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.

Zeitungsmeldungen

- **Eingeloggt, abgezockt** (SZ 26.5.2008)
- **Misstrauen ist angebracht**
  Im Internet gelten die selben Vorsichtsregeln wie im Leben (SZ 26.5.2008)
- **Das Handy macht Onlinebanking sicher** (Welt 31.5.2008)
- **Operation am digitalen Herzen**
  Computerexperten haben ein massives Sicherheitsleck im Internet gestopft (DNS manipuliert) (SZ 10.7.2008)
- **Rekord bei Betrug im Internet** (SZ 3.9.2008)
- **Tatort Geldautomat** (SZ 19.9.2008)
- **Phishing, Spionage, Viren & Co –**
  Internetkriminalität kennt keine Grenzen (VDI 2.10.2008)

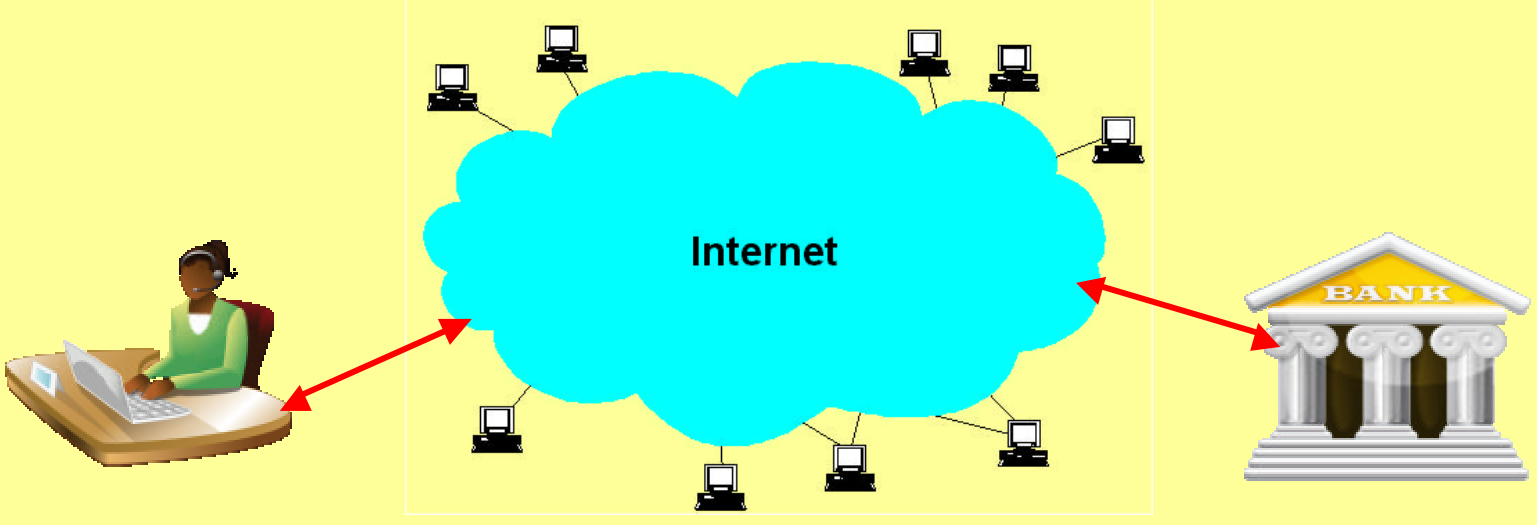
Was ist Online-Banking??

Ihre Bankgeschäfte von zu Hause per PC durchzuführen

- **Kontostandsabfragen**
- **Überweisungen**
- **Dauerauftragsverwaltung**
- **Depotabfragen**
- **Wertpapierhandel**
- **Aktuelle Informationen**

Wie funktioniert das Online-Banking

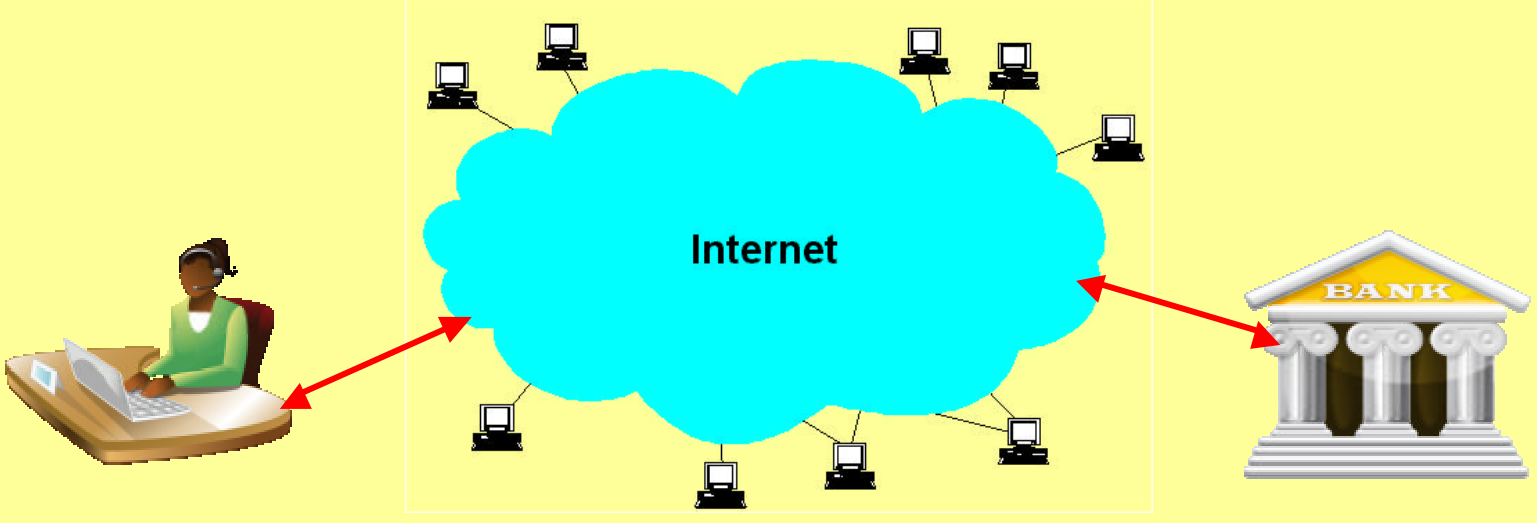
Per Internet-Explorer oder Firefox die Homepage der Bank aufrufen!



Wie funktioniert das Online-Banking

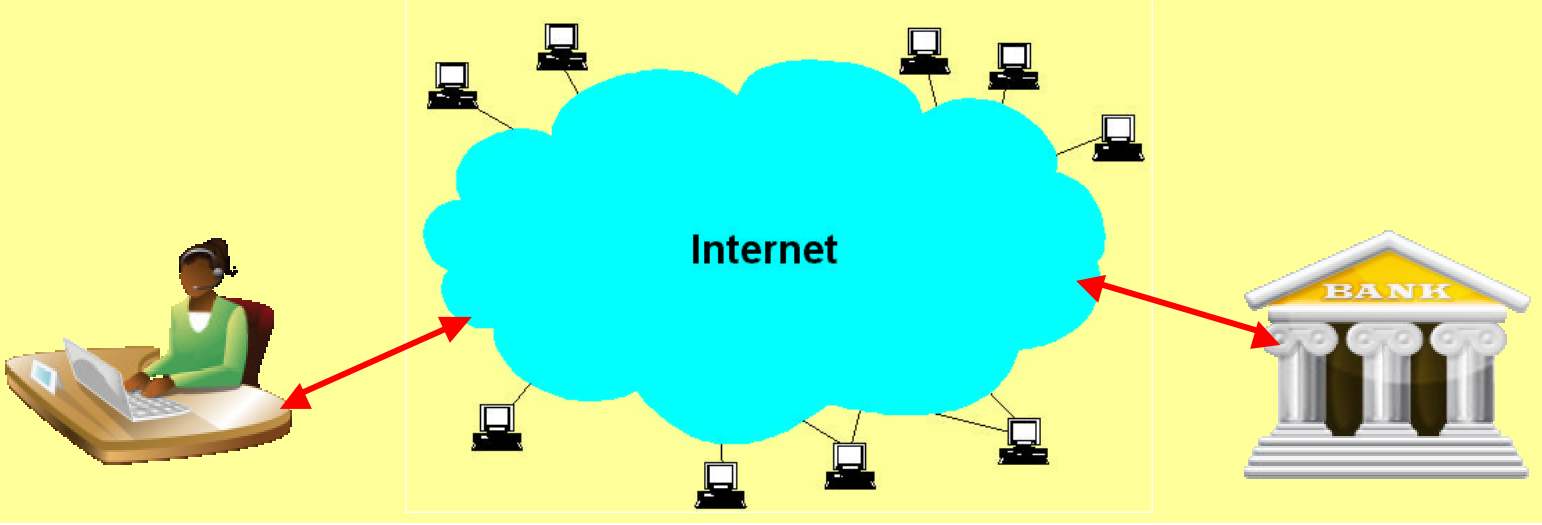
Login per Kontonr. & PIN oder Kennung und Passwort

Bei den meisten Banken muss das Online Banking extra beantragt werden.



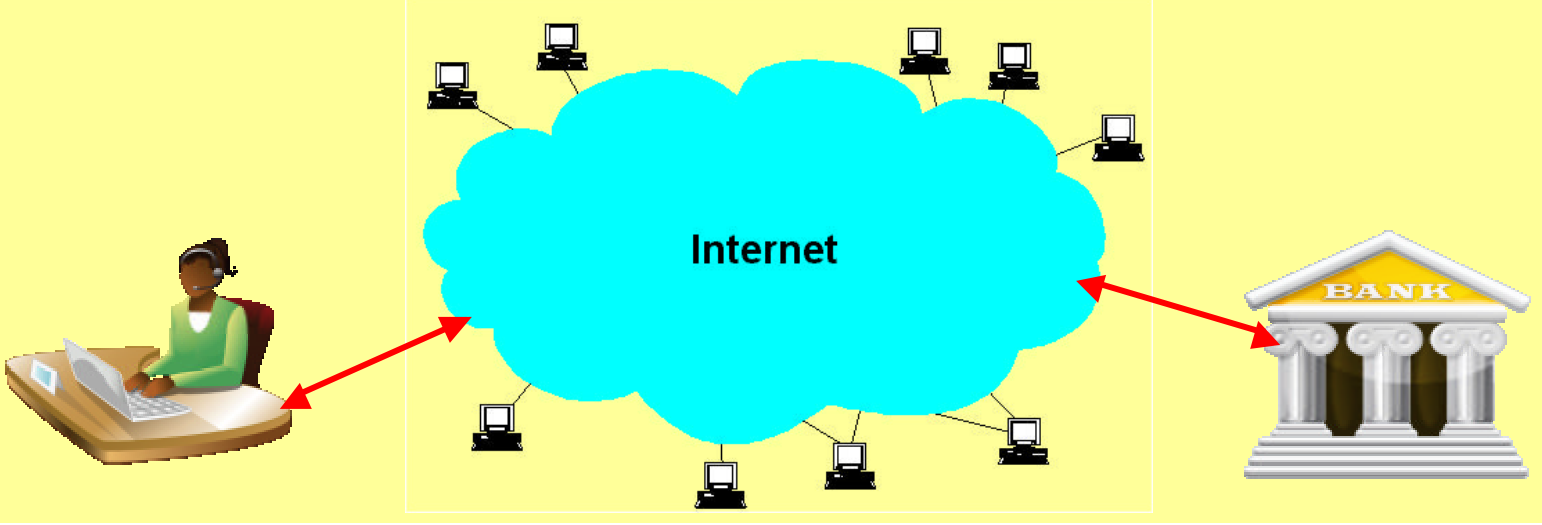
Wie funktioniert das Online-Banking

Kontoauszüge können nun eingesehen und meist auch downgeladen werden.



Wie funktioniert das Online-Banking

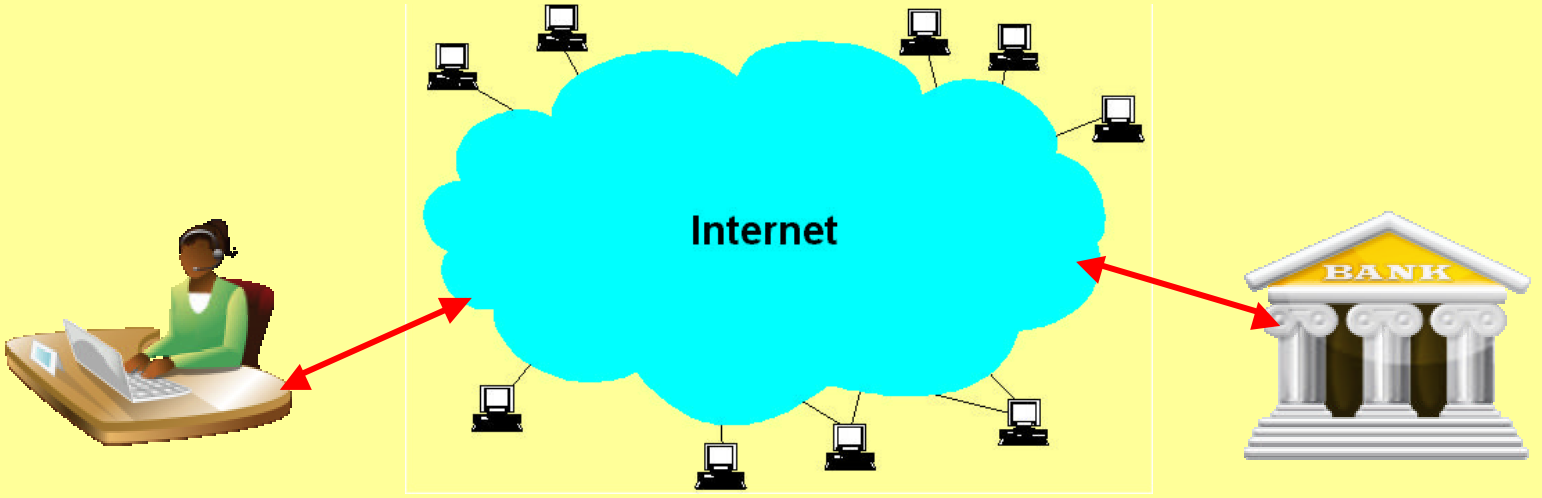
Jetzt können alle Bankgeschäfte getätigt werden



Wie funktioniert das Online-Banking

Überweisungen können am Rechner ausgefüllt und abgesendet werden.

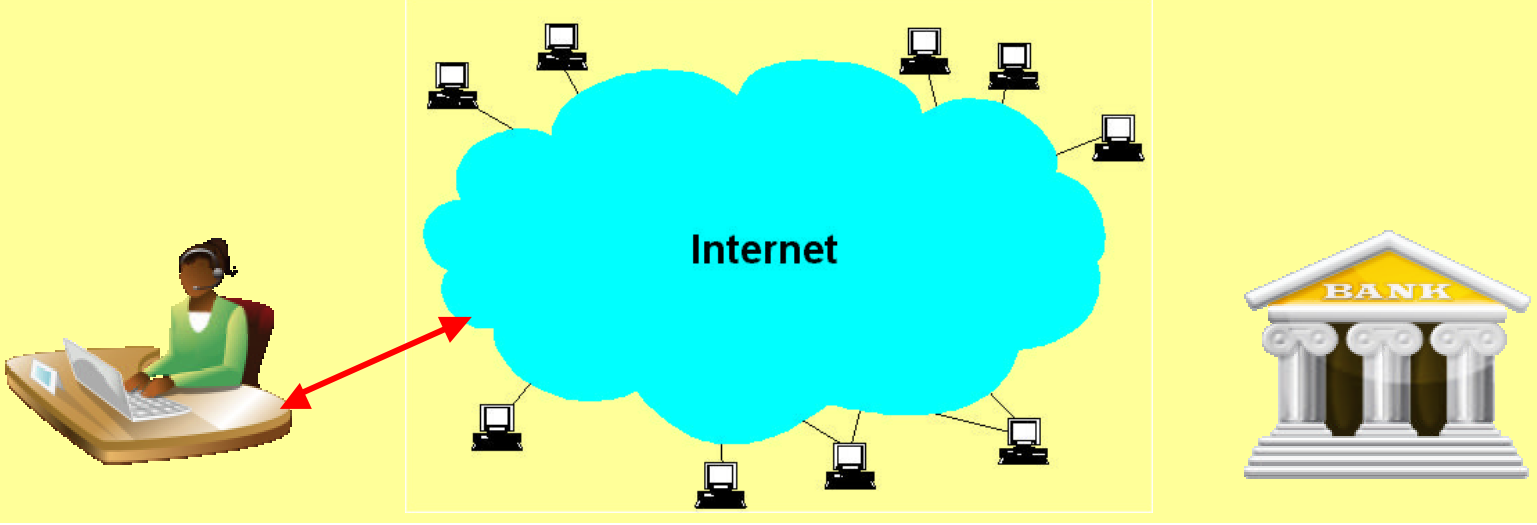
Die Bank fordert pro Überweisung auf, eine TAN einzugeben! Erst dann wird die Überweisung akzeptiert.



Wie funktioniert das Online-Banking

Wenn man fertig ist, sollte man sich unbedingt abmelden. Sonst kann ein Angreifer Ihre Sitzung übernehmen.

Das Bankmenü bietet immer ein Benden, Abmelden oder Logoff an!



TAN = TransAktionsNummer

- TAN = 1 TAN aus einer TAN-Liste selbst auswählen **(Veraltet & Gefählich)**
- iTAN = Die Bank fordert jedesmal eine bestimmte TAN per Index an
- eTAN = Ein elektronisches Zusatzgerät generiert eine TAN
- eTAN plus = Ein elektronisches Zusatzgerät generiert eine TAN unter Berücksichtigung von Summe und Zielkontonummer
- mTAN = Per SMS wird eine TAN von der Bank auf das Handy geschickt zusätzlich wird die Zielkontonummer und die Summe aus der Überweisung mitübermittelt

Wo werden TAN‘s benötigt?

Überweisungen, Daueraufträgen, Änderung wichtiger Daten, Anforderung einer neuen TAN-Liste, Änderungen der Überweisungslimits, usw.

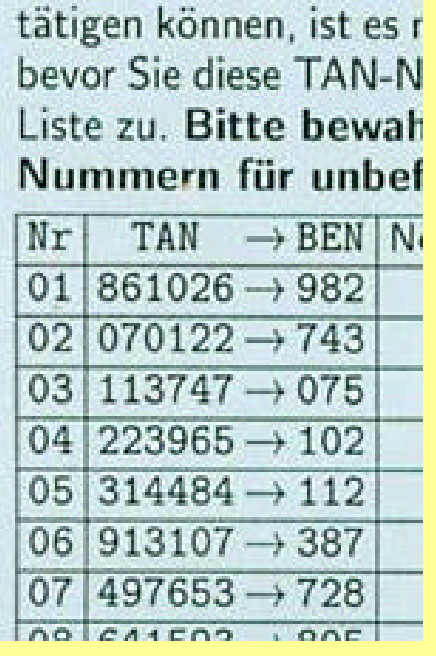
iTAN

Verfahren: Der Kunde erhält von seiner Bank eine persönliche Identifikationsnummer (Pin) und eine Liste mit fortlaufend nummerierten Transaktionsnummern (Tan). Der Name iTan steht für die indizierte Tan-Liste. Wenn der Kunde eine Überweisung freigeben will, nennt ihm die Bank nach dem Zufallsprinzip einen Platz auf der Liste. Die dazugehörige Tan muss der Kunde eingeben. So ist der Auftrag fest mit dieser Tan verknüpft.

Vorteil: **Phishing** funktioniert nicht mehr. Ein Betrüger, der einen eigenen Auftrag ausführen will, muss dazu die von der Bank verlangte iTan kennen. Eine andere Tan, die er abgefangen hat, nützt ihm nichts.

Nachteil: Wenn ein Betrüger mehrere Tan erbeutet, kann er zufällig auch die passende Tan kennen, mit der er dann das Konto plündern kann. Trojanerangriffe und Pharming sind weiterhin möglich.

Bild: iTan-Liste der 1822direkt.



tätigen können, ist es r
bevor Sie diese TAN-N
Liste zu. **Bitte bewah**
Nummern für unbef

Nr	TAN → BEN	N
01	861026 → 982	
02	070122 → 743	
03	113747 → 075	
04	223965 → 102	
05	314484 → 112	
06	913107 → 387	
07	497653 → 728	

eTAN

Verfahren: Der Bankkunde bekommt von seiner Bank eine persönliche Identifikationsnummer (Pin) und ein elektronisches Gerät, den Tan-Generator. Er ist nicht größer als ein kleiner Taschenrechner.

Wenn der Kunde zum Beispiel Geld überweisen will, erzeugt der Bankcomputer eine Kontrollnummer. Diese Ziffern gibt der Kunde in den eTan-Generator ein und erhält eine Antwortnummer. Mit dieser eTan kann der Kunde die Überweisung bestätigen.

Vorteil: **Phishing** funktioniert nicht mehr, weil die Tan erst im Rahmen des Auftrags erzeugt wird.

Nachteil: Der Nutzer muss das Gerät immer bei sich haben. Trojanerangriffe und Pharming sind weiterhin möglich.

Bild: eTan-Generator der GE Money Bank.

eTAN plus

Verfahren: Der Kunde bekommt von seiner Bank eine persönliche Identifikationsnummer, einen von seinem Computer unabhängigen Taschenkartenleser und eine Bankkundenkarte mit Chip. Für eine Überweisung steckt der Kunde die Bankkarte in den Kartenleser, gibt über dessen Tastatur den auf der Überweisungsseite angezeigten Bankcode ein. Danach zeigt das Display eine Tan-Nummer, die der Kunde zur Freigabe der Überweisung in den PC eingibt. Die eTan plus wird aus den Transaktionsdaten und einem geheimen Schlüssel in der Karte berechnet.

Vorteil: **Phishing, Trojanerangriffe und Pharming** funktionieren nicht mehr, weil die Tan von den Daten der Transaktion abhängig ist.

Nachteil: Der Nutzer muss den Kartenleser immer bei sich haben.

Bild: Tan-Box der Wüstenrot Bank.

mTAN

Verfahren: Für die Autorisierung von Aufträgen bieten einige Banken zusätzlich zu anderen Verfahren das Versenden von Transaktionsnummern (Tan) auf ein Handy an. Daher der Name mobile Tan oder kurz mTan. Der Kunde muss sich bei der Bank dafür anmelden. Dabei legt er fest, auf welche Mobilfunknummer die Bank die Tan schicken soll. Hat er die Anmeldung abgeschlossen, bekommt er per Kurzmitteilung (SMS) eine Bestätigung.

Für eine Überweisung klickt der Kunde die Funktion mobile Tan an und erhält wenige Sekunden später eine SMS mit einer Tan auf das angemeldete Handy.

Vorteil: **Phishing, Trojaner und Pharming** können nichts mehr ausrichten, weil die mobile Tan ausschließlich für die in der SMS wiederholte Empfängerkontonummer und den Betrag gültig ist.

Nachteil: Das Handy muss dabei und empfangsbereit sein. Die SMS ist oft kostenpflichtig.

Bild: SMS der Postbank mit mTan.

Sicherheit beim Online-Banking

Neuestes Angebot der Postbank

Die mTAN besteht nicht nur aus Ziffern, sondern enthält Textzeichen.

HBCI

Verfahren: HBCI (Home Banking Computer Interface) ist mit Diskette und Chipkarte möglich. Das Verfahren mit Chipkarte gilt nach derzeitigem Stand der Technik als das sicherste Onlinebanking-Verfahren. Der Bankkunde braucht die HBCI-Software, eine Chipkarte und einen Kartenleser. Zur Autorisierung einer Überweisung steckt er die Karte in das Lesegerät und gibt die Karten-Pin ein. Die Karte versieht die Transaktion mit einer elektronischen Signatur. Das Lesegerät muss der Nutzer meist bezahlen. Je nach Bauart kostet es zwischen 20 und 120 Euro. Hat das Lesegerät eine eigene Tastatur, kann der Betrüger die Eingaben nicht mit einem Programm mitlesen.

Vorteil: **Phishing, Virenangriffe und Pharming** sind nicht mehr möglich.

Nachteil: Onlinebanking ist nur von einem PC möglich, an den ein Kartenleser angeschlossen ist.

Bild: HBCI-Chipkartenleser und Chipkarte der SEB.

Wo gibt es grosse Gefahren und was sollte man auf keinen Fall tun?

Phishing

Das Kunstwort Phishing setzt sich aus „password“ und „fishing“ zusammen. Gauner versuchen mithilfe von gefälschten E-Mails an vertrauliche Daten zu gelangen. Sie verschicken massenhaft E-Mails, die wie vertraute Nachrichten von einer Bank aussehen. Die Mails enthalten Felder, in die der Empfänger seine persönliche Geheimnummer (Pin) und Transaktionsnummern (Tan) eingeben soll. Oder sie enthalten einen Link, der auf einen falschen Webserver führt. Der Bankkunde landet dann nicht bei seiner Hausbank, sondern auf einer nachgemachten Webseite, die der echten täuschend ähnlich sieht.

Pharming

Beim Pharming ersetzt der Betrüger die Webadresse der Bank durch seine eigene und täuscht eine sichere Verbindung vor. Selbst wenn das Opfer sehr vorsichtig ist und die Adresse selbst eingibt, landet es ahnungslos auf der gefälschten Seite. Alle Daten, die der Verbraucher abschickt, gelangen so zum Betrüger. Verbraucher erkennen die Attacke oft erst, wenn Geld vom Konto abgebucht wurde. Sie könnten die Echtheit einer Webseite nur anhand ihres Zertifikats prüfen.

Pharming ist auch unter dem Begriff DNS-Spoofing bekannt und bisher kaum verbreitet. Pharming ist die Weiterentwicklung des Phishing.

Wo gibt es grosse Gefahren und was sollte man auf keinen Fall tun?

Spyware

Spyware oder Schnüffelsoftware sind Programme, die Informationen über PC-Nutzer wie persönliche Daten und Surfgewohnheiten ohne Wissen des Nutzers ausspionieren und an Dritte weiterleiten, wenn der PC online ist. Spyware wird von den gängigen Antivirenschutz-programmen erkannt, wenn sie auf dem neuesten Stand sind.

Viren

Viren sind kleine Programme, die sich selbst vervielfältigen können und sich an andere Programme, Dateien oder auch E-Mails hängen, die der Nutzer aus dem Internet lädt oder von anderen Nutzern bekommt. Viren versuchen den Ablauf des Computerbetriebs zu stören oder Spyware zu installieren.

Wo gibt es grosse Gefahren und was sollte man auf keinen Fall tun?

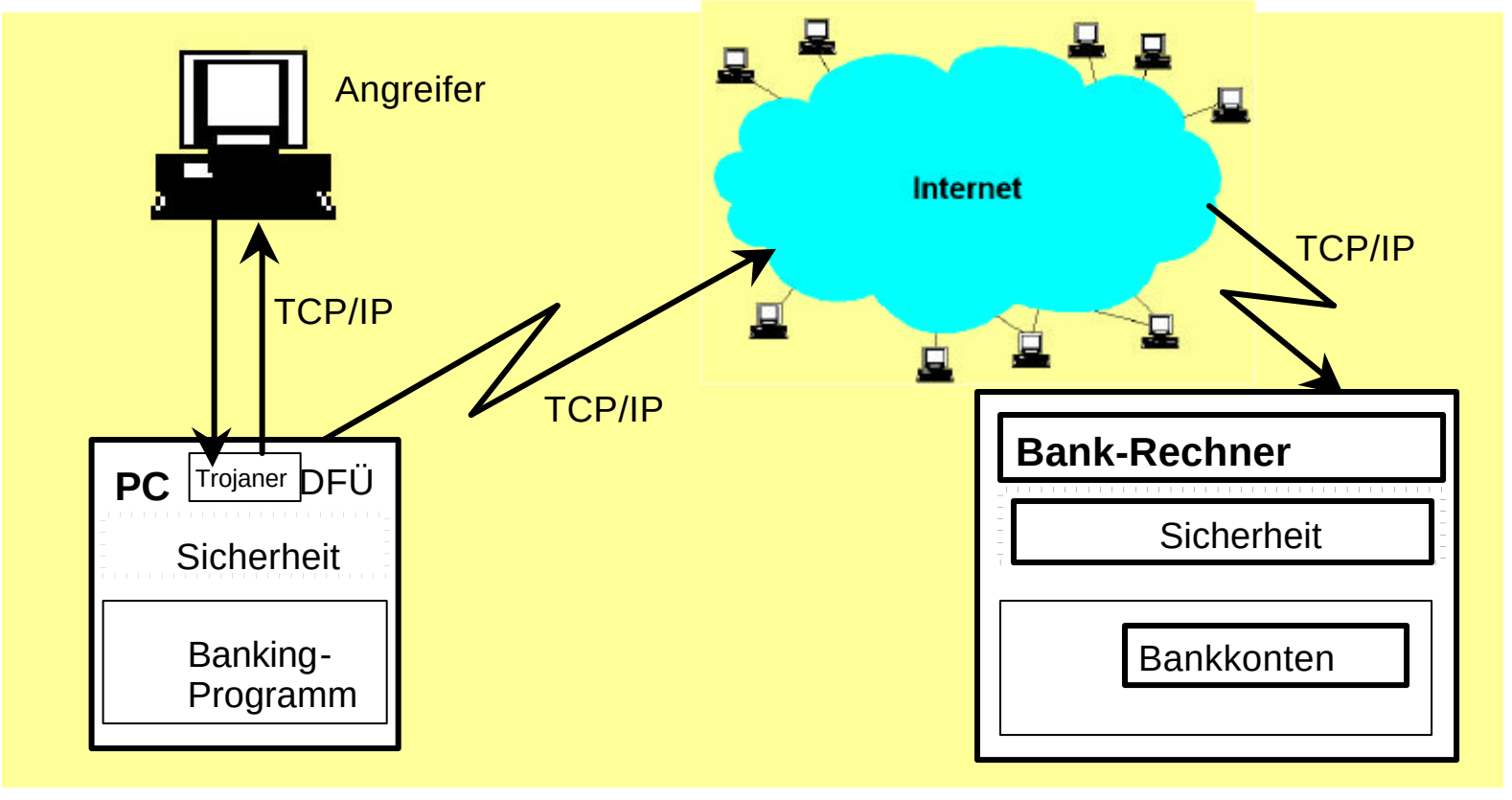
Trojaner

Schädigende Programme, die als nützlich getarnt sind oder mit einem nützlichen Programmen zusammen verbreitet werden, heißen Trojaner. Sie können auf dem PC unerwünschte Aktionen ausführen und dabei unter anderem persönliche Geheimnummern (Pin) und Transaktionsnummern (Tan) abfangen und an den Besitzer des Trojaners senden. Die meisten dieser Schadprogramme werden von Virenschutzsoftware entdeckt. Trojaner spielen auch eine Rolle bei

Man in the middle

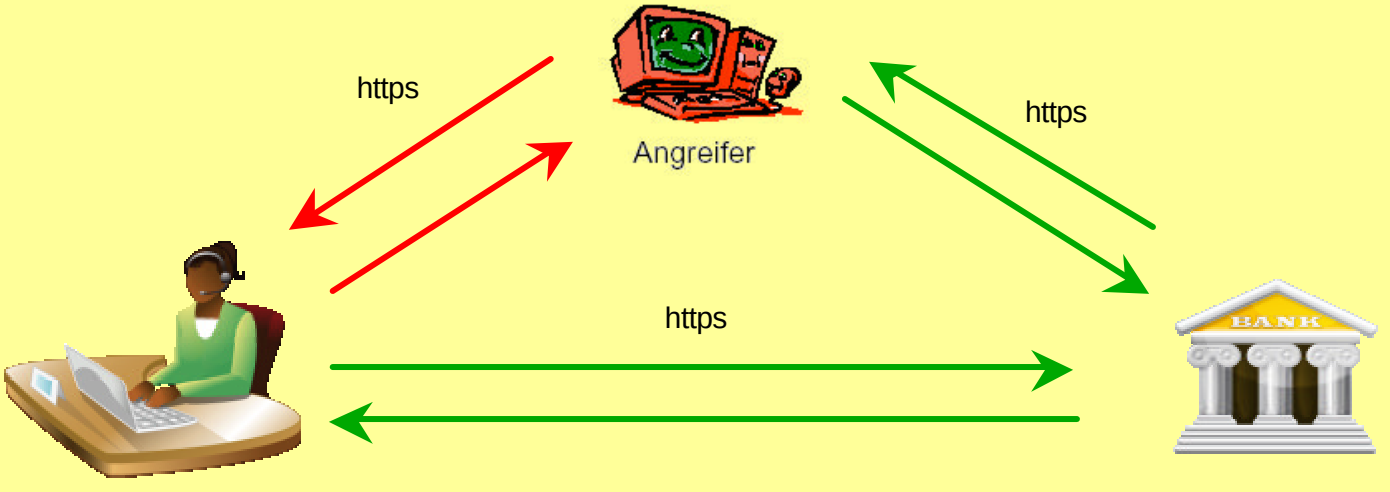
Bei „Man in the middle“ leitet ein Trojaner die Verbindung zur Bank um zu einem Agenten, der dann z.B: Überweisungen fälscht (eine grössere Summe auf ein fremdes Konto) und zur echten Bank weiter sendet. Dies wird verhindert bei eTAN plus, MTAN und HBCI, da die TAN‘s dann abhängig sind von Zielkonto und Überweisungssumme.

Sicherheit beim Online-Banking



Grundsätzliches zu „Man in the middle“

Sicherheit beim Online-Banking



Authentizität (Authentication) = Zertifikat

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!)**

Sicherheit beim Online-Banking

Wechselplatten

SATA-Platte

in

ICY BOX

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

Jedes Handy ist ein Hackertool

Chip 10/2009

WWW.tu-berlin.de

Jedes Handy ist ein Hackertool

Mit einer SMS-Nachricht können Angreifer **SMS ABHÖREN UND GERÄTE LAHMLEGEN** – ohne dass Sie als Besitzer etwas dagegen machen können

VON FABIAN VON KEUDELL

Die Deutschen verschicken jährlich rund 29 Milliarden SMS-Nachrichten – und jede einzelne könnte ihr Handy lahmlegen. Die Sicherheitsexperten Collin Mulliner und Charlie Miller haben herausgefunden, wie sie mithilfe von simplen SMS-Mitteilungen Steuerbefehle an Mobiltelefone schicken und damit die Kontrolle über die Geräte übernehmen können.

Betroffen sind nahezu alle Modelle. Bei herkömmlichen Handys können die Angreifer eine gefälschte Betreiber-SMS an die Geräte schicken, mit der sie etwa die WAP-Konfiguration der Opfergeräte ändern – ohne dass die Besitzer etwas davon mitbekommen. Künftig läuft jeder Datenverkehr über die Hackerserver. Der Hintergrund: Konfigurations-SMS kann normalerweise nur der Netzbetreiber selbst schicken. Die Hacker verwenden dafür einfach eine entsprechende Provider-Absenderkennung. Die Absendernummern kontrollieren die Netze nur bei MMS-Nachrichten, nicht aber bei SMS.

Bei Apples iPhone können Angreifer den CommBoard-Prozess, also die Kommunikationszentrale, zum Absturz bringen. Dadurch unterbricht das Telefon das aktuelle Gespräch, verliert den Netzzugriff und ist für rund 10 Sekunden nicht erreichbar. Wenn die Angreifer allerdings mehrere Hundert SMS schicken, ist das Telefon für Stunden oder gar Tage blockiert. Bei Android-Geräten ist die Schwachstelle das Telefonmodul com.android.phone. Bringen die Hacker dieses zum Absturz, unterbricht das aktuelle Telefonat und der User muss die PIN der SIM-Karte neu eingeben.

Noch schlimmer trifft es Windows-Mobile-Geräte. Hier stürzt das gesamte Handy ab und ist nicht mehr startbar. Erst wenn die Hacker-SMS aus dem Posteingang gelöscht ist, lässt sich das Handy wieder starten. Doch dafür müssen die Opfer die SIM-Karte in ein zweites Mobiltelefon einlegen. Sind Hunderte Hacker-SMS auf den Providerservern mit einem Zeitplan versehen, etwa eine SMS pro Tag, ist das Windows-Mobile-Gerät überhaupt nicht mehr zu gebrauchen.

Zusammen stark: Hilfe kommt von Provider und Hersteller

Einen Patch für die Smartphones bieten bislang nur Apple und Google. Gerade bei den anfälligsten Windows-Mobile-Geräten steht ein Fix noch aus. Bei den normalen Handys arbeiten die großen Provider in Deutschland momentan an einer Möglichkeit, die Absenderkennungen jeder SMS zu verifizieren. Aber auch hier gibt es bislang noch keinen Erfolg. Im Durchschnitt dauert es rund fünf Monate, bis eine so tiefgreifende Lücke im Handynetz beseitigt ist. Bis es so weit ist, überwachen die Provider verstärkt die Handynetze und suchen gezielt nach merkwürdigen SMS-Nachrichten.

INFO: www.tu-berlin.de

Einfallstor Handy Über eine einfache SMS können Hacker Handydaten umleiten oder das Gerät komplett zum Absturz bringen

Sicherheit beim Online-Banking

http://www.handelsblatt.com/technologie/it-internet/schadsoftware-unterwegs-gezielter-angriff-mit-schaedlichen-pdf-dateien;2507218

Handelsblatt

Gezielter Angriff mit schädlichen PDF-Dateien

Eine bekannte Sicherheitslücke in Adobe Reader und Adobe Acrobat ist seit dem Jahreswechsel Ziel einer Attacke mit schädlichen PDF-Dateien. Weder auf Anti-Viren-Software noch auf Adobe sollten sich Anwender derzeit verlassen.

von Andreas Sebayang (golem.de)

BERLIN. Derzeit sollen besonders ausgefeilte Angriffe mit PDF-Dateien im Umlauf sein, berichtet das Internet Storm Center (ISC). Die PDF-Dateien nutzen eine bekannte Sicherheitslücke in Addes PDF-Produkten Reader und Acrobat aus. Diese Angriffe kommen zusätzlich zu den ohnehin schon im Umlauf befindlichen schädlichen PDF-Dateien.

Der Angriff, der anscheinend rund um den Jahreswechsel in Umlauf gebracht wurde, soll verschiedene Stufen haben. Auf den ersten Blick soll der vom ISC analysierte Shellcode der ersten Stufe so aus, als sei er harmlos. Von der ersten Stufe aus wird die zweite Stufe gezündet. Diese öffnet die PDF-Datei direkt. In der PDF-Datei befinden sich gleich zwei schädliche Dateien.

Die erste Datei, svchost.exe, ist die eigentliche Schadsoftware. Die zweite Datei, temp.exe, hinterlässt auf dem Rechner eine harmlose PDF-Datei namens baby.pdf, um den Angriff nicht zu offensichtlich erscheinen zu lassen. Wenn der Angreifer nämlich die Angriffs-PDF-Datei öffnet, stürzt die PDF-Software ab und das Opfer könnte misstrauisch werden. Um das zu verhindern, öffnet temp.exe die harmlose Datei mit dem Namen baby.pdf - eine einfache leere Tabelle, die von einem Excel-Dokument erstellt wurde.

Das ist ein enormer Aufwand, um einen Rechner anzugreifen. Offensichtlich sind Angreifer auch bereit, die PDF-Angriffe den Opfern entsprechend anzupassen. Nutzer von Adobe Software sollten zumindest Javascript im Reader und bei Acrobat deaktivieren. Laut ISC nimmt die Anzahl der Angriffsvarianten derzeit zu, die die PDF-Sicherheitslücke ausnutzen.

Eigenen Bekundungen zufolge will Adobe am 12. Januar 2010 das PDF-Sicherheitsproblem beheben. In der Zwischenzeit empfiehlt es sich, bei unerwarteten PDF-Dateien besonders vorsichtig zu sein. Laut dem ISC erkannten zum Jahreswechsel gerade einmal sechs von 40 Virenscannern den Angriff.

Der Rest wurde ein PDF dieser Machart zunächst durchlassen. Die svchost.exe erkannte immerhin die Hälfte aller Virenscanner. Möglicherweise hat sich die Erkennungsrate in den letzten Tagen verbessert. Prinzipiell besteht aber auch die Möglichkeit, dass die Angriffsdatei in der PDF-Datei durch andere Lücken eingeschleust wird. Letztendlich fungiert die PDF-Datei hier nur als sehr ausgefeilter Träger des eigentlichen Angriffs.

Wer ein verdächtiges PDF-Dokument öffnen oder grundsätzlich auf Nummer sicher gehen möchte, sollte auf einen alternativen PDF-Reader wechseln. Unter Windows gibt es mit Sumatra PDF ein besonders schlankes PDF-Anzeigeprogramm, das allerdings nur Grundfunktionen bietet. Weitere Alternativen sind der PDF X-Change Reader und der Foxit Reader.

Bezahlverfahren im Internet

- Per Mastercard
- Direkt vom Konto
- Vorkasse
- eBay-Bank
- PayPal
- ClickandBuy
- Geldkarte
- T-Pay
- Sofort: Überweisung.de

Dieses Thema füllt vermutlich einen weiteren Abend

Tipp zu Bezahlverfahren im Internet

- Dokumentieren Sie den Vorgang der Bestellung
- und Dokumentieren Sie den Vorgang der Bezahlung

Dazu rufen Sie z.B. Word auf,
drücken pro Bildschirm Seite die Tasten Strg&Print (Drucken),
dann fügen Sie diesen Bildschirmabdruck in Ihr Worddokument ein.
Speichern Sie dieses Worddokument z.B. in einem Ordner „Einkaufen“
mit Namen das Einkaufdatum und ein Stichwort.
Alte Worddokumente können Sie, wenn alles gutgegangen ist nach z.B. einem Jahr wieder löschen!

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 gesetzlichen 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 ausdrücklich zum Haftungsmaßstab erhebt, die Schadensübernahme von einer Strafanzeige des Kunden abhängig macht oder die Haftung für Schäden aus undeutlichen Aufträgen dem Kunden auferlegt.

Si

Bankautomat

Sicherheit beim Online-Banking

- PIN = Persönliche Identifikationsnummer
- TAN = Transaktionsnummer
- iTAN = indizierte TAN
- eTAN = elektronik TAN
- eTANplus = verbessertes eTAN
- mTAN = mobile TAN
- 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)

„Publikationen“

- Der Bankenverband hat verschiedene Publikationen zum Thema ***Sicherheit*** im ***Online Banking*** zusammengestellt **http://www.bankenverband.de/index.asp?channel=161010**
- Checklisten und Anleitungen der **Schweizerbank MELANI** **http://www.melani.admin.ch/dienstleistungen/00132/index.html?lang=de**

„Ratgeber“

- 17. Sept. 2009 **...** Die **PC-WELT** zeigt welche Gefahren beim ***Online-Banking*** lauern und wie Sie die Risiken minimieren. **http://www.pcwelt.de/start/sicherheit/sonstiges/news/69148/immer_noch_zu_wenig_sicherheit_beim_online_banking/**
- **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.**

Sicherheit beim Online-Banking

„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

„Vortragsfolien zum Thema Sicherheit“

- **Vortrag "Wie sicher ist Online-Banking?"** Mark Semmler
  https://www.mark-semmler.de/papers-und-vortraege-zu-themen-der-it-sicherheit/downloads/vortrag_livehacking_online-banking_081201.pdf
- **Vortrag „So viel Schutz muss sein!"** Mark Semmler
  https://www.mark-semmler.de/papers-und-vortraege-zu-themen-der-it-sicherheit/downloads/vortrag_so-viel-schutz-muss-sein_081201.pdf
- **Vortrag "Blockieren Sie diese Netzwerke"** Mark Semmler
  https://www.mark-semmler.de/papers-und-vortraege-zu-themen-der-it-sicherheit/downloads/vortrag_block_these_networks_081201.pdf

Sicherheit beim Online-Banking

- **c‘t Heft 19 2009**
  Heise Verlag
  www.ctmagazin.de
  3,50 €

Beim Bezahlen im Internet wird man leicht mehr Geld los als beabsichtigt. Nicht weil dort alles teuer ist, sondern weil Kriminelle mit Phishing-Seiten und Schadprogrammen darauf lauern, Konten leerzuräumen. Doch Gegenwehr ist möglich.

Literaturangaben

Sicherheit beim Online-Banking

- **c‘t kompakt Security**
  Heise Verlag
  www.ctspecial.de
  8,90 €

Online-Banking

Trotz zahlreicher Angriffe kann man im Internet seine Bankgeschäfte ohne Gefahr erledigen, sofern man einige Tipps beherzigt. Die Chipkarte als Ausweis beim Online-Banking erhöht die Sicherheit noch, doch die Banken spielen nur zögernd mit. Unsere Alternative heißt c't Bankix (auf der DVD), das gegen Manipulationen geschützt ist.

Literaturangaben

Weitere interessante Vortragsthemen:

- Bezahlverfahren im Internet
- Warten anderer Rechner über das Internet mittels VPN

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

Ab 20.1.2010 findet an der VHS-Neubiberg-Ottobrunn ein Kurs statt zu dem Thema

Sicherheit beim Onlinebanking

dort wird das Thema an 2 Abenden = 6 Stunden natürlich viel umfassender behandelt und wir werden in Übungen auch eine c‘t Bankix CD erstellen!