W-LAN
Cookies
Datenschutz
Trojaner
Online-Banking
Viren
Browserkonfiguration
Sicherheitszertifikat
Würmer
Keylogger
Gütesiegel
Firewall
Kreditkartenzahlung
Treuhänder
mTAN
Passwort
Escrow service
Hacker

Sicher durchs Internet

Ein Leitfaden für Verbraucher und Anbieter

Spyware
Kundendaten
Abofallen
Malware
Aktive Inhalte
Bewertung

Deutschland
VERBINDUNGSSTELLE

eCommerce-Verbindungsstelle Deutschland

- Nationale Anlaufstelle für Nutzer und Anbieter –

Die eCommerce-Verbindungsstelle Deutschland wurde zum 1. Januar 2003 beim Zentrum für Europäischen Verbraucherschutz e.V. (vormals Euro-Info-Verbraucher e.V.) eingerichtet.

Dies beruht auf einer Entscheidung des Bundesministeriums der Justiz, welches diese nationale Verbindungsstelle für den elektronischen Geschäftsverkehr seit ihrer Gründung auch finanziert.

Die eCommerce-Verbindungsstelle befasst sich mit allen Fragen rund um den Vertrieb von Waren und Dienstleistungen über das Internet und richtet ihr Beratungsangebot gleichermaßen an Unternehmer wie Verbraucher.

Auf unserer Homepage finden Sie umfangreiche ergänzende und vertiefende Informationen zum Recht im Internet sowie Hinweise auf diverse Organisationen und weitere Ansprechpartner zu speziellen Themen des eCommerce.

Bei konkreten Fragen können Sie gerne direkt Kontakt mit uns aufnehmen:

eCommerce-Verbindungsstelle Deutschland
beim Zentrum für Europäischen Verbraucherschutz e.V.
Bahnhofsplatz 3 | D - 77694 Kehl am Rhein
Telefon: +49 (0)7851 9 91 48-0
Telefax: +49 (0)7851 9 91 48-11

www.ecommerce-verbindungstelle.de
oder ganz einfach: **www.ecom-stelle.de**

Felix Braun
Rechtsassessor
eMail: info@ecommerce-verbindungsstelle.de

Inhaltsverzeichnis

Einleitung

Das Internet ist für viele Menschen heutzutage fester Bestandteil des täglichen Lebens. Ob Einkauf oder Urlaubsplanung und -buchung, Senden und Empfangen privater und geschäftlicher E-Mails, Recherche von Informationen aller Art und nicht zuletzt Engagement in *social networks*: Das World Wide Web bietet eine Fülle von Möglichkeiten, vom PC aus Kontakte zu pflegen, Geschäfte abzuwickeln und sich auf angenehme Weise die Zeit zu vertreiben.

Wichtig bei alledem ist, gerade im elektronischen Geschäftsverkehr, auf die eigene Online-Sicherheit zu achten.

Die Nutzung des Internet birgt unterschiedliche Risiken. Allerdings kann jeder Nutzer selbst dafür sorgen, diese Gefahren gering zu halten. Dazu bietet diese Druckschrift Hilfestellung an.

Die Broschüre wendet sich sowohl an Unternehmer als auch an Verbraucher und bietet wichtige Informationen rund um das Thema „Sicheres Bewegen im Internet“. Dabei verschafft sie einen Überblick über konkrete im Web lauernde Gefahren und gibt Tipps, wie sich der Einzelne – vorbeugend – davor schützen kann. Darüber hinaus werden praktische Empfehlungen gegeben, was zu tun ist, wenn sich eine bislang abstrakte Bedrohung tatsächlich einmal realisiert und ein Schaden eintritt. In diesem Zusammenhang werden technische und rechtliche Hintergründe dargestellt.

Da gerade das Internet immer wieder mit Neuheiten aufwartet, versteht sich dieser Leitfaden auch als Anregung für seine Leser, auf der Grundlage der hier vermittelten Informationen selbst nachzuforschen und aktiv nach Neuheiten Ausschau zu halten.

Selbstverständlich können Sie sich gerne mit konkreten Fragen jederzeit an uns wenden.

Gesicherter Computer

Wer sich möglichst sicher im Internet bewegen will, muss rechtzeitig Vorsorge treffen und seinen Computer schützen. Das ist der erste Schritt zu einer erheblichen Minderung des Schadenrisikos. Art und Umfang der Sicherungsmaßnahmen richten sich primär nach den persönlichen Qualitätsansprüchen und Nutzungsgewohnheiten des jeweiligen Anwenders.

Ein leistungsfähiges **Viren-Schutz-Programm** sowie eine **Personal Firewall** – jeweils mit regelmäßigen Updates sämtlicher Anwendungen – sind unerlässlich. Auch das **Betriebssystem** sollte immer **aktuell** gehalten werden. **Passwörter** und sonstige **Codes** sind sinnvoll auszuwählen und sicher aufzubewahren.

Weitere hilfreiche Informationen können auf dem Internet-Portal der **eCommerce-Verbindungsstelle Deutschland** (www.ecommerce-verbindungsstelle.de) abgerufen werden.

Risiken im Internet

Ob Viren, Würmer oder Trojanische Pferde, Phishing, SPAM oder Kostenfallen – in der Nutzung des World Wide Web lauern die unterschiedlichsten Gefahren. Dieser Abschnitt handelt von den Risiken, auf die der Anwender vorbereitet sein sollte und davon welche vorbeugenden und nachsorgenden Gegenmaßnahmen empfehlenswert sind.

Schadsoftware und -programme

Zu den sog. Schadprogrammen zählt jede Malware, die auf den von ihnen befallenen Rechnern (aus der Sicht des Nutzers) unerwünschte Funktionen ausführt. Zu den bekanntesten zählen **Viren** (Boot-, Datei- bzw. Makro-Viren), **Würmer**, Trojanische Pferde (sog. **Trojaner**) sowie sonstige **Spyware** (z. B. Cookies, Keyloggers etc.). Zusätzliches Gefahrenpotential erwächst daraus, dass viele dieser Programme über das Internet **automatisch weitere Funktionen nachladen** und sich – ähnlich wie ihre natürlichen Namensvettern – **ständig verändern** können. Damit nicht genug: Oft ist diese Malware so programmiert, dass sie den bereits „eroberten“ Computer als Ausgangsbasis für weitere selbständige **Angriffe gegen andere Rechner** benutzt, um auch diese zu infizieren. Und dies bemerken die ahnungslosen Nutzer meist erst viel später.

Die Problem-Software kann auf unterschiedlichen Wegen in den Computer eindringen, etwa durch das Verwenden eines **virus-verseuchten USB-Sticks** oder im **Anhang eingehender E-Mails**, die dem User eine vermeintlich nützliche Anwendung versprechen oder mutmaßlich eine Rechnung enthalten. Beim

Anklicken des Attachments wird dann der Schadorganismus in das Betriebssystem eingeschleust.

Mittlerweile werden von IT-Übeltätern ganze – auch seriöse, allgemein beliebte – Webseiten mit schädlichem Code infiziert. Dies geschieht z. B. über einen dort eingeblendeten **„vergifteten" Werbebanner**, der auf einem fremden Server gehostet wird. Ein Aktivieren der Internetwerbung ist nicht erforderlich, die Ansteckung erfolgt durch einen sog. Drive-by-Download, also „beiläufig".

Eine weitere beträchtliche Risikoquelle steckt in dem enormen Angebot an **kostenlosen** – zum Teil durchaus nützlichen – **Web-Programmen**, in denen sich nicht selten auch Cyber-Geziefer verbirgt. Das gilt auch für sog. Raubkopien und IT-Module zur unbefugten Gratis-Nutzung regulär kostenpflichtiger Programme.

Risikoreich ist auch das Öffnen von E-Mails bzw. Anhängen unbekannter oder zweifelhafter Herkunft. Bei den **Dateitypen** mit den Endungen .exe, .bat, .com, .do*, .xl*, .ppt, .scr oder .vbs ist besondere Vorsicht geboten. Aber auch gängige Dateiformate wie .doc können betroffen sein.

Bei **Verdacht auf Malware-Infektion** des eigenen Computers gilt es folgendes zu beachten:

- Ruhe bewahren! Die Arbeit am Rechner zügig auf dem üblichen Weg beenden. Computer ausschalten!
- Experten-Rat erholen! Zur Eliminierung der Malware bedarf es angesichts der unzähligen verschiedenen Cyber-Schädlinge mitunter besonderer Fachkunde.

- Umstellung des Computers, so dass zuerst das CD-Laufwerk ausgeführt („gebootet") wird. Neustart des Rechners über eine nicht befallene System- bzw. Boot-CD.
- Schadcode-Scan mit einem *aktuellen* Viren-Schutzprogramm und Beseitigung der Problem-Software.
- Datensicherung durchführen.
- Wiederherstellen der ursprünglichen Boot-Reihenfolge des Rechners (Ausführen zunächst von der Festplatte).
- Ggf. virusbedingt gelöschte oder beschädigte Daten durch solche aus der Datensicherung, beeinträchtigte Programme aus den Sicherungskopien der Programme rekonstruieren, bzw. reinstallieren.

- Im Zweifel den Rechner aus einem vertrauenswürdigen Backup neu formieren.

Phishing | Spoofing

Unter „Phishing“ bzw. „Spoofing“ versteht man die Beschaffung persönlicher Daten anderer Personen (z. B. Passwort, Kreditkartennummer etc.) mit gefälschten E-Mails oder Websites. In seriöser Aufmachung getarnt fordern die IT-Betrüger den Empfänger unter einem **Vorwand** (z. B. zur Erneuerung des Passwortes, zur Bestätigung von Kontoinformationen etc.) auf, seine Daten zu „aktualisieren“. Die Cyber-Kriminellen bedienen sich dabei der täuschend ähnlichen **Nachahmung einer vertrauenswürdigen Bank- oder Firmen-Website**. Mit den so ergaunerten Daten erleichtern die IT-Ganoven sodann die Konten ihrer Opfer.

Gegen „Phishing“ hilft nur: Genau hinschauen und im Zweifel in geeigneter Weise – z. B. telefonisch – überprüfen, ob die geforderten Informationen herausgegeben werden sollten.

Vertiefende länderübergreifende Hinweise zu diesem Bereich – einschließlich Phishing-Anzeigen – bietet die *Anti-Phishing Working Group (APWG)* (www.antiphishing.org). In Deutschland stellt die bei der Ruhr-Universität Bochum angesiedelte *Arbeitsgruppe Identitätsmissbrauch im Internet e.V. (A-I3)* (www.a-i3.org) auf ihrem Online-Portal aktuelle Informationen zu Themen der IT-Sicherheit bereit und bietet konkrete Hilfestellungen.

Denial-of-Service-Attacken (DoS)

Als „Denial of Service“ (deutsch: Dienstverweigerung) wird in der digitalen Datenverarbeitung die Nichtverfügbarkeit eines Dienstes bezeichnet. Hierbei wird – soweit es sich nicht um eine unabsichtliche Beeinträchtigung handelt – durch einen mutwilligen Angriff auf einen Server, einen Rechner oder sonstige Komponenten in einem Datennetz deren **Arbeitsunfähigkeit** herbeigeführt. Betroffen hiervon sind allerdings meistens größere Netzwerkeinheiten.

Botnetze

Unter dem Begriff „Bot“ wird ein Programm verstanden, das – meist von IT-Kriminellen kreiert und in großer Zahl auf vielen fremden Computern eingeschleust – ferngesteuert auf dem PC des Nutzers arbeitet. Zentral gelenkt werden diese Bots zu sog. Botnetzen zusammengeführt und für bestimmte Aktionen (z. B. **SPAM**) – in der Regel zum finanziellen Nachteil der Anwender – missbraucht. Auch hier können bereits „eroberte“ private oder geschäftliche Rechner ihrerseits – ohne Wissen und Wollen des Besitzers – **Malware an weitere Web-Teilnehmer** versenden.

Detaillierte Informationen zum Thema „Bots“ und „Botnetze“ hält das Anti-Botnet-Beratungszentrum (www.botfrei.de) bereit.

Hacker | Cracker

Auf dem Gebiet der Computersicherheit wird als „Hacker“ eine Person beschrieben, die versucht, Sicherheitsmechanismen in IT-Systemen zu überwinden, Schwachstellen zu erkennen und/oder zu unterwandern oder in Bezug auf Design- und Programmierfehler zu untersuchen. Völlig unbedenklich ist dies, wenn es auf Weisung von Firmen geschieht, die Sicherheitslücken in ihrem eigenen System aufspüren lassen wollen.

Problematisch kann das „Hacken“ dann sein, wenn es ohne Auftrag eines Berechtigten vorgenommen wird, selbst wenn dadurch kein weiterer Schaden entsteht. Allerdings spüren Hacker bei ihrer Tätigkeit oftmals **Schwachstellen oder Sicherheitsdefizite in öffentlichen oder privaten Computernetzwerken** auf, machen öffentlich darauf aufmerksam und geben damit zum Teil wichtige Anstöße für die Weiterentwicklung der Sicherheit des Internets.

Ist das unbefugte Eindringen in fremde PC-Systeme begleitet von der widerrechtlichen Manipulation von Software, z. B. dem Entfernen von Software-Kopierschutz- und Sicherheitsmechanismen und treten ggf. noch weitere Schädigungsakte hinzu, so spricht man bei den IT-Tätern von „Crackern“.

Wirkungslose Antiviren-Software

In zunehmendem Maße probieren IT-Betrüger, Web-Nutzer dazu zu verleiten, falsche Antivirensoftware auf ihre Computer downzuloaden: Beim Surfen im Internet erscheint plötzlich ein **manipulierter Warnhinweis**, der Rechner habe sich einen Virus oder ein anderes Schadprogramm zugezogen. Zur „Lösung“ des Problems wird dem User ein vorgebliches **Gratis-Virenschutzprogramm** angeboten. Nach dessen Installation kommt in der Regel die Aufforderung, auch noch die kostenpflichtige Version des Programms herunterzuladen. Lehnt der Anwender dies ab, werden immer wieder fingierte Malware-Warnungen angezeigt bzw. Zahlungsaufforderungen verschickt.

Mitunter wird durch das Herunterladen des „Antivirenprogramms“ der eigene Computer **zusätzlich mit Schadsoftware infiziert**. Meist besteht das Ziel der Web-Gauner in erster Linie darin, dem User ein nutzloses Virenschutzprogramm zu verkaufen und dabei an sensible Daten des Kunden (Kontoverbindung, Kreditkarteninformationen etc.) heranzukommen.

Dagegen hilft eine gesunde **Skepsis gegenüber Anbietern angeblich kostenloser Software**. Zwar gibt es durchaus brauchbare kostenlose Antiviren-

Programme, doch sollte man sich diesbezüglich vor einer Registrierung bzw. Installierung genau informieren.

Um festzustellen, ob der eigene Rechner tatsächlich durch Malware befallen ist, sollte man sich im Zweifel der Hilfe eines IT-Experten bedienen.

Imitierte E-Mail-Anschriften

Nicht selten verbergen sich hinter vertrauenerweckenden E-Mail-Adressen Internetkriminelle, die – **als bekannte Organisation oder Unternehmen getarnt** – Malware in fremde Computersysteme einschleusen, die dort ihre schädliche Arbeit verrichten. Ebenso kommt es vor, dass die **E-Mail-Anschriften persönlicher Bekannte, Freunde oder Verwandter** des späteren Opfers von den Tätern missbräuchlich verwendet werden, um Viren, Würmer oder Trojaner beim Adressaten wirksam werden zu lassen, wenn dieser – arglos – die Nachricht öffnet.

Neben einem **aktuellen Virenschutzprogramm** ist es hilfreich, das persönliche E-Mail-Programm so einzustellen, dass sich Nachrichten beim Eingehen nicht automatisch öffnen. Schaltet man diese sog. **Autovorschau aus**, so bleibt in jedem Fall genügend Zeit, sich die sichtbaren Mitteilungsbestandteile (Absender-Adresse, Betreff, ggf. weitere Empfänger-Anschriften, cc-Adressen) genau anzuschauen, bevor sie – und damit auch die Schadsoftware – aktiviert wird. Im Zweifel gilt: Lieber die **dubiose E-Mail ungelesen löschen**, als das Risiko einer Schädlingsinfizierung eingehen.

SPAM

Massenhaft versandte unverlangte E-Mails (SPAM) verstopfen nicht nur die virtuellen Briefkästen ihrer Empfänger; sie sind darüber hinaus – jedenfalls in Deutschland – verboten. An die Adressen ihrer Opfer gelangen die Spammer zum Teil über – **legale wie illegale** – **Adresshändler**. Ebenso werden von ihnen im Internet systematisch Websites, Newsgroups, E-Mail-Verzeichnisse etc. nach entsprechenden IT-Anschriften durchsucht.

Es empfiehlt sich, die entsprechenden Nachrichten auf keinen Fall zu öffnen oder zu beantworten, sondern sofort zu **löschen** bzw. – sofern die PC-Software die entsprechende Mitteilung automatisch in einem SPAM-Ordner ablegt – den Inhalt dieser SPAM-Mailbox regelmäßig – vorzugsweise täglich – zu entfernen. Der **Anti-SPAM-Schutz** des E-Mail-Providers sollte durchgehend aktiviert sein. Hilfreich kann auch sein, sich in die sog. **Robinsonliste** (www.robinsonliste.de) des Interessenverbandes Deutsches Internet e.V. einzutragen. Die kooperierenden Unternehmen haben Einblick in diese Liste und können die eingetragenen Adressen aus ihrer eigenen Datenbank tilgen.

Hoax

Die Bezeichnung „Hoax“ wird für im Internet kursierende **Falschmeldungen** verwendet. Dazu zählen etwa fingierte Warnungen vor angeblich bösartigen Computerprogrammen. Allen Hoax-Mails ist gemeinsam, dass sie lästig sind und den Empfänger Zeit kosten. Riskant wird es für den User dann, wenn er den in solchen Mail-„Enten“ enthaltenen **Verfahrensanweisungen** nachkommt, soweit diese seinen eigenen Rechner berühren. Die Gefahr ist groß, dass beim Befolgen solcher Verhaltensregeln – statt der Beseitigung vermutlich ohnehin nicht vorhandener Viren etc. – z. B. wichtige **Systemdateien gelöscht oder beschädigt** werden und daraus gravierende Komplikationen erwachsen.

Es rentiert sich immer, derlei fragwürdige Nachrichten (z. B. unseriöse Spenden- oder Protestaufrufe, Kettenbriefe etc.) besonnen unter die Lupe zu nehmen. Daher sollten solche E-Mails sofort gelöscht und auch auf keinen Fall an Dritte weitergeleitet werden.

Kostenfallen im Internet

Der Umsatz im Onlinehandel wächst weltweit. Von der großen Bereitschaft, Geld im Internet auszugeben, profitiert allerdings auch das organisierte Verbrechen ebenso wie IT-Einzeltäter. Sie stellen im Internet sog. Kostenfallen auf, bei denen Verbraucher **unbeabsichtigt** eine **kostenpflichtige Leistung** (Waren oder Dienstleistungen) **„einkaufen“**. Die betreffenden Internetofferten sind dabei so raffiniert aufgemacht, dass deren Entgeltlichkeit für den PC-Nutzer **nicht ohne weiteres erkennbar** ist.

Von Filmen und Gratis-SMS, über Routenplaner, Musikdateien, und Software bis hin zu Immobilien und Kraftfahrzeugen – so vielfältig die „vergifteten“ Angebote sind, so ähnlich sind die **Methoden**, mit welchen die Online-Kriminellen vorgehen:

Ausgelegte Köder

Die umworbenen Kunden werden mit allerlei angeblich kostenlosen Zugaben angelockt:

- **Geschenk:** Der Anbieter winkt mit einem Geschenk oder einer anderen Gratis-Leistung (z. B. kostenlose Warenproben) für den Interessenten, sobald dieser sich registriert hat.
- **Kostenloser „Online-Test“:** Das Lockangebot besteht aus einem angeblich unentgeltlichen Psycho- oder Intelligenztest. Doch mit dem Absenden der ausgefüllten Maske, erklärt der Interessent unbemerkt sein Einverständnis zu einem kostenpflichtigen Angebot.

- **Gewinnspiel:** Der ahnungslose User glaubt, an einem kostenlosen Gewinnspiel teilzunehmen. Tatsächlich ist dies aber an ein Abonnement gekoppelt oder es werden doch „Gebühren" für die Teilnahme erhoben.
- **Testphase:** Das Angebot besteht darin, einen Dienst angeblich kostenfrei zu testen. Wenn der Nutzer dann, um von diesem Angebot Gebrauch zu machen, seine Daten übermittelt, meldet er sich für ein Abonnement an, das automatisch kostenpflichtig wird, wenn er sich nicht bis zu einem bestimmten Zeitpunkt (z.B. bis Mitternacht desselben Tages) wieder abmeldet.

Beispiel: Registrierung

Oftmals werden Verbraucher, die angebotene Dienste oder Waren ggf. noch gar nicht in Anspruch nehmen, sondern sich **zunächst nur informieren** wollen, aufgefordert, sich auf der entsprechenden Internetseite zu registrieren und ihre persönlichen Daten einzugeben. Dies wird z. B. damit begründet, dass die Anschrift für die Zusendung des Gratis-Geschenks erforderlich sei; gelegentlich werden auch nur allgemeine Motive (z. B. „Vertrauen" oder „Sicherheit") angeführt. Tatsächlich benötigt der Anbieter die Personalangaben des Users, um ihm später – **nur für die Registrierung** (!) – eine **Rechnung** übersenden zu können. Hier ist aber vor einer Zahlung genau zu überprüfen, ob überhaupt ein wirksamer Vertrag geschlossen wurde oder die Möglichkeit eines Widerrufs besteht. Dies ist nach der seit dem 1. August 2012 in Kraft getretenen Button-Lösung oft nicht der Fall, und die geltend gemachten Forderungen sind dann unberechtigt (siehe hierzu den nachfolgenden Abschnitt *Neuheit: Button-Lösung*, Seite 13 f.).

Beispiel: Immobilien und Kraftfahrzeuge

Betroffen von den illegalen Machenschaften sind z. B. Internetportale, auf denen Häuser, Wohnungen und Kraftfahrzeuge vermittelt werden. Die Vorgehensweise der Web-Anbieter ist stets die gleiche: Sie offerieren auf populären Internet-Plattformen bestimmte Handelsgüter, die sie gar nicht besitzen oder die ihnen nicht gehören. Unter einem **Vorwand** lassen sich die Betrüger von den jeweiligen Interessenten **Vorabzahlungen** leisten. Wenn dann der Schwindel auffliegt, ist das Geld verloren und die Täter unerkannt abgetaucht.

Beim **Immobilien-Betrug** geben sich die Online-Gauner auf großen deutschen Internetportalen als Eigentümer bzw. Vermieter aus und bieten Häuser und Wohnungen zum Kauf oder zur Miete an. Die Annoncen sind unauffällig gestaltet, regelmäßig sogar mit Fotos der einzelnen Objekte, und von seriösen Angeboten kaum zu unterscheiden. Die **Kontaktaufnahme** durch den Interessenten ist meistens **nur per E-Mail** möglich. Will dieser dann Haus oder Wohnung besichtigen, verlangt der vermeintliche Immobilieninhaber vorab eine **Geldzahlung**, oft in Höhe einer Monatsmiete, und zwar regelmäßig nicht durch Banküberweisung, sondern **über einen internationalen Geldtransfer-**

dienstleister. Zahlt der Interessent, ist eine Wiederbeschaffung des Geldes so gut wie ausgeschlossen.

Der **Auto-Betrug** im Internet folgt dem gleichen Muster: Dort wird der Interessent ebenfalls per E-Mail aufgefordert, etwa zum Zweck der **Reservierung** des Fahrzeugs oder als Vorschuss auf den Kaufpreis, eine **Anzahlung per Bargeldtransfer** zu leisten. Auch in diesem Fall existiert das angebotene Fahrzeug in der Regel nicht, und der Käufer kann sein Geld „abschreiben".

Eine besonders **hinterhältige Variante** besteht darin, dass der Online-Betrüger dem Käufer nahelegt, das Geld per Bargeldtransfer **an einen Bekannten oder ein Familienmitglied** zu überweisen und die Kopie des Einzahlungsbelegs per E-Mail zu versenden. Der Käufer wiegt sich dabei in Sicherheit, da nach seiner Vorstellung nur die ihm bekannte Person das Geld in Empfang nehmen kann. Sobald der Gauner jedoch die Identität des Geldempfängers kennt, wird der Betrag mit entsprechend **gefälschten Ausweispapieren** unter dem Namen des Bekannten bzw. Familienmitglieds abgehoben.

Zu bedenken bleibt: Der Umstand, dass eine Annonce auf einem generell als vertrauenswürdig geltenden Portal platziert ist, sagt nichts über die **Seriosität der jeweiligen Offerte** aus. Denn bei den meisten Internet-Anzeigenmärkten wird lediglich der Kontakt zwischen Interessent und Verkäufer/Vermieter hergestellt. Die **Identität** der Anbieter, deren **Bonität** wie auch die **Existenz der angebotenen Handelsware** (Haus, Wohnung, Auto, etc.) werden vom Betreiber des Onlineportals in der Regel **nicht geprüft**.

Als Interessent sollte man bei der Haus-, Wohnungs- und Pkw-Suche im Internet genau die einzelnen **Angaben in der Annonce prüfen** und unbedingt einen **persönlichen Termin zur Besichtigung** der Immobilie bzw. des Fahrzeugs **vereinbaren**. Vor allem gilt: **Niemals einen Vorschuss** an den Anbieter oder sonstige Personen zahlen, erst recht nicht durch Bargeldanweisung über einen Anbieter von weltweiten Bargeldtransfers. Das gilt selbst dann, wenn das Geld als „Sicherheit" oder „Liquiditätsnachweis" an eine persönlich bekannte Person (Freund, Verwandter, etc.) versandt werden soll!

Weitere Beispiele für Kostenfallen im Internet sind auf der Website der E-Commerce-Verbindungsstelle Deutschland verfügbar.

Neuheit: Button-Lösung

Weil unseriöse Geschäftspraktiken im Internet immer wieder für Unmut sorgten, trat zum 1. August 2012 eine gesetzliche Regelung in Kraft,

durch welche speziell Online-Kostenfallen entschärft werden sollen. Diese gilt allerdings nur im Falle der Bestellung eines Verbrauchers bei einem Unternehmer, also im B2C-Bereich.

Beschriftung des Bestellknopfes

Ein wesentliches Kernstück dieser Gesetzesnovelle besteht in der Neufassung des 312 g BGB. Damit werden den Shop-Betreibern zum einen die Beschriftung des sog. Bestell-Buttons vorgegeben und zum anderen neue Informationspflichten übertragen.

Die Schaltfläche des Bestellbuttons ist nunmehr so zu beschriften, dass der Verbraucher bei Abgabe seiner vertragsrelevanten Erklärung **eindeutig und unmissverständlich** die Information erhält, dass seine **Bestellung** nunmehr (mit dem Klick auf diesen Button) eine **finanzielle Verpflichtung auslöst**.

Nicht mehr zulässig sind z. B. die Bezeichnungen „Anmeldung", „Weiter", „Bestellen" oder „Bestellung abgeben". Als **zulässige Beschriftungen** nennen das Gesetz bzw. die Gesetzesbegründung folgende Beispiele: ***„zahlungspflichtig bestellen"***, ***„kostenpflichtig bestellen"***, ***„zahlungspflichtigen Vertrag schließen"*** und ***„kaufen"***.

Weitergehende Informationspflichten

Oberhalb des Bestell-Buttons müssen folgende **Informationen** „*unmittelbar bevor der Verbraucher seine Bestellung abgibt, klar und verständlich in hervorgehobener Weise*" für den Nutzer ersichtlich sein:

- die **wesentlichen Merkmale** der Ware oder Dienstleistung,
- die **Mindestlaufzeit des Vertrages**, wenn dieser eine dauernde oder regelmäßig wiederkehrende Leistung zum Inhalt hat,
- den **Gesamtpreis** der Ware oder Dienstleistung einschließlich aller damit verbundenen Preisbestandteile sowie alle über den Unternehmer abgeführten Steuern oder, wenn kein genauer Preis angegeben werden kann, seine Berechnungsgrundlage, die dem Verbraucher eine Überprüfung des Preises ermöglicht und

- ggf. zusätzlich anfallende **Liefer- und Versandkosten** sowie ein Hinweis auf mögliche weitere **Steuern** oder **Kosten**, die nicht über den Unternehmer abgeführt oder von ihm in Rechnung gestellt werden.

Örtlicher und zeitlicher Zusammenhang | AGB

Diese Informationen müssen in einem direkten örtlichen und zeitlichen Zusammenhang mit der Abgabe der Bestellung durch den Verbraucher gegeben werden. Der Verbraucher soll die **relevanten Informationen direkt zum Zeitpunkt seiner Bestellung zur Kenntnis nehmen** können. Informationen, die bereits zu Beginn des Bestellprozesses (z. B. vor Eingabe der Adressdaten) genannt werden, genügen dann nicht mehr.

Der Bestell-Button muss so platziert sein, dass der **Verbraucher praktisch "gezwungen"** wird, die Informationen zur Kenntnis zu nehmen, bevor er den Bestell-Button betätigen kann. Das bedeutet, dass ein Bestell-Button, der oberhalb der Informationen platziert ist, nicht mehr zulässig ist, weil der Verbraucher dann bestellen könnte, ohne alle Informationen zuvor gelesen zu haben. Auch ein statischer Bestell-Button, der also nicht "mitscrollt", reicht in keinem Fall aus. Denn gerade bei mehreren Produkten im Warenkorb wäre es in diesem Fall möglich, dass der Verbraucher die Bestellung abschließen könnte, ohne alle Informationen vorher zur Kenntnis genommen zu haben. Ebenso nicht mehr in Ordnung ist eine mehrfache Einbettung des Bestell-Buttons. Denn auch dann besteht die Gefahr, dass die obligatorisch zu erteilenden Informationen unterhalb eines der vielen Bestell-Buttons stehen könnten.

Schon nach der vorherigen Rechtslage mussten die Betreiber von Online-Shops die Verbraucher auf ihrem Portal über den **Ablauf des Vertragsschlusses** in ihren Allgemeinen Geschäftsbedingungen bzw. entsprechenden Kundeninformationsseiten in Kenntnis setzen. Auch diese Texte müssen seit dem 1. August 2012 den Vorgaben der Gesetzesnovelle angepasst sein. Zum Beispiel die Information, der Kunde gebe dann eine verbindliche Bestellung ab, wenn er auf den Button „Bestellen" klickt, ist nunmehr falsch, da der Button – wie oben beschrieben – anders beschriftet sein muss.

Die Gesetzesnovellierung gilt für den gesamten – **auch** den **mobilen** – **Online-Handel**, also z. B auch dann, wenn der Online-Shop-Betreiber über eine eigene **„App"** verfügt. Gleiches gilt prinzipiell, wenn der Betreiber z. B. seine Waren über Onlineportale Dritter anbietet. Insbesondere auf sog. **Auktionsplattformen** ist die Angabe von Endpreisen vor Abgabe der Bestellung zwar nicht möglich, dort soll dann das persönliche Höchstgebot angegeben werden. Dort sind **andere Button-Beschriftungen** möglich (***„Gebot abgeben"*** bzw. ***„Gebot bestätigen"***).

Folgen fehlender oder mangelhafter Umsetzung

Ist insbesondere der Bestell-Button nicht richtig beschriftet, kommt **kein Vertrag mit dem Verbraucher** zustande. Alle Online-Unternehmer sollten die oben

angeführten Vorgaben vollständig umgesetzt haben, um Abmahnungen zu vermeiden und um wirksame Verträge mit den jeweiligen Kunden schließen zu können. Fehlende Informationen über den Vertragsschluss haben eine **Verlängerung der Widerrufsfrist** zur Folge. Wegen dieser und anderweitig mangelhafter Umsetzung der gesetzlichen Bestimmungen kann der Shop-Betreiber überdies **wegen Wettbewerbsverstoßes abgemahnt** werden.

Sicheres Agieren im Internet

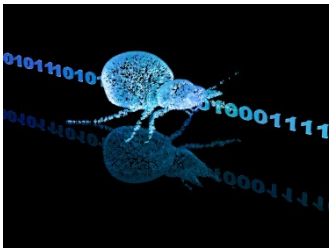
Das Internet bietet nahezu unbegrenzte Möglichkeiten: Telefonieren und chatten, einkaufen und Geld überweisen – viele alltägliche Vorgänge werden heutzutage direkt online erledigt. Doch neue technische Perspektiven lösen auch weitergehende Fragen in Bezug auf die Sicherheit webbasierten Handelns aus. Diesem Thema widmet sich der folgende Abschnitt.

Sicherer Weg ins Internet

Im Internet werden zahlreiche Dienste angeboten, von denen die beiden wichtigsten das **W**orld **W**ide **W**eb („www“) und die „elektronische Post“ („**e**lectronic **M**ail“ – E-Mail) sind. Um überhaupt ins Internet zu gelangen, verwenden viele Nutzer mittlerweile **drahtlose Funknetzwerke, sog. "Wireless Local Area Networks" – WLAN**). Um dann im Internet surfen zu können, wird ein Browser benötigt, also ein EDV-Programm, mit dem Websites gefunden, gelesen und verwaltet werden können.

- **WLAN:** Drahtlose Funknetzwerke ermöglichen die kabelfreie Kommunikation zwischen mehreren lokalen Computern ebenso wie einen mobilen Einstiegsweg ins Internet. Die Zahl der privaten WLAN-Anschlüsse nimmt – ebenso wie die öffentlich eingerichteten WLAN-Zugänge (sog. Hotspots) zu.

  Die Kehrseite der Medaille: Werden Daten durch Funk, also ohne direkte Verbindung zwischen Geräten wie PCs, Tablets oder Smartphones übertragen, so können neben Störungen oder Netzausfällen auch **Sicherheitsprobleme** auftreten. Informationen, die mittels WLAN übertragen werden, können etwa von unbefugten Dritten empfangen, aufgezeichnet und manipuliert werden, wenn sie zuvor nicht ausreichend verschlüsselt und geschützt wurden. Tipps zum sicheren Umgang mit WLAN bietet u.a. das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** (www.bsi-fuer-buerger.de).



- **Browser:** Mit Hilfe eines Web-Browsers können Daten aus dem weltweiten Netz abgerufen und auf dem PC angezeigt und verarbeitet werden. Zu den bekanntesten Browsern zählen u. a. der *Internet Explorer* von Microsoft

und *Firefox* von Mozilla. Mittlerweile können moderne Browser mit Hilfe sogenannter PlugIns, Add-Ons oder Viewer z. B. Graphiken anzeigen, E-Mails versenden sowie für Videokonferenzen und vieles mehr eingesetzt werden.

Genau diese Vielzahl von Funktionen bringt mitunter gravierende Sicherheitsprobleme mit sich. Komplizierte Browser sind potentiell fehleranfällig. Die Hersteller sind bestrebt, auftretende **Programmierfehler** (sog. „Bugs" oder „Bugfixes") zeitnah zu beheben, Sicherheitslücken zu schließen und bislang nicht vorhandene Funktionen nachzurüsten. Dafür bieten sie entsprechende Korrekturauslieferungen, sog. **Patches** (Flicken), an, die der User installieren und damit seinen Browser zu Hause nachbessern kann.

- **Cookies:** Hierbei handelt es sich um kleine Dateien, die ein Web-Anbieter automatisch auf dem Rechner des Nutzers ablegt, um sie jedes Mal dann aufzurufen, wenn der Kunde die Seite desselben Anbieters erneut öffnet. Dies ist für den Kunden komfortabel und von Vorteil, weil er so seinen Warenkorb nicht verliert und auf ihn zugeschnittene Angebote bekommen kann – sollte ihm daran gelegen sein.

Datenschutzrechtlich problematisch sind Cookies, weil der **Datenaustausch** in aller Regel **vom Benutzer unbemerkt** vor sich geht. Zudem kann der Anbieter auf diesem Wege Informationen über das Surfverhalten des Users sammeln, ein **Kundenprofil** entwickeln und dem Nutzer **gezielt Angebote** unterbreiten. Sicherheitsbewusste Internetnutzer können in ihrem Browser einstellen, inwieweit Cookies akzeptiert werden sollen. Wer die Installation von Cookies zulässt, sollte diese **in regelmäßigen Abständen löschen**.

- **Aktive Inhalte:** Firmenseitig voreingestellt gestatten Browser grundsätzlich die Ausführung nicht sichtbarer Programmteile bzw. Skripte, die in den besuchten Internetseiten verborgen sein können (sog. "Aktive Inhalte"). Die bekanntesten sind: Java-Applets, ActiveX-Controls, JavaScripts und VBScripts.

  Über "Aktive Inhalte" können sich so unbemerkt **Spionageprogramme** oder illegale **Dialer** auf dem Computer des Nutzers installieren. Aber auch einmalige Aktionen können beim Besuch einer Website mit Aktiven Inhalten ausgeführt werden, welche die Daten des Users möglicherweise in Mitleidenschaft ziehen.

  Der sicherste Weg dies zu vermeiden, besteht darin, die Funktion **"Aktive Inhalte ausführen"** am eigenen Rechner generell **außer Betrieb** zu setzen und nur bei vertrauenswürdigen Internetseiten gezielt wieder einzuschalten.

Kommunikation über das Internet

Es gibt viele Alternativen, über das Internet mit anderen Teilnehmern in Kontakt zu treten:

- **E-Mail | De-Mail:** Mittels „elektronischer Post“ (E-Mail) werden Informationen und Dokumente unverbindlich übermittelt. Seit dem 3. Mai 2011 ist das **De-Mail-Gesetz** in Kraft, auf dessen Grundlage seither spezielle De-Mail-Dienste angeboten werden. Dadurch ist der verbindliche und vertrauliche Versand elektronischer Dokumente und Nachrichten wesentlich vereinfacht worden. Ihre Bedienung ist mit den bekannten E-Mails vergleichbar, hat aber **zwei wichtige Vorzüge**: Die **Identitäten** der Kommunikationspartner können eindeutig belegt werden, und sie sind **fälschungssicher**. Zudem werden die Nachrichten ausschließlich **verschlüsselt** übertragen und abgelegt; damit sind Sie vor dem Zugriff durch Unbefugte geschützt.

- **Chats:** Sehr beliebt ist die Online-Kommunikation des „Chat“, d. h. der schnelle, direkte Informationsaustausch in Echtzeit. Doch auch hierbei ist Vorsicht geboten: Beispielhaft seien nur fehlende Verschlüsselung, Übermitteln von Schadprogrammen, Verwendung von Skripten sowie gefälschte Benutzerkonten genannt. Dagegen helfen eine **aktuelle Virenschutz-Software** und eine **Personal-Firewall**. Der Nutzer-PC sollte so eingestellt sein, dass Dateien nur nach einer Sicherheitsabfrage gespeichert werden können.

- **Internettelefonie:** Telefonieren über das Internet **("Voice over Internet Protocol" – VoIP)** wird meist dazu genutzt, um sich mit Verwandten oder Freunden im Ausland zu unterhalten. Das Handicap: Telefonate über das Internet können verhältnismäßig **leicht abgehört** werden. Die Übertragung sensibler Daten auf diesem Wege ist daher nicht unproblematisch.

- **Soziale Netzwerke:** Unzählige Menschen weltweit suchen Kontakte und pflegen Freundschaften über das Internet, insbesondere in den sog. „social networks“ (Soziale Netzwerke). Sie offenbaren dabei ihr persönliches „Profil“ mit zum Teil sehr detaillierten beruflichen wie privaten Angaben. Einige der Risiken: Über gefälschte Webseiten versuchen IT-Gauner an die **Zugangsdaten** für soziale Netzwerke heranzukommen oder sie probieren, bestehende **Nutzer-Accounts** zu **hacken**, um diese Identitäten für betrügerische Machenschaften zu nutzen.

Verschlüsselte Kommunikation

Ob E-Mail, Chat oder Internettelefonie: Grundsätzlich besteht die Gefahr, dass Unbefugte mitlesen oder –hören. Eine **zuverlässige Verschlüsselung** stellt sicher, dass nur Berechtigte die Inhalte einer Botschaft entziffern können. Damit werden die **Authentizität** und die **Integrität** von Absender und Empfänger sowie die **Vertraulichkeit** der zwischen ihnen ausgetauschten Verlautbarungen gewahrt.

Suchmaschinen

Programme zur Recherche von Dokumenten, die in einem Computernetzwerk (z. B. World Wide Web) hinterlegt sind (sog. Suchmaschinen), stellen eine unverzichtbare Hilfe beim Aufspüren gesuchter Web-Informationen dar. Sie bergen aber auch Sicherheitsrisiken: In den Ergebnislisten von Maschinen tauchen gelegentlich auch **Links zu gefährlichen Websites** auf, bei deren Besuch Malware-Infektionsgefahr (z. B. Spyware) besteht. Hilfreich sind insoweit eine jeweils aktuelle und aktivierte **Virenschutzsoftware** und **Firewall**.

Der neue Personalausweis

Der zum 1. November 2010 in Deutschland eingeführte neue Personalausweis soll die **Online-Kommunikation** zwischen Bürgern und Behörden sowie Unternehmen **vereinfachen**. Mit ihm ist eine Kennkarte geschaffen worden, die dem Internet-Nutzer eine einfache und zuverlässige **Online-Authentifizierung** ermöglicht. Ein weiterer Vorteil: Mit der neuen Identitätskarte können digitale Dokumente **rechtsverbindlich unterschrieben** werden.

Einkaufen im Internet

Um möglichst sicher online einzukaufen, sollte jeder Internet-Nutzer einige wichtige Ratschläge unbedingt beachten:

- **Angaben des Online-Anbieters:** Zunächst ist es empfehlenswert, den Betreiber des Internetportals anhand seiner **eigenen Angaben** genau unter die Lupe zu nehmen: Ist eine vollständige **Anbieterkennzeichnung** verfügbar? *(Vertiefende Informationen u.a. über **„Das Impressum im Internet“** und **„Shopping Online“** stehen auf dem Internetportal der eCommerce-Verbindungsstelle Deutschland unter www.ecommerce-verbindungsstelle.de zur Verfügung.)* Können die **Allgemeinen Geschäftsbedingungen** eingesehen werden? Sind Informationen zu **Datenschutz** und Datensicherheit greifbar? Sind Angaben zum **Widerrufsrecht**, **Rückgaberecht** und der **Kaufpreisrückerstattung** und verschiedenen **Zahlungsmöglichkeiten** (zu letzterem mehr im nachfolgenden Kapitel *Bezahlen im Internet*, Seite 20 ff.) vorhanden? Stehen Informationen zu **Versandkosten**, **Rücksendekosten** und mögliche **Zusatzkosten** zur Verfügung? Wird der Bestellvorgang durch eine **E-Mail-Bestätigung** verifiziert?

- **Informationen auf Bewertungsportalen:** Beurteilungen von Kunden des entsprechenden Anbieters auf sog. Bewertungsportalen oder in anderen Kommunikationsforen ermöglichen es darüber hinaus, das Bild des Web-Betreibers abzurunden. Man sollte sich jedoch nach Möglichkeit mehrere Bewertungen auf verschiedenen Portalen anschauen und auf das Datum der Beiträge achten.
- **Datenschutz und Datensicherheit:** Es ist darüber hinaus ratsam, dass jeder potentielle Kunde eines Online-Anbieters prüft, wie es um Datenschutz und Datensicherheit beim jeweiligen Web-Händler bestellt ist.
- **Sparsamer Umgang mit Informationen:** Grundsätzlich sollte jeder Internet-User nur die Informationen von sich preisgeben, die zur Abwicklung des jeweils beabsichtigten Geschäfts unerlässlich sind. Es genügt regelmässig, die sog. **Pflichtfelder** auf der Bestellmaske des Anbieters **auszufüllen**. Der **Weitergabe eigener Daten** durch den Händler sollte – von besonders begründeten Einzelfällen abgesehen – **prinzipiell widersprochen** werden. Jeder Web-Nutzer ist gut beraten, sich ebenso gewissenhaft zu fragen, ob die Zusendung von Newslettern und anderen Werbesendungen im Einzelfall tatsächlich erwünscht ist.

Bezahlen im Internet

Online-Händler bieten oft sowohl traditionelle Bezahlmöglichkeiten (z. B. Zahlung auf Rechnung, Nachnahme etc.) als auch elektronische Zahlungsmethoden (z. B. über Bezahlsystem-Anbieter, Kreditkarte etc.) parallel an. Jedes Bezahlverfahren hat Vorzüge und Schwächen. Im Einzelfall gilt es, **Komfort und Sicherheit** in ein vernünftiges Verhältnis zu setzen.

Sollte einem Käufer keines der vom Online-Shop-Betreiber zur Auswahl gestellten Bezahlverfahren zusagen, darf er zwar nicht selbst eine andere Zahlungsart vorgeben. Er kann jedoch mit dem Unternehmer z. B. per E-Mail Kontakt aufnehmen und entsprechend nachfragen. Möglicherweise lässt sich eine Lösung finden, gerade auch bei kleineren Händlern, die ihre Geschäfte weniger automatisiert abwickeln.

Umsicht ist bei **Vorauszahlungen** per Kreditkarte, Überweisung etc. geboten. Generell ist es nützlich, sich bei dem Kreditkartenaussteller bzw. dem Kreditinstitut im Vorfeld eines Online-Vertragsschlusses zu erkundigen, wie eine eventuelle Vorauszahlung abgesichert und unter welchen Bedingungen eine Zahlung auch nachträglich widerrufen werden kann. Ohne eine entsprechende **Rückversicherung** sollten niemals größere Summen überwiesen werden. Am sichersten sind Zahlungen nach Erhalt der Rechnung oder die

Erteilung einer Einzugsermächtigung, weil der gebuchte Betrag innerhalb eines bestimmten Zeitraums zurückgefordert werden kann.

Behauptet der Verkäufer, dass eine Zahlung gar nicht oder nicht rechtzeitig eingetroffen sei, so ist der Kunde beweispflichtig dafür, dass der Geldbetrag rechtzeitig überwiesen wurde. Kontoauszüge, Quittungen und Überweisungsbelege über die geleisteten Zahlungen sollten daher unbedingt aufgehoben werden. Grundsätzlich gilt: Alle **Zahlungsdaten** sollten bei der Übermittlung zum Online-Händler immer **verschlüsselt** übertragen werden.

Aus der Fülle der verschiedenen **Bezahlmethoden** seien einige beispielhaft herausgegriffen:

- **Kreditkarte:** Eine der beliebtesten Zahlungsformen beim Shoppen im Internet ist die Begleichung mit Kreditkarte. Die vom Kunden anzugebenden Daten sind überschaubar: Kreditkartengesellschaft, Kreditkartennummer und Sicherheitsnummer. Der Verkäufer zieht umgehend das Geld von der Kreditkartengesellschaft ein und bringt die Ware zur Versendung. Vorteilhaft für den Kunden ist auch die Option, bei Streitigkeiten bezüglich der Ware ggf. eine Rückbuchung des transferierten Betrages bei seiner Kreditkartengesellschaft herbeizuführen. Wegen der Einzelheiten ist jedoch vor Geschäftsabschluss ein Blick in die Allgemeinen Kreditkartenbedingungen des Ausstellers oder der entsprechenden Bank ratsam. Interessant kann die Nutzung einer Prepaid-Kreditkarte sein, bei der nur der Betrag abgebucht werden kann, der auf die Karte geladen wurde.

- **3D-Secure:** Dieser Begriff steht für ein zusätzliches Sicherheitssystem, das vor Missbrauch bei Online-Kreditkartenzahlungen schützen soll. Der Nutzer muss hier seine Identität durch **Eingabe eines weiteren Kennwortes** gegenüber dem Kartenausgeber bestätigen. Zu diesem Zweck öffnet sich während des üblichen Zahlvorgangs ein zusätzliches Fenster. Dies erhöht allerdings auch wieder das Risiko von Phishing-Attacken über gefakte Websites. Es ist ratsam, sich im Vorhinein bei seinem Kreditinstitut zu erkundigen, ob dort eventuell z. B. durch Phishing entstandene Schäden übernommen werden.

- **Bankeinzug | Lastschrift:** Hier wird der Rechnungsbetrag direkt vom Girokonto des Kunden beim Versand der Ware abgebucht. Für die Übermittlung der Kunden-Bankdaten (Kontonummer, Bankleitzahl, Name des Kreditinstituts) an den Online-Händler gilt: Niemals eine TAN- oder PIN-Nummer bekanntgeben. Mit potenziellen Vertragspartnern, die danach fragen, sollte man sich nicht einlassen. Im Falle einer unberechtigten Abbuchung besteht die Mög-

lichkeit, beim Geldinstitut Widerspruch einzulegen und den eingezogenen Betrag zurückbuchen zu lassen.

- **GeldKarte:** Die Zahlung per GeldKarte kann sowohl im wie auch außerhalb des Internets erfolgen. Für das Aufladen der GeldKarte und das Bezahlen im Internet wird ein Chipkartenleser der Sicherheitsklasse 3 benötigt, und es muss ein Java-Applet im Browser des Web-Nutzers eingerichtet werden. Bislang wird diese Bezahlalternative im Internet eher selten angeboten.

- **Bezahl-System:** Wem die direkte Mitteilung der eigenen Kontoinformationen auf der Website eines Online-Händlers zu gewagt erscheint, kann alternativ ein sog. Bezahl-System nutzen. Zunächst wird in der Regel bei einem der Bezahl-System-Anbieter ein Konto eröffnet. Dabei müssen die üblichen persönlichen Daten sowie die Bankverbindung oder die Kreditkartendaten des Kunden preisgegeben werden. Ebenso werden ein individueller **Benutzername** und ein **Passwort** festgelegt. Wenn ein Online-Shop ein bestimmtes Bezahl-System anbietet, wird der Kunde – sofern er diese Zahlungsart wählt – unmittelbar auf dessen Website dirigiert. Nach der Bestätigung der geplanten Geldtransaktion gibt der Systemanbieter den Betrag an den Online-Händler weiter und zieht die Summe vom Kunden-Girokonto oder der –Kreditkarte ein.

Online-Banking

Unter Online-Banking wird die Abwicklung von Bankgeschäften über Internet-Datenleitungen mit Hilfe von Computern etc. zusammengefasst. Von Anfragen des Kontostandes oder bestimmter Umsatzvorgänge über die Durchführung von Überweisungen bis zur Einrichtung von Daueraufträgen und darüber hinaus – alles kann vom PC zu Hause geregelt werden.

Auch beim Online-Banking versuchen Kriminelle, Konto- und Kreditkartendaten der Nutzer auszuspähen und mit ihrer Hilfe an das Geld der Bankkunden zu gelangen. Phishing mit E-Mails und Trojanern, Datendiebstahl in Internetcafés und Angriffe auf das WLAN sind nur einige Stichworte in diesem Zusammenhang. Deshalb ist beim E-Banking besondere Umsicht am Platze:

- Ganz wichtig ist, dass die Kontodaten über eine verschlüsselte Verbindung zum Kreditinstitut übertragen werden. Das ist daran zu erkennen, dass im Eingabefeld des Browsers das Kürzel **„https://“** am Anfang eingeblendet und oft auch ein Vorhängeschloss-Symbol daneben angezeigt wird.

- **Verschlüsselt** sein sollte auch eine ggf. genutzte WLAN-Verbindung. Dabei ist auf die Auswahl eines dem jeweiligen Stand der Technik entsprechenden Sicherheitsstandards sowie eines hinreichend zuverlässigen Passwortes mit mindestens 20 Zeichen zu achten.
- Online-Banking sollte – soweit möglich – nur vom **eigenen PC** aus erledigt werden. Bei öffentlich zugänglichen Computern, z. B. in Internetcafés, ist Zurückhaltung geboten. Wichtig ist, sich nach jeder Online-Banking-Sitzung ordnungsgemäß (über den Menüpunkt **"Logout"**) abzumelden und den Zwischenspeicher (Cache) des Rechners zu löschen.
- Wer mit seiner Hausbank ein **Limit für tägliche Geldbewegungen** beim Online-Banking vereinbart, stellt damit sicher, dass Internet-Betrüger nicht unbemerkt hohe Summen vom eigenen Konto abbuchen können.
- Regelmäßige **Überprüfungen der Kontobewegungen** und gedruckten Kontoauszüge in kurzen zeitlichen Abständen geben einen weiteren Schutz. Bei fragwürdig erscheinenden Transaktionen, sollte man sofort Kontakt zur Hausbank bzw. dem Kreditkarten-Aussteller aufnehmen.

Gütesiegel

Der Online-Handel wächst in den letzten Jahren kontinuierlich. Etwa zwei Drittel der Deutschen gaben 2011 an, in den zwölf Monaten davor online eingekauft zu haben. Andererseits hatten viele Web-Kunden auch Probleme mit ihrer Online-Bestellung. Zudem sorgen sich zahlreiche Internet-Nutzer, dass ihre Daten beim Surfen ausspioniert werden könnten und haben Bedenken in Bezug auf Zahlungssicherheit und Datenschutz. Mangelndes Vertrauen in das Online-Umfeld ist deshalb inzwischen zu einem ernsten Hindernis bei der Entwicklung einer europäischen Online-Wirtschaft geworden, wie die Europäische Kommission 2011 feststellte. An dieser Stelle setzen Gütesiegel für den Online-Handel an: Sie sollen Verbrauchern und potentiellen Kunden die erforderliche Überzeugung vermitteln, dass es sich bei dem entsprechend **qualitätszertifizierten Online-Shop** um ein seriöses Unternehmen handelt, bei dem ein gefahrloser Einkauf möglich ist.

Nach wie vor gibt es kein einheitliches Gütesiegel für den elektronischen Geschäftsverkehr. Dafür haben sich aber einige seriöse Gütesiegel mehr und mehr durchgesetzt. Die **Initiative D21**, ein Zusammenschluss von Experten für die Informationsgesellschaft aus Politik und Wirtschaft, hatte bereits in der Vergangenheit eine Liste von Qualitätsmerkmalen erstellt und empfiehlt eine kleine Anzahl Gütesiegelanbieter.

Angesichts einer Vielzahl von Prüfzeichen hat das **Zentrum für Europäischen Verbraucherschutz** e.V. (ZEV e.V.) im Juni 2011 (aktualisiert im Juli 2012) eine ***„Studie zu Internetgütesiegeln in Deutschland und Europa“*** veröffentlicht. Ihr Zweck: Bekannte und seriöse Gütesiegel für den Online-Handel nicht nur in Deutschland, sondern europaweit herauszufiltern und aufzuzeigen, was die

Gütesiegel Verbrauchern tatsächlich bieten. Der Schwerpunkt der Untersuchung liegt darauf, wie Gütesiegel-Anbieter Verbrauchern konkret helfen, wenn ein Problem mit einem Online-Shop auftritt. Das **Fazit** der Studie:

- Gütesiegel – sofern qualitativ hochwertig – sind ein Weg, das Risiko für Verbraucher beim Online-Shopping zu minimieren und somit **grundsätzlich empfehlenswert**, denn der Online-Shop wird geprüft, bevor er das Siegel erhält.
- Seriöse Gütesiegel-Herausgeber stehen den Verbrauchern bei Problemen zusätzlich als **Ansprechpartner** – z. B. **mit Beschwerdemöglichkeit** – zur Verfügung, was dann eine erneute Prüfung der Angelegenheit durch den Händler bewirkt.
- Manche Gütesiegel-Aussteller gewähren zusätzliche Vorteile. So bietet ein Siegel-Verleiher Käuferschutz in Form einer **„Geld-zurück-Garantie“** für den Fall an, dass die Geschäftsabwicklung nicht in der erwünschten Weise verlaufen ist.
- Es gibt keine besonderen gesetzlichen Vorschriften zu Gütesiegeln. Die **Verbraucher** müssen **selbst prüfen**, um welches Qualitätszeugnis es sich im Einzelfall handelt. Auch sollte man immer die **Echtheit eines Gütesiegels** überprüfen. Im Zweifel sollte man sich beim jeweiligen Gütesiegelanbieter erkundigen, ob das Siegel dem Händler auch wirklich verliehen wurde. Dies gilt insbesondere dann, wenn ein Klick auf das Siegel, das am Online-Shop angebracht ist, nicht zu einem Zertifikat auf der Seite des Gütesiegelanbieters führt.
- Gütesiegel können **Risiken minimieren**, aber nicht vollständig ausräumen. Gegen die Insolvenz eines Online-Shops beispielsweise sichern auch Zertifikate nicht ab (mögliche Ausnahme: „Geld-zurück-Garantie“, siehe oben). Es ist auch nicht ausgeschlossen, dass ein Shop im Streitfall nicht kooperiert, obwohl er ein Qualitätszeichen trägt. **Gütesiegel** können Shops auch wieder **aberkannt** werden, etwa wenn sie Mängel aufweisen.

Ergänzende Sicherheit verschafft ein Blick auf die **Internetseite des Gütesiegel-Verleihers**, um die Liste der von diesem **geprüften Shops** einzusehen.

Speziell für **Online-Unternehmer** gilt darüber hinaus:

- Seriöse Gütesiegel sind bei den Kunden anerkannt und können durchaus als **Marketingelement** zur Umsatzsteigerung genutzt werden.
- Es kann insofern von Vorteil sein, sich dem Prüfverfahren eines Gütesiegel-Verleihers zu unterziehen, als dort in gewissem Umfang rechtliche **Fehlerquellen** (z. B. ein unzureichendes Impressum oder eine falsche Widerrufs-

belehrung) **entdeckt** werden können. Dadurch lässt sich ggf. die Gefahr von Abmahnungen eingrenzen.

- Gleichwohl gilt: Gütesiegel sind durchweg von unterschiedlicher Qualität, und nicht alle Verleiher unterziehen den Bewerber einer eingehenden und fundierten rechtlichen Prüfung. Eine **umfassende juristische Analyse** kann im Zweifel nur ein spezialisierter Rechtsanwalt bieten, was sich allerdings schon im Hinblick auf das ggf. bestehende Abmahnrisiko lohnen kann.

Die **Gütesiegelstudie** des ZEV e.V. kann unter www.cec-zev.eu/de/veroeffentlichungen/studien-berichte/ abgerufen werden.

Besonderheiten beim mobilen Internet

Bei der Nutzung des Internets mit mobilen Geräten, z. B. Smartphones, Notebooks etc., ist ebenso Umsicht angeraten, wie mit einem stationären Computer. Grundsätzlich gelten die Hinweise im Abschnitt „*Sicheres Agieren im Internet*“ (Seite 16 ff.) entsprechend. Darüber hinaus sind jedoch **einige Besonderheiten** zu beachten.

Basisinformationen

Gespräche mit vertraulichem Inhalt sind nichts für ein Mobiltelefon: Das Telefonieren unter Verwendung des Standardverfahrens für volldigitale Mobilfunknetze (GSM) bietet **keinen Schutz vor Lauschangriffen**. Die Zugangsdaten gehören unter **Verschluss**. Dies gilt insbesondere auch für Zugangscodes für Dienste wie Online-Banking. PINs und Codes sollten nur unbeobachtet eingegeben und **Passwörter** des Öfteren **gewechselt** werden. Bei der Nutzung öffentlicher Hotspots ist erhöhte Vorsicht geboten; besser sind **gesicherte Verbindungen (https)**. Wichtig ist, dass mobile Geräte stets unter Aufsicht bleiben und regelmäßig Sicherheitsupdates durchgeführt werden. Bei Verlust des mobilen Gerätes: unverzüglich die **SIM-Karte sperren** lassen.

Applications (Apps)

„Applications“ (kurz: *Apps*) sind Anwendungen für Smartphones und Tablet-Computer, die schnell und unkompliziert über einen in das Betriebssystem integrierten Onlineshop bezogen und direkt auf dem tragbaren Gerät installiert werden können. So kann sich z. B. jeder Smartphone-Besitzer seine **persönlichen Favoriten-Anwendungen** auf der Benutzeroberfläche verfügbar machen.

Apps ermöglichen so den komfortablen Zugriff auf bestimmte Programme. Sie bergen aber auch Risiken: Mitunter können sie gespeicherte **Daten in unbefugte Hände** befördern oder auch „nur“ hohe Kosten verursachen. Einige bösartige Apps wählen – vom Anwender

unbemerkt – selbständig **teure Telefonverbindungen** an oder versenden kostspielige SMS (sog. Premium-SMS). Wieder andere Spy-Apps können Nutzer dauerhaft überwachen und regelmäßig **Positionsdaten** oder **Passwörter** übermitteln. Folgende **Hinweise** sollten daher unbedingt beachtet werden:

- Dringend zu empfehlen ist, Apps nur **aus verlässlichen Quellen**, z. B. den im Smartphone voreingestellten App-Stores und Markets der Hersteller heraus zu installieren.
- Apps sollten nur auf die Smartphone-Funktionen zugreifen können, die für den jeweiligen Anwendungszweck **tatsächlich erforderlich** sind.
- **Regelmäßige Updates** für Apps und Smartphone-Betriebssystem sind Pflicht. Doch Vorsicht: Elektronische Nachlieferungen können vom Hersteller genutzt werden, um eine scheinbar vertrauenswürdige App nach einer gewissen Benutzungszeit (erneut) mit **zusätzlichen Zugriffrechten** auszustatten. Deshalb: App-Updates besser nicht automatisch, sondern stets **manuell installieren** – nachdem die Zugriffsrechte erneut geprüft wurden.

- Wichtige Hinweise gibt auch die **Statusleiste** auf dem Smartphone-Bildschirm: Anhand dort befindlicher **Symbole** ist erkennbar, wenn eine App Ortungsdaten sammelt oder Funkschnittstellen in Betrieb sind. Sind etwa das GPS oder Bluetooth aktiv, ohne dass die Verbindungsstellen eingeschaltet sind, ist es dringend nötig, die Ursache dafür festzustellen und Gegenmaßnahmen einzuleiten.
- Nützlich ist die Einrichtung eines leistungsfähigen **Prozessmonitors**, um checken zu können, welche Applikationen auf dem Mobilgerät arbeiten.
- Nicht mehr benutzte **Apps** sollten zeitnah **gelöscht** werden, denn jede weitere App kann eine potentielle Einbruchstelle für Cyber-Angriffe sein und dadurch Sicherheitslücken öffnen.

Dessen ungeachtet ist es den Herstellern von Smartphones, Tablet-PCs und Apps sowie den Funknetzbetreibern bereits auf legalem Weg möglich, mit Hilfe der vom Nutzer freiwillig eingegebenen Informationen und Anfragen, sowie der Option, den **Standort eines Mobilfunkgerätes** jederzeit zu bestimmen, umfassende **Persönlichkeitsprofile** der einzelnen User zu erstellen.

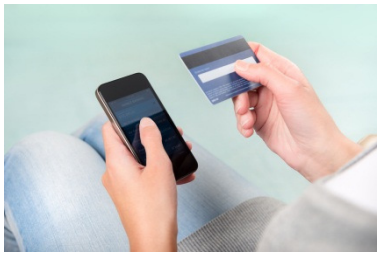
Fremde WLANs

Mobile internetfähige Geräte werden oft – wegen der gegenüber dem Mobilfunknetz höheren Übertragungsgeschwindigkeiten – in WLAN-Netzwerke eingebunden. Die damit verbundenen **Gefahren** wurden bereits im Kapitel *Sicherer Weg ins Internet, Stichwort: WLAN* (Seite 16) beschrieben. Darüber hinaus gilt schlagwortartig:

- WLAN-Funktion nur **bei Bedarf** einschalten.
- Weder Abruf noch **Versendung vertraulicher Daten** über ein fremdes WLAN-Netz.
- Datei- und Verzeichnisfreigaben sollten **deaktiviert** werden. Es besteht die Möglichkeit, dass das mobile Gerät im Netzwerk für andere „sichtbar" ist.
- **Abschalten** der automatischen **Anmeldung** des Mobiles bei bekannten Hotspots.

Mobile Banking

In jedem Fall sollten moderne TAN-Verfahren, wie **mTAN** oder **ChipTAN**, genutzt werden. Die per SMS übertragenen mTANs dürfen dabei nicht auf dasselbe Smartphone übertragen und eingespeist werden, von dem aus das Bankgeschäft erledigt wird. Hierfür muss **ein weiteres Mobiltelefon**, Notebook etc. benutzt werden. Andernfalls wird der Sicherheitsvorteil von mTANs, der darin besteht, dass der Online-Banking-Vorgang und die Übermittlung der TAN zum Schutz vor Missbrauch auf verschiedenen Übertragungswegen erfolgen, wieder neutralisiert.



Datensicherung | Distanzzugriff

Um die Daten auf einem Ersatzgerät (z. B. externe Festplatte, weiteres Mobilgerät etc.) verfügbar zu haben, sollten Sie Ihre **Daten regelmäßig sichern**. Für den Fall, dass das Smartphone oder Tablet mit seinen sensiblen Daten abhandenkommt, ist schnelles Handeln geboten: Um zu verhindern, dass sich Unbefugte dieser Daten bemächtigen, gibt es Optionen, den **Standort** des Gerätes aus der Ferne zu **ermitteln**. Zusätzlich bieten einige Hersteller die sog. **„Remote-Wipe-Funktion"** an, mit deren Hilfe verloren gegangene Geräte aus der Distanz **gesperrt**, und die gespeicherten Daten **zurückgesetzt** oder sogar **gelöscht** werden können.

Hilfe im Notfall

Aller Umsicht zum Trotz: Es kann nie ganz ausgeschlossen werden, dass bei der Nutzung des Internets Fehler unterlaufen und finanzielle, sowie andere Schäden entstehen. Oft sind dann schnelle **„Sofortmaßnahmen"** gefragt. Wie und wo Nothilfe eingesetzt werden kann, zeigt dieser Abschnitt.

Technische Hilfestellung

Sobald der Verdacht aufkommt, der eigene Computer könnte mit Cyber-Schädlingen infiziert sein, ist unmittelbares Handeln erforderlich. Einige Hinweise wurden bereits im Kapitel *Schadsoftware und -programme* (Seite 6 ff.) aufgeführt. Vor allem dann, wenn der jeweilige PC-Nutzer kein IT-Experte ist,

sollte grundsätzlich **Rat und Hilfe eines Profis** eingeholt werden. Selbstversuche schaden unter Umständen mehr, als sie Nutzen bringen.

eCommerce-Verbindungsstelle Deutschland

Beim Zentrum für Europäischen Verbraucherschutz e.V. ist seit 2003 – vom Bundesministerium der Justiz initiiert und finanziert – die eCommerce-Verbindungsstelle angesiedelt. Diese richtet ihr Informations- und Beratungsangebot gleichermaßen an **Anbieter** und **Nutzer** und ist damit die nationale Verbindungsstelle für den elektronischen Geschäftsverkehr. Unter ***www.ecommerce-verbindungsstelle.de*** können umfangreiche ergänzende und vertiefende Informationen zum Recht im Internet und Hinweise auf diverse Organisationen und weitere Ansprechpartner zu speziellen Themen des eCommerce abgerufen werden. Die Zusammenfassung der **Zugangsdaten** findet sich auf den Seiten 2 und 32.

Ersatz bei Kreditkartenzahlung

Sobald der **Verlust** einer Kreditkarte gegenüber dem ausgebenden Institut **angezeigt** wird, hat der Kartenkunde für missbräuchliche Verfügungen, die nach diesem Zeitpunkt getätigt werden, nicht mehr einzustehen. Für Schäden, die vor der Sperre entstanden sind, haftet der Kartenklient nur mit bis zu 50,00 EUR. **Ausnahme:** Verletzt der Karteninhaber **grob fahrlässig** seine Verpflichtungen, etwa zur sorgfältigen Aufbewahrung der Kreditkarte (z. B. Aufbewahrung der Karte im Auto), zur Geheimhaltung der Persönlichen Identifikationsnummer oder zur unverzüglichen Benachrichtigung nach Bekanntwerden des Verlustes und hat dies zum späteren **Missbrauch durch Dritte** beigetragen, so muss der Kunde für den Schaden selbst aufkommen. In solchen Fällen wird in der Regel vermutet, dass das Kreditkartensystem sicher ist und daher dem Dieb die Geheimzahl in irgendeiner Form (z. B. als Notiz) zugänglich war. Diese Annahme ist für den Karteninhaber nur sehr schwer zu entkräften.

Grundsätzlich sind die Haftungsregelungen der Kreditkartenorganisationen in Deutschland sehr ähnlich. Maßgebend sind im Einzelfall allerdings die jeweiligen **Allgemeinen Geschäftsbedingungen** des ausgebenden Instituts.

Ersatz bei Überweisungen

Es ist notwendig, sich sofort mit dem Kreditinstitut in Verbindung zu setzen, bei dem die Überweisung in Auftrag gegeben wurde und die **Transaktion rückgängig** zu machen. Solange das Geld noch nicht auf dem Empfängerkonto gutgeschrieben ist, kann der Betrag zurückgeführt werden.

Ersatz bei Geldtransferdienstleistungen

Auch hier gilt es, sofort Kontakt zu dem Dienstleister aufzunehmen, der mit der Bargeldanweisung beauftragt wurde und den Vorgang sofort anhalten zu lassen. Wenn die Summe noch nicht ausgezahlt wurde, kann der **Betrag rückerstattet** werden.

Kontakt zum Online-Portal

Ratsam ist es ebenfalls, sich als Geschädigter über E-Mail, Kontaktformulare oder telefonisch mit dem jeweiligen Online-Portal, in Verbindung zu setzen, über welches die Geschäftsanbahnung gelaufen bzw. von dem die Malware mutmaßlich ausgegangen ist, und den **Vorgang** und die **eigenen Erfahrungen** zu schildern. Das gilt besonders bei Internet-Auktions- und eCommerce-Versandhäusern. Der Betreiber der Website ist gehalten, dieser Beschwerde nachzugehen und effektive Gegenmaßnahmen einzuleiten.

Rechtsanwalt | Gericht | Vollstreckungsmaßnahmen

Wem durch Internet-Kriminalität etc. ein Schaden zugefügt wird, hat Anspruch auf **Ersatz dieser Einbuße** (z. B. Kostenerstattung für wiederhergerichteten PC, Rückerstattung eines ergaunerten Geldbetrages etc.). Ob und auf welchem Weg zivilrechtliche Forderungen verfolgt und durchgesetzt werden können, sollte der Betreffende zeitnah – ggf. nach vorheriger Erörterung mit der eCommerce-Verbindungsstelle Deutschland – mit einem versierten Rechtsanwalt klären. Grundsätzlich steht jedem Geschädigten der **gesamte Rechtsweg** einschließlich Vollstreckungsmaßnahmen offen.

Das Problem: Dem Opfer sind meistens weder die wahre **Identität**, noch der tatsächliche **Wohnsitz des Gegenübers** bekannt. Zudem tauchen die jeweiligen Anbieter oftmals schnell unter oder halten sich an immer wieder wechselnden Standorten auf.

Trotzdem sollten alle einschlägigen **Dokumente**, z. B. der gesamte E-Mail- oder SMS-Verkehr – etwa mit dem Betrüger – frühzeitig **gesichert**, wenn möglich aussagekräftige Bildschirmkopien (screenshots) z. B. der entsprechenden Online-Annonce erstellt sowie schriftliche Gedächtnisprotokolle der eventuell mit dem Web-Gauner geführten Telefongespräche angefertigt werden – je detaillierter, desto besser. Alles, was der **Beweissicherung** dient, kann hilfreich sein. Das gilt zur Vorbereitung von zivil- und strafrechtlichen Schritten.

Strafrechtliche Maßnahmen

Überlegenswert ist es auch, bei der Polizei oder – besser noch – der Staatsanwaltschaft am Wohnsitz des Betroffenen umgehend **Strafanzeige** zu erstat-

ten und **Strafantrag** zur Verfolgung eventueller krimineller Handlungen zu stellen. Dort können dann auch die vorab genannten gesicherten Unterlagen zu Beweiszwecken vorgelegt werden.

Beschwerden

Zwischenzeitlich existieren einige Einrichtungen, bei denen sich Betroffene mit ihren negativen Internet-Erfahrungen melden und sich beschweren können:

- **eco - Verband der deutschen Internetwirtschaft e.V.:**
  www.internet-beschwerdestelle.de
- **Zentrale zur Bekämpfung unlauteren Wettbewerbs e. V.:**
  www.wettbewerbszentrale.de/de/beschwerdestelle/hinweise
- **Deutscher Schutzverband gegen Wirtschaftskriminalität e.V.:**
  www.dsw-schutzverband.de
- **Homepages der Europäischen Verbraucherzentren (EVZ-Netz):**
  http://ec.europa.eu/consumers/redress_cons/index_en.htm
- **Polizeiliche Kriminalprävention der Länder und des Bundes:**
  www.polizei-beratung.de
- **Verbraucherzentralen der Bundesländer:**
  www.verbraucherzentrale.de
- **Zentrum für Europäischen Verbraucherschutz e.V.:**
  www.cec-zev.eu

Diese Aufzählung ist nicht abschließend. Weitere Informationen zu Beratungs- und Beschwerdestellen im Zusammenhang mit dem elektronischen Geschäftsverkehr stehen z. B. auf der Website der eCommerce-Verbindungsstelle *(www.ecommerce-verbindungsstelle.de)* zur Verfügung.

Weitere ausführliche Informationen zum Thema „Sicheres Agieren im Internet“ sowie zu einer Vielzahl anderer – für Verbraucher wie Unternehmen – wichtiger Fragen, sind erhältlich über die **E-Commerce-Verbindungsstelle Deutschland** *(www.ecommerce-verbindungsstelle.de)*. Sie ist die nationale Einrichtung für den elektronischen Geschäftsverkehr gemäß den Anforderungen der europäischen E-Commerce-Richtlinie und wird vom Bundesministerium der Justiz finanziert.

Interessante Beiträge zu diesem Fragenkomplex hält auch das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** auf seinem Internet-Portal *(www.bsi-fuer-buerger.de)* bereit.

www.cec-zev.eu, Bahnhofsplatz 3, 77694 Kehl

Fotos von www.fotolia.de:

Titelseite: © bilderbox | Seite 6: © tiero #34191220 | Seite 7: © ufotopixl10 #44191792 | Seite 8: LUCKAS #44546674 | Seite 10: © Scanrail #46425844 | Seite 11: © Schlierner #42888905 | Seite 13: © Schlierner #41185638 | Seite 14: © eccolo #39106501 | Seite 15: © James Thew #47006177 | Seite 16: © Gunnar Assmy #42020947 | Seite 17: © alphaspirit #45602048 | Seite 19 (Foto auf der Broschüre): © Kadal | Seite 20: © Santiago Cornejo #44489038 | Seite 21: © PhotoSG #29128664 | Seite 22: © Eisenhans #35138435 | Seite 24: © ferkelraggae #30944576 | Seite 26: © Pro Web Design #18379331 | Seite 27: © bloomua #47156767 | Checkliste: © Johnny Lye #63639

Fotos von www.pixelio.de:

Seite 9: © Gerd Altmann #528472 | Seite 18: © Stephanie Hofschlaeger #411725 | Seite 25: Gerd Altmann #607332 | Seite 28: © Stephanie Hofschlaeger #410237 | Seite 29: © Michael Grabscheit #424811

Stand dieser Information: Dezember 2012

eCommerce-Verbindungsstelle

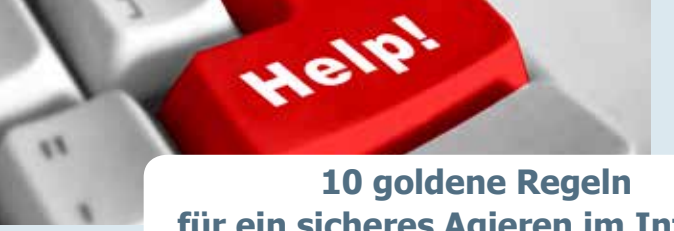
Ansprechpartner für Verbraucher und Anbieter
bei Fragen zu ihren Rechten und Pflichten
im Internethandel

Bahnhofsplatz 3
77694 KEHL

Tel. + 49 78 51 / 991 48 0
Fax + 49 78 51 / 991 48 11

Öffnungszeiten und telefonische Erreichbarkeit:
Di - Do von 9:00 - 12:00 und 13:00 - 17:00 Uhr
eMail: info@eCommerce-Verbindungsstelle.de

www.ecommerce-verbindungsstelle.de



10 goldene Regeln für ein sicheres Agieren im Internet

Checkliste heraustrennen und neben den PC legen!

- **Augen auf beim Online-Kauf: Sind die Website bzw. der Anbieter vertrauenswürdig?**
  - ✓ Selbstdarstellung des Anbieters: **vollständiges Impressum – AGBs – Informationen zu Datenschutz und Datensicherheit – Widerruf/Rückgabe/Kaufpreiserstattung – sämtliche Kosten?**
  - ✓ Wird zumindest ein **sicherer Zahlungsweg** angeboten?
  - ✓ Achtung **Lockvogel-Angebot:** Luxus-Artikel zum Schnäppchen-Preis?
  - ✓ Wie wird der Anbieter auf **Bewertungsportalen** und **Internetforen** beurteilt?
- Sind ein leistungsfähiges und aktuelles **Viren-Schutzprogramm,** ein **Anti-Spyware-Programm,** eine **Personal Firewall** und ein **Anti-SPAM-Schutz** installiert und aktiviert?
- Werden **regelmäßige** – ggf. automatische – **Updates** des Betriebssystems, des Browsers, der Schutzprogramme und sonstiger Anwendungen (z. B. PDF-Reader, Flash-Player etc.) durchgeführt?
- Kein Arbeiten, insbesondere Surfen im Internet als **„Administrator"**
- Bei Verträgen zwischen **Unternehmern und Verbrauchern:**
  - ✓ Ist der **Bestell-Button** richtig beschriftet (z. B. „kaufen")?
  - ✓ Sind alle wesentlichen **Merkmale der Leistung** und die **Preise** (einschließlich Versandkosten, Mehrwertsteuer etc.) über dem Bestell-Button übersichtlich dargestellt?
  - ✓ Ist der Ablauf des Online-Vertragsschlusses verständlich erklärt?
- **Bezahlen im Internet und Online Banking (nur vom eigenen PC!):**
  - ✓ Ist die Datenübertragung verschlüsselt?
  - ✓ Ist die gewählte Bezahlmethode sicher?
- **Downloads** von Software nur aus **vertrauenswürdigen Quellen** (z.B. Original-Produkte von Websites bekannter Firmen)!
- **E-Mails zweifelhafter Herkunft** und/oder mit dubiosen Anhängen niemals öffnen, sondern **ungelesen löschen!**
- **Passwörter und sonstige Codes stets sicher verwahren und nicht an Dritte herausgeben!**
- Generell gilt: So **wenige Daten** wie möglich – so **viele Informationen** wie nötig!

eCommerce-Verbindungsstelle

Bahnhofsplatz 3
77694 KEHL

Tel. + 49 78 51 / 991 48 0
Fax + 49 78 51 / 991 48 11

Öffnungszeiten und telefonische Erreichbarkeit:
Di - Do von 9:00 - 12:00 und 13:00 - 17:00 Uhr
eMail: info@eCommerce-Verbindungsstelle.de

www.ecommerce-verbindungsstelle.de

Angesiedelt beim

Centre **E**uropéen de la **C**onsommation
Zentrum für **E**uropäischen **V**erbraucherschutz e.V.
www.cec-zev.eu

Bahnhofsplatz 3 - 77694 KEHL - Deutschland

Tel.: 07851 991 48 0 - Fax: 07851 991 48 11 - **E-Mail: info@cec-zev.eu**