigen?**

04.04.2017 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Was bedeutet BSI?

https://www.bsi.bund.de/DE/Home/home_node.html

Bundesamt
für Sicherheit in der
Informationstechnik

Was bedeutet Cert?

https://www.cert.org

CERT | Software Engineering Institute | Carnegie Mellon University

Computer Emergency Response Team (CERT),
deutsch Computersicherheits-Ereignis- und Reaktionsteam

Förderverein Bürgernetz München-Land e.V.

Sicherheit beim Online-Banking

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

BSI – Online Banking Übersicht

Reinhard@ReinhardSchmitt.De

1. So funktioniert Online-Banking?

Kapitelübersicht:

Im **Kapitel Grundlagenwissen** erfahren Sie, wie Online-Banking grundlegend funktioniert und welche Sicherheitsmaßnahmen es seitens der Banken gibt.

Mit welchen Risiken das Online-Banking verbunden ist und welche Methoden Kriminelle nutzen, um an Ihr Geld zu kommen – das erfahren Sie im **Kapitel Gefahren und Risiken**.

Wie Sie sich vor den Gefahren schützen können, lesen Sie im **Kapitel Sicherheitsmaßnahmen**.

Inhaltsverzeichnis

So funktioniert das Online-Banking

Gefahren und Sicherheitsrisiken

Sicherheitsmaßnahmen

Mobile Banking

Was tun im Ernstfall?

1.1 Welchen Nutzen hat Online-Banking?

Ihre Bankgeschäfte von zu Hause per PC durchzuführen

- **Kontostände sowie Ein- und Ausgänge abfragen**
- **Kreditkartenumsätze einsehen**
- **Geld ins In- und Ausland überweisen**
- **Terminüberweisungen**
- **Daueraufträge einrichten und stonieren**
- **Depotabfragen**
- **Wertpapierhandel**
- **Aktuelle Informationen**

1.2 Was brauchen Sie für Online-Banking?

- Ein PC oder ein Tablet oder ein Laptop oder ein Smartphone
- Betriebsystem ist egal Windows, MAC OS, Linux
- Internetbrowser Microsoft Internet Explorer, Apple Safari, Mozilla Firefox, Google Crome
- Oder eine Online-Banking Software wie z.B. „WISO Mein Geld“
- Online Konto Vertrag bei Ihrer Bank – PIN und TAN bzw. Zugangsdaten
- Wichtig!! Alle installierten Softwareprodukte per Updates stets auf dem neuesten Sicherheitsstand halten!

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 12 Maßnahmen zur Absicherung gegen Angriffe aus dem Internet

Kernmaßnahmen

1. **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".**
2. **Setzen Sie ein Virenschutzprogramm ein und aktualisieren Sie dieses regelmäßig, idealerweise über die Funktion "Automatische Updates"**
3. **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.**

1.2.3 12 Maßnahmen zur Absicherung gegen Angriffe aus dem Internet

Kernmaßnahmen

4. **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**
5. **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.**

1.2.3 12 Maßnahmen zur Absicherung gegen Angriffe aus dem Internet

Ergänzende Maßnahmen

6. 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.
7. 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.

04.04.2017 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

1.2.3 12 Maßnahmen zur Absicherung gegen Angriffe aus dem Internet

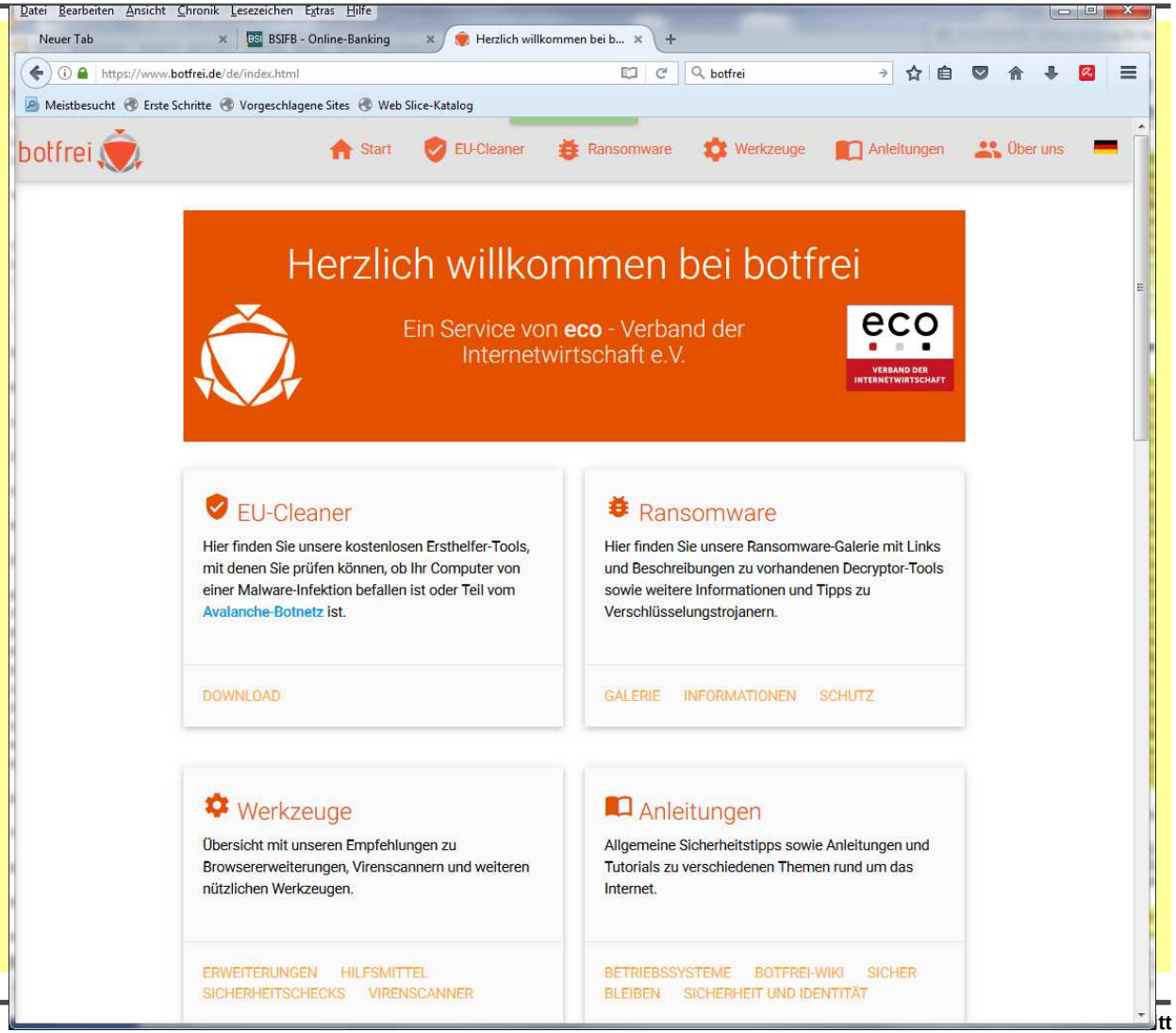
Ergänzende Maßnahmen

8. **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 Kommunikations-protokolls "HTTPS". Sie erkennen dies an der von Ihnen aufgerufenen Internet-adresse, die stets mit "https://" beginnt und an dem kleinen Schloss-Symbol in Ihrem Browserfenster.**
9. **Deinstallieren Sie nicht benötigte Programme. Je weniger Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche Ihres gesamten Systems.**
10. **Erstellen Sie regelmäßig Sicherheitskopien "Backups" Ihrer Daten, um vor Verlust geschützt zu sein. Hierzu können Sie beispielsweise eine externe Festplatte nutzen.**
11. **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.**
12. **Überprüfen Sie in regelmäßigen Abständen den Sicherheitsstatus Ihres Computers. Eine schnelle Testmöglichkeit bietet die Initiative botfrei des eco-Verbands.**

Förderverein Bürgernetz München-Land e.V.

Sicherheit beim Online-Banking

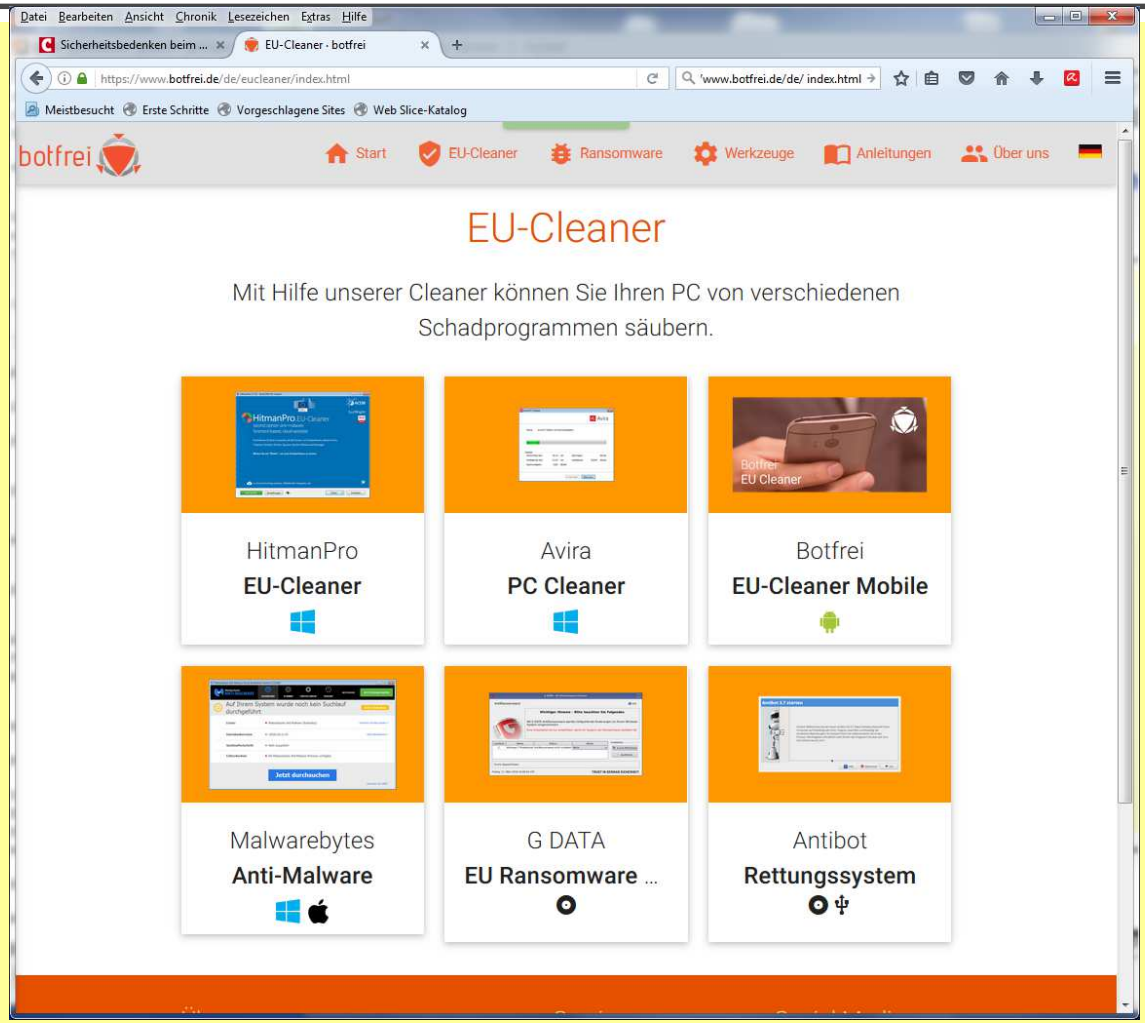
https://www.botfrei.de/de/index.html



tt
Reinhard@ReinhardSchmitt.De

URL von botfrei vom eco-Verband

EU-Cleaner


Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
Sicherheitsbedenken beim ...
EU-Cleaner - botfrei
https://www.botfrei.de/de/eucleaner/index.html
www.botfrei.de/de/ index.html
Meistbesucht Erste Schritte Vorgeschlagene Sites Web Slice-Katalog
botfrei
Start
EU-Cleaner
Ransomware
Werkzeuge
Anleitungen
Über uns
EU-Cleaner
Mit Hilfe unserer Cleaner können Sie Ihren PC von verschiedenen Schadprogrammen säubern.
HitmanPro
EU-Cleaner
Avira
PC Cleaner
Botfrei
EU-Cleaner Mobile
Malwarebytes
Anti-Malware
G DATA
EU Ransomware ...
Antibot
Rettungssystem

1.2.3 12 Maßnahmen zur Absicherung gegen Angriffe aus dem Internet

Weitere Informationen:

- **Zu Fragen der IT-Sicherheit finden Sie Hinweise in unseren Tipps und Checklisten.**
  https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/checklisten_node.html
- **Der Avira PC-Cleaner eignet sich für einen zusätzlichen Schnelltest auf Schadsoftwarebefall, ersetzt jedoch kein vollwertiges Virenschutzprogramm.**
  https://install.avira-update.com/package/pccleanerwebloader/win32/de/avira_pc_cleaner_de.exe

Hinweis:

Ein Programm will sich plötzlich installieren.

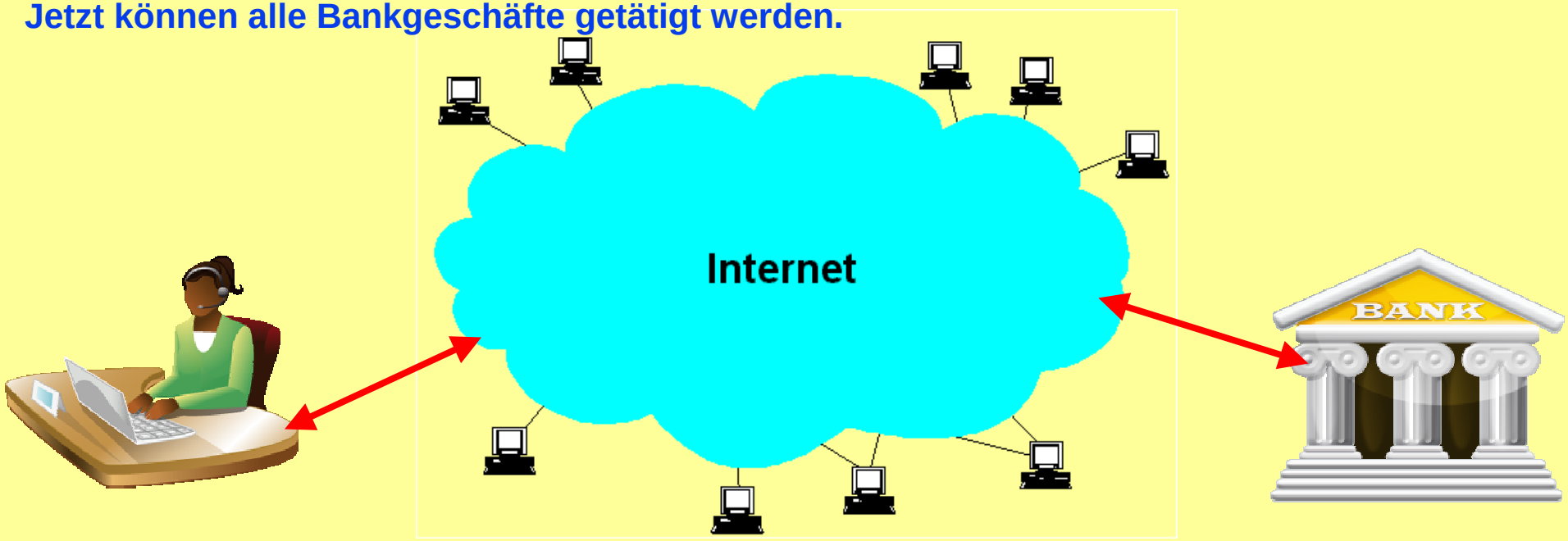
Wenn plötzlich, scheinbar ohne Grund während des Surfens im Internet ein Fenster aufgeht und Ihnen mitteilt, dass sich ein Programm installieren möchte und dazu **nach Ihrem Passwort** fragt, ist höchste Vorsicht geboten. Wenn Sie Zweifel am Zweck des Programms haben, **brechen Sie den Vorgang ab ohne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

Wie funktioniert das Online-Banking

Per Internet-Explorer oder Firefox die Homepage der Bank aufrufen!
(Möglichst die URL der Banken-Homepage eintippen, keinen Link verwenden.)

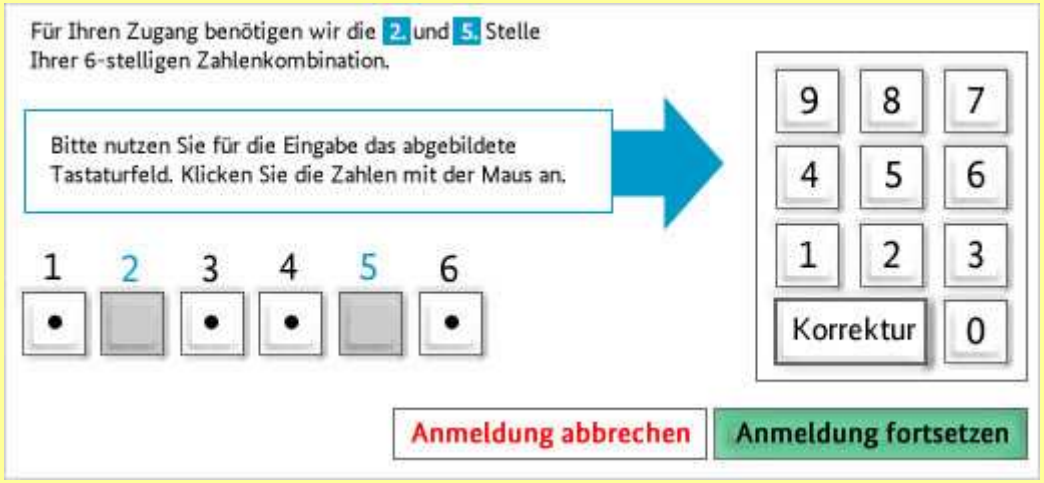
Login per Kontonr. & PIN oder Kennung und Passwort
Bei den meisten Banken muss das Online Banking extra beantragt werden.

Jetzt können alle Bankgeschäfte getätigt werden.



Zusätzliche Sicherheiten zu PIN/TAN bei der Anmeldung

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.



Dieses Verfahren verwendet z.B. die ING-Diba Bank.

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.

1.3.1 Sicherheit im Online-Banking

Inhalt des Dossiers

1. PIN-/TAN-Verfahren allgemein erklärt
2. PIN-/TAN-Verfahren mit TAN-Liste
3. Das mTAN-Verfahren – TAN-Versand per SMS
4. TAN-Generatoren: Individuelle TAN für jeden Auftrag
5. Signaturverfahren: Karte statt TAN

04.04.2017 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

1.3.1 PIN/TAN-Verfahren

PIN = Persönliche Identifikations Nummer **TAN = Transaktions Nummer**

- **Das klassische PIN/TAN Verfahren (nicht mehr üblich) (TAN-Liste, Phishing)**
- **iTAN-Verfahren (jetzt eingestellt) (MAN in the middle)**
- **iTANplus (es wird ein Kontrollbild Chapta eingeblendet mit Betrag, Bankleitzahl & Kontonummer Empfängers, Geburtsdatum, Positionsnummer der angeforderten TAN) (erschwert MAN in the middle)**
- **mTAN – TAN-Versand per SMS („mobileTAN“ oder „smsTAN“ genannt)**
  (Das BSI empfiehlt auf den Einsatz von mTAN-Verfahren zu verzichten.)
- **TAN-Generator**
  - **eTAN-Verfahren**
  - **sm@rtTAN-Verfahren (sm@rtTAN plus /chipTAN manuell, sm@rtTAN optic /chipTAN comfort)**
  - **photo TAN-Verfahren**
- **Signaturverfahren: Karte statt TAN**
  - **HBCI Home Banking Computer Interface**

TAN = TransAktionsNummer

- **TAN** = 1 TAN aus einer TAN-Liste selbst auswählen **(Veraltet & Gefählich)**
- **iTAN** = Die Bank fordert jedesmal eine bestimmte TAN per Index an **(wird eingestellt)**
- **mTAN** = Per SMS wird eine TAN von der Bank auf das Handy geschickt zusätzlich wird die Zielkontonummer und die Summe aus der Überweisung mitübermittelt
- **TAN-Generator**
  - **eTAN** = Ein elektronisches Zusatzgerät generiert eine TAN
  - **eTAN plus** = Ein elektronisches Zusatzgerät generiert eine TAN unter Berücksichtigung von Summe und Zielkontonummer
  - **sm@rt-TAN** mit Einschub für Bank-/EC-Karte
  - **photo-TAN** mit Einschub für Bank-/EC-Karte, der TAN-Generator scannt am Bildschirm die Überweisungsdaten ein.
- **HBCI** = Home Banking Computer Interface **(wird leider nur selten angeboten, da für Banken zu teuer)**

Wo werden TAN‘s benötigt?

Überweisungen, Daueraufträgen, Änderung wichtiger Daten, Änderungen der Überweisungslimits, usw.

1.3.3 Das mTAN-Verfahren – TAN-Versand per SMS

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.

04.04.2017 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

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.

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

04.04.2017 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

1.4 Online-Banking: Gefahren und Sicherheitsrisiken

Inhalt des Dossiers

1. E-Mail-Phishing: Passwortdiebstahl mit manipulierten E-Mails
2. Schadsoftware: Trojanische Pferde sammeln unbemerkt Daten
3. Mobile Banking: Unterwegs lauern Gefahren

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.

04.04.2017 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

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

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.

04.04.2017 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

1.4.1 E-Mail-Phishing: Beispiel einer gefälschten Banken-Website, die auffordert alle unbenutzten Transaktionsnummern einzugeben.

http://banking.postbank.ru/cust_details_conforming.de

E-Mail Adressen-Land .ru = Russland

http: nicht https:
daher fehlt das Sicherheits-schloss in der untersten Zeile

URL's in E-Mails nie anklicken, sondern stehts selbst eintippen. Das ist viel sicherer.

04.04.2017 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

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

Die ersten Phishing E-Mails waren häufig leicht zu erkennen, da sie oft viele Recht-schreibfehler enthielten und ihr Erscheinungsbild von dem der Original-Nachrichten von Banken stark abwichen. 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.

04.04.2017 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

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").

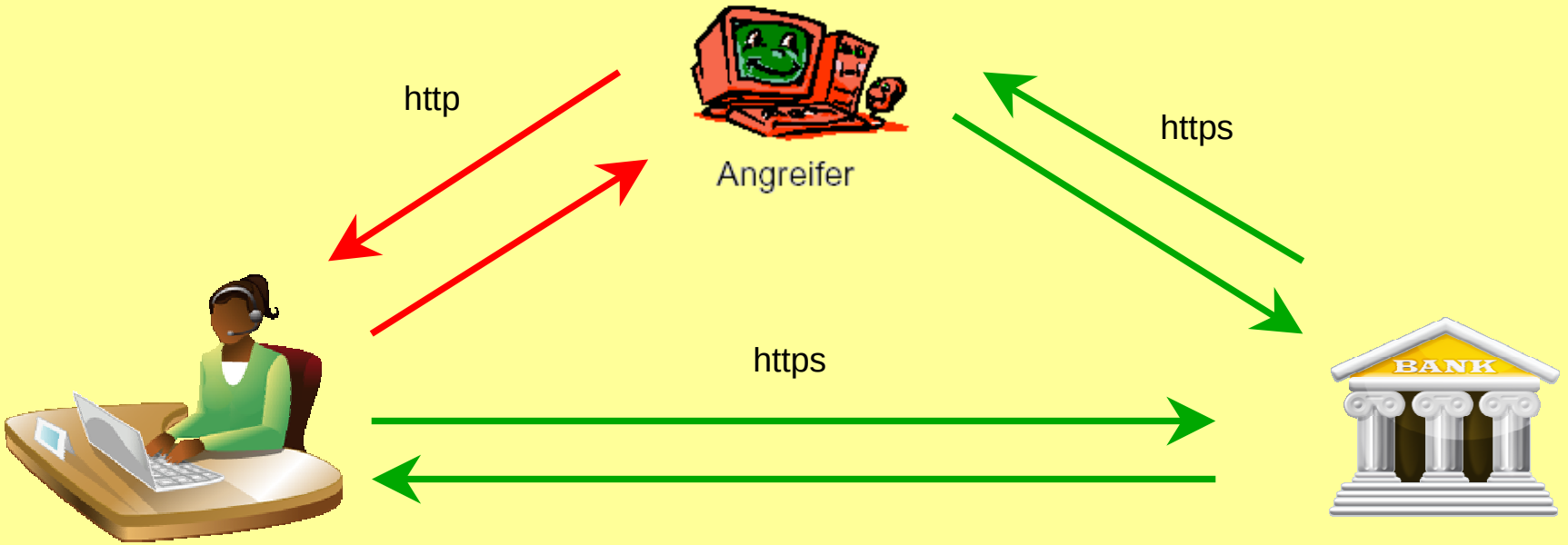
1.4.1.2.4 Woran kann man Phishing-Webseiten erkennen?

- 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

- **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.**

Sicherheit beim Online-Banking



Authentizität (Authentication) = Zertifikat

1.4.3 Mobile Banking: Unterwegs lauern Gefahren

- **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 (Handy nur für Banking):**
  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.
  http://www.heise.de/ct/projekte/Sicheres-Online-Banking-mit-Bankix-284099.html
- **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).**
  https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungWLAN-LAN/WLAN/wlan_node.html

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.
  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.
  http://www.heise.de/security/artikel/iPhone-Banking-Apps-im-Sicherheitscheck-1158091.html
  Mehr Informationen zu Mobile Banking finden Sie auch hier.
  https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/MobileBanking/mobileBanking

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 Spyware 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. http://www.heise.de/download/smartphones/sicherheit/virenscanner-50004301183/

1.4.3.2.3 So können Sie sich schützen

- **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.**

1.5 Online-Banking – Was tun im Ernstfall?

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.**

1.5 Online-Banking – Was tun im Ernstfall?

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.**

Sicherheit beim Online-Banking

Was kann ich tun, um möglichst sicher Online-Banking zu tätigen?

1. **Auf einer extra Platte oder einem extra Smartphone nur Online-Banking mit Betriebssystem installieren.**
   Kein E-Mail, SMS, MMS (Gefahr Phishing) installieren. Auch möglichst keine weiteren Anwendungen. Je weniger destobesser.
   Mit diesem Gerät nicht im Internet Surfen (Gefahr Trojaner).

   Oder Online-Banking Plattformen verwenden, die über USB-Stick oder CD-ROM gebootet werden.
   Nähere Informationen und eine Anleitung bietet zum Beispiel die Fachzeitschrift c't.
   http://www.heise.de/ct/projekte/Sicheres-Online-Banking-mit-Bankix-284099.html
2. **System stets aktuell halten mit Virenscanner.**
3. **Möglichst nur eigenes Home-Netz verwenden.**
4. **URL nicht anklicken, sondern händisch eintippen. Z.B. www.Postbank.de . Dann kann sich hinter einem Hyperlink, keine falsche URL verbergen.**
   Das Passwort selbst eintippen, nicht vom System abspeichern lassen!
5. **Bei Smartphones möglichst eine App der eigenen Bank nehmen, dann haftet die Bank eher bei Fehlern.**

Was ist unsicher beim Online-Banking?

1. **Ein System auf dem ich viele unterschiedliche Tätigkeiten durchführe:**
   Im Internet surfen (Gefahr Trojaner), E-Mail (SMS, MMS) tätige (Gefahr Phishing).
   Spiele und viele sonstige Programme, welche spionieren können.
   Programme wie „Whats App“, welche alle privaten Daten lesen. u.s.w.
2. **Fremde Netze verwenden z.B. im Internet Cafe. Netze im Ausland u.s.w.?**

Was sollte ich auf keinen Fall tun??

- **Geheimnummern (Pin) und Transaktionsnummern (Tan) per Mail versenden. (Phishing)**
- **Eine Bank URL antippen, die mir angeblich von meiner Bank per Mail gesendet wurde. (Phishing, Pharming)**

Was sollte ich unbedingt tun!

- Ein Antivirenprogramm einsetzen
- Eine Firewall verwenden
- Das WLAN sicher einstellen und ggf. abstellen
- Keine Ordner freigeben um von anderen Netzcomputern Daten zu übertragen!
- Möglichst die Bank URL eintippen und nicht abgespeicherte URL‘s verwenden, da diese manipuliert sein können. Am besten die IP-Nummer eintippen.
- Login zur Bank die Kennung und das Passwort selbst eintippen und nicht abgespeicherte Versionen verwenden, da diese manipuliert sein können.

Was sollte ich unbedingt tun!

- Überprüfen, ob es sich um eine https Verbindung handelt. Banken verwenden nur sichere Verbindungen. Ggf. mal das Zertifikat überprüfen. (Vortrag im Bürgernetz Juli 2005)
- Das Betriebsystem möglichst auf neuesten Stand updaten.
- Die Virensoftware möglichst auf neuesten Stand updaten.
- Regelmässig Virenscans durchführen lassen.
- Meine Konten regelmässig überprüfen auf falsche Abbuchungen. Diese kann ich innerhalb von 14 Tagen rückbuchen lassen.

Wie kann ich den Vorgang möglichst sicher machen!

- **Ein Betriebsystem von einer CD starten (c‘t Bankix - Ubuntu, oder PE-Builder - Windows), da dann nicht dauerhaft verändert werden kann (Trojaner, Viren).**
  http://www.heise.de/ct/projekte/Sicheres-Online-Banking-mit-Bankix-284099.html
  http://www.ctmagazin.de/0919102
  http://www.ctspecial.de/cs0906095
- **Ein Betriebssystem von USB-Stick mit Schreibschutz starten (c‘t Bankix - Ubuntu), da dann nicht dauerhaft verändert werden kann (Trojaner, Viren).**
- **Banking-Programme einsetzen, die die Übertragung überwachen (z.B. WISO). Nachteil kosten meist ca 40 - 60€ pro Jahr.**
- **Den PC mit Wechselplatten ausstatten und für Banking von einer eigenen Platte booten. (Mit dieser Platte sonst nicht im Internet surfen!)**

Wenn Sie diese Ratschläge berücksichtigen, dann ist das Online-Banking so sicher wie das Abheben am Bankautomaten!

10 Sicherheitsregeln

1. Setzen Sie Sicherheitssoftware ein – unter anderem einen aktuellen Virenscanner
2. Schützen Sie sensible Daten bei der Übertragung über offene Netze
3. Vergewissern Sie sich, mit wem Sie es zu tun haben
4. Gehen Sie sorgfältig mit sensiblen Daten und Zugangsmedien um
5. Wählen Sie ein sicheres Passwort
6. Setzen Sie nur Programme aus vertrauenswürdiger Quelle ein
7. Nutzen Sie aktuelle Programmversionen
8. Führen Sie einen Sicherheitsscheck auf Ihrem PC durch
9. Aktivieren Sie die Sicherheitseinstellungen des Browsers
10. Stellen Sie Ihr Girokonto nicht für betrügerische Finanztransaktionen zur Verfügung

(Quelle www.infos-finanzen.de)

Haftungsbedingungen

Ob Bank oder Kunde haftet, steht in den allgemeinen Geschäftsbedingungen und in den Sonderbedingungen. Die Bank haftet grundsätzlich für ihr eigenes Verschulden. Ist ein Schaden nicht allein von der Bank verursacht oder verschuldet, haftet der Kunde in dem Umfang, wie er den Schaden mitverschuldet hat. Diese Regelung entspricht den gesetz-lichen Vorgaben, wir haben sie als neutral bewertet. Eine Beschränkung der Haftung auf 10 Prozent des Schadens oder eine Umkehr der Beweislast haben wir positiv bewertet. Wir haben negativ bewertet, wenn die Bank zum Nachteil des Kunden von der gesetzlichen Regelung abweicht und die Haftung des Kunden in den Vordergrund stellt, Sorgfaltspflichten aus-drücklich zum Haftungsmaßstab erhebt, die Schadensübernahme von einer Strafanzeige des Kunden abhängig macht oder die Haftung für Schäden aus undeutlichen Aufträgen dem Kunden auferlegt.

Sicherheit beim Online-Banking

- PIN = Persönliche Identifikationsnummer
- TAN = Transaktionsnummer
- iTAN = indizierte TAN
- eTAN = elektronik TAN
- eTANplus = verbessertes eTAN
- mTAN = mobile TAN
- sm@rtTAN = Eine mit Hilfe des TAN-Generators erzeugte TAN
- photoTAN = Eine mit Hilfe des TAN-Generators erzeugte TAN, der TAN-Generator photographiert, bzw. scannt dabei Daten vom Bildschirm ein.
- HBCI = Home-Banking Computer Interface
- FinTS = Financial Transaction Services
  (FinTS HBCI; FinTS PIN/TAN; FinTS V4.0)
- RDH = RSA-DES-Hybridverfahren
  ein gemischtes hybrides Verschlüsselungsverfahren
- DDV = DES-DES Verfahren (symetrische Schlüssel)
- RSA = Rivest-Shamir-Adleman (asymetrisches Verschlüsselungsverfahren)

Sicherheit beim Online-Banking

Sandbox = SpielSandkasten (Umgebung) zum Ausführen neuer Programme.

Botnetz = Gekaperte Pc‘s die verwendet werden für Angriffe auf meist öffentliche Systeme um diese lahmzulegen. Oder für SPAM-Versand

Spear-Phishing = Spear-Phishing ist ein verfeinertes Phishing mit einem gezielteren persönlichen Ansatz. Daher auch die Bezeichnung Spear Phishing, wobei das englische Wort Spear für Speer steht. Bei diesem Phishing-Ansatz kann der Spear-Phisher das Vertrauen zu seiner Zielperson über Informationen aus sozialen Netzwerken aufbauen. Über die Ausbildungsstätte oder das Unternehmen in dem das potentielle Opfer mal gearbeitet hat oder über Sportaktivitäten, soziale Einstellungen, die gleiche Bank usw. Der E-Mail-Verkehr kommt anscheinend vom Arbeitgeber oder von einem Kollegen.

Spoofing = **Spoofing** (englisch für *Manipulation*, *Verschleierung* oder *Vortäuschung*) nennt man in der Informationstechnik verschiedene Täuschungsmethoden in Computernetzwerken zur Verschleierung der eigenen Identität. Personen werden in diesem Zusammenhang auch gelegentlich als „Spoofer“ bezeichnet.

„Sicherheit“

- **BSI** **B**undesamt für die **S**icherheit in der **I**nformationstechnik
  https://www.bsi.bund.de/DE/Home/home_node.html
- **CERT** **Computer Emergency Response Team (CERT),**
  deutsch Computersicherheits-Ereignis- und Reaktionsteam
  https://www.cert.org
- **www.it-Sicherhei.de** **Sicherheit beim Online-Banking**
  https://www.it-sicherheit.de/ratgeber/it_sicherheitstipps/tipp/sicherheit-beim-online-banking/
  https://www.it-sicherheit.de/ratgeber/it_sicherheitstipps/online_dienste_sicher_nutzen/online_banking/
- **Verbraucher Sicher – ONLINE**
  https://www.verbraucher-sicher-online.de/thema/online-banking
- **Sparkasse** **Sicherheit im Internet**
  https://www.sparkasse.de/service/sicherheit-im-internet.html
- **Chip** **Sicheres Online-Banking: Die 7 besten Tipps**
  http://praxistipps.chip.de/sicheres-online-banking-die-7-besten-tipps_3158

Sicherheit beim Online-Banking

„Ratgeber“

- **NETPLANET** zum Thema Online-Banking.
  http://www.netplanet.org/sicherheit/banking.shtml

- **Geben Sie in das Google-Fenster Ihres Internetexploreres des Text ein „Sicherheit beim Online-Banking“ und Sie erhalten viele Verweise auf gute Internetseiten, natürlich auch auf viel Reklame.**

„Online Banking Projekte“

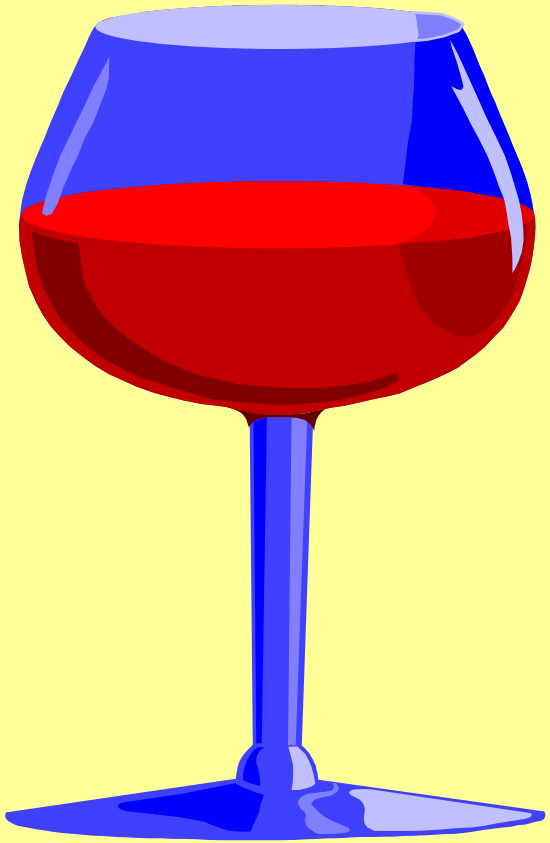
- **Sicheres Online-Banking mit Bankix**
  c't Bankix ist ein Live-Linux-Betriebssystem, das speziell für sicheres Online-Banking konzipiert wurde und von CD oder USB-Stick arbeitet.
  http://www.heise.de/ct/projekte/Sicheres-Online-Banking-mit-Bankix-284099.html

„Bankinstitute“

- **Vergleich mehrerer Bankinstitute**
  http://dynamisch.vergleich.de/vergleich/girokonto/vergleich?Profil=online_nutzer&Variante=hotlineSidebar|button2&extcid=SGOJHAD060000000&track=admatics

Diese Folien werden zum Herunterladen im Internet Bürgernetz (www.muela.de) wie immer bereitgestellt!

04.04.2017 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De



Fragen und Diskussion

04.04.2017 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De