Stiftung Warentest

Pocket

In allen Netzen unterwegs

Leben im Netz

Das Internet fasziniert. Und es ist längst aus unser aller Leben kaum mehr wegzudenken. Gut zwei Drittel aller Bundesbürger sind jeden Tag vier Stunden oder länger im Netz. 70 Prozent sind in sozialen Netzwerken registriert. Und es gibt kaum noch jemanden in der Generation unter 25, der oder die nicht chattet, twittert, surft, skypt, E-Mails verschickt oder andere Angebote des World Wide Web nutzt.

Mit dieser Broschüre wollen wir euch die große weite Digitalwelt keineswegs madig machen. Im Gegenteil: Die Netzwelt informiert, bietet eine Reihe von tollen Serviceangeboten, wir können laufend miteinander in Kontakt treten, alte Freundschaften wiederbeleben, neue knüpfen. Wir können uns einer breiten Nutzerschicht mitteilen und Teile unseres ganzen Soziallebens ins Netz verlegen. Nicht zuletzt macht das Internet Spaß. Für die meisten von uns ist die Netzwelt einfach nicht mehr wegzudenken.

Doch das Internet birgt auch zahlreiche Gefahren. Das alles kann passieren: Ich erhalte Spammails, Viren, Trojaner und die Zugangsdaten für meine privaten Webseiten

werden geklaut. Seltsame Mails werden über mein E-Mail-Konto an meine Bekannten verschickt, ohne dass ich davon etwas weiß. Private Bilder von mir gelangen in die Netzöffentlichkeit, ohne dass ich über diese Bilder bestimmen kann. Ich verliere den Überblick über meine Online-Käufe. Die Handy-Gebühren steigen ins Unermessliche, weil ich mit meinem Smartphone im Ausland vergessen habe, dass es laufend Daten saugt. Vor allem Facebook bringt es immer wieder in die Schlagzeilen, weil das weltweit am meisten genutzte soziale Netzwerk es mit dem Datenschutz nicht so genau nimmt.

Diese Broschüre soll euch einen Überblick über mögliche Gefahren im Netz verschaffen. Es soll als Wegweiser dienen und helfen, euch sicher in der Netzwelt zurechtzufinden – damit euch das Internet auch dauerhaft euer Leben erleichtert und nicht erschwert.

Inhalt

I. Sicher Surfen

Die Internet-Welt ist nahezu unendlich. Zwischen all den tollen Angeboten gibt es aber auch sehr viele Seiten und Foren, in denen leider sehr viel Schindluder betrieben wird. Ihr kommt vielleicht auf Seiten mit grausamen Bildern. In manchen Foren finden hässliche Beschimpfungen statt. Übel sind auch Angebote, die euch zu undurchschaubaren Ausgaben verleiten. Viele Seiten sind nicht jugendfrei, einige gar komplett verboten. Das heißt: ihr oder eure Eltern könnt rechtlich belangt werden, wenn ihr sie anklickt.

TIPP: Haltet euch an Vereinbarungen mit euren Eltern, auf welchen Foren ihr euch unbedenklich bewegen könnt und von welchen Webseiten ihr die Finger lassen solltet.

Schutz vor Viren, Würmen und Trojanern

Das Internet ist voller Gefahren vor allem wegen sogenannter Schadsoftware. Eine ganze kriminelle Industrie hat sich weltweit entwickelt, die allein darauf aufbaut, Kapital aus erbeuteten persönlichen Daten zu schlagen. Da gibt es Viren, die Programme infizieren und sie kaputt machen. Würmen verschicken sich von alleine auf andere

Rechner. Und Trojaner tarnen sich zunächst als harmlose Programme und entfalten erst dann ihre Wirkung, wenn ihr sie als ahnungslose Nutzer aus Versehen durch etwa einen Mausklick weckst. Hier eine Übersicht über die häufigsten Schädlinge:

Computerviren. Ein Virus infiziert Programme und führt bei ihrem Start bestimmte Aktionen aus, über die ihr keine Kontrolle habt. Häufig zerstören sie Datensätze oder eure Anwendungsprogramme.

Wurm. Beim Wurm kommt hinzu, dass er sich von allein auf andere Computer verschickt – ohne dass ihr davon Kenntnis habt.

Trojaner. Sie tarnen sich als harmlose Programme und entfalten erst dann ihre Wirkungs, wenn ihr sie als ahnungslose Nutzer ausgeführt habt. Sie können Datensätze und euren ganzen Rechner lahm legen.

Rootkits. Dabei handelt es sich um Werkzeug-Sammlungen, mit denen Hacker auch ohne Programmierkenntnisse auf anderen Rechnern Administratorenrechte erlangen können. Auf diesem Wege ist es möglich, dass sie eure Rechner manipulieren, ohne dass Virenscanner diese Veränderungen registrieren.

Backdoor. Dies ist im wahrsten Sinne des Wortes eine Hintertür. Sie hält eure Programme für die Entwickler offen, die eure Anwendungen programmiert haben. Manchmal ist das für euch als Anwender von Nutzen, wenn sie nämlich Sicherheitslücken füllen. Zuweilen können sie euch aber auch Schaden zufügen.

Exploits. Exploits sind Programmcodes, die Sicherheitslücken von weit verbreiteten Programmen wie Browser, Foto- oder Textverarbeitungsprogrammen ausnutzen. Sie verschaffen anderer Schadsoftware Zugang zu eurem Rechner.

Spyware. Diese Software sammelt Informationen über euch und gibt sie an die Entwickler dieser Schadsoftware weiter. Manche von ihnen installieren etwa sogenannte Keylogger, die alle die alle Tastaturanschläge von euch sammeln und aufzeichnen, unter anderem auch eure eingegebenen Passwörter.

Phishing. Ein weiterhin ungelöstes Problem. Über E-Mails oder Anfragen auf sozialen Netzwerken werdet ihr über vertrauliche Daten von euch ausgefragt.

TIPPS: Auf jeden Fall solltet ihr immer die inzwischen fast auf jeden Rechner vorhandene Firewall aktivieren. Außerdem solltet ihr dafür sorgen, dass euer Virenschutzprogramm auf dem aktuellen Stand ist, sprich: Jedes Sicherheits-Update auch sofort installieren (kostenlose Antivirensoftware findet ihr etwa auf www.freeav.com). Zum Schutz vor Trojanern und anderen schadhaften Programmen bietet sich Sypbot an (www.safer-networking.org/de). Ganz wichtig: Überlegt es euch zwei Mal, bevor ihr einen Anhang in einer E-Mail öffnet oder Programme von unsicheren Quellen herunterladet. Was euch nicht bekannt vorkommt – lieber nicht anklicken.

Spuren vermeiden

Aber es müssen gar keine Trojaner oder Viren sein, die einen ausspionieren. Das ganz normale Surfen genügt. Denn mit jedem Aufruf auf einer Internetseite hinterlasse ich Spuren. Und sie sind anders als Viren und Würmer zunächst einmal sehr viel harmloser. Sie nennen sich „Cookies", „Beacons" oder „Caches" und sind häufig nur wenige Bytes groß. Aber auch sie haben es in sich. Denn einmal auf unserem Rechner gelandet können sie Zugriff, Uhrzeit, Verweildauer und die IP-Adresse vom Nutzer notieren und diese Informationen weiterleiten.

Vor allem Google, der am häufigsten genutzten Suchmaschine, gelingt es mit immer raffinierteren Methoden das eigene Surfverhalten auszuspähen. Viele von uns ahnen gar nicht, wie sehr wir inzwischen durchleuchtet werden. Was habe ich angeklickt, wie lange verharre ich auf einer Seite, in welcher Reihenfolge habe ich eine Seite aufgerufen – Google weiß Bescheid, protokolliert und speichert das auf firmeneigene Datenbanken. Aus diesen Informationen entstehen in kurzer Zeit Verhaltensprofile, die dann an andere Firmen weiterverkauft werden. Eine gruselige Vorstellung, zumal ich als Nutzer keine wirkliche Kontrolle über diese Datensammelei habe.

TIPP: Löscht in eurem Browser regelmäßig unter „Einstellungen" die Liste der besuchten Seiten, die Cookies und leert auch den Cache. Beim Surfen selbst lässt sich auf den meisten Browsern der Privatmodus einstellen. Das

solltet ihr auch tun. Allerdings: Einige bestimmte Cookies und Beacons lassen sich nicht deaktivieren. Manche Browser wie etwa Firefox bieten aber Programme an, die diese Kleinstprogramme sichtbar machen und solche Cookies von sich aus löschen.

Wenn ihr auch vermeiden möchtet, dass Google eure Suchabfrage für Werbekunden auswertet, könnt ihr diesen Mechanismus unter www.google.com/ads/preferences deaktivieren. Insgesamt ist es inzwischen sehr schwer geworden, im Netz komplett anonym zu bleiben. Jeder Betreiber einer Seite kann zumindest nachprüfen, von welchem Rechner aus in welchem Land und in welcher Stadt, wann die Seite aufgerufen wurde. Dennoch gibt es einige Anonymisierungsdienste, die man beim Surfen dazwischenschalten kann. Allerdrings drosseln diese Anwendungen häufig ganz massiv die Surfgeschwindigkeit. Das macht dann auch keinen Spaß.

Gehört ihr auch zu den 90 Prozent aller Jugendlichen, die mindestens einmal täglich online sind? Und längst sind für euch Begriffe wie Instant Messenger, Communities oder Chats keine Fremdwörter mehr und stehen auch bei euch hoch im Kurs? Wenn dem so ist – das ist an und für sich nicht schlimm. Worauf es ankommt, wo, wie und in welchem Ausmaß ihr euch täglich im Netz aufhaltet.

So wie in der realen Welt das Plaudern, das Präsentieren und bestimmte Kommunikationsformen gelernt sein wollen, kann auch nicht jeder auf Anhieb gleich chatten und facebooken. Auch das muss erlernt werden und ist nicht ganz unwichtig – zumal ihr auch mit Blick auf eure berufliche Zukunft den angemessenen Umgang in den neuen Kommunikationsmedien beherrschen solltet. Besonderes Augenmerk verdienen hierbei soziale Netzwerke, und hier im speziellen das bislang am weitesten verbreitete: Facebook.

Besser facebooken

Es vergeht kaum eine Woche, in der nicht wieder ein Streit zwischen Datenschützern und Facebook vom Zaune bricht. Tatsächlich hat sich Facebook von einem einst

reinen sozialen Netzwerk zu einer gigantischen Datenkrake entwickelt. Was mal als Projekt junger Studenten zum simplen Austausch mit guten Freunden begonnen hat, ist inzwischen zu einem Großkonzern geworden mit weltweit inzwischen rund 800 Millionen Nutzern und einem Umsatz von mehreren Milliarden Dollar im Jahr. Das macht sich auch im Kleingedruckten bemerkbar. So erteilt der Nutzer per se „eine nicht-exklusive, übertragbare, unterlizenzierbare, unentgeltliche, weltweite Lizenz" für die Nutzung der eigenen Texte und Bilder. Was Facebook genau damit alles anstellt, ist unklar. Zusammen genommen sind diese ganzen gesammelten Daten aber Millionen wert.

Interview mit Michael Sittig

Rechtsredakteur von der Stiftung Warentest

Herr Sittig, sind Sie Nutzer von Facebook?
Ja. Ich bin Nutzer von Facebook.

Was ist Ihrer Meinung nach so reizvoll an Facebook?
Das Leben meiner Freunde und Verwandten ist mir durch Facebook einfach sehr viel präsenter als früher und ich

weiß sehr viel schneller, was in deren Leben passiert. Wenn etwa eine Freundin auf Facebook einen tollen Kinofilm empfiehlt oder mein bester Freund darüber schreibt, dass sein Baby einen Zahn bekommen hat, dann erfahre ich diese Dinge nicht wie früher zwei, drei Wochen später beim nächsten Treffen oder Telefonat, sondern via Facebook sofort. Außerdem benutze ich Facebook, um über Musik, Politik und Kultur informiert zu werden. Auf Facebook laufen Informationen zusammen, die ich früher einzeln etwa durch unzählige E-Mail-Newsletter zusammentragen musste.

Würden Sie sagen: Wer im Leben stehen will, der kann heutzutage ohne Facebook nicht mehr auskommen?
Ich glaube, dass die sozialen Netzwerke aus unserem Leben nicht mehr verschwinden werden. Das verächtliche Herabschauen mancher älterer auf die Facebook-Generation kommt mir manchmal so vor wie damals bei der Einführung des Handys. Was wurden die Nutzer von Mobiltelefonen als „Wichtigtuer" abgetan. Heute geht es kaum mehr ohne. So wird es mit den sozialen Netzwerken auch sein – egal ob sie Facebook heißen oder künftig vielleicht anders.

Ist das nicht bedenklich – zumal Facebook wegen mangelnder Datensicherheit immer wieder auch negative Schlagzeilen macht?
Facebook hatte und hat nach wie vor bedenkliche Bedingungen in den Verträgen stehen. Immer wieder laufen Gerichtsverfahren, um gegen diese Missstände vorzugehen. Das ist auch gut so. Neben der juristischen Auseinandersetzung müssen wir aber im Auge behalten, wie Facebook ganz praktisch mit den Daten umgeht. So lässt sich zum Beispiel über die persönlichen Einstellungen sehr wohl verhindern, dass Facebook mit meinem Foto für irgendeine Marke wirbt. Unsere Aufgabe ist es, auf diese Möglichkeit hinzuweisen und zu erklären wie sie einzustellen sind. Sollte es Facebook übertreiben, werden wir von der Nutzung dieser Dienste abraten.

Sie befürchten nicht, dass nicht doch persönliche Informationen über Sie an die Öffentlichkeit geraten, die Sie gar nicht veröffentlicht haben wollen?
Die Gefahr, dass vertrauliche Informationen öffentlich werden, ist nicht neu. Lästere ich im Vertrauen mit meinem Arbeitskollegen über meinen Chef und wird das an ihn weiter geplappert, kann mir das sehr schaden.

Facebook verstärkt dieses Risiko. Aber letztlich muss doch jeder selbst aufpassen, wen er zum Facebook-Freund macht. Bei jedem Eintrag gilt es, den Adressatenkreis meines Posts neu zu überdenken. Ich sehe tatsächlich viele Menschen, deren Profile uneingeschränkt einsehbar sind. Das halte ich für sehr gefährlich. Ich persönlich habe kein Foto von meinem Gesicht als Profil. Das ist sicher Geschmackssache. Aber jeder angehende Azubi oder Angestellte muss damit rechnen, dass potenzielle Arbeitgeber in den Netzwerken nach ihm suchen.

Was sollte ich auf keinen Fall von mir preisgeben?
Im Prinzip gelten die gleichen Maßstäbe wie im persönlichen Gespräch. Meine Begeisterung für einen Film oder eine Band habe ich früher schon auch in größeren Runden kundgetan. Das poste ich auch auf Facebook. Will ich über jemanden lästern, dann habe ich das früher im vertraulichen Gespräch getan. So halte ich das auch heute noch. Allenfalls schicke ich bei Facebook eine Privatnachricht.

Welche Grundeinstellungen sollte ich vornehmen?
Erstens: Überdenkt bei jedem Post, wie sichtbar ihr seid und justiert die Einstellungen gegebenenfalls nach. Will ich etwas nur meiner Verwandtschaft mitteilen, schicke ich meinen Post nur an die Liste „Verwandschaft". Soll die Verwandtschaft nichts erfahren, wird sie beim Posting aus dem Adressatenkreis herausgenommen.

Zweitens: Seid vorsichtig beim sogenannten Taggen, also der Markierung von Fotos. Ich persönlich würde die Privatsphäre-Einstellungen immer so treffen, dass Markierungen von mir auf Fotos, die Freunde eingestellt haben, nicht bei mir im Profil zu sehen sind. Markierungen habe ich unter Vorbehalt gestellt. Facebook informiert mich, dass ich markiert worden bin und dann entscheide ich, was bei mir zu sehen ist. Wer das nicht tut, riskiert, dass Fotos auf dem Profil landen und gesehen werden, bevor ich sie tatsächlich bemerke.

Wenn ich einmal bei Facebook mitgemacht habe, kann ich meine Spuren auch wieder komplett löschen?
Darüber wird heiß diskutiert. Ich persönlich kann nur sagen: Von Zeit zu Zeit lösche ich alte Beiträge oder Fotos von mir, die ich nicht mehr mag. Als ich vor kurzem die Facebook-Funktion genutzt habe, mit der ich all meine auf Facebook befindlichen Daten herunterladen kann,

waren meine zuvor gelöschten Daten nicht mehr dabei. Was Facebook mit meinen Daten gemacht hat oder noch macht, weiß ich natürlich nicht. Solange Facebook versichert, dass nichts Unerlaubtes damit geschieht und auch noch nichts Gegenteiliges bewiesen ist, glaube ich dem Unternehmen, so wie ich auch dem Postboten vertraue, dass er meine Post nicht aufmacht und liest.

Nervig sind Werbungen für Produkte, die an meine Freunde versandt werden, angeblich mit der Behauptung, mir gefiele das Produkt. Wie kann ich das verhindern?
Ganz einfach: Konto-Einstellungen, dann „Facebook-Werbeanzeigen" und dann „Niemand" einstellen.

Was tun, wenn es dennoch schon zu Datenmissbrauch gekommen ist?
Bevor man zum rechtlichen Hammer samt Anwalt ausholt, würde ich immer erst das Gespräch mit dem suchen, der meine Daten missbraucht. Landet ein Bild von mir auf einer Seite, auf der ich es nicht sehen möchte: Hinschreiben und zur Entfernung auffordern. Kommt der Missbrauch von Unternehmen und droht großer Schaden, sollte man einen Anwalt einschalten. Wer das Gefühl hat, dass systematisch Datenschutzrechte verletzt werden, sollte darüber auch den Datenschutzbeauftragten informieren.

Foto-Markierung

Eigentlich als lustiges Gadget gemeint, aber mit besonders heiklen Nebenwirkungen: Bei der sogenannten Foto-Markierung können Freunde Fotos von euch nicht nur auf ihre oder deine Pinnwand stellen, sondern dies auch namentlich kenntlich machen. Doch so manch eine markierte Person wird das sicherlich gar nicht lustig finden. Verständlich. Wer will schon auf einer Sauftour am Badestrand mit üblem Sonnenbrand auf einem Bild für alle befreundeten Nutzer verewigt werden? Auch das eine oder andere Kinderfoto hat auf meiner Pinnwand nicht wirklich etwas zu suchen. Im schlimmsten Fall ist das peinliche Bild schon einige Stunden im Netz und der einzelne hat es noch gar nicht bemerkt.

Ihr solltet euch ohnehin immer genau überlegen, welche Bilder und Videos ihr auf Facebook stellt. Denn es sind bei weitem nicht nur „Freunde", die ganz ohne Hintergedanken auf eurem Profil und eurer Pinnwand

herumstöbern. Auch Personalchefs, Lehrer, vor allem aber auch kommerzielle Firmen schauen sich ganz genau eure Postings an. Und anders als vielleicht ihr selbst – das Netz vergisst nie. Über Bilder, die einmal ins Netz gestellt sind, habt ihr anschließend keine Kontrolle mehr.

TIPPS: Ihr solltet eure Privatsphäre auf eurem Facebook-Konto so einstellen, dass mit eurem Namen versehene Bilder zunächst auf eurem Profil sichtbar sind und ihr es selbst freigeben könnt. Markiert dich jemand das nächste Mal auf einem Foto, erhältst du zunächst die Info „Benötigt Überprüfung". Erst wenn du dein Okay gegeben hast, ist es auch für andere sichtbar. Falls du ablehnst, ist das Bild zwar weiterhin bei Facebook zu sehen, allerdings ohne die Markierung mit deinem Namen und zumindest nicht in deinem Profil.

Stellt ihr Fotos ins Internet, auf dem auch andere Personen erkennbar abgelichtet sind, solltet ihr vorher fragen, ob das in Ordnung ist.

„Gefällt mir"-Button

Für den Nutzer ein einfacher Klick, für den Facebook-Konzern aber eine Schlüsselfunktion: Werbeunternehmen und Website-Betreiber können diese kleine Schaltfläche mit dem gehobenen Daumen in ihre Online-Präsenz einbinden. Klickt ein Nutzer darauf, wird das sofort im Facebook-Profil des Nutzers im Bereich „Aktivitäten und Interessen" vermeldet. Doch das ist noch nicht alles. Was der Nutzer nicht sehen kann: Facebook gibt das Klickverhalten an die Unternehmen weiter, damit sie die Werbung genau auf euer Alter, eure Hobbys und eure Interessen zuschneiden können. Für Facebook ist das ein lukratives Geschäft, für Datenschützer ein Graus. Denn hinzu kommt, dass für euch als Nutzer kaum zu erkennen ist, was Facebook genau über euch speichert.

TIPP: Wer nicht gezielt von der Werbewirtschaft ausgespäht werden möchte, sollte es vor allem bei Produkten vermeiden, den Gefällt-mir-Button anzuklicken.

Cyber-Mobbing

Was euch in der Schule oder im Sportverein zuweilen an Schikanen oder Hänseleien begegnet, kann im Netz zum

unkontrollierten dauerhaften Mobbing ausarten. Rund 30 Prozent der Jugendlichen zwischen 12 und 19 Jahren sehen im Cyber-Mobbing eine der größten Gefahren im Internet. Fast jeder siebte Jugendliche gibt an, dass über ihn schon mal Lügen im Netz verbreitet wurden. Anders als im realen Leben, wo Lehrer, Trainer oder Mitschüler einschreiten oder zur Hilfe eilen können, seid ihr im Netz zuweilen uneingeschränkten Aggressionen manchmal sogar Unbekannter ausgesetzt. Es kann eine Dynamik entstehen, der kaum jemand Grenzen setzt. Stattdessen werdet ihr beschimpft, beleidigt oder gar sexuell belästigt. Bis hin zu Morddrohungen werden ungehindert Drohungen im Netz ausgesprochen.

TIPPS: Auch wenn es euch zuweilen schwer fällt, euch als Opfer von Cyber-Mobbing zu offenbaren – berichtet unverzüglich euren Eltern, Lehrern oder anderen Erziehungsberechtigen von den Vorfällen im Netz. Fragt euch: Sind die Täterinnen und Täter bekannt und kann man sie auffordern, das Mobbing einzustellen? Kann man die Betreiber der Plattform ausfindig machen, damit sie die beleidigenden Inhalte löschen? Wenn das nicht hilft, sucht gegebenenfalls Beratungsstellen oder Jugendämter auf, wenn nichts anderes hilft, auch die Polizei.

Der Mensch ist keine Maschine

Bedenkt eins: So nett und vielseitig ihr mit euren Freunden chattet, skypt oder euch sonst wie austauschen könnt – letztendlich kommuniziert ihr über eine Maschine. Online-Freunde ersetzen nicht reale Freunde. Weder interagiert ihr online von Face to Face, noch habt ihr gemeinsame Erlebnisse, die euch zusammenschweißen. Vor allem aber bewegt ihr euch vor dem Rechner zu wenig. Achtet darauf, dass ihr euch nicht zu einseitig in virtuellen Räumen verliert.

TIPPS: Ihr solltet klare Vereinbarungen mit euren Eltern treffen, wie lange, wo und mit wem ihr chattet oder auf Facebook netzwerkt. Vergesst vor allem eins nicht: Online-Freunde können reale Freunde nicht ersetzen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt Folgendes:

Daten. Haltet euch zurück bei der Angabe persönlicher Informationen.

Bedingungen. Erkundigt euch über die allgemeinen Geschäftsbedingungen des Netzwerks und die Bestimmungen zum Datenschutz.

Freunde. Seid wählerisch bei Kontaktanfragen – Kriminelle „sammeln" Freunde, um Personen zu schaden.

Passwort. Verwendet für jede Internetanwendung ein unterschiedliches und sicheres Passwort.

Arbeitgeber. Gebt keine vertraulichen Informationen über euren Arbeitgeber und eure Arbeit preis.

Links. Klickt nicht wahllos auf Links – soziale Netzwerke werden verstärkt für Phishing genutzt.

Rechte. Prüft kritisch, welche Rechte ihr den Betreibern an den von euch eingestellten Bildern, Texten und Informationen einräumt.

Misstrauen. Bei zweifelhaften Anfragen solltet ihr euch außerhalb sozialer Netzwerke nach der Vertrauenswürdigkeit erkundigen.

Aufklärung. Sprecht mit euren Eltern und Lehrern über Gefahren, die bei der Nutzung sozialer Netzwerke bestehen. Lasst euch bei der Profileinstellung helfen.

III. Shoppen im Web

Vorbei die Zeiten, in denen man für eine hippe Jeans oder ein besonders trendiges Oberteil auf den nächsten Großstadtbesuch warten musste. Übers Internet lässt sich inzwischen so ziemlich alles ausfindig machen, was die große, bunte Warenwelt zu bieten hat. Und bequem ist das ganze auch. Ein bisschen stöbern, ein paar Klicks und schon ist die Bestellung draußen. Zwei, drei Tage später halte ich das gute Stück in den Händen. Passt es nicht oder gefällt es mir doch nicht so gut wie ich dachte, kann ich es mit dem beigelegten Rücksendeformular kommentarlos wieder zurückschicken.

Entsprechend viel wird inzwischen im Internet gekauft. Mehr als jeder zweite Bundesbürger zwischen 16 und 74 Jahren kauft regelmäßig übers Internet ein. Tendenz weiter steigend. Doch so bequem das ganze Prozedere inzwischen geworden – auch hier gibt es Einiges zu beachten. Generell gilt:

Mindestalter. Nach deutschem Recht ist man erst ab 18 voll geschäftsfähig. Ab sieben Jahre könnt ihr zwar Kaufverträge abschließen – allerdings nur mit Erlaubnis eurer Eltern oder wenn ihr mit frei dafür verwendbarem

Taschengeld bezahlt. Haben euch eure Eltern den Kauf vorher nicht erlaubt oder innerhalb von zwei Wochen nachträglich genehmigt, dann ist es, als wäre nie etwas geschehen. Ihr müsst die Ware des Versandhandels zurückschicken. Gesetzlich ist geregelt, dass die Rücksendekosten dann der Händler übernimmt, wenn die bestellte Ware über 40 Euro wert und bereits Geld geflossen ist. Die meisten Shops sind kulant und übernehmen auch bei geringeren Werten die Versandkosten.

In der Praxis kann ein Online-Shop nicht erkennen, wer da gerade wirklich als Käufer im Netz unterwegs ist und wie alt die Person ist. Es gibt zwar seit Jahren Pläne, ein funktionierendes System zur Identifizierung und Altersprüfung im Netz zu etablieren, das ist aber bislang nicht geschehen.

Rechnung. Die Zahlung erfolgt meist gegen Vorkasse per Überweisung, Lastschrift oder Kreditkarte. Bezahlung per Nachnahme ist hingegen meistens teuer.

Widerruf. Wenn ihr als Privatpersonen bei einem Händler online kauft, habt ihr generell ein 14-tägiges Widerrufsrecht ab dem Zeitpunkt, an dem ihr die Ware erhalten habt. Ohne Angabe von Gründen könnt ihr sie innerhalb dieses Zeitraums zurückgeben. Ausgeschlossen vom Widerrufsrecht sind verderbliche Lebensmittel, entsiegelte CDs und DVDs oder etwa Kleidungsstücke, die auf Sonderwunsch gefertigt wurden. Für den Widerruf genügt eine E-Mail oder ein formloses Schreiben per Post. Damit ihr einen Beweis habt, ist ein Fax oder ein Einschreiben zu empfehlen. Belege solltet ihr immer aufbewahren.

Rücksendekosten. Generell hat der Händler die Versandkosten zu tragen. Sperrige Ware muss der Händler abholen lassen. Lässt sich die Ware als Paket befördern, müsst ihr als Kunde sie zurückschicken. Bei Ware bis zu einem Preis von 40 Euro können Händler die Erstattung der Rücksendekosten zwar generell ausschließen. Doch inzwischen hat sich beim Online-Versand eingebürgert, dass die Kosten auch darunter getragen werden. Meistens werden für eine eventuelle Rücksendung spezielle Paketmarken und Formulare bereits mitgeschickt. Verkaufen allerdings Händler die Ware auf Rechnung, ist ihnen gestattet die Regeln so auszugestalten, dass sie die Rücksendekosten im Widerrufsfall nicht erstatten. Das ist aber nur noch selten der Fall.

Checkliste Onlineshoppen

Allgemeine Geschäftsbedingungen. AGB sind nur dann gültig, wenn sie wirksam in den Vertrag einbezogen wurden. Dazu müssen sie mühelos lesbar, übersichtlich, leicht abrufbar und speicherbar sein. Auch wenn sie lang und umständlich formuliert sind, lest das Kleingedruckte vor Vertragsschluss. Oft stecken in den AGB auch Infos zu den Versandkosten oder zur Frage, ob ihr die Rücksendekosten nach einem Widerruf des Kaufs tragen müsst.

Sicheres Bezahlen. Seid ihr im Besitz eines eigenen Kontos, solltet ihr darauf achten, dass die Kontodaten nicht in falsche Hände gelangen. Das Passwort solltet ihr immer getrennt von den restlichen Zugangsdaten aufbewahren. Zahlt im Zweifel auf Rechnung, wenn das möglich ist.

Persönliche Daten. Gebt nur die Informationen an, die für die Abwicklung des Vertrages notwendig sind. Das sind regelmäßig Name, Anschrift, Alter (um die Geschäftsfähigkeit zu überprüfen) und gegebenenfalls Kontodaten.

Werbung. Achtet darauf, dass ihr eure Daten nicht für Werbezwecke freigebt, sofern ihr keine Werbung erhalten möchtest. Auch wenn das nicht mehr erlaubt ist, müsst ihr oft ein bereits gesetztes Häkchen entfernen.

Kasse. Bitte unbedingt noch mal im Kassenbereich kontrollieren, was ihr bestellt habt. Manchmal gibt es Zusatzversicherungen oder ähnliches, die ihr vielleicht gar nicht haben wollt. Oder ihr habt aus Versehen in den Warenkorb zwei Stücke hineingelegt, obwohl ihr nur eines haben wolltet.

Opt-Out

Für Newsletter und Werbung ist das von selbst gesetzte Häkchen bereits seit einigen Jahren verboten. Beim Einkaufen geht die Rechtsprechung allerdings noch nicht so weit. Opt-Out bezeichnet sinngemäß sich gegen etwas zu entscheiden. Beim Online-Shopping ist es in der Bestellmaske meistens ein bereits mit einem Häkchen angewähltes Produkt. Wenn ihr es nicht möchtet, müsst ihr es explizit bei der Bestellung abwählen. Das Problem

dabei: Häufig wird der Haken schlicht übersehen. Das heißt: Das Produkt wird euch zunächst einmal mitgeschickt, auch wenn ihr das gar nicht wolltet. In der Rechnung taucht die Ware dann natürlich auf.

Beim regulären Verkauf wird euch dieses tückische Häkchen in der Regel nicht untergejubelt. Etwas anders sieht es bei Flugportalen aus. Bei „Opodo.de" etwa ist der „Reiserücktritt-Vollschutz" für 11,68 Euro in der Buchungsmaske bereits angewählt. Als Kunde müsst ihr das Häkchen also extra wegklicken. „Fluege.de", ein anderes Reiseportal, hat bis vor kurzem auf diese Weise eine Versicherung gleich für ein ganzes Jahr anzudrehen versucht. Verbraucherschützer haben gegen diese Praxis bereits geklagt. Mit Erfolg. Das Häkchen ist nicht mehr zu sehen.

TIPPS: Achtet beim Online-Kauf immer darauf, ob euch nicht noch zusätzlich etwas angedreht wird, was dann auch noch angeklickt ist. Falls es doch passiert: Sofort anprangern und das Produkt wieder zurückschicken. Auch hier gilt das 14-tägige Widerrufsrecht.

eBay

Online-Auktionshäuser erfreuen sich seit Jahren großer Beliebtheit. Aber keines ist so populär wie eBay. Daran hat sich auch in den vergangenen Jahren kaum etwas geändert, obwohl es immer wieder neue Anbieter gibt, die versuchen, das Geschäftsmodell von eBay nachzumachen. Das US-amerikanische Portal hat im Schnitt ständig mehr als 30 Millionen Artikel im Angebot. Und das machen die Konkurrenten eBay nicht so schnell streitig. Dennoch aufgepasst: Polizei und Verbraucherschützer warnen, dass auch in etablierten Auktionshäusern ständig Gefahren lauern. Wir haben an dieser Stelle die wichtigsten Hinweise zusammengestellt, damit ein Schnäppchen nicht zum Reinfall wird.

Schnäppchen. Viele denken, dass Artikel in Online-Auktionen per se günstig sind. Das sind sie aber häufig gar nicht. Als Bieter solltet ihr daher immer vorher die Preise vergleichen. Schaut euch zunächst laufende Auktionen für ähnliche Produkte an, damit ihr einen Überblick über die Preise erhaltet. Zudem ist es ratsam, vor der Auktion festzulegen, wie viel ihr höchstens bieten wollt oder könnt, um nicht in eine Art Rausch zu verfallen.

Und auch über die anfallenden Versand- und Nebenkosten solltet ihr euch genau informieren.

Enttäuscht über die Ware. Bevor ihr loslegt mit dem Ersteigern, solltet ihr euch immer ganz genau die Produktbeschreibung durchlesen. Die eBay-Regeln sind streng und demnach müssen die Verkäufer auch genau das liefern, was sie geschrieben haben. Je ungenauer die Beschreibung ist, desto misstrauischer solltet ihr sein. Sowohl bei Texten als auch bei Fotos solltet ihr immer beachten, dass der Verkäufer die Ware ja im besten Licht präsentieren will. Lasst euch also nicht allzu sehr blenden.

Verkäufer einschätzen. Schaut euch immer das Bewertungsprofil an. Außerdem solltet ihr grundsätzlich solche Verkäufer meiden, die nur spärliche Informationen über sich abgeben. Fehlt etwa eine Anschrift oder eine Kontaktnummer, ist Misstrauen angesagt.

Mangelhafte Ware. Bei kaputter Ware könnt ihr von gewerblichen Händlern eine Reparatur oder eine Ersatzlieferung verlangen und das zwei Jahre lang. Private Verkäufer können diese Gewährleistung ausschließen, aber nur, wenn sie das vor der Versteigerung explizit erwähnt haben.

Sicher bezahlen. Verbraucherschützer verweisen darauf, dass ihr bei Internetauktionen immer ein gewisses Risiko eingeht, da ihr meistens in Vorkasse gehen müsst. eBay selbst empfiehlt das Bezahlsystem PayPal. Vorteil: Als Käufer könnt ihr euer Geld zurück erhalten, wenn die Ware nicht ankommt oder anders als vereinbart geliefert wird. Bei besonders teuren Artikeln solltet ihr aber einen Treuhandservice nutzen, der das Geld erst an den Verkäufer überweist, wenn die Ware einwandfrei bei euch angekommen ist.

Versandkosten. Meistens tragt ihr als Käufer die Versandkosten. Und da werden bei eBay zum Teil sehr unterschiedliche Preise verlangt. Deshalb solltet ihr vor dem Bieten immer darauf achten, was angegeben ist – damit ihr hinterher nicht böse überrascht werdet.

Der Online-Ticketkauf Viagogo

Klingt praktisch. Die Karten für das Konzert eurer Lieblingsband sind ausverkauft. Doch beim Online-Tickethandel Viagogo werden noch welche angeboten. Nichts wie kaufen.

Doch Viagogo hat seine Tücken. Denn auf der Plattform tummeln sich Zweithändler. Das heißt: Im Prinzip kann jeder, der bereits ein Ticket ergattert hat, es weiter verhökern. Allerdings haben längst einige ein lukratives Geschäftsmodell darin gefunden: Sie verkaufen die Tickets deutlich teurer. Geht trotz doppelt oder dreifach gezahltem Preis beim Verkauf mit diesen Privathändlern dennoch etwas schief, kann Viagogo noch nicht einmal belangt werden.

Wer aber dann? Das beantwortet Viagogo allerdings nicht. Und eine Garantie, dass der Verkäufer das angebotene Ticket überhaupt besitzt, übernimmt die Online-Firma nicht. Es fängt bereits mit der Kontaktaufnahme an: Auf der Webseite gibt Viagogo weder eine E-Mail-Adresse an, noch eine Telefonnummer. Das ist eigentlich nicht erlaubt.

Die Details liest man dann im Kleingedruckten. Dort steht geschrieben: „Wir können nicht gewährleisten, dass ein Käufer oder Verkäufer ein Geschäft wirklich vollständig durchführt." Die gibt es auch beim Internetauktionshaus eBay nicht. Anders aber als bei eBay erfahrt ihr als Käufer über Viagogo nicht, von wem ihr die Karten gekauft habt. Auch eine Garantie gibt es nicht.

Nach Ansicht eines Düsseldorfer Fachanwalts für IT-Recht kommt Viagogo mit dieser Geschäftspraxis auf Dauer nicht durch. Es gebe vergleichsweise klare Regelungen im Telemediengesetz und da könne ein Unternehmen sich nicht einfach herausreden, dass es eine Plattform zur Verfügung stellt, ohne aber die Verantwortlichen zu benennen, heißt es.

Was hinzu kommt: Viagogo begünstigt den gewerblichen Weiterverkauf von Tickets. Verkäufer lassen sich nicht eindeutig identifizieren. Und das ist verboten. Daher: Lasst lieber die Finger von solchen Online-Portalen.

Musikpiraterie

Die neuesten Hits aus den Charts auf den iPod hochladen, einen Hollywood-Blockbuster auf den Rechner „saugen" oder auch abgefahrenere Songs von irgendwelchen Garagenbands mit der besten Freundin autauschen – längst alles kein Problem mehr. Noch nie war es so einfach, so zügig an Musik zu kommen. Ein paar Mausklicks genügen.

Natürlich lässt sich in diesem Zusammenhang das Thema „Download-Piraterie" Zusammenhang nicht ausblenden. Denn so sehr sich iTunes und andere kommerzielle Musikdienste sich längst etabliert haben, bleibt das illegale Herunterladen von Liedern über Tauschbörsen eine weit verbreitete Möglichkeit, eure Musiksammlung gratis aufzustocken.

Dabei ist das Risiko aufzufliegen erheblich gewachsen. Denn sowohl die Musik- als auch die Filmindustrie sind nicht untätig geblieben und haben technisch und juristisch enorm aufgerüstet. Im Jahr 2004 wurden erstmals Privatpersonen rechtlich verfolgt, die mit Uploads gegen das Urheberrecht verstoßen hatten. Seitdem stieg die Zahl der Verfahren auf über 100 000. Die Zahl der illegalen Downloads ist seitdem von über 600 Millionen auf etwa 316 Millionen im Jahr 2008 zurückgegangen. Der Bundesverband der Musikindustrie gibt für 2009 die Zahl der Zivilverfahren mit 13 000 an.

Und doch: Es gibt immer noch viele Leute, sowohl Jugendliche als auch ihre Eltern, die sich nicht darüber im Klaren sind, wie hoch das Risiko mit illegalen Downloads inzwischen ist. Das böse Erwachen kommt meistens erst, wenn eine Abmahnung mit Schadenersatzforderung der Musikindustrie im Briefkasten landet. Und das kann teuer werden. Je nach Schaden kann die Strafe bei einigen Hundert Euro, bei vielen Downloads sogar mehrere Tausend Euro betragen. Wer eine solche Abmahnung erhält, sollte aber nicht sofort unterschreiben, sondern zunächst einen Anwalt aufsuchen.

Generell gilt: Alles, was ihr im Netz an Fotos, Liedern, Texten oder Videos findet – egal ob verschlüsselt oder offen – unterliegt dem Urheberrecht und gehört euch daher nicht. Das Urheberrecht schützt die Urheber, also die Schöpfer von kreativen Werken wie zum Beispiel Texte, Fotos und Filme. Allein der Urheber entscheidet, ob, wann und wer sein Werk nutzen und verbreiten darf. Grundsätzlich muss der Urheber also um Erlaubnis gebeten werden.

Deswegen: Veröffentlicht nichts davon auf euren Pinnwänden oder ohne Genehmigung auf euren Webseiten. Denn das Urheberrecht unterscheidet nicht, ob ein Bild, Video oder Lied privat oder professionell gemacht wurde und ob es für einen privaten oder kommerziellen Zweck verwendet wird. Sobald ihr auch nur ein Bild auf eurer Pinnwand postet, das nicht von euch selbst stammt und von dem die Zustimmung des Urhebers fehlt, stellt dies einen Rechtsverstoß dar. Denn dieses Foto wird Dritten zugänglich gemacht, ohne dass man die Rechte an dem Bild besitzt.

Besonders heftig wird der Streit zwischen der Musikindustrie und den Portalbetreibern selbst ausgetragen. Die Verwertungsgesellschaft Gema, die deutschlandweit von mehr als 60 000 Musikern, Labels und Verlegern die Urheberrechte wahrt, lässt auf YouTube oder anderen Videoplattformen per einstweiliger Verfügung immer wieder Musikstücke verbieten, wenn sich Youtube weigert, eine Gebühr pro Abruf zu bezahlen. Weigert sich der Betreiber, wird er meistens verklagt. Doch theoretisch kann die Gema auch denjenigen belangen, der das Video hineingestellt hat.

Was jeder Musikliebhaber im Netz wissen sollte:

Verbot. Grundsätzlich solltet ihr davon ausgehen, dass der Download von Musik in Tauschbörsen verboten ist. Denn die meisten Werke sind urheberrechtlich geschützt. Mit solchen Börsen findet ja immer auch eine Verbreitung des heruntergeladenen Werkes statt.

Legales Herunterladen. Downloads sind dann erlaubt, wenn die Quelle, von der ihr etwas herunterladet, dies ausdrücklich gestattet. Es gibt Bands und Labels, die ihre Musik bewusst kostenlos zur Verbreitung anbieten. Das ist legal. Wenn ihr jedoch auf Seiten stoßen solltet, auf denen etwa die Top-100-Charts zum Download angeboten werden, sollte euch das stutzig machen. Dann ist davon auszugehen, dass ihr euch auf illegalem Terrain im Netz bewegt.

Legales Kopieren. Das deutsche Urheberrecht sieht vor, dass unter bestimmten Voraussetzungen einzelne Kopien von einem Werk, etwa einer CD, angefertigt werden dürfen – aber nur, wenn dies ausschließlich zum privaten Gebrauch erfolgt und ein Kopierschutz auch nicht umgangen wird. Das heißt: Zur musikalischen Untermalung für das Familienurlaubsvideo darf auch urheberrechtlich geschützte Musik verwendet und das Video dann entsprechend im Familien- oder Freundeskreis gezeigt werden.

Strafe. Wer Videos oder Musik über eine Tauschbörse herunterlädt, kann abgemahnt werden. Aber auch die Nutzer können abgemahnt werden. Und das kann kosten. Zwischen 400 und 6 000 Euro Strafe droht

einem Downloader – je nachdem, wieviele Lieder er heruntergeladen hat.

Haftung. In der Regel trifft es die Anschlussinhaber, also eure Eltern, selbst wenn sie nicht wissen, was ihr im Netz heruntergeladen habt. Und da das sehr teuer ist, dürfte Ärger vorprogrammiert sein. Damit der Familiensegen nicht schief hängt, solltet ihr euch an die Abmachungen mit euren Eltern halten. Sie müssen letztendlich für euch haften.

Bezahlter Download. Was bleibt, ist der reguläre Download von Musik- und Filmdateien gegen Bezahlung. Hier gilt zu beachten: Anders als beim Online-Kauf von Kleidungsstücken oder Gegenständen gibt es beim Herunterladen von Dateien bislang keine Widerrufs- und Rückgabemöglichkeit. Das heißt: ihr solltet euch genau überlegen, ob ihr die angebotene Musik, die Software oder den Film wirklich kaufen möchtet. Seid ihr unzufrieden, bleibt ihr auf eurem Download sitzen.

IV. Smart telefonieren

Telefonieren ist für viele nur noch ein Randaspekt. Moderne Smartphones können sehr viel mehr. Dabei handelt es sich genau genommen um Minirechner, die von überall aus den Zugang ins Internet ermöglichen und mit zahlreichen Multimedia-Funktionen ausgerüstet sind. Zur Grundausstattung der meisten Smartphones gehören eine Kamera, ein Mediaplayer, ausreichend viel Speicher für Musik, Videos, Fotos, Terminplaner und umfangreiche Adressen-Datenbanken. Und neben dem Telefonieren kommen auch der Zugang ins Internet inklusiver E-Mail-Funktion, Online-Navigationsdienste und Social Media hinzu. Was die Software angeht, da ist das Angebot fast unendlich. Das gilt allerdings auch für die Gefahren.

Roaming

Mit Smartphones und anderen internetfähigen Handys könnt ihr selbst fern der Heimat von fast jedem Ort der Welt eure E-Mails abrufen, twittern, euren Facebook-Status aktualisieren oder die Spiele eurer Lieblingsfußballmanschaft im Livestream mitverfolgen. Doch so sehr das innerhalb Deutschlands kein Problem darstellt, weil die meisten über eine Flatrate verfügen – sobald die Landesgrenzen überquert sind, wird es rasch teuer. Roaming

nennt sich das Telefonieren und Surfen im Ausland. Der Begriff kommt aus dem Englischen und bedeutet so viel wie „streunen“. Schaltet ihr im Ausland euer Handy ein, macht sich euer Gerät auf die Suche nach einem verfügbaren Netz und verbindet euch, es streunert sozusagen durch ausländische Netze. Vor allem in Ländern, die nicht zur EU gehören, kann der Datentransfer auf eure Handys unbemerkt sehr schnell sehr teuer werden. Während das Abrufen einer Text-Mail nur sehr wenig Datentransfer verursacht, kann der Versand von Urlaubsfotos per Mail zu horrenden Rechnungen führen. Denn ein Bild hat schnell eine Dateigröße von einem Megabyte und mehr.

Zudem haben viele Leute nicht im Blick, dass sich die meisten Smartphones automatisch im Hintergrund ins Netz einwählen und Daten übertragen, ohne dass ihr bewusst eure Geräte eingeschaltet habt. Tückisch sind Betriebssysteme und installierte Apps, die sich regelmäßig selbst auf den aktuellen Stand bringen. Das sorgt ebenfalls schnell und vor allem unbemerkt für erheblichen Datenverkehr. Selbst das Anzeigen der aktuellen Position auf dem Stadtplan im Smartphone oder das Abrufen von Video- oder Musikstreams schlägt dort zu Buche.

Gebühren innerhalb der EU. Seit 2010 gilt innerhalb der Europäischen Union eine monatliche Obergrenze von 59,50 Euro. Das heißt: Ihr als Mobilfunkkunden seid automatisch vor allzu hohen Rechnungen fürs Internet-Surfen per Handy geschützt. Erreicht ihr mit eurem Handy diese Grenze, kappt euer Anbieter die Datenverbindung. Zuvor, nämlich bei einer Grenze von 47,60 Euro, werdet ihr bereits per SMS, E-Mail oder über ein Pop-Up-Fenster gewarnt, dass ihr das Limit bald erreicht haben werdet. EU-weit gelten beim Roaming mittlerweile einheitliche Höchstpreise: 41 Cent pro Minute für abgehende Anrufe und 13 Cent für eingehende. SMS dürfen nicht mehr als 13 Cent kosten, auch wenn ihr in Deutschland mehr bezahlen müsst. Für das Internetsurfen per Handy gibt es allerdings noch keine EU-weiten Höchstpreise. Die Preise für ein Datenpaket von einem Megabyte Größe variieren zwischen 49 Cent und 19,80 Euro.

Gebühren außerhalb der EU. Befindet ihr euch außerhalb der EU-Grenzen, gibt es diese Einschränkung nicht. Das heißt, ihr müsst selbst darauf achten, wie viele Internetkosten anfallen. Und das kann teuer werden. Surfen außerhalb der EU, etwa in den USA, der Schweiz oder der Türkei, kostet euch zwischen 2,49 und 25,80 Euro pro Megabyte. Wer aus solchen Ländern gleich reihenweise Urlaubsfotos per Handy verschickt, seine Updatefunktion und die Ortungsfunktion nicht ausschaltet, kann sich zügig eine Rechnung von mehreren hundert Euro einhandeln.

TIPPS: Ihr solltet die automatischen Datenverbindungen und Updatefunktionen eurer Smartphones während des Urlaubs im Ausland unbedingt abschalten. Wenn ihr nur regelmäßig eure E-Mails abrufen oder einfache Seiten aufrufen wollt, kann das WLan im Hotel wesentlich günstiger sein. Erkundigt euch vor Reiseantritt bei euren Mobilfunkanbietern nach den Preisen im Ausland. Einige bieten günstige Auslandstarife an.

Kostenkontrolle

Warum kostspielige Verträge mit langen Laufzeiten abschließen, wenn man mit Prepaid-Verträgen rechnerisch viel günstiger wegkommt? Hinzu kommt, dass ihr mit einem Prepaid-Tarif, bei dem ihr vorab das Geld auf ein Konto überweist und so lange telefonieren könnt, bis das Konto leer ist, die Handygebühren viel besser im

Griff habt – sollte man meinen. Doch das ist leider nicht immer so.

Was viele bei Abschluss eines Prepaid-Vertrags nicht bedenken: Es gibt unterschiedliche Arten von Prepaid-Verträgen. So wie bei einem Girokonto kann bei manchen Anbietern auch ein Prepaid-Konto ins Minus rutschen. Zwar mit Untergrenze, aber einige Hundert Euro können auch da zusammen kommen. Besonders tückisch: Wenn sich euer Smartphone ohne Flatrate unbemerkt ins Internet einwählt und nicht etwa wie vermutet ins heimische WLan-Netz.

Guthaben weg bedeutet eigentlich ja auch keine Gespräche mehr, keine SMS und auch kein Internet. Das war mal so. Längst steht im Kleingedruckten so mancher Anbieter, dass auch bei Prepaid-Verträgen Schulden angehäuft werden können. Von „Negativsaldo“ ist dann die Rede. Wer einen solchen Begriff findet, sollte alarmiert sein. Denn ihr als Kunde müsst die Schulden in diesem Fall sofort bezahlen. Sonst fallen auch noch Zinsen an.

Besonders gefährlich: Wenn eine alte SIM-Karte solcher Anbieter in einem neuen Smartphone landet. Denn häufig sind die alten Tarife nicht für Daten ausgelegt, wie euer neues Gerät in Anspruch nimmt. Das kann dann sehr teuer werden. Hinzu kommt, dass die Internetverbindungen oft nicht über das aufgeladene Guthaben abgerechnet werden, sondern zusätzlich anfallen. Bei 8 Megabyte Datenverkehr kommen schnell mal 180 Euro oder mehr zusammen.

TIPPS: Achtet beim Abschluss eines Prepaid-Vertrags unbedingt auf das Kleingedruckte. Taucht der Begriff „Negativsaldo“ auf, solltet ihr auf ein anderes Angebot ausweichen.

Volle Kostenkontrolle

Eure Eltern sind grundsätzlich bereit, eurem Betteln nachzugeben und euch ein eigenes Handy zu erlauben. Zugleich befürchten sie, dass ihr ein Vermögen vertelefonieren könntet? Die Mobilfunkanbieter haben auf dieses Dilemma reagiert. Sie bieten grundsätzlich zwei Möglichkeiten an.

Partnerkarten. Eure Eltern können zu ihrem Vertragshandy für euch zusätzliche SIM-Karten besorgen. Mit der Combicard Teens von T-Mobile etwa oder mit der CallYa Juniorkarte von Vodafone werden kostenpflichtige Service- und Sondernummern gesperrt. Auch Kostentreiber wie Anrufe ins Ausland, aus dem Ausland (Roaming) und mobiles Internet sind nicht möglich. Der Vorteil: Eure Eltern oder ihr zahlt einen monatlich festgelegten Betrag – bei T-Mobile mindestens 5 Euro und bei Vodafone 10 Euro. Ist das Guthaben aufgebraucht, können eure Eltern euch immer noch erreichen. Anrufe zu den Eltern sind bei Vodafone immer kostenlos, bei T-Mobile immerhin noch innerhalb der ersten 30 Sekunden. Telefonate mit anderen sind nicht möglich. Läuft der Hauptvertrag der Eltern aus oder werdet ihr 18 Jahre alt, geht die Karte bei T-Mobile automatisch in einen Zweijahresvertrag mit monatlicher Grundgebühr über. Außerdem sind die Minutenpreise mit 29 Cent bei T-Mobile und 30 bis 50 Cent bei Vodafone vergleichsweise teuer. Die Tarife für unterschiedliche Telefoniertypen findet ihr laufend aktualisiert auf test.de (kostenpflichtig).

Guthabenkarten. Deutlich preiswerter sind Prepaidkarten. Eure Eltern laden einen frei wählbaren Betrag auf. Ist er aufgebraucht, könnt ihr nicht mehr telefonieren, seid aber noch erreichbar. Auch Notrufe sind noch möglich. Der Vorteil: Die Gesprächskosten sind deutlich niedriger. Viele Betreiber bieten Community-Tarife für preiswerte Anrufe untereinander an. Bei Aldi Talk, Callmobile, Ja! Mobil und Penny Mobil telefoniert ihr für 3 Cent pro Minute, wenn ihr im gleichen Netz miteinander sprecht. Bei Simply friends 4free könnt ihr sogar kostenlos untereinander telefonieren. Allerdings lassen sich Sonderrufnummern, Auslandsrufnummern und Klingelton-Abos meist nicht sperren.

App-Store

Nur drei oder vier Klicks auf dem berührungsempfindlichen Bildschirm – und schon ist ein komplettes Programm auf das Smartphone geladen. Und das Angebot ist gigantisch: Allein der App Store von iPhone-Hersteller Apple bietet eigenen Angaben zufolge mehr als 100 000 Apps an. Doch so toll das Angebot sein mag – was den Umgang dieser Shops mit Nutzerdaten anbelangt, gibt es noch einigen Verbesserungsbedarf.

Besonders beim App-Store von Apple finden sich beim Kauf dieser Miniprogramme immer wieder unzulässige Klauseln und schwammig formulierte Datenschutzerklärungen. Aber auch die anderen App Stores etwa der Android-Market von Google bieten häufig kein ordnungsgemäßes Impressum. Was besonders ärgerlich ist: Habt ihr als Kunde beim Herunterladen der Apps Probleme, gibt es keine Möglichkeit, auf einfachem Weg in Kontakt mit dem Anbieter zu treten. Das nervt, zumal das Konto für den Kauf womöglich dennoch belastet wird.

Datenschützer warnen davor, dass App-Stores oder auch die App-Entwickler bei zahlreichen dieser Apps unzu-

lässig auf einige eurer Daten zugreifen können, etwa auf euren gespeicherten Adressen eurer Smartphones. Die App-Stores von Windows Phone Marketplace, Android Market und AndroidPIT bemühen sich immerhin um etwas Transparenz und informieren Kunden darüber, auf welche Telefonfunktionen und damit auch welche eurer Daten zugegriffen wird. Die anderen Stores, darunter auch der von Apple, lassen euch darüber im Unklaren.

TIPPS: Bevor ihr eine App herunterladet, solltet ihr euch genau informieren, um was es sich dabei genau handelt. Was steht im Kleingedruckten und in den allgemeinen Geschäftsbedingungen? Werden Ortungsdaten gespeichert? Auf welche sonstigen Daten greift die App zu? Eine Vielzahl von Apps ist kostenlos – was aber nicht heißt, dass sie auch wirklich gratis sind. Für einige Zusatzdienste werden dann doch noch Kosten erhoben, oder ihr bezahlt mit euren Daten. Diese sind vielen Firmen sehr viel Geld wer. Prüft, wie die Zahlungsmodalitäten tatsächlich aussehen.

Lest euch die Bewertungen durch, die bei den meisten Miniprogrammen vor dem Herunterladen einsehbar sind.

Sie bieten oft einen guten Überblick über die Stärken und Schwächen dieser Miniprogramme.

Lokalisierungsdienste

Ihr seid in einer euch fremden Stadt auf der Suche nach dem nächsten Café? Kein Problem. Ein paar Berührungen auf dem Smartphone und die spezielle App zeigt einem prompt nicht nur die kürzeste Strecke zum Eisbecher des Tages, sondern was ihr auf dem Weg dorthin noch alles zu sehen bekommt. Das alles dank des Ortungsdienstes, dessen sich auch die Apps Google Map, Foursquare und selbst der Navi der Deutschen Bahn bedienen. Und nicht nur das: Über Kontaktvermittlungsapps erfahrt ihr auch, wer sich von euch bekannten Leuten noch alles in der unmittelbaren Umgebung befindet.

Aber: Unmengen an Daten fließen über diese sogenannten Lokalisierungsdienste an irgendwelche gigantischen Server und werden dort gespeichert. Euer momentaner Standort wird nicht nur an sie übermittelt, wenn ihr diese Dienstleistung bewusst mithilfe der entsprechenden Apps abruft. Oft gibt die Anwendung in regelmäßigen Abständen eure momentane Position automatisch durch.

Ob angemeldet oder nicht, das Unternehmen weiß, wo ihr steckt. Und damit nicht genug: Die App vom Verkehrsverbund Berlin-Brandenburg etwa greift auch auf euer Adressbuch zu, dies kann nur dann nützlich sein, wenn ihr direkt aus dem Adressbuch die mögliche Fahrtroute zu einem Freund erfragen wollt. Besonders dreist ist die Anwendung des Lokalisierungsdienstes Gowalla. Diese App leitet alle Namen und E-Mail-Adressen weiter, die ihr auf euren Smartphone gespeichert habt. Ihr selbst könnt aber nicht erkennen, was genau übertragen und erst recht nicht, was damit angestellt wird. So praktisch diese Lokalisierungsdienste auf euren Smartphones im Alltag sind – sie können auch zum ernsthaften Problem werden.

In Deutschland sind diese ungefragten Ortungsdienstleistungen rechtlich gar nicht gestattet. Das Telemediengesetz ist da sogar recht eindeutig: Euer Standort darf nur dann erhoben werden, wenn ihr das explizit erlaubt habt. Das Problem: Viele dieser Apps haben ihre Server im Ausland stehen, das heißt, die Daten werden dort verarbeitet und nicht hierzulande. In den Vereinigten Staaten etwa gibt es keinen so ausgeprägten Datenschutz wie in Europa. Dort kann jedes Unternehmen sich seine Datenschutzrichtlinien selbst geben, eine umfassende Aufsicht fehlt.

Amerikanische Unternehmen wie Amazon, Google, Microsoft oder Facebook haben sich selbst verpflichtet, mit den Daten nach europäischen Richtlinien umzugehen. Eine Kontrolle findet allerdings nicht statt. Man sollte vorsichtig sein. Viele kleinere Anbieter halten sich jedoch nicht daran – und kaum jemand kontrolliert dieses Geschäftsgebaren. Wo der Weg hingeht? Das ist im Moment noch offen. Eine einheitliche internationale Regelung wird es wahrscheinlich auch in naher Zukunft nicht geben.

TIPPS: Meidet Apps mit Ortungsdiensten und anderen Leistungen, die sich ohne eure Zustimmung Zugriff auf eure persönlichen Daten verschaffen. Nutzt diese wirklich nur, wenn ihr es als sinnvoll erachtet.

V. Sicher zocken

Abtauchen in eine womöglich selbst gestaltete Fantasiewelt, Städte bauen, Abenteuer erleben, Helden sein, Kontakte knüpfen – für viele von euch ist die Welt eines Online-Spiels regelmäßiger Bestandteil eures täglichen Alltags geworden. Besonders bei virtuellen Rollenspielen, in denen ihr euch einen eigenen Charakter aufbaut und euch damit durch eine Fantasiewelt bewegt, ist der Suchtfaktor groß. Hinzu kommt, dass sich in einigen dieser Spiele die Ereignisse weiter drehen, auch wenn ihr nicht dabei seid. Es wird euch vermittelt, ihr könntet etwas verpassen.

Studien belegen, dass jeder zehnte Jugendliche wegen dieser Spiele süchtig ist. Das kann solche Ausmaße annehmen, dass ihnen das reale Leben unwichtiger wird als die Spielewelt im Netz. Süchtige sind unausgeschlafen, in der Schule unkonzentriert, es kommt zu Verhaltensstörungen im wahren Leben, Gefühle gehen verloren, einige von ihnen vernachlässigen sogar das Essen und Trinken. In Südkorea gab es sogar schon Tote. Sie haben gespielt, bis sie dehydriert waren. Besonders suchtkranke Jugendliche gehen auch nicht mehr auf die Toilette. Spielsucht kann also alle möglichen Folgen haben.

Wenn es so weit gekommen ist, dann helfen nur noch Suchthilfen, die es in jeder größeren Stadt gibt. Aber auch wenn der Körper noch nicht unmittelbar leidet, kann es sein, dass Hilfe von außen nötig ist. Ziel einer Therapie ist es, Süchtige aus der virtuellen Welt zurück ins wirkliche Leben zu holen.

Damit es aber gar nicht so weit kommt, solltet ihr vor Beginn des Spielens klare zeitliche Grenzen ziehen und euch eventuell sogar den Wecker stellen. Nach Meinung von Experten kommt es auch auf die Art des Spiels an: Am besten sind Spiele, die von sich aus klare Begrenzungen haben. Sie sind einfach irgendwann zu Ende. Und zwar besser nicht erst nach drei oder vier Stunden.

Nützliche Links

www.surfer-haben-rechte.de Hier findet ihr ausführliche Informationen des Verbraucherzentrale Bundesverbandes (vzbz) allgemein über Verbraucherrechte im Internet.

www.bsi-fuer-buerger.de Das Bundesamt für Sicherheit in der Informationstechnik informiert euch hier über Schutzmaßnahmen im Netz. Diese Seite wird laufend auf den neusten Stand gebracht.

www.klicksafe.de Die Seite ist Bestandteil des Safer Internet Programms der Europäischen Union. Unter „Materialien" findet ihr interessante Broschüren, die sich vor allem an euch Jugendliche oder auch an eure Eltern richten.

www.yprt.eu Hier hat die Stiftung Digitale Chancen für euch ausführliche Informationen zum Jugendmedienschutz eingestellt.

www.ausgestiegen.com Auf dieser Seite findet ihr eine Anleitung zum Ausstieg aus sozialen Netzwerken und wie ihr es schafft, ohne Spuren von euch zu hinterlassen.

www.chatten-ohne-risiko.de Ein Wegweiser sowohl für Eltern als auch für Jugendliche, der auf die Gefahren der sozialen Netzwerke aufmerksam macht.

Und zum Schluss

Habt ihr noch Fragen? Oder etwas nicht verstanden? Mehr Infos gibt es unter www.test.de (zum Teil kostenpflichtig). Wir freuen uns auch über eure Anregungen.

Impressum
Herausgeberin: Stiftung Warentest
Redaktionelle Verantwortung: Heike van Laak
Redaktion, Konzept: Petra Rothbart
Text: Felix Lee
Gestaltung: Martina Römer, www.nahtief.de
Stand: Januar 2012


www.test.de