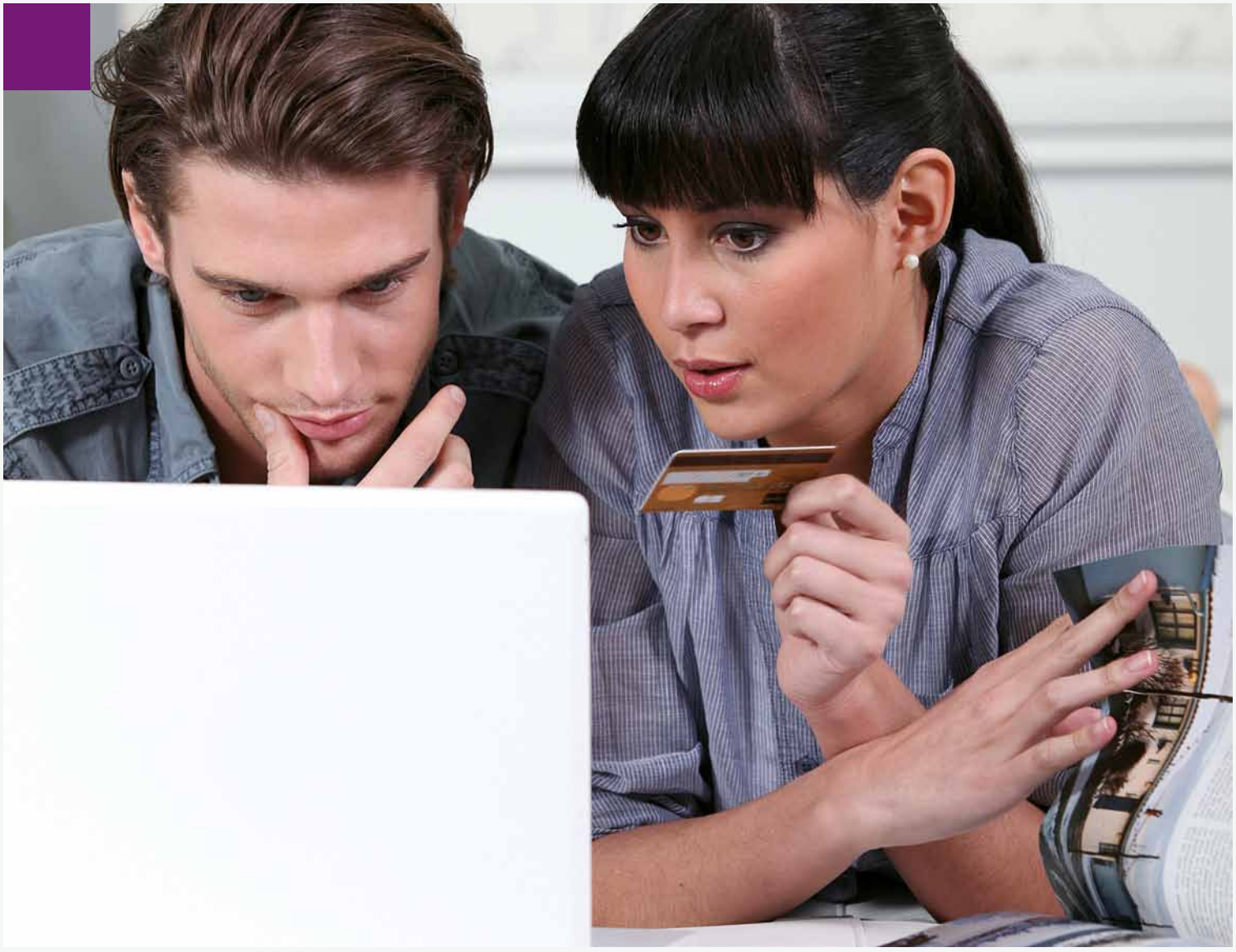
IM BLICKPUNKT:

Bezahlen im Web



Staatskanzlei
des Landes Nordrhein-Westfalen

Bezahlen im Web

Der kleine Junge steht vor einer Ladentheke, auf der große Bonbongläser locken. Er kauft einige Karamellbonbons, zahlt – und isst das erste direkt im Laden. In der nächsten Szene ist er längst erwachsen, die Verkäuferin deutlich ergraut, aber die Szene läuft immer noch genauso ab: Er kauft, zahlt und steckt sich das Bonbon in den Mund. Bloß ein TV-Spot? Eine romantisch aufgeladene Erinnerung an die gute alte Zeit? Eine Szene aus dem Wirtschaftsleben mit Auslaufcharakter?

Der Onlinehandel boomt. Mittlerweile ist alles über das Internet handelbar – vom Auto über Bonbons bis hin zu einzelnen Musikstücken oder Zeitungsartikeln. Rund um die Uhr sind die „Ladentheken“ hier geöffnet, ohne dass die Menschen ihr Haus verlassen müssten – und Verkäufer(innen) noch gebraucht würden. Während Ende 2008 nur jede(r) zweite Deutsche online einkaufte, waren es einer Umfrage des Marktforschungsinstituts Forsa zufolge 2009 bereits zehn Prozent mehr. Dadurch findet auch das Bezahlen im Web immer mehr Verbreitung. Gleichzeitig ist der Onlinezahlvorgang der häufigste Abbruchgrund für den Onlinekauf. Paradox?

IM BLICKPUNKT: Bezahlen im Web stellt Vor- und Nachteile bestimmter Formen von Onlinebezahlsystemen vor sowie Gütesiegel, Sicherheitstipps für das (risikoärmere) Bezahlen im Web und anderes mehr.

Reine Formsache?

Die meisten Bezahlvorgänge im Internet gehen in Deutschland (immer noch) recht klassisch vonstatten. Das ergab der Bitkom-Webmonitor, eine repräsentative Forsa-Umfrage im Auftrag des Branchenverbands Bitkom:

- Die meisten Internet-Einkäufe in Deutschland (41 Prozent) werden immer noch per **Rechnung** beglichen, während mehr als jeder Dritte (36 Prozent) per Vorkasse zahlt. Vorteile bei der Zahlung per Rechnung (und Überweisung): Die Zahlung erfolgt erst nach dem Warenerhalt, so dass die Ware vor der Bezahlung geprüft werden kann. Leider bieten noch zu wenige Internethändler den Rechnungskauf an. Bei Vorkasse entfällt diese Möglichkeit, gilt hier doch: „Erst das Geld, dann die Ware“. Deshalb ist Vorsicht geboten, insbesondere, wenn es sich bei der Vorkasse um größere Geldbeträge handelt. Geringer fällt das Risiko bei Kleinbeträgen aus, weshalb die Vorkasse hier eher eine akzeptable Zahlungsform ist. Ein weiteres Problem kommt hinzu: Wird der Händler nach der Vorkassezahlung zahlungsunfähig und hat die Ware noch nicht geliefert, ist das Geld in der Regel verloren.

- **Einzugsermächtigungen** nutzten rund ein Fünftel (22 Prozent) der Deutschen, Zahlungen per Nachnahme etwas weniger (16 Prozent). Bei der Einzugsermächtigung übermittelt der Kunde oder die Kundin dem Händler zunächst die persönlichen Kontodaten, wenn er oder sie sich für ein bestimmtes Produkt entschieden hat (oder hinterlegt diese mehr oder weniger dauerhaft beim Anbieter). Das geschieht zumeist online, was – je nach Verschlüsselung – das Risiko der Ausspähung birgt. Die Kunden erlauben gleichzeitig, den Warenpreis von ihren Konten abzubuchen. Entspricht die Ware bei der Zustellung dann nicht den Kundenwünschen, können diese die Abbuchung problemlos – innerhalb der angegebenen Frist – bei der Bank widerrufen. Das bietet eine relative Sicherheit. Bei der **Zahlung per Nachnahme** bezahlt der Kunde oder die Kundin die Ware sofort bei Erhalt, wofür aber oftmals zusätzliche Gebühren anfallen. Auch entfällt die Möglichkeit zur Warenprüfung. Der Vorteil: Es müssen keine sensiblen Daten (per Internet) übermittelt werden.

- Mit der Zahlung per Nachnahme anteilsmäßig gleichauf ist die **Zahlung per Kreditkarte** (15 Prozent). In der Regel ist die Übermittlung der Kartendaten (online) notwendig, und aus Sicherheitsgründen wird zusätzlich noch die dreistellige Kreditkartenprüfnummer erfragt. Bei Missbrauch

der Kartendaten haftet jedoch fast immer der Händler, wenn er nicht nachweisen kann, dass kundenseitig fahrlässig mit den Kartendaten umgegangen wurde.

Onlinezahlungssysteme
Für den Internethandel wurden spezielle Onlinebezahlsysteme entwickelt, die sich insbesondere für die Abrechnung von Kleinstbeträgen (engl. „Micropayment“) eignen, wie zum Beispiel für einzelne Musikstücke oder Zeitungsartikel. In der Regel braucht der Kunde hierzu keine Extra-Software zu installieren, die Zahlung ist mit allen gängigen Browsern, Betriebssystemen und Providern möglich. Üblicherweise reicht hierfür die einmalige Anmeldung, aber bei einigen Onlinebezahlsystemen ist noch nicht einmal dies erforderlich.

Natürlich können die populären Onlinezahlungsysteme auch größere Summen übermitteln, was auch immer üblicher wird. Hierfür sind sie aber eigentlich nicht ausgelegt beziehungsweise verursachen in der Praxis häufig (unangenehme) Sicherheitsrisiken. Für die Abrechnung von größeren Beträgen sollten daher andere Alternativen bevorzugt werden.

Zu den Zahlungssystemen zählen unter anderem:

- **Click & Buy**: Das System der Deutschen Telekom wird beispielsweise von Onlinemusikkaufhäusern genutzt. Kund(inn)en melden sich mit Namen, Anschrift, Geburtsdatum und E-Mail-Adresse an und entscheiden dann, ob sie per Kreditkarte oder Lastschrift bezahlen wollen. Nach dem Erhalt eines Nutzernamens und eines Passworts kann künftig ohne Angabe weiterer Daten die Bezahlung per Click & Buy abgewickelt werden.
  http://clickandbuy.com/DE_de/bezahlen/

- **GiroPay**: Das Angebot richtet sich speziell an Onlinekund(inn)en der Postbank, der Sparkasse oder der Volks- und Raiffeisenbank und funktioniert wie das Onlinebanking (siehe unten ausführlicher), was die Bedienung vereinfacht.
  www.giropay.de

- **PayPal**: Das Onlinebezahlsystem des Onlineauktionshauses eBay gehört zu den populärsten Zahlungssystemen und wird inzwischen auch von zahlreichen anderen Anbietern genutzt. Kunden können entweder per Lastschrift, Kreditkarte, Onlineüberweisung (mittels GiroPay) oder per Guthaben auf dem PayPal-Konto bezahlen. Aber Achtung: Vielen ist nicht klar, dass die Käuferschutzvorkehrungen nur für Transaktionen in Zusammenhang mit dem Onlineauktionshaus gelten – und nicht darüber hinaus.
  www.paypal.de

- **Guthabenkarten**: Apple bietet die Möglichkeit, Guthabenkarten zu erwerben, mit denen man Musik, Bücher, Filme, Serien und Applikationen im iTunes Store kaufen kann. Die Karten können sowohl online als auch in verschiedenen Super- und Elektronikmärkten erworben werden. Der Vorteil beim Einkauf im Geschäft: Man muss keine Kreditkarten- oder Bankdaten online angeben, die Bezahlung erfolgt ganz „analog“.

Bei aller gebotenen Vorsicht muss jedem klar sein: Hundertprozentigen Schutz vor Enttäuschungen und illegalen Praktiken gab es früher nicht, als Bezahlvorgänge nur ohne Webunterstützung möglich waren, gibt es jetzt nicht und wird es voraussichtlich niemals geben – mit keinem System, mit keiner Methode. Der Warenhandel findet zunehmend im Internet statt und dieser Trend ist unumkehrbar. Medienkompetente User achten daher beim Bezahlen im Web kontinuierlich auf sichere Rahmenbedingungen. Denn im Internet ist ein hohes Maß an Sicherheit und Datenschutz nur ein relativer Zustand, der immer erst wieder hergestellt werden muss – von allen Beteiligten.

Onlinebanking
Onlinebezahlsysteme wie GiroPay machen deutlich: Eng verknüpft mit dem Bezahlen im Internet ist das Onlinebanking – und wirft ähnliche Fragen nach der Sicherheit der Datenübermittlung auf. Dabei gehört das Onlinebanking heute für viele zum Alltag. Bankkunden mit Internetzugang schalten inzwischen häufiger für ihre Bankgeschäfte den PC ein, als dass sie in ihre Filiale gehen, belegt etwa der (N)Onliner-Atlas

2010. Und weiter: Die Bankfiliale im Internet wird noch weiter an Bedeutung gewinnen, denn heute nutzt bereits mehr als die Hälfte der Smartphone-Besitzer ihr Gerät, um ihre Bankgeschäfte von unterwegs aus zu erledigen.

Verfahren

Beim sog. **PIN-TAN-Verfahren** legitimiert sich der Kunde oder die Kundin durch die individuelle PIN-Nummer und gibt dann Transaktionen durch eine TAN frei, die er oder sie zuvor in Form einer Liste von der Bank erhalten hat. Dieses Verfahren ist relativ unsicher, weshalb die meisten Banken mittlerweile andere Verfahren nutzen: Beim **iTAN-Verfahren** kommt beispielsweise eine „indizierte TAN-Liste" (daher iTAN-Verfahren) zum Einsatz. Einzelne Transaktionsnummern werden hierbei nach dem Zufallsprinzip aus einer Liste ausgewählt und verschlüsseln dann die jeweilige Transaktion. Aber auch dieses Verfahren wurde schon „geknackt" und gilt maximal als eingeschränkt sicher.

Darüber hinaus wurden andere sichere Methoden entwickelt, die oft den Einsatz von Zusatzgeräten zur Authentifizierung und/oder Verschlüsselung notwendig machen:

- Beim **mTAN-Verfahren** schickt die Bank zuvor registrierten Teilnehmer(inne)n Transaktionsnummern für die Autorisierung von Bankaufträgen auf das Mobilgerät, etwa das Handy. Ansonsten funktioniert diese Methode wie das eingangs beschriebene TAN-Verfahren. Die Zusendung und Aufbewahrung von TAN-Listen fällt weg – ein Sicherheitsplus. Nachteilig: Die mobile Übermittlung kann ausgespäht werden und der Mobilfunkempfang ist nicht überall und nicht zu jeder Zeit gewährleistet.

- Beim **eTAN-Verfahren** – teils auch smart-TAN genannt – erhalten die Bankkunden neben einer PIN-Nummer einen etwa taschenrechnergroßen eTAN-Generator, der spontan Kontrollnummern auswirft. Mit deren Eingabe bei der Onlineüberweisung wird die Transaktion dann erst perfekt. Das eTAN-plus-Verfahren funktioniert ähnlich, wird aber durch eine zusätzliche Authentifizierung noch sicherer.

- Das **HBCI (Homebanking Computer Interface)-Verfahren** wurde von verschiedenen Bankengruppen in Deutschland entwickelt und vom Zentralen Kreditausschuss (ZKA) überprüft und freigegeben. Auch hier kommt ein externes Zusatzgerät zum Einsatz. Das hat seinen Preis: Je nach Bauart kostet die Anschaffung zwischen zwanzig und hundertzwanzig Euro. Und neben Anschaffung des Zusatzgeräts ist in der Regel die Installation spezieller Software notwendig.

Eine besondere Form des Onlinebanking bietet Sofortüberweisung.de: Hier füllt der Käufer auf der Shopseite ein Überweisungsformular aus und der Händler erhält eine Bestätigung, dass das Geld verschickt wurde. Die Überweisung folgt. Vorteil: User müssen kein Kundenkonto erstellen oder sich registrieren. Nachteil: Der Nutzer muss PIN und TAN auf einer fremden Seite angeben, was die Banken regelrecht verbieten, weil sie dann eine Haftung (entsprechend der AGB) ausschließen – zum Schaden der Kunden.

Social Payment

Anders als beim Onlinewarenhandel gibt es bei den informativen Internetinhalten – Nachrichten, Artikel und anderes mehr – weit verbreiteten Widerstand gegen das Bezahlen. Inhalteanbieter – hierzu zählen auch Blogbetreiber, freie Journalisten, Wissenschaftler und andere mehr – sind deshalb auf der Suche nach Alternativen in Sachen Finanzierung.

- Mit **Flattr** und **Kachingle** könnten sich diese womöglich ergeben, zumindest hinsichtlich einer Teilfinanzierung. Dabei handelt es sich in beiden Fällen um eine Art Onlinespendenkonto, bei dem der Benutzer einen selbstgewählten Monatsbetrag auf ein Konto einzahlt (per PayPal etwa). Bei Flattr beträgt der Mindestbetrag zwei Euro im Monat, bei Kachingle das Doppelte. Und so geht's: Besucht man eine Seite, die wahlweise einen Flattr- oder Kachingle-Button trägt, zahlt – oder

Links

- FOCUS (12/2009): Online-Shopping. So bezahlt man im Internet.
  www.focus.de/digital/internet/tid-7045/online-shopping-so-bezahlt-man-im-internet_aid_68985.html
- Internet Gütesiegel
  www.internet-guetesiegel.de
- Verbraucherzentrale NRW: Wie funktioniert der Internet-Einkauf?
  www.vz-nrw.de/UNIQ127894099712858/link5370A.html
- Phishing, Pharming und weitere internetspezifische Gefahren (und deren Abwehr) beschreibt die Broschüre IM BLICKPUNKT: Internetkriminalität
  www.grimme-institut.de/imblickpunkt/
- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt Tipps zum sicheren Umgang mit Online-shopping und -banking
  www.bsi-fuer-buerger.de

besser spendet – man für den Konsum nur dann, wenn man möchte. Per Click auf den Button wird die Webseite für einen Spendenanteil vorgemerkt – und am Monatsende teilen die beiden Dienste den zuvor eingezahlten Monatsbetrag durch die aufgelaufenen Clicks, so dass der entsprechende Anteil an die Inhalteanbieter geht. Der wichtigste Unterschied zwischen beiden Angeboten: Flattr verteilt die Summe gleichmäßig auf alle „geflatterten" Inhalte, egal ob eine Seite nur einmal oder häufiger besucht wurde. Kachingle berücksichtigt die Häufigkeit der Webseitenbesuche bei der Auszahlung.
http://flattr.com
www.kachingle.com

Qualitäts- und Sicherheitsfragen

Das sichere Bezahlen im Web ist nicht nur eine Frage des Bezahlsystems, sondern betrifft auch ganz generelle Fragen, wie etwa die, wem man beim Internethandel Vertrauen schenkt, oder auch Fragen der Datensicherheit – von der Verschlüsselung persönlicher Daten, über den Einsatz von Sicherheitssoftware bis hin zur Einhaltung spezieller Verhaltensregeln.

Schlüsselfragen

Verbraucherschützer fordern Kund(inn)en immer wieder dazu auf, sich gerade bei unbekannte(re)n Onlinehändlern gründlich über die Allgemeinen Geschäftsbedingungen zu informieren: Wer ist es, der mir etwas verkaufen will? Und zu welchen Bedingungen?

Häufig müssen für die Bezahlvorgänge persönliche Kontodaten übertragen werden. Hierfür sollte unbedingt auf eine gesicherte Verbindung geachtet werden, um das Ausspährisiko möglichst gering zu halten. Bieten Internethändler diese Technik für die Datenübermittlung nicht an, scheint die Wahl eines Konkurrenten für den Internetkauf sinnvoll. Anders formuliert: Die Verfügbarkeit dieser Technik ist ein Kriterium für die Anbieterauswahl.

Ob Daten bei der Übermittlung mit der gängigen Technologie SSL (Secure Sockets Layer) verschlüsselt werden, lässt sich zum einen an der URL im Browser erkennen: Statt „http://..." steht hier dann „https://...". Zum anderen erscheint im Browser ein Sicherheitsschloss, das bei der Datenübertragung geschlossen sein muss.

Gütesiegel

Sicheres Onlineshoppen sollen Gütesiegel gewährleisten, die von einer ständig wachsenden Zahl von Anbietern auch erworben werden – als Marketinginstrument. Die Initiative D21 hat Qualitätskriterien für Onlineangebote entwickelt und führt eine Liste empfehlenswerter Gütesiegelanbieter. Auf sie verweist auch das Bundesministerium für Justiz.

Der Umkehrschluss, ein Shop ohne Gütesiegel sei unseriös, gilt nicht zwangsläufig. Die Internet-Gütesiegel kosten Geld – teilweise erhebliche Summen. Ein umfangreiches Zertifizierungsverfahren ist zu durchlaufen, eine gehörige Investition also, die gerade Neulinge und kleine Anbieter scheuen dürften. Was genau „besiegelt" wird, ist dabei recht unterschiedlich und oftmals wenig aussagekräftig, was aber viele Verbraucher nicht wissen beziehungsweise was oft nicht auf Anhieb durchschaubar ist. Als weiteres Kriterium für die Anbieterauswahl eignen sich Gütesiegel also nur bedingt.

Achtung Abofallen!

Immer wieder sorgen Abofallen für das ungewollte „Bezahlen im Web". Die Hamburger Verbraucherzentrale gibt Tipps, wie man diesen (wieder) entgehen kann beziehungsweise welche Verbraucherrechte hier gelten. Daneben findet sich eine ständig aktualisierte Liste auffällig gewordener Betreiber-Internetseiten.

- **www.vzhh.de/~upload/rewrite/TexteTelekommunikation/AbofallenimInternetLeitartikel.aspx**

Links

- Harald Gapski / Lars Gräßer (Hrsg.) (2010): Verbraucherschutz und Medienkompetenz. Junge Konsumenten im Web. Band 10 der Schriftenreihe Medienkompetenz des Landes Nordrhein-Westfalen, Düsseldorf. **www.grimme-institut.de/schriftenreihe/**
- (N)Onliner-Atlas 2010: Sonderauswertung Online-Banking **www.initiative21.de/wp-content/uploads/2010/07/100708_PI_NOA2010_FIDUCIA_final.pdf**
- Sicher durchs Internet – ein Leitfaden für Verbraucher und Anbieter **www.ecommerce-verbindungsstelle.de/ecommerce/pdf/Sicher durchs Internet.pdf**

Datensicherheit
Internetspezifische Gefahren entstehen beim „Bezahlen im Web" durch die Anfälligkeit von Datennetzen, aber auch durch die Einbruchsmöglichkeiten in die „digitale Privatsphäre". Einige Beispiele zeigen, worauf es zu achten gilt:

Phishing bezeichnet alle Verfahren, bei denen versucht wird, mithilfe gefälschter E-Mails vertrauliche Zugangs- und Identifikationsdaten von Dritten auszuspähen. Mit diesen Daten wird dann – unter der Identität des Inhabers – im Onlineverkehr gehandelt: Waren werden angeboten und abkassiert und/oder PIN/TAN-Kombinationen dazu missbraucht, Abbuchungen durchzuführen und noch anderes mehr.

Vorbei sind die Zeiten, als Phishing-Mails noch durch zahlreiche Rechtschreib- und Grammatikfehler, unprofessionelle Formulierungen und ein amateurhaftes Layout auffielen. Neben den Anschreiben wirken aber auch die gefälschten Webseiten, die die Nutzer(innen) zur Eingabe ihrer Logins und Passwörter verleiten, professioneller als in der Vergangenheit. Sie sind von den Originalseiten immer schwerer zu unterscheiden. Nutzer(innen) sollten daher keinen Links aus E-Mails folgen, die zur PIN- beziehungsweise Passwort-Eingabe auf Webseiten auffordern. Als Faustregel gilt: Banken versenden E-Mails fast ausschließlich zu Marketingzwecken. Werden andere Zwecke verfolgt, womöglich nach PIN/iTAN-Kombinationen gefragt, dürfte die E-Mail „Ihrer Bank" gefälscht sein. Das ist auch übertragbar auf Telefonate mit der Bank.

Darüber hinaus sollten stets die neueste Version des jeweiligen Webbrowsers verwendet und Sicherheitskorrekturen (engl. „Patches") installiert werden. Auch Virenschutzprogramme und Firewalls sollten immer auf dem aktuellen Stand sein. Nachlässigkeiten können hier als fahrlässig ausgelegt werden.

Auf der Internetpräsenz der eCommerce-Verbraucherstelle finden sich umfangreiche Informationen zum Recht im Internet, Hinweise auf diverse Organisationen und weitere Ansprechpartner rund um das Thema eCommerce. Gebündelte Informationen bietet eine 35seitige Broschüre mit dem Titel „Sicher durchs Internet – ein Leitfaden für Verbraucher und Anbieter", die kostenlos erhältlich ist.

Ausblick

Der Onlinehandel boomt, das Bezahlen im Web wird zunehmend selbstverständlich. Dabei fallen die Formen für das Bezahlen im Web immer unterschiedlicher aus – von Micro- bis „Macropayment", vom Computer zuhause bis hin zur mobilen Anwendung von jedem Ort der Welt.

Hier den Überblick zu behalten und Risiken realistisch einschätzen zu können, ist nicht nur eine Frage des Verbraucherschutzes, sondern auch der Medienkompetenz – für ein mündiges Konsumverhalten im Web.

Impressum

Diese Broschüre ist mit Mitteln der Staatskanzlei Nordrhein-Westfalen entstanden. Sie kann kostenlos unter **www.grimme-institut.de/imblickpunkt** heruntergeladen werden.

Redaktion:
Grimme-Institut
Gesellschaft für Medien, Bildung und Kultur mbH
Eduard-Weitsch-Weg 25 · D-45768 Marl
Tel: +49 (0) 2365 9189-0 · Fax: +49 (0) 2365 9189-89
E-Mail: info@grimme-institut.de
Internet: www.grimme-institut.de

Bildquellen:
auremar (Titelfoto), by-studio (S. 1 u. 2), Eisenhans (S. 1. u. 3), m.schuckart (S. 1 u. 4) / alle fotolia.com

Stand: August 2010