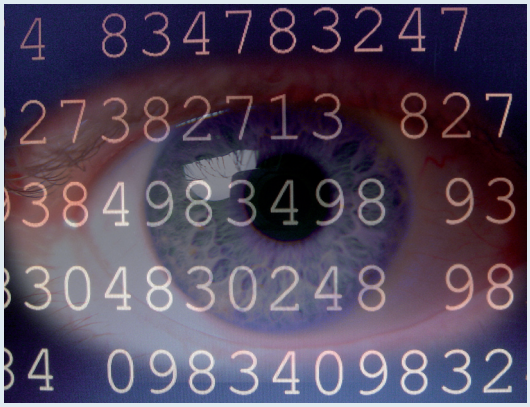
W-LAN
Cookies
Datenschutz
Trojaner
Online-Banking
Viren
Browserkonfiguration
Sicherheitszertifikat
Würmer
Keylogger
Gütesiegel
Firewall
Kreditkartenzahlung
Treuhänder
mTAN
Passwort
Escrow service
Hacker



Sicher durchs Internet

Ein Leitfaden für Verbraucher und Anbieter

Spyware
Kundendaten
Abofallen
Malware
Aktive Inhalte
Bewertung

Deutschland
VERBINDUNGSSTELLE

Die eCommerce-Verbindungsstelle Deutschland

- Nationale Anlaufstelle für Anbieter und Nutzer -

Die eCommerce-Verbindungsstelle Deutschland wurde zum 01. Januar 2003 bei Euro-Info-Verbraucher e.V. eingerichtet.

Die Ansiedlung der eCommerce-Verbindungsstelle bei Euro-Info-Verbraucher e.V. beruht auf einer Entscheidung des Bundesministeriums der Justiz in Berlin, das diese nationale Verbindungsstelle für den elektronischen Geschäftsverkehr seit ihrer Gründung am 1. Januar 2003 auch finanziert.

Auf unserer Homepage **www.ecom-stelle.de** finden Sie umfangreiche weitergehende Informationen zum Recht im Internet und Hinweise auf diverse Organisationen und weitere Ansprechpartner für spezielle Themen des eCommerce.

Bei konkreten Fragen können Sie uns direkt kontaktieren:

eCommerce-Verbindungsstelle Deutschland
bei Euro-Info-Verbraucher e.V.
Rehfusplatz 11
D - 77694 Kehl
Tel.: 0049 (0)7851 991 48 0
Fax.: 0049 (0)7851 991 48 11
Sprechzeiten: Di-Do 9-12 Uhr und 13-17 Uhr

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

Inhaltsverzeichnis

Einleitung

Einleitung

Sie können sich ein Leben ohne Internetzugang nicht mehr vorstellen? Sie nutzen das Netz zum Einkaufen und für die Urlaubsplanung? Sie lesen Ihre eMails sowie aktuelle Nachrichten und tätigen Überweisungen online? Sie bestellen Ihr neues Sofa oder ersteigern das neue Küchenregal vom PC aus? Dann sind Sie längst Teil der Informationsgesellschaft des 21. Jahrhunderts!

Doch achten Sie auch immer ausreichend auf Ihre Online-Sicherheit?

Jede Internet-Nutzung birgt unterschiedlichste Risiken. Doch Sie können und sollten selbst dafür sorgen, sie gering zu halten.

Diese Broschüre bietet Ihnen Informationen rund um Online-Zahlungen, Viren, Trojaner, Datenschutz und Gütesiegel sowie zu vielen weiteren sicherheitsrelevanten Aspekten. Dabei werden sowohl technische als auch rechtliche Hintergründe dargestellt.

Wichtig ist, dass Sie Grundsätze kennen. Da gerade das Internet stets mit Neuheiten aufwartet, versteht sich diese Broschüre auch als Anregung, auf der Basis der hier vermittelten Grundlagen selbst nachzuforschen und aktiv nach Neuheiten Ausschau zu halten.

Daher finden Sie neben vertiefenden Link-Empfehlungen ebenfalls Raum für Ihre persönlichen Ergänzungen - in Form von „Notizzetteln“ nach jedem größeren Themenkomplex.

Auch dabei gilt: Bei konkreten Fragen können Sie uns jederzeit direkt kontaktieren!

Viren, Trojaner und weitere Schädlinge

Auch das Internet ist nicht vor Krankheiten geschützt.

Seinem biologischen Vorbild entsprechend benutzt der klassische **Computervirus** die Ressourcen seines Wirtes und vermehrt sich durch die Weitergabe von infizierten Dateien (z.B. per eMail) recht unkontrolliert.

Würmer sind eine weitere häufig auftretende Form von Infektion. Sie verbreiten sich aktiv und versuchen sich über Sicherheitslücken einzuschleusen. Für großes Aufsehen sorgte 2009 etwa der Conficker-Wurm.

Die gefährlichste Variante ist wohl der „**Trojaner**“, der den Computer nach außen öffnet, so dass der Erschaffer des Trojaners den infizierten Rechner beherrschen kann. Seinem Namen entsprechend wird hier wie in der Antike bei der Eroberung Trojas verfahren: In einem harmlosen, bisweilen nützlichen Programm versteckt sich ein anderes, das Ihren PC erobern soll. So können vertraulichste Daten ausgelesen und Passwörter erspäht werden oder Ihr Computer könnte als Absender von Spam-Mails und als Lagerplatz für illegale Software genutzt werden.

Doch Sie können sich in hohem Maße selbst gegen solche Gefahren zur Wehr setzen, etwa durch regelmäßige Updates Ihres Betriebssystems oder gar durch die Auswahl eines nicht virenanfälligen Betriebssystems, durch die Installation eines Virenschutzprogramms oder eines Programms gegen bestimmte Arten sonstiger Schadprogramme.

Solche Programme laufen im Hintergrund eines Systems und überprüfen neu installierte Software sowie den Internet-Datenverkehr auf Muster digitaler Schädlinge. Da Computerviren wie echte Viren weiterentwickelt werden, sollten Sie auch regelmäßig für eine Aktualisierung Ihres Virenschutzes und Ihres Betriebssystems sorgen. Der Schutz ist nur dann effektiv, wenn er regelmäßig auf den neuesten Stand der im Netz verbreiteten Schädlinge gebracht wird. Entsprechende Software finden Sie

- auch als Gratisversion - im Internet. Doch prüfen Sie, ob diese Programme wirklich gratis angeboten werden und nicht über eine sog. Online-Abo-Falle vertrieben werden (in letzterem Fall besteht aber meist ein Widerrufsrecht oder der Vertrag ist bereits unwirksam, mehr unter www.ecom-stelle.de).

Zudem sollten Sie keine unbekannten eMails oder Anhänge öffnen. Lassen Sie die eMails auf Viren untersuchen bevor Sie Anhänge öffnen. Gefahr droht übrigens auch von Dateien auf einem USB-Stick oder ähnlichem. Besonders bei den Anhängen mit den Dateitypen .exe, .bat, .com und .vbs sollten Sie vorsichtig sein, aber auch gängige Dateiformate wie .doc sind betroffen. Auch das Vorschaufenster Ihres eMail-Programms ist ein zusätzliches Sicherheitsrisiko, da diese kleine Lücke einigen Schädlingen bereits genügt, um sich auf Ihrer Festplatte festzusetzen.

Um einem unvorgesehenen Datenverlust vorzubeugen, sollten Sie im Übrigen immer Sicherheitskopien von wichtigen Dateien anfertigen, etwa auf einer CD, einer DVD oder einer externen Festplatte.

Im Übrigen sollten Sie für den Fall der Fälle eine sog. Boot-CD im Hause haben, mit der Sie Ihren Rechner hochfahren können, falls das installierte System nicht startet. So wird auch eine Reparatur leichter.

Weiterführende Links

Eine Übersicht über zahlreiche Antivirenprogramme bietet die TU Berlin:

http://hoax-info.tubit.tu-berlin.de/software/antivirus.shtml

Vertiefte Informationen bietet auch eine Seite des Bundesamts für Sicherheit in der Informationstechnik:

http://www.bsi-fuer-buerger.de

Ihre Notizen zum Thema:

Viren, Trojaner und weitere Schädlinge

Weitere Gefahrenquellen im Netz

Mit der Dauer der Online-Verbindung steigt auch die Gefahr für Ihren Computer.

Häufigstes Werkzeug der IT-Sicherheit ist die **Firewall** (Brandschutzwand). Firewalls sind digitale Schutzmauern, die private Netzwerke von Zugriffen des Internets trennen sollen. Sie sollen unerwünschte Eindringlinge abwehren und gleichzeitig den gewünschten Datenverkehr möglichst wenig behindern.

Hacker-Angriffe treffen gerne ungesicherte oder schlecht gesicherte Computer. Deshalb sollten Sie Ihr W-LAN verschlüsseln und die integrierte Firewall Ihres Routers aktivieren. Ganz besonders wichtig ist dies auch aus Haftungsgründen. Einige Gerichte sind der Ansicht, dass bei schlecht gesicherten Netzen, die Folgen, die durch Ausnutzung der Sicherheitslücken entstanden sind, vom Privaten mitzutragen sind. Auch Ihr W-LAN sollte deshalb nach neuestem Stand abgesichert sein, fragen Sie im Zweifel bei Ihrem Anbieter nach. Detaillierte Informationen zum Thema W-LAN-Haftung gibt es in unserem Merkblatt „Vorsicht Falle: W-LAN-Nutzer aufgepasst“ auf unserer Internetseite www.ecom-stelle.de.

Ein weiteres Risiko beim Surfen birgt **Spyware**. Dies sind Programme, die heimlich Ihr Surfverhalten ausspionieren. Sie landet häufig durch Anwendungen, die eigentlich die Funktion der Webseiten unterstützen, das Surfen für Sie also in gewisser Weise angenehmer machen, auf dem PC. Auch als Teil von sogenannter Free- oder Shareware kann Spyware auf Ihrem Rechner einziehen. Einmal angekommen, durchsucht sie Ihren Computer nach unterschiedlichsten Informationen über Ihre Hard-, Software oder Aktivitäten im Internet, um sie dann vor allem an den Hersteller oder Werbefirmen weiterzuleiten. Gerne versteckt sich Spyware auch in Cookies und Aktiven Inhalten, die beim Surfen auf dem PC abgelegt werden.

Aktive Inhalte erlauben die automatische Ausführung von Funktionen einer Webseite ohne dass der Benutzer sich dessen bewusst wird. Darin können gefährliche Programme enthalten sein. **Cookies** ermöglichen bei erneutem Aufrufen der Webseite, dass der Benutzer wiedererkannt wird und er z.B. seine Nutzerdaten nicht neu eingegeben muss.

Spyware kann auch besonders gefährlich werden, wenn sie in Form von Keyloggern auftritt! **Keylogger** sind Programme, die die Eingaben eines Nutzers auf seinem Keyboard, also auf seiner Tastatur, mitlesen, um so Passwörter oder andere Daten zu speichern und an andere Personen weiterzugeben.

Schützen können Sie sich mit Virenschutzprogrammen, einer Firewall und speziellen Spyware-Entfernungs-Programmen. Und denken Sie daran, dass Sie die Risiken bereits minimieren können, indem Sie Ihren Browser Ihren Bedürfnissen entsprechend einstellen, z.B. indem Sie die Ausführung von Aktiven Inhalten verhindern.

Weiterführende Links

Mehr Informationen erhalten Sie wie bereits oben erwähnt auf den Seiten des Bundesamts für Sicherheit in der Informationstechnik (BSI):

http://www.bsi-fuer-buerger.de

Ein Projekt des BSI zur Warnung vor Sicherheitslücken und Viren finden Sie unter:

http://www.buerger-cert.de

Ihre Notizen zum Thema:

Weitere Gefahrenquellen im Netz

Bezahlen im Internet

Bei einem Geschäftsabschluss über das Internet muss die Art der Bezahlung geklärt werden.

Der Vertrag soll so unkompliziert und schnell abgewickelt werden wie beim Einkauf in der realen Welt. **Für beide Parteien ist eine verlässliche Zahlungsweise wichtig.**

Dafür wurden einst spezielle Systeme für die Zahlung im Internet entwickelt, die aber nur teilweise wie die herkömmlichen Zahlungsarten (Überweisung, Kreditkarte und Nachnahme) von den Kunden angenommen wurden. Die gebräuchlichsten Varianten und ihre Vor- und Nachteile sind neben allgemeinen Fragen nachfolgend aufgeführt.

Was sollten Sie generell bei Zahlungen im Internet beachten?

• **Sie sollten sich über die Zahlungsmodalitäten vor der Bestellung genauestens informieren.** Dazu gehören auch mögliche Gebühren oder Versandkosten, damit Sie später nicht von der Höhe des Kaufpreises überrascht sind. **In den meisten Fällen bietet ein Verkäufer verschiedene Zahlungsmöglichkeiten an, aus denen der Käufer wählen kann.** Dem Käufer steht es aber nicht zu, eine andere Bezahlungsart vorzugeben. Kommt es dem Käufer aber gerade darauf an, hindert ihn nichts, dem Unternehmer eine eMail zu schicken oder nachzufragen. Vielleicht lässt sich eine Lösung finden, gerade auch mit einem kleineren Händler, der seine Geschäfte weniger automatisiert organisiert.

• **Ebenso sollten Sie sich bei Vorauszahlungen** per Kreditkarte, Überweisung o.ä**. im Vorfeld über Ihren Vertragspartner erkundigen**, um Ihre Gutgläubigkeit nicht im Nachhinein zu bereuen. Bringen Sie auch in

Erfahrung (z.B. bei Ihrer Bank), wie Sie Ihre Zahlung absichern und unter welchen Bedingungen Sie eine Zahlung auch nachträglich widerrufen können. **Ohne sich abzusichern, sollten Sie niemals größere Summen überweisen**, denn hier wird eine Rückbuchung auf Ihren alleinigen Wunsch so gut wie nie möglich sein. Am sichersten sind Zahlungen nach Erhalt der Rechnung oder die Erteilung einer Einzugsermächtigung, weil Sie den gebuchten Betrag innerhalb eines bestimmten Zeitraums zurückfordern können.

• Zur rechtzeitigen Zahlung des Kaufpreises sind Sie verpflichtet. Behauptet der Verkäufer, dass eine Zahlung gar nicht oder nicht rechtzeitig eingetroffen sei, sind Sie beweispflichtig dafür, dass Sie den Geldbetrag rechtzeitig überwiesen haben. Sie sollten deshalb Kontoauszüge, Quittungen und Überweisungsbelege über die von Ihnen geleisteten Zahlungen unbedingt aufheben.

Welche speziellen Zahlungssysteme stehen Ihnen für Online-Einkäufe zur Verfügung?

Die speziell für das Internet entwickelten Zahlungssysteme konnten sich nur begrenzt durchsetzen, zum Teil wurden die Angebote auch mangels Nachfrage wieder eingestellt. Es lassen sich **verschiedene Ansätze** für die bargeldlose Zahlung im Internet herauskristallisieren. Über einige davon können Sie sich im Folgenden ein Bild machen; jedenfalls ist klar: In technischer Hinsicht ist vieles möglich und es lohnt sich, Entwicklungen im Auge zu behalten.

Die Guthabenkarten (Prepaidkarten)

Die Guthabenkarten fürs Internet funktionieren ähnlich wie Guthabenkarten für Handys: Der Kunde kauft an einer Tankstelle oder an einem Kiosk eine Karte in Höhe eines bestimmten Einkaufswertes und kann mit Hilfe dieser Karte im Internet anonym einkaufen. Unter Angabe des

Namens der Karte, eines PIN-Code und eines Passwort kann er bezahlen. Der Betrag wird daraufhin von seinem Kartenguthaben abgebucht.

Allerdings muss der Verkäufer auch die Möglichkeit zu einer solchen Zahlungsweise anbieten. Nach wie vor ist dies nicht häufig der Fall - und wenn, dann meistens für kleinere Beträge.

Mobile Payments

Zu den neueren Zahlungsverfahren gehören auch die so genannten „Mobile Payments“, die oft das (Mobil-)Telefon in den Zahlungsvorgang einbeziehen.

Dieses Zahlungsverfahren basiert auf der Idee, dass der Kunde stets mobil mit seinem Telefon zahlen kann. Seine sensiblen Kontendaten müssen hier trotz Online-Einkaufs nicht über das Internet übertragen werden. Das Telefon wird dazu eingesetzt, eine weitere „Sicherung“ in das Verfahren einzubauen, so kann z.B. eine PIN abgefragt werden.

Elektronisches Geld: eCash / CyberCoins

Unter diesen Namen wurden Verfahren zur Bezahlung mit elektronischem Geld eingeführt. Ähnlich der Bezahlung mit einer Geldkarte buchte der Kunde einen bestimmten Geldbetrag von seinem Konto ab und speicherte diesen auf seinem Rechner. Mit diesem virtuellen Geld konnte er im Internet Einkäufe vornehmen.

Dieses Zahlungsmittel sollte es ermöglichen, Online-Geschäfte jeglichen Umfanges sicher zu tätigen. Nach den uns vorliegenden Informationen wurden jedoch derzeit in Deutschland alle Projekte zu diesem Zahlungsverfahren eingestellt.

Giropay

Dieses Verfahren wird von der deutschen Kreditwirtschaft als Online-Bezahlungsverfahren angeboten. Als Kunde werden Sie vom Shop zur Bezahlung direkt auf Ihr Online-Banking-Konto weitergeleitet.

Es entspricht also insofern dem gebräuchlichen Online-Banking und führt zu einer weiteren Identifizierungsprüfung.

Diese Art zu bezahlen muss auch von Verkäuferseite angeboten werden. Zudem bestehen hier dieselben Risiken wie beim klassischen Online-Banking auch – doch lesen Sie dazu weiter unten noch mehr.

3D-Secure

Dieser Begriff steht für ein zusätzliches Sicherheitssystem, das bei Seiten vor Missbrauch bei Online-Kreditkartenzahlungen und deren Folgen schützen soll.

Der Verwender muss hier seine Identität durch Eingabe eines weiteren Kennworts gegenüber dem Kartenausgeber bestätigen. Zu diesem Zweck öffnet sich während des üblichen Zahlvorgangs ein zusätzliches Fenster.

Online-Bezahlsysteme

Der Vorteil und die Sicherheit bei Online-Bezahlsystemen liegen darin, dass der Kunde seine sensiblen Daten zu Bankverbindung bzw. Kreditkarte nicht an den unbekannten Verkäufer übermittelt, sondern nur dem Betreiber des Bezahlsystems bekannt sind.

Ohne das Sicherheitsrisiko, sensible Daten unsicher oder unverschlüsselt durch das Netz zu schicken, muss der Kunde lediglich das Online-Bezahlsystem anweisen, die Zahlung zu tätigen. Der Verkäufer bekommt dann den Betrag gutgeschrieben, den das Online-Bezahlsystem wiederum vom Kunden per Lastschrift oder Kreditkartenzahlung einzieht. Manche

Anbieter verlangen, dass der Kunde ebenfalls vorleistet indem er eine Guthabenkarte erwirbt, von deren Betrag dann die Zahlungen an den Verkäufer ausgeführt werden.

Zusätzlich wird mittlerweile häufig ein sogenannter Käuferschutz angeboten: Sollte die Ware nicht geliefert werden, dann erhält der Kunde den Betrag zurück. Ob, in welcher Höhe und unter welchen Bedingungen ein Käuferschutz angeboten wird, sollte im Vorfeld geklärt werden. Insbesondere können hier oft recht enge Fristen gelten.

Es hängt aber auch bei dieser Zahlungsart davon ab, ob sie der Verkäufer anbietet. Weiterhin sollten Sie beachten, dass nicht jedes dieser Online-Bezahlsysteme völlig gleich ist, eben z.B. im Hinblick auf Fristen.

Treuhänder ("escrow service")

Bei diesem Service ist ein Dritter Mittler des Geldbetrags. Bei diesem Dritten ist der Geldbetrag hinterlegt und wird ausgezahlt, wenn die Ware angekommen ist und überprüft wurde. Der Verkäufer kann sich seinerseits auf den Eingang der Zahlung verlassen und wird vor Rückbuchungen durch den Käufer im Streitfall geschützt. Somit wir sichergestellt, dass beide Seiten ihren Pflichten nachkommen.

Dieser Service ist nicht gebührenfrei und wird wegen des gestiegenen Bedarfs an internationalem Geldtransfer weniger durch die klassischen Treuhänder wie Rechtsanwälte, Notare oder Banken, sondern durch Treuhandfirmen angeboten, deren Verfahren automatisiert und schnell sind.

Allerdings gibt es auch betrügerische Treuhandfirmen, die das Sicherheitsbedürfnis der Kunden verknüpft mit vermeintlichen Schnäppchen ausnutzen. Lassen Sie sich z.B. nie von einem allzu schönen Gebrauchtwagen blenden, der weit entfernt zu einem unglaublich günstigen Preis angeboten wird, der Verkäufer aber auf Zahlung über einen bestimmten Ihnen nicht bekannten Treuhandservice besteht. Ist alles in

Ordnung, lässt sich der Verkäufer bestimmt auf eine andere Zahlung ein, die ihm die nötige Sicherheit garantiert.

Was sollten Sie ansonsten beim Bezahlen beachten?

Bei einer Zahlung direkt über das Internet aber auch bei einer Anmeldung zu einem Online-Bezahlservice oder ähnlichen Diensten besteht die Gefahr, dass sensible Daten von Ihnen ausgespäht und missbraucht werden. **Achten Sie darauf, dass die Daten über eine verschlüsselte Verbindung übertragen werden.** Das erkennen Sie insb. daran, dass im Eingabefeld des Browsers „https://“ am Anfang steht und oft auch ein Vorhängeschloss-Symbol daneben angezeigt wird.

Bedenken Sie, dass auch bei ganz klassischen, Internet-unabhängigen Zahlungen Risiken bestehen können. Wenn Sie etwa nach einer Online-Bestellung durch eine Überweisung vorleisten, dann kann der Verkäufer das Geld einfach behalten und verschwinden, d.h. die Ware nicht versenden und Sie stehen mit leeren Händen da. Informieren Sie sich also im Zweifel im Voraus über den Händler, z.B. indem Sie den Namen des Online-Shops in eine Suchmaschine eingeben oder indem Sie prüfen, ob ein korrektes Impressum mit Postadresse vorliegt. Durch diese und andere einfach durchzuführende Maßnahmen dämmen Sie Risiken jedenfalls ein gutes Stück weit ein.

Wollen Sie weder in Vorleistung gehen, noch online zahlen, können Sie versuchen auf Rechnung zu bestellen oder Nachnahme zu vereinbaren. Im letzteren Fall entstehen aber Zusatzkosten.

Ihre Notizen zum Thema:

Bezahlen im Internet

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Online-Banking und Kreditkarten

Online-Banking, d.h. insbesondere die Überweisung per Computer, ist für viele schon seit längerem zur Gewohnheit geworden. Es ist bequem und zeitsparend. Doch natürlich sollte man auch Risiken vorbeugen.

So bereitet insbesondere das sog. „**Phishing**“ Sorge. Bei dieser Betrugsart erhält das Opfer vom Angreifer verfasste eMails, die solchen von Unternehmen und Banken täuschend ähnlich sehen. Das Opfer soll meist durch einen in dieser eMail enthaltenen Internetlink dazu verleitet werden, auf die Seite des Angreifers zu gehen und dort vertrauliche Informationen - insbesondere Kontoinformationen, PIN und TAN (Transaktionsnummer für Überweisungen und ähnliche Bankgeschäfte) – einzugeben. Weil gerade die Anschreiben und ebenfalls die Internetseiten fast perfekt gefälscht sind, ist es schwierig den Betrug zu erkennen. Auch Konten bei Online-Auktionen oder Spielen sind übrigens betroffen.

Daher sollten Sie die Webadresse Ihrer Bank am Besten immer von Hand in den Browser eingeben und **nicht sorglos Links aus eMails folgen**. Die Verbindung muss dabei natürlich gesichert sein. Achten Sie darauf, dass in der Adresszeile Ihres Browsers **https:// anstatt http://** steht. Je nach Browser wird auch ein Vorhängeschlosssymbol angezeigt.

Ihre PIN und TANs sollten Sie auch nicht auf Ihrem PC speichern, auch wenn Sie dies komfortabel und praktisch finden.

Ebenso sollten Sie häufig Ihren Kontostand prüfen, um Missbrauchsfälle schnell bei Ihrer Bank zu melden.

Fragen Sie bei Ihrer Bank nach: Zusätzliche Sicherheit können z.B. **spezielle TAN-Verfahren** (mTAN oder die Verwendung von TAN-Generatoren, die quasi auf Knopfdruck neue, einmalige TANs kreieren) oder Chipkartensysteme (hier benötigen Sie aber ein zusätzliches Lesegerät) bieten.

Die **Zahlung mit der Kreditkarte** ist ebenso eine häufig genutzte Variante, um im Internet zu bezahlen. Obwohl mittlerweile viele Kreditkartenanbieter einen **umfassenden Kundenschutz**, wie zum Beispiel die Möglichkeit des Rückbuchens oder Widerrufs anbieten, wird von der Nutzung der Kreditkarte oft abgeraten. Dies ist nicht unbedingt die richtige Empfehlung. Wichtig ist es aber, sich bei seiner Bank zu erkundigen, binnen welcher Frist und unter welchen Voraussetzungen Beträge auf Ihr Konto zurückgebucht werden können. Daneben können Sie sich überlegen, sich eine zweite Kreditkarte zur Zahlung in Online-Shops zuzulegen, die nur über einen sehr begrenzten Verfügungsrahmen verfügt – im schlimmsten Fall bleibt auch der Schaden sehr begrenzt. Sinnvoll ist das aber nur, wenn Sie sich bei Ihren Einkäufen selbst lediglich in diesem Rahmen bewegen.

Wie beim Online-Banking ist es bei einer Kreditkartenzahlung selbstverständlich wichtig, auf die oben beschriebenen sichere Internet-Verbindung – Stichwort: https:// und Vorhängeschlosssymbol – zu achten.

Für Kreditkartenzahlungen gilt genauso wie für das Online-Banking, dass der heimische PC immer noch der sicherste Ort ist. **Nach Möglichkeit sollten Sie daher Online-Banking nicht von fremden Rechnern nutzen.** In Internetcafés könnte eine Webcam auf Sie gerichtet sein und Ihre Eingaben auf der Tastatur aufnehmen. Und auch ein prüfender Blick um Sie herum hilft wenig: Eine zwischen Tastatur und Computer installierte Box oder ein entsprechendes Programm könnte sämtliche Ihrer Tasteneingaben aufzeichnen.

Ihre Notizen zum Thema:

Online-Banking und Kreditkarten

Gütesiegel für Internetshops

Der Einkauf in Internetgeschäften wird attraktiver und für manche schon zur Normalität. Wie jedoch lässt sich feststellen, ob der Verkäufer vertrauenswürdig ist? Wer negative Erfahrungen macht, wird zwar umsichtiger, aber auch unsicherer.

Um das notwendige Vertrauen in den Online-Handel nicht durch unseriöse Anbieter zu zerstören, wurden auch für das Internet Gütesiegel entwickelt, die bereits in anderen Bereichen der Wirtschaft einen **Hinweis auf die Qualität des Produkts** geben. Neben Online-Bewertungen sind daher Gütesiegel ein weiteres Hilfsmittel, um zu entscheiden, ob gerade bei diesem Händler eingekauft werden soll.

Nach wie vor gibt es **kein einheitliches Gütesiegel** für den Online-Geschäftsverkehr. Dafür haben sich aber einige seriöse Gütesiegel mehr und mehr durchgesetzt. **Vorsicht:** Es gibt daneben eine große Zahl von dubiosen Gütesiegeln, bei denen teilweise z.B. nur die Identität des Anbieters geprüft wird. Daneben werden Gütesiegel auch gefälscht und dementsprechend verwendet.

Machen Sie sich also damit vertraut, was das Gütesiegel im Einzelnen verspricht, mit dem sich der Online-Shop schmückt, bei dem Sie bestellen möchten. Erkundigen Sie sich bei Zweifeln bei der Gütesiegel-Vergabestelle, ob ein Unternehmen auch tatsächlich dort registriert ist. Und erkundigen Sie sich nach der Qualität der Gütesiegels.

Die Initiative D21 hatte bereits in der Vergangenheit eine Liste an Qualitätsmerkmalen erstellt und empfiehlt bestimmte Gütesiegel. Das heißt aber nicht, dass andere Gütesiegel deshalb schlecht oder die empfohlenen Gütesiegel die einzig verlässlichen sind. Auch hier gilt wieder: Erkundigen Sie sich möglichst tagesaktuell, sei es in Fachzeitschriften, in Internetforen oder bei Informationsstellen wie der eCommerce-Verbindungsstelle.

Welche Vorteile bieten Gütesiegel den Käufern?

Dem Kunden wird mit dem Gütesiegel mehr Schutz geboten. Die Shops müssen ihr Angebot grundsätzlich einer Prüfung unterziehen und die Qualitätskriterien des Gütesiegels erfüllen.

Zudem bieten seriöse Anbieter eine Beschwerdemöglichkeit an, die dann eine erneute Prüfung des Händlers auslöst.

Manche Gütesiegel-Aussteller bieten zudem einen Käuferschutz in Form einer Geld-zurück-Garantie an, für den Fall, dass der Geschäftsprozess nicht in der erwünschten Weise abgelaufen ist.

Worauf müssen Sie achten?

Auf das Vorhandensein des richtigen Gütesiegels müssen Sie achten. Die unten aufgeführten Links können Ihnen bei der Suche danach helfen. Wichtig ist, dass Ihnen bewusst ist, dass es unseriöse Anbieter gibt, die ausschließlich an den Zahlungen des Shops (um eben das Siegel führen zu dürfen) interessiert sind und sich wenig um die Interessen des Kunden kümmern. Daneben gibt es auch Shops die vertrauenswürdige Gütesiegel unberechtigterweise auf ihrer Seite aufführen. Sicherheit verschafft ein Blick auf die Internetseite des Gütesiegels, um die Liste der geprüften Shops einzusehen.

Und die Vorteile für den Unternehmer?

Vertrauen ist das wichtigste Gut im Onlinegeschäft. Ohne Kunden, die Ihnen das Vertrauen entgegenbringen, dass Sie mit seinen Daten und der

Ware sorgfältig umgehen, riskieren Sie, bald nicht mehr auf dem Markt mitzumischen.

Seriöse Gütesiegel sind bei den Kunden anerkannt und können als **Marketingelement** zur Umsatzsteigerung genutzt werden.

Im Übrigen kann es insofern von Vorteil sein, sich dem Gütesiegelverfahren zu unterziehen, als dort in gewissem Umfang rechtliche Fehlerquellen, wie beispielsweise ein fehlerhaftes Impressum oder bei einer Widerrufsbelehrung, entdeckt werden können. Dadurch lässt sich die Gefahr von Abmahnungen eingrenzen.

Aber auch hier ist für Unternehmer Vorsicht geboten, denn nicht jedes Gütesiegel ist von gleicher Qualität und nicht alle unterziehen den Bewerber einer eingehenden und fundierten rechtlichen Prüfung. Eine umfassende rechtliche Prüfung kann Ihnen im Zweifel nur ein Anwalt bieten, was sich aber allein im Hinblick auf das Abmahnrisiko lohnen kann.

Weiterführender Link

http://www.internet-guetesiegel.de, ein Projekt der Initiative D21

Ihre Notizen zum Thema:

Gütesiegel für Internetshops

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Datenschutz

Wer sich im Internet bewegt, hinterlässt ständig Spuren. Denn das Surfen basiert auf dem Austausch von Informationen, ohne die es nicht möglich wäre, die Seiten im Internet zu erreichen. Allein dadurch ist es für den Netz- oder Seitenbetreiber möglich zu erkennen, woher Sie angesurft kamen oder wohin Sie sich bewegen. Werden auf einer Seite mehr Daten hinterlassen, zum Beispiel wie, wann und welche Bücher oder Waren Sie ansehen und bestellen, dann bekommen die Informationen einen echten Marktwert. Rund um solche und andere Daten hat sich mittlerweile ein einträgliches Geschäft entwickelt.

Immer wieder kam es gerade in letzter Zeit zu negativen Schlagzeilen. Fast täglich kommen neue und unterschiedlichste Aspekte der Problematik ans Licht:

- Internet-Händler erstellen unbemerkt Profile aus den Kundendaten;
- Soziale Netzwerke sammeln Nutzerdaten, um individuelle Werbung zu schalten;
- Unternehmen speichern unerlaubt Krankheitsdaten;
- Daten werden illegal auf dem Schwarzmarkt verkauft;
- Kriminelle buchen mit den Daten heimlich Geld von Konten ab.

Was regelt Datenschutz eigentlich?

Datenschutz umfasst jede Handlung, die in irgendeiner Weise dem Schutz personenbezogener Daten dient. Darunter fallen rechtliche, organisatorische sowie technische Maßnahmen.

Wichtig ist aber auch, dass das Datenschutzrecht nicht ausschließlich dem Schutz des Einzelnen im Sinne des Rechts auf informationelle Selbstbestimmung dient, sondern an der Schnittstelle von Zugangsrechten Dritter – sei es Presse oder Forschung - und der Privatsphäre Dritter steht.

Das Bundesdatenschutzgesetz schützt demnach alle Informationen über eine Person, seien es Name und Anschrift, Beruf, Staatsangehörigkeit, aber auch zum Beispiel die Schuhgröße.

Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist also nur dann zulässig, wenn sie durch das Datenschutzrecht oder durch eine andere Rechtsvorschrift, wie z.B. die Landesdatenschutzgesetze oder das Telekommunikationsgesetz gestattet ist oder eine Einwilligung des Betroffenen vorliegt. Ist eine solche erforderlich, darf diese nicht über ein Kästchen auf der Website erfolgen, bei der das „Einwilligungshäkchen" schon vom Betreiber voreingestellt wurde – Sie müssen es aktiv setzen.

Welche Rechte habe ich als Nutzer

Über eine sog. **Datenschutzerklärung** muss ein Nutzer hinreichend von dem Webseitenbetreiber zu dem Thema aufgeklärt werden. Schauen Sie also in Zukunft auf der Seite eines Online-Shops ruhig einmal nach, einen Link zur Datenschutzerklärung müsste es geben. Aber auch wenn dem Nutzer bei Vertragschluss der Umfang der Verarbeitung seiner persönlichen Daten oft mehr oder minder unbekannt bleibt, weil er die Datenschutzerklärung nicht gelesen hat, hat er ein Recht auf Auskunft, Benachrichtigung, Löschung, Einwilligung und Widerspruch hinsichtlich dieser Daten.

2009 wurden übrigens zahlreiche Neuerungen des Datenschutzrechts beschlossen, von denen aber noch einige nicht in Kraft getreten sind. Verfolgen Sie also die Diskussion, es kann sich noch einiges tun, zumal sich die Dynamik der ständigen Fortentwicklungen des Internet nicht zuletzt beim Thema Datenschutz zeigt.

Worauf sollten Nutzer grundsätzlich achten?

Datensparsamkeit ist das Schlagwort. Geben Sie nicht wahllos Ihre persönlichen Daten im Netz heraus!

Bedenken Sie insbesondere: Einzeln betrachtet scheinen zwar viele der abgegeben Daten nur wenig über Sie auszusagen. **Aber aus der Summe dieser Einzeldaten kann sich schon ein ganz anderes Bild ergeben. Überlegen Sie sich also auch bei scheinbar insignifikanten Daten, ob Sie diese wirklich preisgeben möchten.**

Und im Übrigen besteht ein gewisses Grundrisiko, dass Daten von Dritten abgefangen, gespeichert und weiterverbreitet werden.

Sind „Cookies?“ wirklich so gefährlich?

Bei den sogenannten Cookies handelt es sich um Dateien, die ein Anbieter automatisch auf dem Rechner des Kunden anlegt, um sie jedes Mal dann aufzurufen, wenn der Kunde die Seite des Anbieters öffnet.

Dies ist für den Kunden komfortabel und von Vorteil, weil er so seinen Warenkorb nicht verliert oder auf ihn zugeschnittene Angebote bekommen kann – sollte ihm daran gelegen sein.

Datenschutzrechtlich problematisch sind Cookies, weil der Datenaustausch in aller Regel geschieht, ohne dass der Benutzer etwas davon bemerkt. Zudem kann der Anbieter auf diesem Wege Informationen über das Surfverhalten des Nutzers sammeln, ein Nutzerprofil entwickeln und dem Nutzer gezielt Angebote unterbreiten.

Ein Anbieter, der Cookies verwenden und anlegen möchte, muss den Nutzer daher genau über deren Zweck, Inhalt und die Dauer der Datenverarbeitung informieren, sofern es sich letztlich um personenbezogene Daten handelt. Bei einer weitergehenden Nutzung muss er per Mausklick das Einverständnis des Verbrauchers einholen.

Sicherheitsbewusste Internetnutzer können in ihrem Browser einstellen, inwieweit Cookies akzeptiert werden. Wer Cookies zulässt, sollte diese in regelmäßigen Abständen löschen.

Woran sollten Unternehmer grundsätzlich denken?

Prinzipiell gilt wie so oft im Leben: **Weniger ist manchmal mehr**. Gerade mit der steigenden Angst der Verbraucher „**gläserner Kunde**“ zu sein, sollten Unternehmer überlegen, nur solche Daten zu erheben, die für den Bestellvorgang auch wirklich notwendig sind. D.h. Name, Adresse, eMail und/ oder Telefonnummer.

Es gibt spezielle **Datenschutz-Gütesiegel** und weitere sind geplant. Eine Zertifizierung kann sich lohnen; schon unter Marketingaspekten, da für Verbraucher Datensicherheit immer wichtiger werden wird.

Machen Sie sich mit Themen wie Datenschutzerklärung, Datenschutzbeauftragter, Versenden von Werbung und Newslettern usw. vertraut und fragen Sie gezielt nach, etwa bei den zuständigen Aufsichts-behörden Ihres Landes oder bei einem Anwalt. Bei Nichtbeachten der einschlägigen Bestimmungen drohen Ihnen u.a. empfindliche Bußgelder.

Weiterführende Links

http://www.bfd.bund.de/ - Der Bundesbeauftragte für Datenschutz

http://www.datenschutz.de/ - Virtuelles Datenschutzbüro

http://www.datenschutzzentrum.de/ – Landeszentrum für Datenschutz Schleswig-Holstein

Ihre Notizen zum Thema:

Datenschutz

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Checkliste sicheres Surfen

Um sicher durchs Internet zu reisen, sollten Sie auf bestimmte Grundregeln achten. In diesem Abschnitt finden Sie noch einmal einem Überblick über einige besonders wichtige Aspekte, die in der Broschüre schon näher vorgestellt wurden.

- Das Speichern von sensiblen Daten auf dem PC ist nicht empfehlenswert. Gerade Ihre Passwörter, Bank- oder Kreditkartendaten sind besonders gefragt und könnten ausspioniert werden. Ebenso sollten Sie diese Daten nicht per eMail versenden, denn auch diese können leicht abgefangen werden.

- Sorgen Sie für Ihren PC mit Internetzugang für ein Virenschutzprogramm, das sich zudem regelmäßig aktualisieren sollte. Es gibt sehr gute kostenfreie Virenprogramme zum Herunterladen, die sich mit vielen kommerziellen Angeboten messen lassen können!

- Auch sollten Sie keine eMails von unbekannten Absendern und insbesondere nicht ohne weiteres Dateianhänge öffnen - sie könnten mit Viren o.ä. infiziert sein.

- Geben Sie Ihre eMail-Adresse nicht wahllos heraus, damit Sie nicht mit unerwünschten Werbe-eMails und „Spam-Mails“ überschüttet werden. Zudem finden sich darunter immer öfter sogenannte Phishing-Mails, die Sie unter falscher Identität zur Herausgabe Ihrer Daten und Passwörter bewegen wollen.

- Sollte Ihnen aus dem Nichts heraus ein angeblicher Gewinn angeboten werden, obwohl Sie an keinem Gewinnspiel teilge-

nommen haben, dann halten Sie sich davon fern. Niemand verschenkt einfach so Geld! Dasselbe gilt für dubiose Erbschaften oder angeblich auf den Bankkonten vergessenes Geld früherer afrikanischer Diktatoren.

- Wenn Sie auf einer Internetseite um Ihren Namen und Ihre eMail-Adresse gebeten werden, um die Seite nutzen zu können, dann sollten Sie genau prüfen, ob Sie nicht gerade im Begriff sind, einen kostenpflichtigen Vertrag oder ein Abonnement abzuschließen. Schon viele Verbraucher haben „aus Versehen“ eine Bestellung abgeschickt. Trotz der Möglichkeit einen Vertragsabschluss zu bestreiten, widerrufen oder anzufechten, haben Sie zumindest tatsächlich erstmal den Ärger, penetrant mit drohenden Mahnungen belästigt zu werden. Mehr Informationen zu „Online-Abo-Fallen“ bekommen Sie auf unserer Internetseite unter www.ecommerce-verbindungsstelle.de.

- Um sicher im Internet einzukaufen, sollten Sie sich die Anbieter sorgfältig ansehen. Hat er alle Kontaktdaten (eMail, Telefon, vollständige Adresse) angegeben und ist er leicht zu erreichen? Mehr Informationen zum Online-Einkauf bietet die Broschüre „Shopping Online“ auf unserer Internetseite unter www.ecommerce-verbindungsstelle.de .

- Es lohnt sich nachzulesen, wie der Verkäufer bewertet wurde, wenn Sie an einer Onlineauktion teilnehmen: Wurde er in letzter Zeit oft negativ bewertet, oder ist dies sein erster Verkauf überhaupt? Dann sollten Sie vorsichtig sein und genauer hinsehen, warum die schlechte Bewertung vergeben wurde. Bestehen noch Zweifel, dann kaufen Sie wenn überhaupt nur für kleinere Geldbeträge ein. Beachten Sie aber, dass auch eine positive Bewertung keine absolute Sicherheit bietet oder negative Bewertungen von Konkurrenten gesetzt werden können!

- Achten Sie auf Gütesiegel! In Deutschland gibt es verschiedene Anbieter von Gütesiegeln, die Internetshops auszeichnen. Wichtig ist aber auch ein vertrauenswürdiges Gütesiegel. Nicht jedes Gütesiegel hält auch was es verspricht. Manche Shops führen auch unberechtigt ein Siegel. Prüfen Sie bei Zweifel also in mehrere Richtungen nach!

- Überweisen Sie auf keinen Fall größere Beträge ohne Absicherung! Insbesondere nicht, wenn ein Schnäppchen gar zu günstig ist.

Ihre Notizen zum Thema:

Checkliste sicheres Surfen

Grenzüberschreitendes Surfen

Gerade beim Kauf über das Internet wohnen die Vertragsparteien oft weit voneinander entfernt, teilweise sogar in anderen Ländern und sprechen nicht immer dieselbe Sprache.

Ohne sich dessen überhaupt bewusst zu sein, kaufen Verbraucher manchmal über das Internet bei einem Unternehmer aus einem anderen Staat, der ein anderes Rechtssystem hat als sein eigenes Land. Zu einigen Sicherheitsstandards gibt es in der EU ein Mindestmaß an Vorgaben. Es kann aber Unterschiede von Land zu Land geben.

Hier können die eCommmerce-Verbindungsstelle und die Europäischen Verbraucherzentren Hilfe bieten.

Das Europäische Verbraucherzentrum Deutschland in Kehl bildet zusammen mit 28 weiteren Europäischen Verbraucherzentren ein europaweites Netzwerk, das ECC-Net. Gemeinsam mit dem Europäischen Verbraucherzentrum Frankreich und der eCommerce-Verbindungsstelle Deutschland ist es unter dem Dach von Euro-Info-Verbraucher e.V. angesiedelt.

Bei grenzüberschreitenden Streitfällen mit Unternehmern aus einem anderen EU-Mitgliedstaat kann es Ihnen helfen: Entweder durch Information oder durch aktive Vermittlung. So kann Ihr Fall mit Hilfe des Netzwerks an einen geeigneten Schlichter im Ausland weitergeleitet werden oder aber die ausländischen Kollegen nehmen direkt Kontakt mit dem Unternehmer auf, um den Streit außergerichtlich beizulegen. Derart lassen sich große Entfernungen oder auch Sprachbarrieren zwischen den Streitparteien überbrücken. Eine außergerichtliche Streitbeilegung lässt sich natürlich meistens nur bei redlichen Online-Shops erzielen.

Nehmen Sie also die Hilfe gerne schon im Vorfeld in Anspruch und fragen Sie nach, wenn Sie Zweifel haben, ob das angestrebte Geschäft auch wirklich erstrebenswert ist.

Diese Broschüre erhebt keinen Anspruch auf Vollständigkeit, sondern soll einen verständlichen Überblick über wesentliche Problem- und Themenfelder bieten. Für die Richtigkeit der in dieser Broschüre enthaltenen Angaben können wir trotz sorgfältiger Prüfung keine Gewähr übernehmen.

Stand dieser Information: Dezember 2009

eCommerce-Verbindungsstelle

Rehfusplatz 11
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 bei

Euro-Info-Verbraucher e. V.

Rehfusplatz 11 - 77694 KEHL - Deutschland

Tel.: 07851 991 48 0 - Fax: 07851 991 48 11 - **mail: info@euroinfo-kehl.eu**