

# Wie sicher ist Online-Banking?

Ein Überblick und aktuelle Handlungsempfehlungen

Dienstag, 11.08.2009

- Aus der Abteilung „Grundsätzliches“ -  
**Die Ziele des Angreifers**

## Warum wird Online-Banking angegriffen?

- Beim Online-Banking geht es um viel, viel Geld: die Infrastruktur wird von Millionen Benutzern verwendet und es werden in ihr Abermillionen kritischer Daten pro Stunde ausgetauscht.
- Die Aussichten sind deshalb für Angreifer viel versprechend. Hier kann ein Krimineller schnell viel Geld verdienen.
- Betrüger nehmen hohe Aufwände bzw. Anlaufinvestitionen in Kauf, um Online-Banking anzugreifen, weil es sich einfach lohnt!
- Nicht zuletzt: die Masse machts!  
Auch wenn ein Angriff in nur 0,5% aller Fälle erfolgreich ist, so kann er sich doch lohnen, wenn er nur oft genug durchgeführt wird.

## Wann hat ein Angreifer gewonnen?

- Heute gibt es eine Vielzahl von Angriffen gegen Online-Banking.
- Alle Angriffe lassen sich in zwei Kategorien unterteilen:
  - ✘ **Kategorie 1: Informationsdiebstahl**  
Der Angreifer klaut Informationen, um anschließend im Namen des Benutzers betrügerische Bankgeschäfte durchzuführen.
  - ✘ **Kategorie 2: Transaktionsmanipulation**  
Der Angreifer schiebt dem Benutzer betrügerische Transaktionen unter, die dieser (unwissentlich) legitimiert.

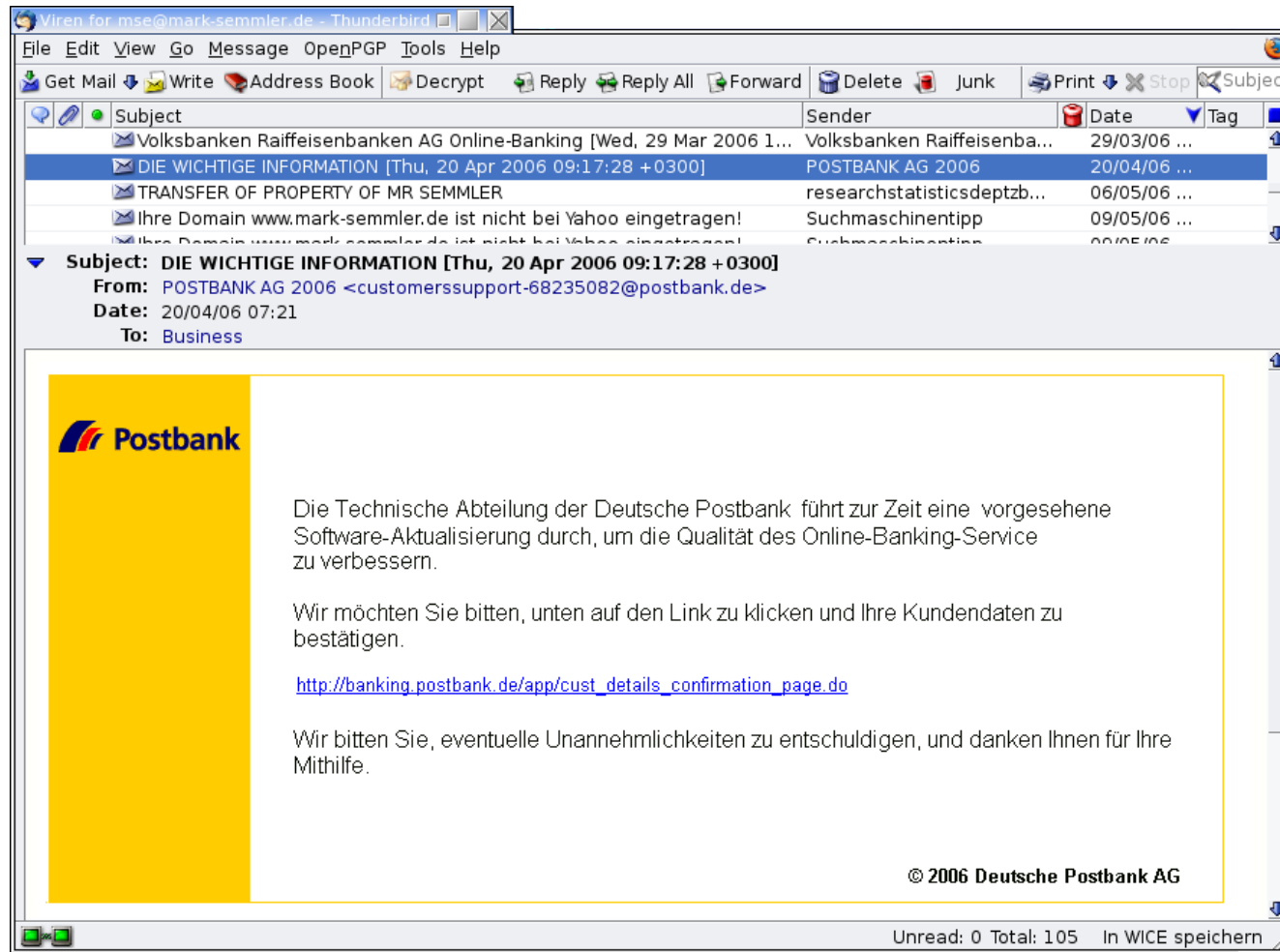


- Aus der Abteilung „Monster im Wald“ -  
**Welche Angriffe gibt es heute?**

## Phishing: Erschleichen von PIN und TAN via Mail

- Der Angreifer versendet Mails mit dem Layout einer Bank.
- Inhalt der Mail:  
"Loggen Sie sich auf dieser Webpage ein!"...  
...und eine abenteuerliche Begründung.
- Die in der Mail angegebene Webpage ist eine nahezu identische Kopie des Internetauftritts der Bank. Hier soll das Opfer nun seine Kontonummer, seine PIN und eine bzw. mehrere TANs eingeben.
- Der Betrüger nutzt die erschlichenen Informationen, um per Online-Banking das Konto des Opfers zu plündern.
- Ähnliches funktioniert natürlich auch mit ebay, paypal oder anderen Zugängen.

## Hier eine Phishing-Mail...



## ...und die dazugehörige Webseite

The screenshot shows the Postbank website interface. The top navigation bar includes links for Sitemap, Kontakt, FAQ, and Hilfe. A search bar is present on the right. The main content area features a security warning titled 'Vorsicht vor Betrügern!' with a 'Wichtiger Hinweis' about phishing and the use of mobile TANs. Below the warning is a login form with fields for Name, Familienname, Telefon-Nr., Kontonummer, PIN, TAN, and Geheimfrage. The left sidebar contains a menu with categories like 'Produkte & Preise', 'Online-Services', and 'Vermögensberatung'. The bottom right corner features a logo for 'Postbank ist nationaler Förderer der FIFA WM 2006™'.

## Pharming: Umleitung per DNS

- Der Angreifer versucht, die Namensauflösung des Opfers zu manipulieren, um Anfragen an falsche Server umzuleiten.
- Dies geschieht in der Regel durch die Manipulation der Datei „C:\WINDOWS\system32\drivers\etc\hosts“ oder der Einstellungen der DNS-Auflösung des angegriffenen Systems und wird durch eingeschleuste Schadsoftware durchgeführt.
- Folge: Die korrekte URL wird im Browser eingegeben, das Opfer landet jedoch auf dem Server des Angreifers.
- Nützlicher Nebeneffekt für den Angreifer: Updates der Virens Scanner bzw. von Windows werden verhindert (falsche Namensauflösung!)...
- Merke: Wer die DNS-Auflösung des Opfers manipulieren kann, hat (fast) gewonnen!

## Perfidere Methoden von Schadsoftware

- Mittlerweile haben die Programmierer von Schadsoftware eine ganze Reihe Ansatzpunkte implementiert, um die Datenströme zwischen Opfer und Bank zu unterbrechen, zu verfälschen oder umzulenken.
- Eine ganze Familie von Schädlingen ist mittlerweile bekannt, die verschiedene Angriffe implementiert (z.B. die Win32.Banker-Familie)
- Instrumente dieser Schadsoftware sind z.B.
  - ✗ Keylogger (Protokollieren von Tastatureingaben)
  - ✗ Unterbrechen und Umleiten von Datenströmen, wenn PIN und TAN eingegeben werden
  - ✗ automatische Manipulation von Eingaben beim Online-Banking
  - ✗ ...

- Aus der Abteilung „Das. Will. Ich. Haben!!!“ -

# Forderungen an sicheres Online-Banking

## Unsere Forderungen

- Authentizität der Geschäftspartner:  
Kunde und die Bank müssen sich fälschungssicher gegenseitig ausweisen.
- Transparenz der Transaktion:  
Der Kunde muss fälschungssicher sehen können, welche Transaktion er gerade legitimiert.
- Integrität der Transaktion:  
Die Transaktionsdaten dürfen niemals unbemerkt von einem Angreifer geändert werden können.
- All das muss selbst dann gewährleistet sein, wenn das System des Kunden komplett unter der Kontrolle des Angreifers steht.
- ...und alles muss bitte völlig narrensicher und einfach sein!

- Aus der Abteilung „Gute (?) alte (!) Zeit“ -  
**Online-Banking mit PIN & TAN**

## Wie funktioniert?

- Die Bank übersendet dem Kunden eine PIN und eine Liste von TANs.
- Die Persönliche Identifikationsnummer (PIN) ist eine nur einer oder wenigen Personen bekannte Zahl, mit der diese sich gegenüber der Webseite für das Online-Banking ausweisen können.
- Eine Transaktionsnummer (TAN) ist ein Einmalpasswort, das üblicherweise aus sechs Dezimalziffern besteht.
- Das Online-Banking wird bei TAN und PIN i.d.R. über den Browser des Kunden abgewickelt:  
Der Kunde loggt sich mit seinem PIN auf der Webseite der Bank ein und legitimiert die finanziellen Transaktionen mit einer TAN, die danach ungültig ist (Einmal-Gebrauch).

## Authentizität? Integrität? Transparenz?

- Authentizität:  
Wird PIN und eine beliebige TAN geklaut, kann der Angreifer sich als Kunde ausgeben. Gibt der Kunde nicht acht, so kann er auf gefälschte Webseiten umgeleitet werden und dem Angreifer unwissentlich PIN und TAN übergeben.
- Integrität & Transparenz:  
Der Kunde verlässt sich auf sein lokales System. Ist das von Schadsoftware unterwandert, hat der Kunde verloren – die Schadsoftware kann ihm Transaktion X anzeigen, seine PIN entgegen nehmen und Transaktion Y durchführen.

- Aus der Abteilung „Stahlwollschaf“ -  
**Sicherheit mit PIN & TAN**

## Grundsätzliches beim Einsatz von PIN & TAN (I)

- Gehen Sie verantwortungsvoll mit Ihrer PIN um!  
Geben Sie Ihre PIN ausschließlich beim Einloggen auf der Webseite des Online-Bankings ein. Geben Sie Ihre PIN niemals am Telefon, in Briefen, im persönlichen Gespräch oder im bei anderer Gelegenheit im Internet an Dritte weiter – egal wie gut das Argument Ihres Gegenübers ist oder mit wem auch immer Sie glauben, zu reden!
- Niemand, wirklich absolut niemand außer die Webseite des Online-Bankings hat ein berechtigtes Interesse an Ihrer PIN. Auch nicht der nette Bankangestellte, Polizist oder Kundenberater. Absolut Niemand!
- Schreiben Sie Ihre PIN nicht auf und speichern Sie Ihre PIN nirgends ab (z.B. auch nicht in Ihrem Handy).

## Grundsätzliches beim Einsatz von PIN & TAN (II)

- Gehen Sie verantwortungsvoll mit Ihren TANs um!  
Geben Sie Ihre TANs ausschließlich auf der Webseite des Online-Banking ein. Geben Sie eine TAN niemals am Telefon, in Briefen, im persönlichen Gespräch oder im bei anderer Gelegenheit im Internet an Dritte weiter – egal wie gut das Argument Ihres Gegenübers ist oder mit wem auch immer Sie glauben, zu reden!
- Niemand, wirklich absolut niemand außer die Webseite des Online-Bankings hat ein berechtigtes Interesse an Ihrer TAN. Auch nicht der nette Bankangestellte, Polizist oder Kundenberater. Niemand!
- Speichern Sie Ihre TANs in keinem Computersystem ab - auch nicht in Ihrem Handy, Ihrem Laptop oder PDA/MDA.
- Wenn Sie Ihre PIN irgendwo aufgeschrieben haben (das sollten Sie nicht!): heben Sie PIN und TAN unbedingt getrennt voneinander auf.

## Sicherheit beim Online-Banking: Rechner sichern!

- Führen Sie die grundsätzlichen Schutzmaßnahmen durch:
  - ✓ regelmäßige Backups
  - ✓ aktueller Anti-Virus
  - ✓ lokale Firewall
  - ✓ gute Passwörter
  - ✓ gesundes Misstrauen
  - ✓ ...
- Wer hier mehr wissen möchte, schaut in den Vortrag „So viel Schutz muss sein!“

## Sicherheit beim Online-Banking: Browser

- Die Browser-Sicherheit kann in diesem Vortrag nicht erschöpfend behandelt werden. Deshalb hier nur einige kurze Hinweise.
  - ✓ Verwenden Sie einen aktuellen Browser, der über sämtliche Updates verfügt.
  - ✓ Wechseln Sie den Internet-Explorer gegen einen alternativen Browser (z.B. Firefox oder Opera). Wenn Sie den Internet Explorer verwenden möchten oder müssen, dann bitte nur in der aktuellsten Version.
  - ✓ Installieren Sie zusätzliche Add-Ons für den Firefox, wie z.B. „NoScript“, um Ihre Sicherheit weiter zu erhöhen.
  - ✓ Löschen Sie nach dem Online-Banking den lokalen Cache des Browsers (geht bei Firefox z.B. auch automatisch).

## Sicherheit beim Online-Banking: Wer? Bist? Du?

- Vergewissern Sie sich, dass Sie tatsächlich auf der Webseite des Online-Bankings Ihrer Bank gelandet sind. Ihr Browser gibt Ihnen hier ganz eindeutig Auskunft:
  - ✓ Die Adresse muss mit dem Begriff „https://“ beginnen.
  - ✓ Der Verbindungsaufbau muss fehlerfrei geschehen sein.
  - ✓ Neben der Adresszeile muss ein geschlossenes Schloss zu sehen sein.
  - ✓ Die Adresszeile muss golden oder grün hinterlegt sein.
- Wenn auch nur eine der oben genannten Bedingungen nicht erfüllt ist: WEG HIER! Irgendetwas stimmt nicht!

## Abschließend ein sehr offenes Wort...

- Vergessen Sie PIN und TAN! Es existieren Angriffe, die dieses System überwinden. Wechseln Sie auf ein anderes Verfahren.
- Wenn dies nicht möglich ist:
  - ✓ Begrenzen Sie bei Ihrer Bank das Limit für Online-Überweisungen pro Tag und Woche.
  - ✓ Lassen Sie sich von Ihrer Bank eine Haftungsübernahme bestätigen: Die Bank soll für alle Schäden haften.
  - ✓ Kontrollieren Sie Ihre Kontoauszüge zeitnah.
  - ✓ Besser: Verlassen Sie Ihre rückständige Bank und gehen Sie zu einem modernen Geldinstitut!

- Aus der Abteilung „Gammel bleibt Gammel“ -  
**Das iTAN-Verfahren**

## Wie funktioniert?

- Die Bank übersendet dem Kunden eine PIN und eine Liste von TANs.
- Die Persönliche Identifikationsnummer (PIN) ist eine nur einer oder wenigen Personen bekannte Zahl, mit der diese sich gegenüber der Webseite für das Online-Banking ausweisen können.
- Eine Transaktionsnummer (TAN) ist ein Einmalpasswort, das üblicherweise aus sechs Dezimalziffern besteht.
- Das Online-Banking wird bei TAN und PIN i.d.R. über den Browser des Kunden abgewickelt:  
Der Kunde loggt sich mit seinem PIN auf der Webseite der Bank ein und legitimiert die finanziellen Transaktionen mit einer TAN, die danach ungültig ist (Einmal-Gebrauch).
- Im Vergleich mit PIN und TAN hat sich nur eines geändert:  
Die TANs sind nun nummeriert (iTAN = Indiziertes TAN) und die Bank fordert bei jeder Transaktion die Eingabe einer spezifischen TAN.

## Welche Vorteile bringt's?

- Das iTAN-Verfahren ist vor allem als Maßnahme gegen Phishing entwickelt worden.
- Ein Angreifer muss sowohl die PIN als auch die gesamten (noch gültigen) TANs eines Opfers kennen, um mit Sicherheit eine Transaktion durchführen zu können.
- Über normales Phishing kann man nur sehr wenige Opfer dazu bringen, eine gesamte iTAN-Liste einzugeben.
- Besitzt ein Angreifer nur eine iTAN des Opfers, so reduziert sich die Wahrscheinlichkeit eines erfolgreichen Angriffs sehr deutlich.

## Welche Nachteile hat's?

- Der Benutzer muss die gesamte iTAN-Liste mit sich führen, wenn er (z.B. von unterwegs oder im Urlaub) Bankgeschäfte durchführen möchte.
- iTAN-Listen werden deshalb häufig in elektronische Medien (Handy, PDA, Blackberry, Laptop, ...) übertragen.

## Authentizität? Integrität? Transparenz?

- Authentizität:  
Wird PIN und eine beliebige TAN geklaut, kann der Angreifer sich nur noch sehr schwer als Kunde ausgeben. Gibt der Kunde nicht acht, so kann er auf gefälschte Webseiten umgeleitet werden.
- Integrität & Transparenz:  
Der Kunde verlässt sich auf sein lokales System. Ist das von Schadsoftware unterwandert, hat der Kunde verloren – die Schadsoftware kann ihm Transaktion X anzeigen, seine PIN entgegen nehmen und Transaktion Y durchführen.

- Aus der Abteilung „Stahlwollschaf+“ -  
**Sicherheit mit PIN & iTAN**

## Schutz für das iTAN-Verfahren

- Prinzipiell gelten alle Sicherheitsmaßnahmen wie beim Gebrauch von PIN und TAN.
- Zusätzlich gilt:  
Übertragen Sie iTAN-Listen niemals in mobile Endgeräte.

## Auch hier ein offenes Wort

- Das iTAN-Verfahren stellt für Kriminelle kein Problem mehr dar, erklärte Mirko Manske, Kriminalhauptkommissar im Bundeskriminalamt (BKA) auf dem 11. IT-Sicherheitskongress des Bundesamts für Sicherheit in der Informationstechnik in Bonn. Zwar seien Phishing-Angriffe mit iTAN schwieriger geworden, so Manske "aber nicht unmöglich".
- Bereits Ende 2005 hatte eine Arbeitsgruppe der Ruhr-Universität Bochum einen Angriff auf das Online-Banking Verfahren mit indizierten TANs erfolgreich demonstriert.
- Anfang 2007 tauchten dann erste Phishing-Kits auf, die in der Lage waren, per Man-in-the-Middle-Attacke abgephischte iTANs in Echtzeit für eigene Transaktionen zu benutzen.
- Quelle: heise online vom 18.05.2009

- Aus der Abteilung „Elektronisches Fort?“ -  
**HBCI mit Chipkarte**

## Was ist's und wie funktioniert's?

- HBCI steht für Home Banking Computer Interface. Es ist ein offener Standard für Homebanking, der verschiedene Arten von Online-Banking Verfahren unterstützt (unter anderem auch PIN und TAN!).
- HBCI mit PIN und TAN lassen wir außen vor. Hier gelten genau die gleichen Einschränkungen wie bei PIN und TAN ohne HBCI.  
**Nicht verwenden!**
- Ebenfalls außen vor: HCI mit Schlüssel auf Diskette.  
**Nicht verwenden!.**
- Aktuelles HBCI funktioniert wie folgt: Der Kunde besitzt eine Chipkarte, auf der ein Schlüssel gespeichert ist. Der Kunde muss die Chipkarte mit einer einer PIN-Nummer freischalten und die Transaktion wird dann mit Hilfe des Schlüssels legitimiert.

## Welche Vorteile bringt HBCI mit Chipkarte?

- Ein Angreifer muss die PIN kennen und zugleich Zugriff auf den Schlüssel besitzen, um illegale Transaktionen durchführen zu können.
- Da der Kartenleser vom Rest des Systems getrennt ist (und mit diesem nur über eine definierte Schnittstelle mit wenigen Funktionen kommuniziert, kann er von Schadsoftware nicht angegriffen werden.
- Das Authentifizierungsmerkmal (der Schlüssel) kann die Chipkarte nicht verlassen – ist also vor dem Ausspähen sicher.
- Ein Angreifer muss die PIN kennen und gleichzeitig Zugriff auf die Chipkarte besitzen, um eine illegale Transaktion durchführen zu können.

## HBCI mit dummem Kartenleser: Igitt!

- Wie sicher HBCI mit Chipkarte ist, hängt stark vom Kartenleser ab, der eingesetzt wird!
- Absolut unsicher: „Dummer Chipkartenleser“:  
Eine Schadsoftware kann z.B. die PIN des Benutzers ausspähen (Eingabe über die Tastatur des Rechners!) und dann der Chipkarte beliebige Transaktionen zur „Unterschrift“ vorlegen.



## HBCI mit Klasse-2-Kartenleser: gut, nicht optimal

- Klasse-2-Kartenleser besitzen eine eigene Tastatur und unterstützen die sichere Eingabe der PIN-Nummer
- Die Eingaben über die Tastatur des Kartenlesers verlassen niemals das Gerät.
- Ein Schlupfloch bleibt aber:  
Eine Schadsoftware kann die originale Transaktion abfangen, bevor die das Lesegerät erreicht und gegen eine illegale Transaktion ersetzen.
- Problem:  
Der Benutzer sieht nicht, welche Transaktion er legitimiert...



## HBCI mit Klasse-3-Kartenleser: Super sicher!

- Kartenleser der Klasse 3 zeichnen sich dadurch aus, dass sie ein autonomes Display besitzen.
- Das Display kann unabhängig vom PC betrieben werden und zeigt z.B. die Transaktion vor der Freigabe an.
- Wichtig:  
Die Online-Banking-Software muss Klasse-3-Geräte voll unterstützen und die Features des Geräts auch nutzen!



## Welche Nachteile hat HBCI mit Kartenleser?

- Der Kartenleser kostet Geld (die Banken sind plötzlich taub, wenn man als Kunde den Kartenleser umsonst bekommen möchte...).
- Der Benutzer muss den Chipkartenleser und ggf. spezielle Software mit sich führen, um Online-Banking nutzen zu können.

- Aus der Abteilung „Autonome Wege“ -  
**Mobile TAN (mTAN)**

## Was ist's und wie funktioniert's?

- Das mTAN-Verfahren kommt ohne Chipkarte aus.
- Prinzip:  
Der Kunde benutzt Online-Banking mit seinem Browser.  
Nachdem er die Transaktion abgeschickt hat, übermittelt ihm die Bank eine TAN per SMS auf sein Handy.
- Die TAN ist ausschließlich für diese spezielle Transaktion gültig, verfällt nach einigen Minuten und fasst die Transaktion noch einmal zusammen.

## Welche Vorteile bringt's?

- Ein Angreifer muss die PIN für das Online-Banking kennen und darüber hinaus im Besitz des (betriebsbereiten) Handy's des Benutzers sein.
- Beides in Kombination ist sehr unwahrscheinlich (ein Benutzer bemerkt in aller Regel den Verlust seines Telefons schneller als den Verlust seiner Geldbörse...)
- Der Benutzer bleibt mobil. Es wird keine zusätzliche Hardware, keine spezielle Software oder gar TAN-Listen mehr benötigt.

- Aus der Abteilung „Fazit“ -  
**Kommen wir zum Ende**

## Wie sollte man heute Online-Banking betreiben?

- Klare Aussage:  
Entweder HBCI mit einem Klasse-3-Kartenleser oder mTAN.
- Bei allen anderen Verfahren ist Vorsicht angebracht...
- ...oder die Haftungsübernahme der Bank angesagt!

# Vielen Dank für Ihre Aufmerksamkeit.

Bei Fragen stehen wir gerne zur Verfügung.  
Bis demnächst auf Ihrem Server.

