Online-Banking ohne Fallstricke – Tools auf CD DVD

SICHERHEIT beim Online-Banking

Ist Ihr Online-Konto wirklich sicher? Millionen Deutsche erledigen ihre Bankgeschäfte übers Internet. Doch viele sind dabei sehr leichtsinnig und riskieren im schlimmsten Fall, dass das Konto geplündert wird.

Von **Tobias Weidemann**

Jeder dritte deutsche Bankkunde setzt mittlerweile auf den Internet-Service seines Kreditinstituts. Doch bei vielen bleibt ein mulmiges Gefühl: Ist das Geld dabei wirklich sicher? Was passiert, wenn sich Räuber an meinem Konto bedienen? Denn während bei einem Banküberfall das Kreditinstitut oder dessen Versicherung den finanziellen Schaden trägt, gibt es bei Diebstahl über das Internet oft Streit, wer haftet.

Damit es gar nicht erst so weit kommt, sollten Sie als Kunde die nötigen Sicherheitsvorkehrungen treffen. Setzen Sie auf eine Bank, die Ihr Geld mit den besten Methoden sichert. Welche das sind, worauf Sie allgemein beim Online-Banking achten sollten, erfahren Sie in diesem Artikel. Außerdem haben wir uns Banking-Software angesehen und sagen Ihnen, für wen sich Star Money und Co. eignen – und welche Gratis-Alternativen es gibt. Und zu guter Letzt erfahren Sie, wie Sie im Falle eines Diebstahls rechtlich abgesichert sind.

HIER LESEN SIE ...

- **mit welcher** Software Sie alle Konten im Blick behalten
- **was** sicherer ist als die TAN-Listen, mit denen viele Banken arbeiten
- **warum** es nicht reicht, Phishing-Mails zu ignorieren
- **worauf** Sie in Internet-Cafés zusätzlich achten müssen, wenn Sie Ihre Banking-Website aufrufen

Gut geschützt: Auf das Protokoll kommt es an

Eine wichtige Rolle beim Online-Banking spielt die Frage, wie Ihr Konto geschützt ist. Hierfür gibt es eine Reihe von Methoden.

Standard-PIN-TAN-Verfahren: Immer noch weit verbreitet ist die Kombination aus PIN (Personen-Identifikationsnummer) und TAN (Transaktionsnummer). Die PIN wird quasi als Eintrittskarte benötigt, mit einer TAN bestätigt der Kunde eine Überweisung, einen Dauerauftrag oder eine andere Aktion, bei der Geld den Besitzer wechselt. TANs sind deswegen vergleichsweise unsicher, weil für eine Transaktion eine beliebige TAN aus der aktuell gültigen Liste verwendet werden kann.

Fortgeschrittenes PIN-TAN-Verfahren: Sicherer ist die iTAN, wobei „i“ für indiziert, also durchnummeriert steht. Anders als bei einer Standard-TAN-Liste gibt hier die Bank pro Transaktion vor, welche der 100 TANs aus der aktuellen Liste sie wissen möchte. Hat ein Betrüger etwa über Phishing eine oder zwei TANs erbeutet, ist es unwahrscheinlich, dass gerade diese ver-

Foto: Volkmar Schulz / Keystone

langt werden, wenn er Geld auf ein fremdes Konto überweisen will.

Bei der **iTAN Plus** wird ein Kontrollbild angezeigt, das das Geburtsdatum des Kunden enthält. Das hilft gegen Man-in-the-middle-Attacken, da einem Fremden dieses Datum in aller Regel nicht bekannt sein dürfte. Zusätzlich wird als Antwort eine Bestätigungsnummer (BEN) generiert, die ebenfalls auf der iTAN-Liste zu finden ist und dem Kunden als Kontrollmöglichkeit dient, ob alles korrekt geklappt hat.

Bei der **mTAN** kommt ein zuvor bei der Bank angemeldetes Handy ins Spiel. Der Kunde erhält hier nicht eine gedruckte Liste, sondern jeweils eine Transaktionsnummer per SMS. Diese ist nur für kurze Zeit gültig und an eine bestimmte Überweisung gebunden. Der Kunde sieht zu seiner eigenen Sicherheit einen Teil der Kontonummer des Empfängers in seiner SMS.

„HBCI ist die sicherste Lösung, lässt sich aber nicht ganz einfach bedienen“

Die **Smart-TAN** funktioniert auf ähnlicher Basis. Statt eines Mobiltelefons ist hier ein von der Bank ausgegebenes externes Gerät beteiligt – meist in Form eines Schlüsselanhängers mit kleinem LCD-Display. Bei **Smart-TAN Plus** kommt ein individuell auf den Anwender bezogener geheimer Schlüssel hinzu.

HBCI-Banking: Einen hohen Sicherheitsstandard erreicht auch das HBCI-Protokoll, das in seiner heutigen Form auch Financial Transaction Services (FinTS) heißt. Bei diesem Homebanking Computer Interface Protocol handelt es sich um einen bankenübergreifenden Sicherheitsstandard, der auf der Basis eines Chipkartenlesers mit Tastatur zur PIN-Eingabe funktioniert. Doch gerade diese zusätzliche Hardware hat dazu geführt, dass der Standard keine allzu weite Verbreitung gefunden hat. Erstens kostet so ein Gerät entweder die Bank oder den Kunden Geld, zweitens arbeitet es nicht immer problemlos mit allen Betriebssystemen und Rechnerumgebungen zusammen – und drittens muss man es herumtragen, wenn man mal von unterwegs aus eine Überweisung tätigen will. ›

TOP 5 Diese Gratis-Sicherheits-Tools können wir empfehlen

Für sicheres Online-Banking brauchen Sie im Grunde nichts anderes, als was generell für einen sicheren PC nötig ist: Gute Schutz-Software, die immer auf dem neuesten Stand ist. Wir empfehlen folgende Gratisprogramme:

1 Gegen Viren: Antivir Personal Free Antivirus – der umfassendste Schutz, wenn Sie für Ihre PC-Sicherheit kein Geld ausgeben wollen. Das Antiviren-Tool bietet einen Virenwächter und sucht gezielt nach Schädlingen aller Art.

2 Gegen Angriffe von außen und gegen die Übertragung von Daten aus Ihrem PC: Zone Alarm – die Gratis-Firewall überzeugt durch eine gute Handhabung und einen einfachen Regel-Editor.

3 Gegen Spyware: Ad-Aware Free – das kostenlose Anti-Spyware-Tool sucht gezielt nach Routinen, die Ihre Eingaben am Rechner protokollieren und weiterleiten.

4 Zur Warnung vor Phishing: Firefox – der Gratis-Browser warnt Sie, wenn eine Seite versucht, Sie auf eine betrügerische Site umzuleiten, die möglicherweise Ihre Daten ausspioniert oder Schad-Software auf Ihrem Rechner installieren könnte.

5 Zum verschlüsselten Ablegen von Daten: Keepass – die einfach zu handhabende Open-Source-Software speichert Zugangscodes zu Banking-Servern und anderen sicherheitsrelevanten Sites. Sicherer ist es freilich, wenn Sie die Passwörter im Kopf haben.

CD DVD ONLINE-BANKING Übersicht wichtiger Software

Programm	Einsatzzweck	Betriebssysteme	Internet	Sprache	Preis	Seite
◉ **Ad-Aware 2008 Free 7.1.0.11**	Spyware-Jäger	Windows 2000, XP, Vista	*www.lavasoft.de*	Deutsch	Privat: gratis	65
◉ **Antivir Personal Free Antivirus 8.2.0.334**	Antiviren-Programm	Windows 2000, XP, Vista	*www.free-av.de*	Deutsch	Privat: gratis	65
◉ **Firefox PC-WELT-Edition 3.0.4**	Profi-Web-Browser	Windows 2000, XP, Vista	*www.pcwelt.de/1b0*	Deutsch	Gratis	68
◉ **GNU Cash 2.2.7**	Banking-Software	Windows 2000, XP, Vista	*www.gnucash.org*	Deutsch	Gratis	68
◉ **Keepass Portable 1.14**	Passwortverwaltung	Windows 98/ME, 2000, XP, Vista	*http://keepass.info*	Deutsch	Gratis	65
◉ **Star Money 6.0** 1)	Banking-Software	Windows 98/ME, 2000, XP, Vista	*www.starmoney.de*	Deutsch	49,90 Euro	68
◉ **Zone Alarm 7.0.483**	Zwei-Wege-Firewall	Windows XP, Vista	*www.zonealarm.com*	Deutsch	Privat: gratis	65

◉ auf CD/DVD und unter *www.pcwelt.de/heft* 1) 60-Tage-Testversion auf ◉ CD/DVD

10 SICHERHEITSREGELN So schützen Sie sich vor einer Plünderung via Internet

Egal, auf welches Sicherheitssystem Sie setzen und ob Sie eine Software verwenden oder sich per Browser auf der Banking-Site bewegen: Es gibt einige Regeln zu beachten, mit denen Sie mehr Sicherheit im Internet-Zahlungsverkehr erzielen können.

Sichern Sie Ihren PC

1 **Halten Sie Ihre Windows-Installation auf dem neuesten Stand,** und verwenden Sie aktuelle Sicherheits-Software. Schon mit ein paar kostenlosen Tools sind Sie hervorragend gesichert: Es genügen ein Virenscanner mit aktivem Virenwächter, ein Spyware-Killer und eine Zwei-Wege-Firewall mit gutem Regel-Assistenten. Welche Tools wir für diese Aufgaben empfehlen, sehen Sie im Kasten Seite 65.

2 **Sichern Sie Ihren Browser ab.** In letzter Zeit haben Trojaner-Angriffe zugenommen. Schad-Software wird hierbei oftmals über ein Active-X-Element oder Javascript eingeschmuggelt. Sie sollten daher diese Elemente im Browser abschalten. Bei Firefox etwa geht das unter „Extras, Einstellungen, Inhalt" – wobei der Open-Source-Browser Active-X-Elemente aus Sicherheitsgründen ohnehin nicht unterstützt.

3 **Wenn Ihr Browser Sie vor einer Site warnt** und am Betreten hindern will, sollten Sie ihm vertrauen – selbst wenn Sie im ersten Moment nichts Verdächtiges bemerken. Es kann beispielsweise sein, dass die Site Malware auf Ihren Rechner schleust, die dann im Hintergrund Ihre Eingaben protokolliert und sie an einen entfernten Server überträgt.

4 **Speichern Sie keine Zugangscodes** oder TAN-Nummern unverschlüsselt auf Ihrem PC, beispielsweise im Browser. Gegen das Speichern in einer Banking-Software ist nichts einzuwenden, ebenso geht es über ein spezielles Passwort-Tool - vorausgesetzt, die Software setzt ein hinreichend sicheres Verschlüsselungssystem ein. Am besten ist eine Kombination aus AES und Blowfish, wie sie beispielsweise bei **Keepass** (auf ◉ CD/DVD) zum Einsatz kommt (siehe Kasten Seite 65). Verschlüsselung ist vor allem auf Notebooks und USB-Sticks wichtig, die verloren gehen können.

5 **Besonders vorsichtig sollten Sie bei öffentlichen oder halböffentlichen Rechnern (im Internet-Café, in der Bibliothek, an der Uni) sein.** Schließlich können Sie nicht wissen, ob hier nicht sämtliche Tastaturanschläge protokolliert werden. Falls Ihre Bank eine virtuelle Tastatur anbietet – das ist eine Tastatur auf dem Bildschirm, die Sie mit Mausklicks steuern –, sollten Sie diese unbedingt nutzen. Falls nicht, setzen Sie auf *www.gate2home.com*: Hier können Sie eine Tastatur im Browser aufrufen. Sie ist ursprünglich für Anwender gedacht, die im Ausland nicht auf landesspezifische Zeichen (etwa Umlaute) verzichten möchten. Die per Klicks erstellten Zeichenketten kopieren Sie über das Kontextmenü in Ihr Formular.

Sichern Sie Ihr Konto

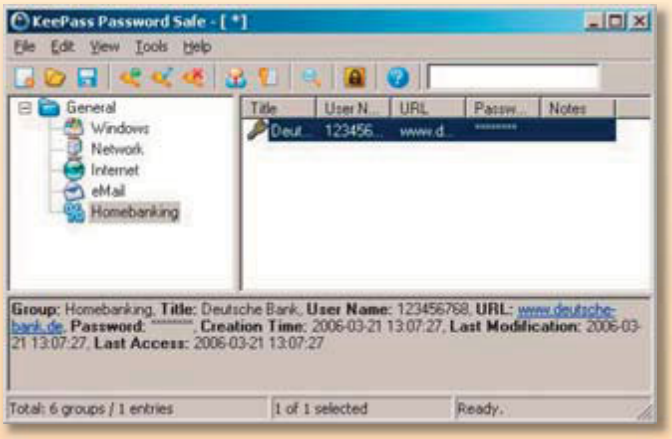
6 **Wichtig ist die Wahl des richtigen Zugangscodes.** Er sollte einerseits so einprägsam sein, dass Sie ihn nirgendwo notieren müssen, andererseits aber auch für Ihr privates Umfeld nicht zu erraten sein. Wählen Sie unter keinen Umständen für verschiedene Zugänge denselben Zugangscode.

7 **Legen Sie ein Limit für Überweisungen fest** – dies ermöglichen inzwischen viele Banken. Wenn Sie nicht darauf angewiesen sind, sollten Sie Auslandsüberweisungen ganz unterbinden oder zumindest ein Limit einrichten. Falls darüber hinaus gehende Transaktionen anstehen, können Sie sie über Ihre Filiale anweisen.

8 **Informieren Sie sich im Vorfeld bei Ihrer Bank,** welche Daten Sie im Notfall brauchen, um Ihr Konto zu sperren, und über welche Rufnummer das am schnellsten geht. Oft ist ein gesondert vereinbartes Kennwort zusätzlich zur Telefon-PIN erforderlich, um Missbrauch durch Dritte zu verhindern.

9 **Prüfen Sie regelmäßig Ihren Kontostand**. In vielen Betrugsfällen wird Geld auf ein ausländisches Konto übertragen. Ist es dort erst einmal abgehoben, haben Sie in jedem Fall das Nachsehen.

10 **Aus vorgenanntem Grund sollten Sie einen Betrugsverdacht schnellstmöglich melden.** Spätestens ab diesem Zeitpunkt muss nämlich die Bank die Haftung übernehmen. Notieren Sie sich dabei unbedingt, mit wem Sie wann gesprochen haben. Oft erhalten Sie auch eine Vorgangsnummer.



Verschlüsselt: Legen Sie geheime Banking-Zugangsdaten – wenn überhaupt – nur in einer verschlüsselten Datenbank wie Keepass ab.

Unser Rat: Grundsätzlich empfehlen wir, nicht auf die klassische PIN-TAN-Lösung, sondern zumindest auf eine der fortgeschrittenen Lösungen zu setzen. Schon eine iTAN- oder iTAN-Plus-Lösung bietet mit nur wenig Mehraufwand einen beachtlichen Sicherheitsgewinn. Das HBCI-Verfahren ist sicher, aber recht aufwendig. Außerdem sind Sie mit HBCI zunächst auf Ihren PC daheim festgelegt oder müssen den Kartenleser mit sich herumtragen.

Fiese Tricks: So plündern Betrüger Konten

Grundsätzlich gibt es zwei Kategorien des Datenabfangens, auch Phishing genannt – die Spionage durch gefälschte Websites oder per Trojaner.

Klassisches Phishing funktioniert vor allem durch gefälschte Sites, die so aussehen wie das Internet-Portal Ihrer Bank. Meist per Mail wird der Anwender aufgefordert, sich aus irgendeinem Grund auf der Site anzumelden – beispielsweise um seine Daten zu aktualisieren oder seinen Kontostand zu checken. Beigefügt ist ein Link, der allerdings nicht auf die Site der Bank führt, sondern auf eine präparierte Kopie davon. So können die Betrüger die eingegebenen Daten des Anwenders abfischen. Sie können sich relativ einfach davor schützen – indem Sie sämtliche Mails ignorieren, in denen angeblich Ihre Bank Sie um die Eingabe Ihrer PIN und einer oder mehrerer TANs bittet.

Die gefälschten Sites sehen immer echter aus: Bei jedem Phishing-Betrugsfall werden im Schnitt mehr als 4000 Euro erbeutet

Sicher und übersichtlich: Wer mehrere Konten hat oder Ebay-Accounts einbinden will, findet in Star Money eine leistungsfähige Software

Das mag banal klingen, ist es aber nicht: Aus dem Jahr 2007 sind immerhin 4100 Fälle bekannt, in denen Anwender um rund 19 Millionen Euro erleichtert wurden – das sind rund 4600 Euro pro Schadensfall. Nicht mitgerechnet sind hier die Fälle, in denen keine Anzeige erfolgte, weil sich der Kunde mit dem Kreditinstitut geeinigt hat. In vielen Fällen geben die Banken dem Kunden die Schuld – nicht selten unterstellen sie sogar, er wäre selbst der Betrüger. Manchmal lenken sie aber dennoch ein, um Streitigkeiten und Imageverlust in der Öffentlichkeit zu verhindern. Das klassische Phishing ist seltener geworden, aber es spielt noch immer eine Rolle.

Phishing per Trojaner – der „Mann dazwischen“: Im Fall eines „Man in the Middle“-Angriffs werden Daten nicht an das vorgesehene Ziel weitergeleitet – sprich: an Ihre Bank oder Sparkasse –, sondern an einen betrügerischen Server. Der Anwender bekommt davon oftmals nichts mit oder bemerkt den Fehler erst, wenn es schon zu spät ist: Ihm wird entweder vorgetäuscht, alles sei in Ordnung, oder er erhält eine Fehlermeldung. Diese kommt dann aber nicht vom Banking-Server, sondern vom Server der Betrüger.

Tipp: Der Browser **Firefox** (PC-WELT-Edition auf ◉ CD/DVD) warnt in Version 3 bei zahlreichen bekannten Phishing-Sites vor dem Aufruf und unterbindet auf Wunsch, dass Sie auf eine solche Seite gelangen können. Gerade beim Browser sollten Sie immer auf die aktuellste Version setzen – bekannte Sicherheitsmängel werden vor allem bei Firefox und Opera relativ schnell ausgeräumt, nachdem sie bekannt werden.

Banking-Software: Star Money und GNU Cash

Der Frage, ob Sie sich auch wirklich auf der richtigen Banking-Site einloggen, müssen Sie sich nicht mehr stellen, wenn Sie eine sichere Banking-Software nutzen. Diese stellt dann für Sie den Kontakt mit dem Kreditinstitut her und kümmert sich um die Sicherheitsfragen. Ein Finanzprogramm eignet sich auch für Anwender, die über mehrere Konten und Depots verfügen – so lässt sich alles übersichtlich darstellen.

„Mit einem Banking-Tool verwalten Sie mehrere Kontenarten und Depots“

Setzen Sie unbedingt auf eine Software, der Sie vertrauen können. Wir haben uns das bei Banken beliebte **Star Money** und die kostenlose Open-Source-Lösung **GNU Cash** (beide auf ◉ CD/DVD) näher angesehen. Beide sind seit einigen Jahren auf dem Markt und haben sich bewährt.

Star Money: Im Bereich Online-Banking ist Star Money 6.0 eines der bekanntesten Programme. Die Software für regulär 49,90 Euro wird von vielen Banken als Zugabe zu HBCI-Paketen vertrieben und ist dann oft deutlich billiger. Sinnvoll ist die Software für alle, die längerfristig ihre Ausgaben oder Geldanlagen im Blick behalten wollen. Neben Girokonto, Bankdepot und Co. lassen sich auch Konten von Ebay, Paypal, Giropay und anderen Online-Bezahlsystemen einbinden und sogar Bonuspunktekonten für Systeme wie Bahn-Bonus oder Payback verwalten.

Während man im Online-Angebot der Banken seine Buchungen in der Regel nur für den Zeitraum von 60 bis 90 Tagen zurückverfolgen kann, lädt Star Money auf Wunsch die Kontenbewegungen und Veränderungen herunter und archiviert sie auf dem Rechner. So haben Sie auch Jahre später noch alle Daten verfügbar.

Das Programm ist in vier Funktionsbereiche gegliedert: „Zahlungsverkehr“, „Wertpapier“, „Festgeld“ und „Auswertung“. Wenn Sie ein bestehendes Konto importieren wollen, lädt das Programm die aktuellen bankspezifischen Dialogdateien herunter und bietet verschiedene Sicherheitssysteme an.

Praktisch sind die Funktionen „Kontenrundruf“ und „Depotrundruf“, die Ihnen auf einen Klick den aktuellen Stand zu sämtlichen Konten und Depots auflisten, sofern Sie sämtliche Zugangsdaten hinterlegt haben.

Dieses Plus an Bequemlichkeit geht übrigens mit einem nur geringen Mehr an Risiko einher. Der Anwender hinterlegt seine Kontodaten und Passwörter in der Software, er tut dies aber in einer mit 128 Bit codierten Datei mit zwei kombinierten Verschlüsselungsverfahren – das ist auch nach Ansicht der Banken hinreichend sicher.

› **GNU Cash:** Unkompliziert zeigt sich auch GNU Cash, ein kostenloses Open-Source-Tool. Wer bereits mit anderen Banking-Anwendungen – etwa Lexware Quicken oder Microsoft Money – gearbeitet hat, kann aufgrund der Importmöglichkeit von QFX- oder QIF-Dateien hierauf zurückgreifen. Allerdings wurden in unserem Test nicht alle Details korrekt importiert.

Etwas gewöhnungsbedürftig ist bei GNU Cash der Begriff „Konten“. Hierunter versteht das Programm keine Bankkonten, sondern einzelne Buchungskonten, also Einnahmen- und Ausgabenbereiche (bei Quicken als „Kategorien“ bezeichnet).

„Leistungsfähige Banking-Software bekommt der Anwender auch kostenlos“

Praktisch: Beim ersten Start kann der Nutzer angeben, welche finanziellen Verhältnisse er hat – beispielsweise ob er einen Kredit abzubezahlen hat, Autobesitzer ist oder Kinder hat. Wenn das Programm nun die Finanzen im Überblick zeigt, listet es nur Felder auf, die den Nutzer auch betreffen. Änderungen und Ergänzungen lassen sich nachträglich einfügen.

Die Bedienung ist durchdacht und spart beispielsweise durch eine Auto-Vervollständigen-Funktion in den Beschreibungsfeldern Arbeit. Bei einigen Punkten kommt allerdings mit der Open-Source-Software etwas mehr Konfigurationsarbeit auf Sie zu: Beispielsweise lassen sich automatisierte Kursabfragen zu Aktien und anderen marktgehandelten Wertpapieren nur über ein Perl-Script einfügen. Sie bekommen es unter *www.pcwelt.de/0f0*.

Fazit zu den beiden Banking-Tools: Unterm Strich hat uns die Open-Source-Software GNU Cash gut gefallen – schnörkellos und übersichtlich ermöglicht das Programm alle benötigten Einträge. Wer allerdings Support benötigt, ist auf Informationen im Internet angewiesen. Die Hotlines der Banken helfen bei Star Money besser weiter und verweisen im Zweifelsfall auf das von Ihnen angebotene Programm.

IHR GUTES RECHT Wann Sie haften und wann nicht

Wenn von einem Kundenkonto Geld entwendet wird, kommt es oft zu Streitigkeiten, wer hierfür verantwortlich ist. Denn anders als bei einem physischen Bankraub kann neben technischen Fehlern auch Fahrlässigkeit des Kunden im Spiel sein.

Sicherheits-Software ist ein Muss

Nach einem aktuellen Urteil des Amtsgerichts Wiesloch (Az.: 4 C 57/08) haftet ein Bankkunde, der nachweist, dass er ein Antiviren-Programm mit aktuellen Signaturen betreibt, nicht für Schäden, die durch das Ausspionieren von Zugangsdaten entstehen. Der Kunde habe, so das Gericht, seine Sorgfaltspflicht nicht verletzt.

Tipp: Wenn Sie online bestohlen worden sind, sollten Sie sofort ein Image Ihres Systems anlegen. Es zeigt etwa, dass aktuelle Schutz-Software auf Ihrem PC läuft. Ein solcher Beweis ist möglicherweise später vor Gericht wichtig.

Achtung Zahlendreher

Wenn Sie online Geld überweisen, prüfen Sie Ihre Eingaben unbedingt auf Tippfehler und Zahlendreher bei Kontonummer oder Bankleitzahl. Denn laut einem Urteil des Amtsgerichts München ist die empfangende Bank nicht verpflichtet, die angegebenen Daten mit dem Namen des Kontoinhabers abzugleichen (Az. 222 C 5471/07).

Doppelte Last: Bleibt eine Rückbuchung aus, muss sich der Überweiser selbst mit dem tatsächlichen Empfänger des Geldes auseinandersetzen, damit dieser den Betrag erstattet. Die Empfängerbank ist zur Herausgabe des Namens und der Anschrift des Geldempfängers an den Überweiser verpflichtet. Hat der Empfänger das Geld aber bereits ausgegeben und ist zahlungsunfähig, muss der Überweiser die offene Rechnung erneut bezahlen.

Diese Meinung deckt sich übrigens mit anderen Urteilen, wonach bei einer Überweisung Kontonummer und Bankleitzahl entscheidend sind, nicht der Empfängername.