Es lohnt sich also, URLs genauer anzusehen, bevor man diese aufruft.

Qualität prüfen

Angenommen, Sie suchen im Internet nach Informationen über Martin Luther King und stoßen dabei auf die Seite *www.martinlutherking.org*. Der Domain-Name legt die Vermutung nahe, dass es sich um Informationen einer nichtkommerziellen Organisation handelt, und dies bestätigt auch die Betrachtung der Website. Zudem führen Google, Yahoo und LiveSearch diese Seite unter den ersten zehn Treffern, was ihr eine große Popularität bescheinigt. Doch der erste Blick trügt. Diese Website wird von einer Vereinigung weißer Rassisten betrieben, was sich erst ersehen lässt, wenn man die Seite ganz nach unten scrollt und liest: »Hosted by Stormfront«. Folgt man diesem Link, gelangt man zu einer Seite, die sich »White Nationalist Resource Page« nennt und für die Interessen der »weißen westlichen Kultur« kämpft. Auf dieser Seite »lernt« man, dass Martin Luther King zeit seines Lebens ein Plagiator gewesen sei, dass ihm seine akademischen Qualifikationen in betrügerischer Weise zuerkannt worden seien, dass er Kirchengelder für eigene Zwecke verwendet habe und so weiter. Dieses Beispiel zeigt, wie Informationsqualität vorgetäuscht werden kann und wie wichtig es ist, bei unbekannten Websites den Inhalt kritisch zu prüfen und sich immer das Impressum beziehungsweise den Betreiber der Seite genau anzusehen. Das Aufkommen des Web 2.0 erschwert es zusätzlich, eine zuverlässige Bewertung von Inhalten im Web vorzunehmen, da es sich um Inhalte handelt, die nicht vom Anbieter eines Webangebots, sondern von dessen Nutzern erstellt werden (User Generated Content). Das gilt auch für die Lexikonartikel von Wikipedia. Viele nutzen die Informationen sorglos, ohne sie zu überprüfen. Man sollte bei der Verwendung von Informationen aus Wikipedia stets darauf achten, dass Quellen angegeben sind und dass die benutzten Informationen durch andere Quellen belegt werden können. Da Wikipedia keine Wertung hinsichtlich der Standpunkte und Meinungen der Texte unternimmt und keine Maßnahmen gegen Extremismus ergreift, muss man besonders aufpassen, welcher Tenor zwischen den Zeilen kolportiert wird.

2 Abzocke und andere Fallen

Mit den verbesserten Kommunikationsmöglichkeiten im Internet wachsen auch die Gefahren und Risiken für Abzocke und andere Fallen im Netz. Mit vermeintlich kostenlosen Angeboten ziehen dubiose Firmen den Nutzern das Geld aus der Tasche. In jedem vierten Fall erwischt es Jugendliche unter 18 Jahren. Die Abzocker versenden ihre Rechnungen per E-Mail und üben Druck aus, wenn nicht bezahlt wird. Ihre durchschnittliche Forderung beträgt 120 Euro. Jeder Zehnte überweist den Betrag, insbesondere wenn die Abzocker Mahnungen und Androhungen von teuren Gerichtsverfahren senden, Inkassobüros beauftragen oder Schreiben von Rechtsanwälten versenden lassen. Um zu vermeiden, dass man auf Betrüger hereinfällt, sollte man wissen, wie die Abzocker im Internet arbeiten.

Die einen locken mit angeblichen Nachrichten vom Nachbarn oder Frei-SMS, andere ködern mit Hausaufgabendiensten, Softwareprogrammen, Intelligenztests oder Rezeptvorschlägen. Um die Kunden abzuzocken, stellen ihnen die Betrüger zunächst mit scheinbar billigen Angeboten Fallen. Wer möchte nicht kostenlos SMS verschicken, Klingeltöne herunterladen, wissen, wie alt er wird, seine Intelligenz testen oder schon mal prüfen, ob er die theoretische Führerscheinprüfung besteht. Die Betrüger verlangen für diese Angebote horrende Beträge, indem sie tückische Preisklauseln auf ihren Seiten verstecken. Dass für den vermeintlichen Service Kosten von 30 bis 200 Euro anfallen, verschweigen die Firmen gern bei der Vorstellung des Angebots. Ein weiterer Köder sind Sach- und Geldgewinne wie Handys, Spielkonsolen, Reisen, Bargeld und vieles mehr. Man muss seine persönlichen Daten wie Name, Anschrift und E-Mail-Adresse auf den Seiten angeben. Statt der vermeintlichen Gewinne erhält man anschließend jedoch horrende Rechnungen.

Bevor man sich bei einem Angebot registriert, sollte man sich daher die Seite und ihre Allgemeinen Geschäftsbedingungen (AGB) aufmerksam und in aller Ruhe bis ans Seitenende durchlesen. Dabei sollte man nach einem versteckten Kostenhinweis suchen. Ist in den Geschäftsbedingungen von Vertragslaufzeiten oder Kündigungsfristen die Rede, weist dies meistens auf eine vertragliche Bindung hin, die mit Kosten verbunden ist. Die Farbe und Größe der Schrift verschleiern auf Abzockseiten häufig den tatsächlichen Preis der Angebote: Wem fällt schon ein hellgrauer Hinweis vor weißem

Hintergrund links unten in einem schwarzen Text mit allerlei langweiligen Informationen auf? Noch dazu, wenn der Betrag nicht in Ziffern und mit Euro-Zeichen geschrieben wird, sondern alles ausgeschrieben erscheint (z. B. zehn Euro pro Monat statt 10,– €/Monat)?

Eine besonders perfide Masche von Abzockern ist das Verwenden von Internetadressen, die denen seriöser Institutionen ähneln. So unterscheidet sich die Seite *»www.berufs-wahl.de«* nur durch den Bindestrich von *»www.berufswahl.de«*, der offiziellen Plattform zur Studien- und Berufswahl von der Bundesagentur für Arbeit. Die Anbieter der Abzockerseiten verstecken sich in aller Regel hinter Scheinfirmen im Ausland, wo sie rechtlich kaum belangt werden können. Hinter deutschen Adressen steckt oft nur ein Briefkasten, hinter Telefonnummern nur eine Bandansage. Außerdem schließen diese Seiten oft nach kurzer Zeit und werden unter leicht geänderten Namen und mit einem neuen Impressum mit der gleichen Masche fortgesetzt. Grundsätzlich sollte bei Verträgen die Möglichkeit des zweiwöchigen Widerrufs und der Zahlung per Nachnahme bestehen. Wer vorab Geld überweist, geht ein großes Risiko ein, weil die Beträge im Betrugsfall nur schwer wieder zurückzubekommen sind.

Wenn man plötzlich eine hohe Rechnung für nicht bestellte Waren erhält, sollte man nicht darauf eingehen und auf keinen Fall zahlen, auch wenn Mahnungen und Inkassoschreiben von Rechtsanwälten zugestellt werden. Die Betrüger und ihre Anwälte haben keinerlei Pfändungsrechte. Man sollte den Forderungen in einem Brief per Einschreiben und Rückschein widersprechen, um einen Nachweis in Händen zu halten. Musterbriefe zum Widerspruch, die man entsprechend anpassen kann, und Tipps gibt es auf vielen Ratgeberseiten zum Thema Betrug im Internet. Handlungsbedarf besteht erst, wenn man einen gerichtlichen Mahnbescheid erhält. Die Polizei hat Experten, die beraten und helfen, wenn man zum Opfer von Internetbetrügern wird.

Neben Abzockseiten sind auch massenhaft versendete E-Mails mit sogenannten 0190-Dialern ein Problem. Oft werden Links auf gefährliche Webseiten, Viren oder die Dialer-Software über Kettenmails oder auch Messenger-Nachrichten verschickt. Diese an automatisch aus dem Netz herausgefilterte Internetadressen gesendeten Kettenmails laden Programme auf den lokalen Rechner, die sich über teure Vorwahlen (vor allem, aber nicht nur die 0190) ins Internet einwählen. Man sollte daher grundsätzlich nicht seine E-Mail-Adresse im Internet auf Foren, in Sozialen Netzwerken oder anderen öffentlich zugänglichen Seiten angeben oder am besten mit mehreren E-Mail-Adressen arbeiten. Grundsätzlich sollte man nur E-Mails öffnen, die von Absendern kommen, die man kennt, oder mit Spam- und Virenschutzprogrammen arbeiten.

Lebenslang gespeichert? Vom richtigen Umgang mit persönlichen Daten

Wer online ist, ruft Daten aus dem Netz ab – und auch umgekehrt werden gleichzeitig immer vom Netz Daten aus dem lokalen Rechner gesammelt. Jeder Nutzer hinterlässt daher nicht nur bewusst, sondern auch unbewusst persönliche Datenspuren im Internet. Mit speziellen Programmen, so genannten Firewalls (wörtlich übersetzt: Brandschutzmauern), kann man verhindern, dass ungewollt vertrauliche Informationen im Internet landen. Ein zunehmend größeres Problem als das Hacken von Privatrechnern stellt das mangelnde Problembewusstsein vieler Nutzer bezüglich des Umgangs mit ihren persönlichen Daten im Internet dar. Dazu zählen nicht nur Informationen, die man auf populären Seiten wie StudiVZ, Facebook, MySpace, oder YouTube hinterlässt, sondern auch Inhalte, die von Dritten veröffentlicht werden. Personenbezogene Daten werden zum Beispiel über Mitgliedschaften in diversen Organisationen sichtbar, wenn diese ihre Informationen ungeschützt ins Netz stellen.

Wer im Internet unterwegs ist, sollte daher sehr sorgfältig mit seinen persönlichen Daten umgehen. Damit lässt sich nicht nur vermeiden, dass man von Abzockern attackiert wird, sondern auch verhindern, dass private Informationen von Leuten gefunden werden, für die sie nicht bestimmt sind. Personalabteilungen von Firmen, bei denen man sich für ein Praktikum oder einen Job bewirbt, nutzen Soziale Netzwerke, Chatrooms, Foren und Gästebücher im Internet, um einen persönlichen Eindruck von einer Person zu gewinnen. Man sollte daher auf Online-Seiten, die zur Eingabe von Daten auffordern, immer die Angaben von Anbietern zum Datenschutz lesen, die meist unter den Allgemeinen Geschäftsbedingungen zu finden sind. Denn was einmal im Netz steht, bekommt man schwer wieder heraus. Wer nicht möchte, dass ein Partybild oder andere private Informationen von heute in zehn Jahren bei einem Bewerbungsgespräch zum Verhängnis werden kann, sollte die Inhalte gar nicht erst ins Netz stellen und auch anderen verbieten, sie online zu veröffentlichen. Das Persönlichkeitsrecht schützt uns davor, dass Inhal-

te über uns im Internet veröffentlicht werden, von denen wir nicht möchten, dass sie publiziert werden. Daher kann sich auch strafbar machen, wer Cybermobbing betreibt, indem er schädliche Informationen über andere im Internet publiziert.

Bei der Weitergabe von privaten Informationen in Form von Namen, (E-Mail-)Adressen, Bildern, Videos oder Kommentaren ist vor allem in den Sozialen Netzwerken Vorsicht geboten. Wer sie nutzt, überträgt den Unternehmen, die sie betreiben, mitunter die Rechte zur Nutzung der Daten. Die privaten Informationen sind quasi die Währung, mit der man die Nutzung der Software »zahlt« und die von den Betreibern der Seiten für Werbezwecke oder durch Weiterverkauf ökonomisch verwertet werden.

Die Netzwerke profitierten dabei davon, dass sich die Geräte, Profile und Betriebssysteme synchronisieren. Dabei hilft beispielsweise eine beliebte Applikation namens »Friend-Sync«, die auf dem iPhone gespeicherte Kontakte einer Person mit seiner Facebook-Freundesliste synchronisiert. Fotos, Vor- und Nachnamen sowie Geburtstage werden abgeglichen – und zu Facebook übertragen, egal, ob die Person sich dort bereits selbst registriert hat oder nicht. Man weiß daher nie, welche Bekannten auf diese Weise schon die eigenen Daten in das Netzwerk geladen haben. Facebook-Mitglieder können auf Fotos, die sie in Facebook-Alben verwalten, Personen mit vollem Namen markieren, obwohl die gar nicht angemeldet sind und nichts davon merken. Nicht nur Facebook, auch andere Soziale Netzwerke, E-Mail-Dienste und Online-Anbieter arbeiten mit diesen Vernetzungstechniken, die persönliche Daten im Internet für Suchdienste lebenslang verfügbar machen. Die Löschung der Informationen ist problematisch und häufig auch kostspielig, da Spezialunternehmen für Online-Reputationsmanagement beauftragt werden müssen.

Datenschützer versuchen daher rechtliche Lösungen für den problematischen Umgang mit den privaten Informationen im Internet zu finden. Da das Internet aber in weiten Teilen nicht an nationales Recht gebunden ist und Netzwerke wie Facebook auf Servern im Ausland betrieben werden, ist eine Lösung nach europäischen Datenschutzstandards nicht in Sicht. Wer Soziale Netzwerke nutzt, sollte die Bedenken der Datenschützer ernst nehmen und sich gut über die Privacy-Optionen informieren. Internetseiten wie Netzcheckers *(www.netzcheckers.de)* und Datenparty *(www.datenparty.de)* geben Tipps für den richtigen Umgang mit den eigenen Daten im Internet.

Weitere Informationen im Netz

- www.netzcheckers.de
  Informationen für Jugendliche zur digitalen Welt: Medien-Know-how, Sicherheit in Sozialen Netzwerken« der richtige Umgang mit den eigenen Daten in SchülerVZ, Facebook und Co.
- www.klicksafe.de
  Tipps und Materialien zum Jugendmedienschutz im Internet
- www.datenparty.de
  Tipps für den Umgang mit den persönlichen Daten im Internet
- www.chatten-ohne-risiko.net
  Chat-Atlas und Messenger-Check für Jugendliche und Unterrichtsmaterialien für Lehrer
- www.schulen-ans-netz.de
  Kompetenzzentrum für die Nutzung digitaler Medien im schulischen und außerschulischen Bereich
- www.time4teen.de
  Beratungsangebot der Polizei für Jugendliche mit Informationen zum Internet: Urheberrecht, Viren, Dialer und sicheres Chatten
- www.recherchetipps.de
  Praktische Informationen zur Recherche im Internet