orell füssli

Norbert Pohlmann / Markus Linnemann

Sicher im Internet

Tipps und Tricks für das digitale Leben

Sicher im Internet
Norbert Pohlmann
Markus Linnemann
orell füssli

Ein Projekt vom Institut für Internet-Sicherheit:

securityNews: Kostenlose App für mehr Sicherheit im Netz

- Kostenlose App vom Institut für Internet-Sicherheit
- Aktuelle Sicherheitshinweise für Smartphone, Tablet, PC und Mac
- Warnung vor Sicherheitslücken in Standardsoftware, dank BSI-Schwachstellenampel
- Konkrete Anweisungen für Privatanwender und Unternehmen

» www.it-sicherheit.de

Available on the App Store

ANDROID APP ON Google play

Mit freundlicher Unterstützung

Bundesamt für Sicherheit in der Informationstechnik

Norbert Pohlmann/Markus Linnemann

Sicher im Internet Tipps und Tricks für das digitale Leben

Teil 4: Sicher bewegen im Internet – Onlinebanking, E-Commerce, Auktionshäuser im Internet

orell füssli Verlag AG

Onlinebanking – Sicher, wenn's ums Geld geht

«Das Geld hat noch keinen reich gemacht», sagte schon der römische Philosoph und Dichter Lucius Annaeus Seneca (4 v. Chr. – 65 n. Chr.). Trotzdem ist jeder aus verständlichen

Gründen bemüht, es zu bekommen und nicht leichtfertig zu verlieren. Die digitale Technik hält dabei immer stärker Einzug in das private Finanzwesen. Bezahlt wird häufig mit der ec-Karte, die einen kleinen Computerchip sowie einen Magnetstreifen besitzt, und das Bankkonto wird online verwaltet. Und genau wie im realen Leben gibt es auch in der digitalen Welt Betrüger, die es auf Ihr Geld abgesehen haben. Deshalb sollten Sie bei der Abwicklung Ihrer Finanzgeschäfte im Internet unbedingt einige Punkte beachten. Sie lernen in diesem Kapitel die häufigsten digitalen Angriffe kennen und erfahren, wie Sie sich davor schützen können. Zudem erhalten Sie einen Überblick über die aktuell üblichen Onlinebanking-Verfahren und werden grundsätzlich für den Umgang mit kritischen Finanzdaten im Internet sensibilisiert.

Risiken beim Onlinebanking – Angiffsszenarien

Die Angriffsfläche beim Onlinebanking ist deutlich größer als beim Besuch bei einer Bank, da der digitale Angreifer keinen überschaubaren und überprüfbaren physischen Zugriff benötigt, sondern von überall auf der Welt – oft von Strafverfolgung verschont – agieren kann. Doch sind die Angriffe auf Bankdaten nur selten gegen eine bestimmte Person gerichtet. Die organisierte Kriminalität hat sich darauf spezialisiert, mithilfe globaler Attacken möglichst viele Zugangs- und Transaktionsdaten zu stehlen, um die entsprechenden Bankkonten übernehmen und ausrauben zu können. Die Angriffe richten sich dabei meist gegen Privatpersonen, da der Schutzlevel hier in der Regel am niedrigsten ist (Unternehmen beschäftigen nicht selten ganze Abteilungen, die sich um die Sicherheit kümmern).

Onlinebanking-Attacken haben Tradition. Sie werden permanent weiterentwickelt und sind so effektiv und präsent, dass sie nach wie vor eine große Gefahr darstellen. Hersteller von Banking-Software und Browsern sowie auch die Banken selbst versuchen zwar, immer neue Abwehrmechanismen zu finden, diese können jedoch nur zusammen mit dem korrekten und vorausschauenden Verhalten des Nutzers zum gewünschten Ergebnis führen.

Erschwerend kommt hinzu, dass jeder mit ein bisschen krimineller Energie und ohne Angst vor dem Gesetz diese Angriffe mehr oder weniger gut durchführen kann, weil die Software, die er dazu benötigt, mehr oder weniger offen zum Kauf angeboten wird. Die kriminellen Verkäufer stellen sogar einen Support für die Angriffssoftware zur Verfügung. Doch Sie können sich schützen.

Der Phishing-Angriff

Der bekannteste Angriff, der speziell beim Onlinebanking seit Jahren Hochkonjunktur feiert, ist der Phishing-Angriff. Der Begriff setzt sich aus den Wörtern «Password» und «Fishing» zusammen und tauchte Anfang 1996 erstmals im Zusammenhang mit dem Diebstahl von Internetzugangsdaten (IDs und Passwörter) von AOL-Kunden auf. Inzwischen hat er sich jedoch als allgemeiner Ausdruck für den Identitäts- und Passwortdiebstahl im Internet etabliert.

Phishing ist ein Problem, das zahlreiche Branchen betrifft, eine jedoch ganz besonders: Laut einer Statistik der Anti-Phishing Working Group sind über 80 Prozent aller Phishing-Angriffe gegen den Finanzdienstleistungssektor gerichtet. Die ersten Attacken gegen deutsche Bankkunden wurden im Juli 2004 verzeichnet, und sie nehmen seitdem massiv zu. Wurden

im Jahr 2004 noch 200.000 Phishing-E-Mails pro Monat registriert, steigerte sich die Zahl 2005 auf 100.000 Phishing-E-Mails pro Tag. Im Frühjahr 2008 war durchschnittlich eine Phishing-Mail pro 150 E-Mails zu beobachten.

Basis des Phishing-Angriffs ist im Finanzsektor häufig eine präparierte E-Mail, die optisch einer E-Mail der Bank nachempfunden ist.

In dieser E-Mail werden die Internetnutzer gebeten, auf einen bestimmten Link zu klicken, der zu einer gefälschten Onlinebanking-Webseite führt, die der echten Bank-Webseite oft haargenau gleicht. Auf der falschen Webseite geben die Nutzer dann wie gewohnt ihre Zugangsdaten ein und spielen sie so dem Angreifer direkt in die Hände. Das ermöglicht ihm zwar einen Überblick über das «gestohlene Bankkonto», aber noch keine Überweisung, denn dazu benötigt er mindestens eine Transaktionsnummer (TAN). Also

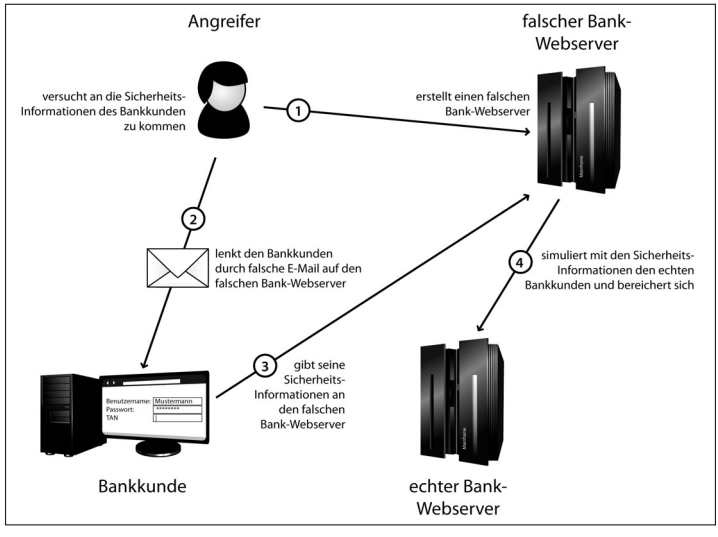

Abbildung 24: Der Ablauf einer Phishing-Attacke

werden die Nutzer bei diesem Verfahren zusätzlich aufgefordert, eine oder mehrere TANs einzugeben. Diese nutzt der Angreifer dann umgehend, um Geld vom Bankkonto zu stehlen, indem er einen bestimmten Betrag auf ein Angreifer-Bankkonto überweist (siehe Abbildung 24).

In der Regel ist das ein Konto, das von einer Bank geführt wird, die ihren Sitz in einem Land hat, in dem eine Strafverfolgung nicht möglich ist – oder die Gelder werden mithilfe leichtgläubiger Bürger «gewaschen» (siehe Seite 79).

Allerdings muss eine Phishing-Attacke nicht zwangsläufig durch eine E-Mail ausgelöst werden. Grundsätzlich können Internetnutzer über jede Art von gefälschten Links auf die Phishing-Webseiten gelangen. Eine Möglichkeit, Webseiten dahingehend zu manipulieren, ist das sogenannte Cross Site Scripting (siehe Seite 32f.). So kann beispielsweise auf der Webseite eines Onlinekaufhauses eine Information stehen, die auf Probleme mit Onlinekonten hinweist und einen Link anbietet, der den Nutzer vermeintlich direkt zu seiner Bank weiterleitet.

TIPP: So schützen Sie sich vor Phishing-Angriffen

- Klicken Sie nie auf Links in E-Mails, die angeblich zu Ihrer Bank führen. Banken schreiben keine E-Mails, wenn es um sicherheitskritische Vorgänge geht.
- Verwenden Sie generell keine Links, um auf die Webseite Ihrer Bank zu gelangen. Tippen Sie die Webadresse immer per Hand in die Adresszeile Ihres Browsers ein.
- Geben Sie auf einer Webseite niemals mehr als eine TAN-Nummer ein, auch wenn Sie dazu aufgefordert werden – und diese eine auch nur zum Ausführen einer regulären Banktransaktion.

Der Pharming-Angriff

Das sogenannte Pharming könnte als die Weiterentwicklung von Phishing angesehen werden, da der Pharming-Angriff wesentlich komplexer und die Täuschung für den Onlinebanking-Nutzer – besonders für den technisch eher unversierten – schwerer zu durchschauen ist.

Wie bereits beschrieben, werden Webseiten üblicherweise über ihre Webadresse (URL) aufgerufen, zum Beispiel in der Form www.name.de. Diese namentlichen Webadressen «zeigen» auf eine bestimmte IP-Adresse und werden vom sogenannten Domain Name Server (DNS) entsprechend umgewandelt (siehe Seite 42f.). Beim Pharming-Angriff wird nun der Name einer Webadresse durch Manipulation auf eine andere IP-Adresse gelenkt, sodass der Nutzer auf eine gefälschte Webseite gelangt. Das kann auf zwei Arten geschehen. Entweder werden die Domain Name Server manipuliert, was einen hohen Aufwand bedeutet und daher nur sehr selten passiert. Oder es wird – was meist der Fall ist – mithilfe von Malware eine bestimmte Datei, die sogenannte Hosts-Datei, auf dem Computer des Nutzers verändert. Diese Datei löst ebenfalls die Webadresse in eine IP-Adresse auf, noch bevor ein DNS befragt wird. Sie kann jedoch nur manipuliert werden, wenn die dazu nötigen Schreibrechte vorhanden sind. Das ist ein weiterer Punkt, warum Sie nicht als Administrator im Internet surfen sollten (siehe Seite 23f.).

Sie können diese Datei auch selbst überprüfen, wenn Sie das Gefühl haben, Opfer eines Pharming-Angriffs geworden zu sein (siehe Screenvideo, Softlink 341). Die Hosts-Datei ist am einfachsten zu finden, indem Sie eine Suche auf der Systempartition (meistens C:) nach «hosts» durchführen. Bei Windows XP befindet sich die Hosts-Datei zum Beispiel

unter C:\WINDOWS\system32\drivers\etc\hosts. Steht in der Datei – sie kann mit einem Editor oder einem Textverarbeitungsprogramm geöffnet werden – der Name einer Bank oder einer anderen Webseite, die mit sicherheitskritischen Vorgängen wie Bezahldiensten zu tun hat, kann das ein Indiz für einen Pharming-Angriff sein. Abbildung 25 zeigt den typischen Aufbau einer Hosts-Datei. Relevant sind nur die Einträge ohne «#». Im Normalfall ist dort nur der «Localhost-Eintrag» zu finden, und dieser ist völlig unbedenklich.

```
# Copyright © 1993-1999 Microsoft Corp.
#
# Dies ist eine HOSTS-Beispieldatei, die von Microsoft TCP/IP
# für Windows 2000 verwendet wird.
#
# Diese Datei enthält die Zuordnungen der IP-Adressen zu den
jeweiligen Hostnamen.
# Jeder Eintrag muss in einer eigenen Zeile stehen.
# Die IP-Adresse sollte in der ersten Spalte gefolgt vom
# zugehörigen Hostnamen stehen.
# Die IP-Adresse und der Hostname müssen durch mindestens
ein
# Leerzeichen getrennt sein.
#
# Zusätzliche Kommentare (so wie in dieser Datei) können in
# einzelnen Zeilen oder hinter dem Computernamen eingefügt
werden,
# müssen aber mit dem Zeichen '#' eingegeben werden.
#
# Zum Beispiel:
#
#   102.54.94.97    rhino.acme.com      # Quellserver
#    38.25.63.10    x.acme.com          # x-Clienthost

127.0.0.1    localhost
```

Abbildung 25: Aufbau einer nicht manipulierten Hosts-Datei

TIPP: So schützen Sie sich vor Pharming

- Stellen Sie sicher, dass der Basisschutz (siehe Seite 10 ff.) eingehalten ist, um sich keine Schadsoftware auf Ihrem Computer «einzufangen».
- Zusätzlich sollten Sie darauf achten, dass die Webseite ein gültiges Zertifikat Ihres Onlinebanking-Anbieters beinhaltet und dieses gegebenenfalls überprüfen (siehe Seite 36 ff. sowie Workshop «SSL/TLS», Softlink 223). Besondere Vorsicht ist geboten, wenn eine Warnmeldung («Ungültiges Zertifikat») erscheint, sobald Sie auf Ihre Bankseite gehen. Stoppen Sie sofort das Onlinebanking und fragen Sie Ihre Bank, wenn Sie sich nicht sicher sind, wie Sie die Seite überprüfen können.
- Wenn Sie vermuten, einer Pharming-Attacke zum Opfer gefallen zu sein, oder auch etwas zur Prävention tun möchten, überprüfen Sie die Hosts-Datei Ihres Computers. Finden Sie dort Einträge von Bank- oder Bezahldienstseiten, holen Sie sich Rat beim Experten und stoppen Sie alle sicherheitskritischen Vorgänge am Computer.

Angriffe über Schadsoftware

Grundsätzlich ist ein Betriebssystem wie Windows, Linux oder Mac OS angreifbar. Gelingt es einem Angreifer, beispielsweise ein Trojanisches Pferd auf dem Computer zu installieren, erlangt er die vollständige Kontrolle und ist unter anderem in der Lage, alle Tastaturanschläge mitzulesen (sogenanntes Key-Logging). Die auf diese Weise ausgespähten Informationen senden die Key-Logger – für den Nutzer unsichtbar – direkt oder indirekt zu den Angreifern. Und diese sind natürlich in erster Linie an Passwörtern und anderen sensiblen Daten interessiert, weshalb das Key-Logging – neben Phishing und Pharming – ebenfalls eine Gefahr für Sie als

Onlinebanking-Nutzer darstellt. Eine wirksame Abwehrmaßnahme ist auch hier der Basisschutz.

Onlinebanking-Verfahren – Welches ist wie sicher?

Zur Durchführung und zum Schutz der Transaktionen gibt es verschiedene Verfahren, die auch ein unterschiedlich hohes Maß an Sicherheit bieten. Die meisten Onlinebanking-Verfahren, mit Ausnahme des FinTS/HBCI-Verfahrens, basieren auf der Kombination aus PIN und TAN. Diese werden im Folgenden kurz erläutert und im Hinblick auf die Sicherheit bewertet. Dabei ist zu beachten, dass alte und unsichere Verfahren mit der Einführung neuer Verfahren abgeschaltet werden müssen, um mögliche Hintertüren zu schließen. Bei einem kürzlich aufgetretenen Betrugsfall war zwar ein neues iTAN-Verfahren eingeführt worden, aber das alte TAN-Verfahren wurde nicht deaktiviert. Somit konnten durch Phishing gewonnene iTANs auch weiterhin uneingeschränkt als TANs genutzt werden. Zuständig dafür ist die Bank. Fragen Sie dort explizit nach und probieren Sie Ihr altes Verfahren nach der «offiziellen» Umstellung noch einmal aus, um sicherzugehen, dass es deaktiviert ist.

TAN

Das einfache TAN-Verfahren basiert auf einer Liste von einmalig zu verwendenden TANs. TANs sind numerische Einmalpasswörter, die meist eine Länge von sechs Stellen haben und dem Nutzer in Form einer Liste von seiner Bank ausgehändigt werden. Dieser wiederum verwendet sie, um seine Transaktionen, zum Beispiel eine Überweisung, zu bestätigen, nachdem er sich per PIN in sein Bankkonto eingeloggt

hat. Erst durch die Eingabe einer korrekten TAN, die der Bank ebenfalls bekannt ist, wird die gewünschte Transaktion tatsächlich ausgeführt. Dabei kann jede TAN auf der Liste nur einmal verwendet werden, die Reihenfolge ist egal. Die TAN-Nummern sind also nicht an bestimmte Transaktionen gebunden. Die TAN wird, bildlich gesprochen, nach ihrer Verwendung aufseiten der Bank und beim Nutzer von der Liste gestrichen.

Dieses Verfahren wird heute als unsicher eingestuft, da bei einem Phishing-Angriff mehrere TANs ausgespäht werden können, die der Angreifer dann flexibel für seine Zwecke verwenden kann.

iTAN

Bei der iTAN (der indizierten TAN) muss eine ganz bestimmte TAN benutzt werden, um eine Transaktion zu legitimieren. Die TANs sind zu diesem Zweck auf der TAN-Liste entsprechend nummeriert. Das erschwert dem Angreifer seine Arbeit, da er bei seinem Phishing-Angriff genau die richtige TAN «erbeuten» muss. Er ist somit gezwungen, entweder in Echtzeit zu arbeiten oder eine ganze TAN-Liste zu ergaunern, wodurch sich der Sicherheitslevel beim iTan-Verfahren ein wenig erhöht. Das Verfahren kann aber auch nicht mehr empfohlen werden.

mTAN

mTAN (mobile TAN, auch SMSTAN genannt) verbessert die Sicherheit bereits erheblich, da neben der Bindung an eine bestimmte TAN auch noch ein Medienbruch erfolgt. Das bedeutet, dass die TAN bei der Initiierung einer Transaktion per SMS von der Bank an ein bestimmtes Handy des Onlineban-

king-Nutzers gesendet wird. In der SMS befinden sich neben der TAN auch Informationen zu der gewünschten Transaktion, zum Beispiel der Betrag und die Zielkontonummer, um auszuschließen, dass ein Angreifer die Transaktion manipuliert hat (Filme zu TAN-Verfahren siehe Softlink 342). Aktuell ist mTAN eines der sichersten Onlinebanking-Verfahren, da es für einen Angreifer sehr schwer ist, die Computerkommunikation und parallel die Handykommunikation zu überwachen. Allerdings fallen dabei meist zusätzliche Kosten für die SMS an (teilweise werden diese jedoch auch von den Banken übernommen). Aber es ist eine lohnende Investition, die einen angemessenen Sicherheitsstandard garantiert.

Sm@rtTAN, Sm@rtTAN Plus und ChipTAN

Das Sm@rtTAN-Verfahren stellt eine weitere Alternative zur TAN-Liste dar. Die Basis von Sm@rtTAN ist ein kleines zusätzliches Gerät mit Display, auch Token genannt, in das der Nutzer seine ec-Karte einführen kann. Der Token errechnet dann auf Knopfdruck die TAN, die für die gewünschte Transaktion verwendet werden soll. Dieses Verfahren ähnelt sicherheitstechnisch dem iTAN-Verfahren, da der Vorgang keine Man-in-the-middle-Angriffe verhindern kann, also Angriffe, bei denen sich der Angreifer in die Kommunikation zwischen Absender und Empfänger einklinkt und die Kommunikation zu seinen Gunsten verändert. Das bedeutet, dass der Nutzer nicht nachvollziehen kann, ob beim Transaktionsvorgang direkt mit der Bank kommuniziert wird oder ob sich ein Angreifer dazwischengeschaltet hat.

Daher wurde das Sm@rtTAN-Plus-Verfahren eingeführt, je nach Kreditinstitut auch ChipTAN genannt. Der hierfür benötigte Token besitzt zusätzlich eine eigene Tastatur. Startet

der Nutzer eine Transaktion, erhält er von der Bank zwei Nummern als Antwort angezeigt. Eine beinhaltet Teile der Kontonummer des Empfängers, die zweite ist ein Bankcode. Die Kontonummernteile werden mit der Transaktion verglichen. Dann gibt der Nutzer beide Nummern in den Token ein, der daraus – zusammen mit den Informationen von der eingesteckten ec-Karte – eine TAN errechnet (Filme zum TAN-Verfahren siehe Softlink 334).

Das Sm@rtTAN- beziehungsweise ChipTAN-Verfahren gibt es ganz aktuell auch in einer optischen Lösung. Dazu erhalten die TAN-Generatoren (Token) eine optische Schnittstelle. Nach Eingabe der Transaktionsdaten erscheint eine Animation. Der TAN-Generator wird dann vor den Monitor gehalten und liest den Code aus. Aus dem optischen Code, den Transaktionsdaten und den Daten der Karte werden die TANs generiert und auf der Anzeige des Tokens angezeigt. Dieses Onlinebanking-Verfahren ist vom Sicherheitslevel her ebenfalls gut geeignet. Achten Sie darauf, dass Sie alle Eingaben genau überprüfen. Allerdings fallen auch hier eventuell zusätzliche Kosten für den Token an.

HBCI/FinTS

Mit HBCI (Homebanking Computer Interface) wurde schon vor vielen Jahren ein solider offener Homebanking-Standard in Deutschland eingeführt, der in einer neuen Version inzwischen als FinTS (Financial Transaction Services) bekannt ist. Er sieht die Verwendung einer SmartCard vor, die mit einer elektronischen Signatur ausgestattet ist. Der sogenannte Klasse-3-Kartenleser zeigt in diesem Fall die Überweisungsdaten auf seinem Display an, und der Nutzer bestätigt die Transaktion mit seiner PIN, die direkt in den

Kartenleser eingegeben wird und nicht auf dem Computer. Das bedeutet, dass Computer und PIN völlig unabhängig voneinander sind, wodurch einer Malware auf dem Computer die Angriffsfläche entzogen wird. Der Einsatz von Kartenlesern der Klasse 2 und 1 wird nicht empfohlen, denn die Integrität und die Verbindlichkeit beim Transaktionsvorgang sind nur mit dem Klasse-3-Kartenleser gegeben. Dieser Kartenleser garantiert, dass die Tastatur und das Display des Kartenlesers während einer PIN-Eingabe nur unter der Kontrolle des Kartenlesers stehen und nicht vom Computer beeinflusst werden können.

Das HBCI/FinTS-Verfahren ist in Bezug auf das Sicherheitsniveau mit dem mTAN-Verfahren vergleichbar. Leider ist es jedoch kaum verbreitet, da sowohl die Kartenleser als auch die entsprechende Onlinebanking-Software deutlich teurer sind als andere, unsichere Verfahren.

TIPP: Onlinebanking-Verfahren

- Nutzen Sie für das Onlinebanking möglichst eines der folgenden Verfahren: mTAN, Sm@rtTAN Plus oder FinTS.
- Nutzen Sie neue Verfahren, wenn diese ein höheres Sicherheitsniveau bieten – auch wenn sie möglicherweise mit Zusatzkosten verbunden sind. Die Investition lohnt sich in jedem Fall!
- All diese Verfahren bieten nur dann optimalen Schutz, wenn Sie sie richtig anwenden. Achten Sie also beispielsweise darauf, dass Sie Ihr Handy, in dem Ihre Zugangsdaten gespeichert sind, nicht aus der Hand geben, wenn Sie mTan verwenden.

Onlinebanking mit Banking-Software

Alternativ zum browserbasierten Onlinebanking können Sie auch eine Banking-Software verwenden. Diese Anwendun-

gen sind zwar im Allgemeinen kostenpflichtig, bieten aber in den aktuellen Versionen sehr guten Schutz und zusätzlichen Komfort. Phishing-Angriffe sind hier – genau wie alle anderen browserrelevanten Angriffe – im Grunde ausgeschlossen. Sämtliche aktuellen Onlinebanking-Programme unterstützen darüber hinaus die empfohlenen Verfahren mTAN, FinTS und Sm@rtTAN Plus. Trotzdem sind auch sie angreifbar, vor allem mithilfe von Trojanischen Pferden. Sorgen Sie also stets für einen optimalen Basisschutz (siehe Seite 10 ff.)!

Besonders empfehlenswert ist die Banking-Software, wenn Sie technisch nicht so versiert sind und/oder mehrere Konten verwalten wollen. Bedenken Sie jedoch, dass Sie dann an den Computer gebunden sind, auf dem die Software installiert ist.

TIPP: Die wichtigsten Verhaltensregeln zum Onlinebanking

- Rufen Sie die Webseite Ihrer Bank beim browserbasierten Onlinebanking immer durch die manuelle Eingabe der Bankadresse auf. Nutzen Sie keine Links aus E-Mails oder von unbekannten Webseiten.
- Überprüfen Sie nach Eingabe der Bankadresse die Verschlüsselung der Verbindung, indem Sie darauf achten, dass die Webadresse in der Adresszeile mit «https» beginnt, der Name der Bank – je nach Browser – entsprechend markiert ist und ein Schloss-Symbol angezeigt wird.
- Gehen Sie sorgfältig mit Ihren Zugangsdaten um: Geben Sie diese nicht weiter, speichern Sie sie nicht in Klartext auf Ihrem Computer und schreiben Sie sie nicht auf.
- Verwenden Sie ein sicheres Passwort (siehe Seite 53 f.) beziehungsweise eine zusammenhangslose PIN (nicht das Geburts-

datum!) und ändern Sie diese sicherheitsrelevanten Daten regelmäßig – möglichst alle drei Monate.

- Onlinebanking sollte nie an einem fremden Computer, zum Beispiel im Internetcafé, durchgeführt werden. Nutzen Sie nur Ihren eigenen, gut geschützten Computer.
- Nutzen Sie das Onlinebanking-Angebot nicht in öffentlichen Netzen wie Hotspots im Bahnhof oder in Cafés. Das gilt auch für fremde WLANs und kabelgebundene Netze, denen Sie nicht vertrauen können. Hier sind Ihre Daten in Gefahr.
- Stellen Sie sicher, dass Ihr Computer gemäß den Sicherheitsgrundregeln geschützt ist (siehe Seite 10ff.), bevor Sie online gehen, um Ihre Bankgeschäfte zu erledigen.
- Überprüfen Sie regelmäßig Ihre Bankkontobewegungen auf Ungereimtheiten und fragen Sie in einem solchen Fall sofort bei Ihrer Bank nach.
- Vereinbaren Sie mit Ihrer Bank ein Limit für tägliche Geldbewegungen beim Onlinebanking.
- Achten Sie bei der Nutzung einer Banking-Software immer auf die Aktualität des Programms.
- Um bei Ungereimtheiten auf Nummer sicher zu gehen, können Sie das Zertifikat überprüfen und den Fingerprint des Zertifikats mit der Bank abgleichen. Dieses Verfahren ist jedoch sehr aufwändig und stellt sozusagen das letzte Mittel dar (siehe Seite 36ff.).

Exkurs: die wichtigsten Verhaltensweisen offline

Die meisten Bankgeschäfte lassen sich mittlerweile bequem vom heimischen Computer aus erledigen. Aber auch wenn Sie den Geldkartenchip Ihrer ec-Karte bereits im Internet aufladen können, Bargeld müssen Sie sich nach wie vor am

Bankschalter oder an Geldautomaten holen. Und auch Letztere sind Teil der digitalen Welt. Deshalb finden Sie hier, um das Thema Onlinebanking abzurunden, zudem die wichtigsten Grundregeln zur Nutzung von Geldautomaten. Denn auch diese werden vielfach manipuliert – man nennt das Skimming –, um an die Zugangsdaten von Ihrem Konto zu gelangen.

TIPP: Die Nutzung von Geldautomaten

- Kontrollieren Sie den Geldautomaten vor der Nutzung auf Manipulationsspuren an Tastatur und Karteneinschub.
- Während der Interaktion mit dem Automaten sollten Sie sich in keinem Fall ablenken lassen, sondern stets den Vorgang beobachten.
- Schützen Sie Ihre Eingaben und Aktionen vor Blicken und Kameras von potenziellen Angreifern.

E-Commerce – Shoppen «hoch n»

Das Internet ist wohl das größte Einkaufszentrum, das man sich vorstellen kann, und es gibt fast nichts, was man dort nicht bekommt. Ganz im Gegenteil: Gegenüber dem realen Leben kommen sogar noch neue Angebote hinzu. So ist es im Internet kein Problem, bestimmte Artikel aus Zeitschriften einzeln zu erwerben. Auch kostenpflichtige Software kann problemlos online gekauft werden, indem Sie eine entsprechende Lizenz erwerben und das gewünschte Programm einfach herunterladen. Alles geht sehr schnell und kann bequem von zu Hause aus erledigt werden. Weitere Vorteile des Onlineshopping sind: keine Parkplatzprobleme, keine Warte-

schlangen, kein Ladenschluss, der berücksichtigt werden muss, und keine «Zensur» durch die Nachbarn an der Kasse. Einer der größten Vorteile des Interneteinkaufs ist aber wohl die Möglichkeit, ohne großen Aufwand Preise zu vergleichen und so das günstigste Angebot herauszufiltern – wobei Sie immer auch die Kosten für den Versand berücksichtigen sollten.

Doch diese schöne neue Warenwelt wirft auch Fragen auf: Wie vertrauenswürdig ist der von mir besuchte Onlineshop? Was geschieht mit den sensiblen Daten, die der Anbieter für Lieferung und Bezahlung von mir erhält? Wie sicher ist der Onlinekauf? Und wie funktionieren die verschiedenen Bezahlverfahren im Internet?

Ein vertrauenswürdiger Onlineshop

Jeder Mensch hat seine Lieblingsgeschäfte, egal ob er Lebensmittel, Kleidung, Möbel, Musik oder Autos kauft. Die Verkäufer sind sympathisch, die Lage praktisch und das Ambiente angenehm – Vertrauen hat sich über die Zeit entwickelt. Und genau das ist im Internet schwierig, weil alles virtuell ist und es keinen persönlichen Verkäufer gibt, zu dem ein Vertrauensverhältnis aufgebaut werden kann. Wie aber können Sie dann feststellen, ob der Anbieter, bei dem Sie online ein Schnäppchen ergattern möchten, tatsächlich seriös ist?

Ein Aspekt, auf den Sie achten sollten, ist eine professionelle, aufgeräumte Webseite. Das allein reicht jedoch als Entscheidungsgrundlage noch nicht aus. Der Onlineshop sollte zudem auf jeden Fall schon länger existieren. Auch der Blick ins Impressum kann einen Hinweis auf dessen Vertrauenswürdigkeit geben (siehe Tipp). Zusätzlich können Sie prüfen, ob sich per Suchmaschine Referenzen zu dem fraglichen

Onlineshop finden lassen, denn die lassen sich in ihrer Gesamtheit nur schwer fälschen. Fragen Sie darüber hinaus Freunde und Bekannte, ob sie bereits Erfahrungen mit diesem Onlineshop gemacht haben. All diese Informationen zusammen bilden dann die Basis für einen vertrauenswürdigen Einkauf (Softlink 344).

Eine weitere Entscheidungshilfe können Browser-Add-ons sein (zum Beispiel für den Firefox), die bei Betreten bestimmter Onlineshops eine entsprechende Empfehlung anzeigen. Ein Beispiel dafür ist das Add-on WoT (Softlink 351), das auf den Bewertungen zahlreicher Nutzer im Hinblick auf Vertrauenswürdigkeit, Händlerzuverlässigkeit, Datenschutz oder auch Jugendschutz basiert. Ist WoT installiert, signalisiert es per Ampelfarben, ob die Webseite bedenkenlos genutzt werden kann oder eher mit Vorsicht zu genießen ist. WoT steht übrigens für «Web of Trust» und zeigt ein sehr positives Phänomen des Internets: Immer wieder finden sich viele Freiwillige zu großen Projekten zusammen, um das Internet für seine Nutzer sicherer zu machen.

TIPP: So erkennen Sie vertrauenswürdige Onlineshops

- Schauen Sie im Impressum eines Onlineshops auf die rechtlichen Merkmale (Organisationsform, verantwortliche Person, Anschrift, Gründungsdatum usw.) und überprüfen Sie diese gegebenenfalls.
- Kaufen Sie nur bei Onlineshops, die schon länger bestehen und sich im Internet etabliert haben. Bleiben Sie aber auch hier wachsam, da Onlineshops genau wie «reale» Geschäfte den Besitzer wechseln können.
- Geben Sie den Namen des Onlineshops in eine Suchmaschine ein und überprüfen Sie die Ergebnisse.

- Nutzen Sie zudem entsprechende Bewertungsseiten (zum Beispiel idealo.de, preissuchmaschine.de und günstiger.de) oder auch Add-ons wie WoT (Softlink 351).
- Kaufen Sie bevorzugt bei Onlineshops, die Ihnen von Personen Ihres Vertrauens empfohlen werden, oder fragen Sie Bekannte und Freunde, ob Sie mit dem Onlineshop, den Sie nutzen möchten, bereits positive Erfahrungen gemacht haben.

Das richtige Verhalten beim Onlineeinkauf

Wer sich bei vielen Onlineshops registriert, verteilt natürlich auch seine persönlichen Daten (personenbezogene Daten und Finanzdaten) im Internet. Daher sollten Sie eine Auswahl treffen. Beziehen Sie bei dieser Überlegung auch die Frage ein, welche Daten Sie preisgeben wollen/müssen und ob bestimmte Dienste des Onlineshops für Sie überhaupt sinnvoll sind. Bei Amazon können Nutzer zum Beispiel Wunschlisten – für den Hochzeitstisch oder den Geburtstag – und Ähnliches erstellen, die, verknüpft mit dem Namen des Nutzers, teilweise über Google zu finden sind. Das stimmt natürlich nicht mit dem Grundsatz der Datensparsamkeit des Datenschutzes überein. Eine gute Möglichkeit zu testen, ob ein Onlineshop vertrauliche Daten offen zugänglich macht, ist die Eingabe des eigenen Namens in eine Personensuchmaschine wie www.123people.de oder www.yasni.de. Diese finden nämlich auch Wunschlisten etc.

Wenn Sie jedoch Ihre Auswahl sorgfältig treffen und alle wichtigen Hinweise beachten, steht einem ungetrübten Shopping-Vergnügen im Internet nichts im Wege – auch wenn es manchmal schöner ist, durch eine Einkaufsstraße zu schlendern.

TIPP: Die wichtigsten Verhaltensregeln beim Onlineeinkauf

- Melden Sie sich nicht bei jedem x-beliebigen Onlineshop an. Machen Sie es ähnlich wie im realen Leben und entscheiden Sie sich für bestimmte Anlaufpunkte für die verschiedenen Produktgruppen.
- Nutzen Sie nicht jeden Dienst in einem Onlineshop, wie zum Beispiel Wunschlisten. Diese Daten sind oft unter Ihrem Namen frei im Internet verfügbar.

Sicher anmelden und registrieren

Haben Sie sich für einen Onlineshop entschieden, sollten Sie darauf achten, dass dieser eine verschlüsselte SSL/TLS-Übertragung der Registrierungsdaten zwischen dem Computer und dem Webserver gewährleistet (siehe Seite 36 ff.). Die Verschlüsselung ist allerdings erst erforderlich, wenn Sie Ihre persönlichen Daten eingeben, und nicht schon beim Stöbern im Warenangebot.

Damit Sie Ihre Daten nicht jedes Mal von Neuem eingeben müssen, speichern die meisten Onlineshops die Angaben, die bei der Registrierung gemacht werden, und verlangen zusätzlich einen Benutzernamen und ein Passwort. Das sollte gemäß den Regeln für ein sicheres Passwort gewählt werden (siehe Seite 53 f.). Beim nächsten Bestellvorgang reicht dann die Kombination aus Benutzername und Passwort.

Allerdings muss hier noch eine Unart mancher Anbieter angesprochen werden: Manchmal geben Nutzer ihre persönlichen Daten verschlüsselt auf einer Webseite ein und bekommen danach eine Bestätigung per E-Mail. Das ist grundsätzlich auch in Ordnung, solange Passwort und Benutzername

darin nicht in Klartext genannt werden. Denn E-Mails sind primär nicht verschlüsselt (siehe Seite 82 f.). In diesem Fall sollten Sie dem Onlineshop seinen Fehler mitteilen und das Passwort sofort ändern. Wird Ihnen auch dieses wieder übermittelt, sollten Sie die Registrierung löschen oder sperren, damit kein Schaden entstehen kann. Das gilt auch für Benutzerkonten, die Sie nicht mehr benutzen.

TIPP: Anmelden bei einem Onlineshop

- Geben Sie persönliche Daten nur ein, wenn Sie von der Vertrauenswürdigkeit des Onlineshops überzeugt sind.
- Nutzen Sie bei jedem Onlineshop ein anderes, sicheres Passwort (siehe Seite 53 f.).
- Erhalten Sie nach der Anmeldung eine unverschlüsselte E-Mail mit Ihren Zugangsdaten, also Benutzername und Passwort, machen Sie den Onlineshop auf den Missstand aufmerksam und ändern Sie Ihre Daten telefonisch oder online.
- Onlineshops und Dienste, die Sie nicht mehr nutzen, sollten Sie kündigen; lassen Sie Ihre Bank- und Kundendaten dann vollständig löschen. Weisen Sie den Onlineshop explizit auf die vollständige Löschung aller persönlichen Daten hin.

Sicher bezahlen im Internet

Ist das Produkt gefunden und ausgewählt, stellt sich die Frage nach der Bezahlung. Die Onlineshops bieten dazu eine Vielzahl von Möglichkeiten, die von der Kreditkarte über die normale Banküberweisung und den Bankeinzug bis hin zu Internetbezahldiensten wie PayPal und ClickandBuy reichen. Einige dieser Bezahldienste übermitteln dem Anbieter direkt eine Bezahlbestätigung, sodass dieser den Versand der Ware

unmittelbar einleiten kann. All diese Zahlungsarten haben Vor- und Nachteile, die in der folgenden Abbildung aufgelistet sind. Eine generelle Empfehlung, für welche Methode Sie sich entscheiden sollten, gibt es nicht. Wählen Sie die Methode immer entsprechend dem Einkauf. Die Vorabüberweisung beispielsweise birgt immer die Gefahr, dass Sie etwas bezahlen, was später nicht geliefert wird; sie ist also nur bei kleinen Beträgen und vertrauenswürdigen Händlern sinnvoll. Das Wichtigste ist, sich immer mit unterschiedlichen, sehr guten Passwörtern – oder zukünftig mit dem elektronischen Personalausweis (siehe Seite 61 ff.) – abzusichern. Teilweise bieten die Bezahldienste zusätzliche Sicherheitsmechanismen wie eine Treuhandfunktion an, die Sie auch verwenden sollten.

Die sicherste Art zu zahlen ist, sich die Ware auf Rechnung schicken zu lassen und den Betrag im Nachhinein zu überweisen. So geht der Käufer nicht in Vorleistung und kann die Ware prüfen. Leider wird diese Möglichkeit nur selten angeboten, da sie ein größeres Risiko für den Onlineshop darstellt, nicht oder nur mit Verzögerung an sein Geld zu kommen.

TIPP: Sicher bezahlen

- Versuchen Sie, die Bezahlart dem Onlineshop anzupassen. Beim ersten Kauf ist der Lastschrifteinzug nicht die beste Wahl.
- Denken Sie daran, dass Ihnen als privater Käufer ein gesetzliches Umtauschrecht innerhalb von zwei Wochen zusteht.
- Kaufen Sie möglichst bei Onlineshops aus dem Inland, um rechtliche Schwierigkeiten im Ausland zu vermeiden.
- Überprüfen Sie Ihre Kontoauszüge auf Richtigkeit, wenn Sie etwas im Internet bezahlt haben.
- Bewahren Sie Bestellbestätigungen und Rechnungen in gedruckter oder digitaler Form auf!

Bezahlart	Vorteile	Nachteile
Kredit-karte	• Schnell • Weltweit anerkannt • Geldrückbuchung bei Missbrauch möglich	• Oft erneute Dateneingabe notwendig – Gefahr der Ausspähung • Verteilen von Finanzinformationen im Internet
Vorkasse	• Bekanntes Verfahren (einfach) • Es werden keine Finanzdaten des Käufers über das Internet ausgetauscht	• Langsam, da die Ware erst nach Geldeingang versendet wird • Basiert auf dem Vertrauen, dass der Onlineshop die Ware tatsächlich schickt • Einmal überwiesenes Geld lässt sich nicht zurückholen
Rechnung	• Kein finanzielles Risiko • Schnell • Es werden keine kritischen Finanz-daten über das Inter-net ausgetauscht	• Wird meist nur für Firmen oder Stammkunden angeboten
Nach-nahme	• Schnell • Es werden keine Finanzdaten über das Internet ausgetauscht	• Das Paket muss persönlich entgegen-genommen werden • Bei fehlerhafter Ware kann es zu Schwierig-keiten bei der Rücknahme kommen • Hohe Gebühren
Last-schrift-verfahren	• Geld kann in einer bestimmten Frist «zurückgeholt» werden	• Es werden Finanz-daten über das Internet ausgetauscht

	• Schnell	• Kontodeckung muss muss gewährleistet sein, sonst fallen teure Gebühren an
PayPal	• Sehr schneller Geldtransfer (wenige Minuten) • Käuferschutz bei ebay, teilweise Kostenvorteile beim Versand • Daten werden nur bei PayPal gespeichert, nicht bei mehreren Shops • Giropay, Kreditkarte, Lastschrift und Überweisung nutzbar	• Ein zentraler Account; ein Angreifer sollte Ihren PayPal-Account keinesfalls knacken können, deshalb unbedingt ein absolut sicheres Passwort wählen • Nicht bei jedem Onlineshop verfügbar
Online-Überweisung Giropay	• Vorteile wie bei «Rechnung» • Konzept der Banken • Daten nur der Bank bekannt (PIN und TAN) • Händler bekommt sofort Bezahlbestätigung	• Nicht bei jedem Onlineshop verfügbar • Nicht mit jeder Bank möglich
Clickand Buy (Firstgate)	• Vorteile wie bei «PayPal» (bis auf Käuferschutz bei ebay)	• Siehe PayPal

Abbildung 26: Vor- und Nachteile verschiedener Zahlungsarten im Internet

Auktionshäuser im Internet – 3, 2, 1 … Falle

Zum Ersten, zum Zweiten und zum Dritten. Etwas Nervenkitzel ist immer dabei, wenn eine Auktion läuft, und er macht den Kauf oftmals zu einem richtigen Erlebnis. Auch online ist das Ersteigern von Waren ganz groß in Mode und soll sogar süchtig machen. Stolze 8,541 Milliarden Euro betrug der Umsatz von ebay im Jahr 2008 und belegt damit eindrucksvoll die Beliebtheit von Onlineauktionen. Das bekannteste und weltweit größte Internetauktionshaus ist eine Instanz im Internet und soll hier als Beispiel dafür dienen, wie sicher oder unsicher Onlineauktionen sind. Auch die Frage, wie man sich dabei optimalerweise verhält, wird natürlich beantwortet.

Diese Fallen lauern bei Internetauktionen

Was das Bezahlen und die Registrierung angeht, gelten für Internetauktionen genau dieselben Regeln wie für den Onlineeinkauf (siehe Seite 113 ff.). Allerdings lauern auf Auktionswebseiten zusätzliche Gefahren. Denn im Gegensatz zu Einzelhändlern, bei denen es einen Verkäufer und viele Kunden gibt, kann bei ebay jeder die Rolle des Käufers und des Verkäufers übernehmen. Die geschäftlichen Verbindungen sind also extrem vielfältig und verwoben. Beliebt bei den Angreifern ist es daher, einen fremden ebay-Account zu «übernehmen». Die Zugangsdaten eines ebay-Mitglieds werden ausspioniert, und der ebay-Account eignet sich dann hervorragend, um fiktive Waren zu verkaufen. Die Folgen muss der Besitzer des ebay-Accounts ausbaden, der in den meisten Fällen überhaupt nichts davon mitbekommen hat. Es sei denn, er schaut während der falschen Auktionen in seinen ebay-Account, was jedoch

nur möglich ist, wenn die Angreifer sein Passwort und seine Daten in der Zwischenzeit nicht bereits geändert haben. Und genau das werden sie, damit der Nutzer nicht mehr an seinen ebay-Account herankommt. Die Übernahme Ihres ebay-Accounts können Sie vermeiden, indem Sie sichere Passwörter (siehe Seite 53f.) verwenden und die Zugangsdaten nicht weitergeben. Wenn sich alle daran halten, wird es für Angreifer sehr schwer, hier Missbrauch zu betreiben.

Aber warum sollte jemand auf die Idee kommen, die Zugangsdaten seines ebay-Accounts weiterzugeben? Diese Frage wird oft gestellt, und die wenigsten denken dabei an elektronische Fallen, die im Internet aufgestellt werden. Hier kommt das klassische Phishing zum Einsatz (siehe Seite 100ff.), bei dem der Nutzer aufgefordert wird, auf einen Link zu einer manipulierten Webseite zu klicken. Als Grund wird in diesen Fällen oftmals eine Neuerung am ebay-Account angegeben. Auch ist es möglich, über Cross-Site-Scripting-Angriffe Webseiten entsprechend zu verändern (siehe Seite 32f.). Daher sollten Sie niemals kleine, ominöse Anzeigen anklicken, die beispielsweise Gewinne offerieren oder angeblich zu ebay beziehungsweise einer anderen bekannten Webseite führen. Gewöhnen Sie sich zudem an, sich das Ziel eines Links in der Statusleiste des Browsers anzeigen zu lassen, bevor Sie tatsächlich draufklicken (siehe Seite 29f.).

TIPP: Onlineauktionen

- Verwenden Sie bei Auktionswebseiten nur sichere Passwörter und geben Sie Ihre Zugangsdaten nicht an Dritte weiter.
- Klicken Sie weder in E-Mails noch auf Webseiten auf seltsam erscheinende Angebote, die angeblich zu einem Auktionshaus führen.

- Beachten Sie zudem die Tipps aus den Abschnitten «Internetbrowser» (siehe Seite 26ff.) und «Bezahlen im Internet» (siehe Seite 118ff.).

So bieten Sie sicher mit

Auktionshäuser sind aber keinesfalls ein reiner Sündenpfuhl. Manchmal findet sich durchaus das ein oder andere Schnäppchen, und die Freude ist groß, wenn der Kauf günstig und erfolgreich war. Damit es hinterher jedoch keine bösen Überraschungen gibt, sollten Sie das Angebot und den Anbieter im Vorfeld genau unter die Lupe nehmen. Lesen Sie die Artikelbeschreibungen sorgfältig, damit Ihnen völlig klar wird, was genau zum Verkauf steht. Wenn ein Foto dabei ist, zeigt es eventuell mehr, als letztendlich zu ersteigern ist. So ist nicht selten ein Auto abgebildet, obwohl nur die Reifen angeboten werden.

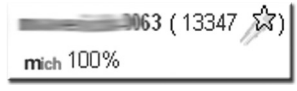

Abbildung 27: Benutzername mit Bewertung bei ebay

Ist ein Anbieter schon lange dabei und hat viele positive Bewertungen erhalten, ist das ein wichtiger Hinweis auf seine Vertrauenswürdigkeit. Deshalb sollten Sie nach jeder Auktion – egal ob Sie Käufer oder Verkäufer sind – eine Bewertung abgeben. Die Anzahl der Bewertungen zeigt sich hinter dem jeweiligen Nutzernamen.

So hat der Verkäufer in Abbildung 27 beispielsweise bereits an 13.347 Auktionen mitgewirkt und im Schnitt eine positive Bewertungsrate von 100 Prozent erhalten. Diesem Verkäufer

sollten potenzielle Bieter eher vertrauen als einem Verkäufer mit 74 oder 30 Prozent. Wollen Sie es genauer wissen, führt Sie ein Klick auf die Zahl hinter dem Verkäufernamen direkt zu den einzelnen Bewertungen.

Die Anbieter bei ebay können sowohl Privatpersonen als auch gewerbliche Händler sein, deren Zahl stark zugenommen hat. Diese unterliegen dann natürlich auch den gesetzlichen Pflichten. Das ist insofern gut zu wissen, da Sie die Ware bei einem offiziellen Händler innerhalb von zwei Wochen zurückgeben können. Wenn sich trotz Bewertung und genauen Studiums des Angebotstextes kein rechtes Vertrauen einstellen will, hilft es oftmals, den Verkäufer per E-Mail anzuschreiben und unklare Punkte noch einmal abzuklären. Die Geschwindigkeit und Art der Antwort gibt ebenfalls Aufschluss über die Vertrauenswürdigkeit des Anbieters.

Hat es dann schließlich mit dem Kauf geklappt, gilt es noch die passende Zahlungsart auszuwählen (siehe Seite 118 ff.), denn gerade bei wertvolleren Produkten ist es nicht unbedingt empfehlenswert, gegen Vorkasse zu bezahlen. Handelt es sich um kleinere Beträge, ist PayPal eine gute Alternative, da es einen Käuferschutz für ebay-Auktionen anbietet und in Fällen von falscher oder nicht gelieferter Ware das Geld erstattet. Bei größeren Summen bietet sich ein Treuhandservice an, der das Geld verwahrt, bis der Artikel ordnungsgemäß an seinem Bestimmungsort angekommen ist (Softlink 361).

TIPP: Sicheres Mitbieten bei Onlineauktionen

- Lesen Sie das Angebot genau, damit Sie exakt wissen, worum es sich bei dem Verkaufsgegenstand handelt.
- Fragen Sie bei Unklarheiten per E-Mail beim Händler nach, bevor Sie mitbieten.

- Überprüfen Sie die Bewertungen des Anbieters und wie lange er schon bei ebay aktiv ist.
- Beachten Sie, ob ein Händler oder eine Privatperson anbietet.
- Überprüfen Sie die angebotenen Zahlungsmöglichkeiten und nutzen Sie bei höheren Summen eine Bezahlart mit Käuferschutz oder sogar einen Treuhandservice.

Freuen Sie sich auf Teil 5:
Sicher bewegen im Internet – Internettelefonie & Chatten,
Kindersicherung fürs Internet

Ab 04.02.2013 zum kostenlosen Download auf
www.internet-sicherheit.de