Internet: Chancen und Risiken

Nutzen wir die Chancen und lernen wir mit den Risiken umzugehen!

Jürg Bieri

Das Internet ist aus dem beruflichen und privaten Alltag vieler Menschen nicht mehr wegzudenken. Es bietet viele Chancen, aber es birgt auch Risiken und Gefahren. Damit wir das Internet im Griff haben und nicht umgekehrt, müssen wir und unsere Kinder wissen, wie es funktioniert, und lernen mit den daraus entstehenden Herausforderungen umzugehen.

Was ist das Internet?

Das Internet ist ein Computernetzwerk, in dem unzählige einzelne Computer aus aller Welt zusammengeschlossen sind. Mit Hilfe von Internet und Computer können Menschen Daten austauschen. Wenn Sie also „aufs Internet gehen“, treten Sie eigentlich über das Internet mit einem anderen Computer in Verbindung, der Ihnen bestimmte Daten liefert.

Über das Internet laufen verschiedene Dienste. Am bekanntesten sind zweifellos E-Mail und das World Wide Web (kurz WWW). Neben WWW und E-Mail gibt es eine Reihe weiterer Internet-Dienste wie FTP, Chat, Internet-Telefonie und so weiter.

Wenn umgangssprachlich vom Internet gesprochen wird, ist damit meist das WWW gemeint. Hier kann man Inhalte (Texte, Bilder, Musik, Videos etc.) auf Webseiten weltweit zugänglich zu machen. Damit Sie diese Inhalte zu Hause anschauen können, brauchen Sie einen Computer, einen Internetzugang und ein spezielles Programm, welches Webseiten darstellen kann: einen Browser. Die bekanntesten Browser im deutschen Sprachraum sind Internet Explorer und Mozilla Firefox.

Soweit die kurze und vereinfachte Erklärung. Falls Sie genauere Infos möchten, finden Sie Links zu informativen Websites in einer kleinen **Linksammlung** auf der Schulwebsite (geanuere Angaben auf der letzten Seite des Berichts).

Wer braucht das Internet wozu?

Gemäss einer Umfrage des Bundesamtes für Statistik nutzten 2009 mehr als 3/4 der Bevölkerung das Internet täglich oder mehrmals pro Woche. Auffällig ist, dass Personen unter 40 das Internet viel häufiger nutzen als Personen über 60 und dass Leute mit geringerer Bildung oder geringerem Einkommen es deutlich seltener nutzen als jene mit höherer Bildung oder höherem Einkommen.

Gemäss derselben Umfrage wird das Internet vor allem für die Kommunikation (E-Mail, Chat) und die Suche nach Informationen aller Art gebraucht (Lexika, Fahr- und Flugpläne, Reiseinfos, Strassenkarten, Wetter, Nachrichten etc.). Erwähnenswert sind auch Bankgeschäfte via Internet, Online-Shopping, das Herunterladen von Musik und Filmen sowie die Internettelefonie (z.B. Skype).

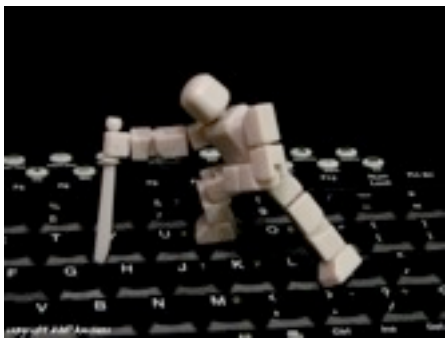
Zusammenfassend kann man also festhalten, dass das Internet von einem grossen und wachsenden Teil der Bevölkerung regelmässig für Kommunikation, Information, Dienstleistung und Unterhaltung genutzt wird. (Link zur Umfrage in **Linksammlung**).

Gefahren und Risiken im Internet

Wie in der wirklichen Welt gibts in der Internet-Welt leider auch Menschen, die böse Absichten haben. Dementsprechend gibts auch Gefahren und Risiken. Ich habe diese vereinfachend in drei Kategorien eingeteilt: Schädlinge, Abzockerei und weitere Risiken.

Schädlinge und ihre Bekämpfung im Internet

Die bekanntesten Schädlinge sind wohl die Viren. Diese kleinen Programme oder Progammteile hängen sich an Dateien oder nutzen andere Programme eines befallenen Computers, um sich zu verbreiten und Schaden anzurichten (z.B. Dateien löschen oder den Computer komplett unbrauchbar machen). Würmer haben ähnliche Folgen wie Viren, aber sie verbreiten sich selbstständig.



Leider sind Angriffe auf Computer in der Regel nicht so harmlos! (Foto: kmevans/flickr.com)

Trojaner und Spyware sind kleine Programme, die auf unterschiedliche Weise einen Computer bzw. dessen Nutzer ausspionieren. Dabei werden vertrauliche Daten gesammelt und übers Internet weitergeschickt. So erhalten Unberechtigte Zugriff auf Ihren Computer, missbrauchen Ihren Computer für illegale Tätigkeiten oder erstellen mit den persönlichen Daten ein Kauf-Profil, mit dem man Ihr Kaufverhalten manipulieren will.

Hoaxes und Spam sind unerwünschte Werbemails, Kettenbriefe oder Falschmeldungen. Sie sind nicht nur lästig und zeitraubend, sondern ihre Datenmenge belastet das Internet und die Server unnötig.

Wenn Sie verhindern wollen, dass Ihr Computer missbraucht wird, müssen Sie sich schützen! (Foto: Don Hankins/ flickr)

Kann man sich vor Schädlingen schützen?

Die Antwort auf diese Frage ist einfach: Ja, man kann sich vor diesen Schädlingen schützen. Weniger einfach ist hingegen die Antwort auf die Frage, wie man sich vor Schädlingen schützen kann. Deshalb kann ich Ihnen hier keine Schritt-für-Schritt-Anleitung anbieten, sondern nur die wichtigsten Tipps in Kürze. Sie finden aber in der **Linksammlung** einige Links zu Websites mit guten und detaillierten Informationen zu Schädlingen und dem Schutz davor:

Tipp 1: Verwenden Sie unbedingt ein Anti-Viren-Programm und aktualisieren Sie dieses regelmässig.

Tipp 2: Aktualisieren Sie auch Ihre anderen Programme laufend.

Tipp 3: Schützen Sie Ihren Computer mit einer „Firewall“. Eine „Firewall“ ist eine Schutzvorrichtung, die den Datenverkehr zwischen Netzwerken - z.B. zwischen Ihrem Computer und dem Internet - kontrolliert und dann entscheidet, welche Daten auf den Computer kommen und welche nicht.

Tipp 4: Verwenden Sie unbedingt immer die neuste Browser-Version! Ältere Browser-Versionen funktionieren zwar noch, aber sie haben Sicherheitslücken. (Kurzrepetition: Der Browser ist das Programm, das Sie brauchen, wenn Sie im World Wide Web surfen wollen, z.B. Internet Explorer oder Firefox).

Tipp 5: Überprüfen Sie die Sicherheitseinstellungen im Browser. So können Sie das Risiko klar verkleinern.

Tipp 6: Öffnen Sie nie E-Mail-Dateianhänge, wenn Ihnen der Absender unbekannt ist. Seien Sie auch mit E-Mail-Anhängen von bekannten Absendern vorsichtig. Würmer schicken oft automatisch E-Mails an alle Adressen im Adressbuch. Um alle Unsicherheiten zu beseitigen, überprüfen Sie die Datei mit einem aktuellen Antiviren-Programm.

Tipp 7: Schützen Sie Ihren Computer und Ihre Daten mit starken Passwörtern und gehen Sie sorgfältig mit Passwörtern um.

Es gibt keine hundertprozentige Sicherheit, aber wenn Sie diese Tipps gewissenhaft befolgen, ist das Risiko nicht mehr gross. Dennoch ist es empfehlenswert (**Tipp 8**), regelmässig Sicherheitskopien wichtiger Daten von Ihrem Computer zu erstellen. Falls trotz aller Vorsichtsmassnahmen ein Schädling zuschlägt, halten Sie auf diese Weise wenigstens die Folgen in Grenzen.

Abzockerei: Phishing und Co.

Abzockerei gibts im Internet in den unterschiedlichsten Formen. Ich gehe hier nur auf zwei Arten kurz ein. Beim **Phishing** versuchen Betrüger mit Hilfe von E-Mails Benutzernamen und Passwörter zu „fischen“ und so Zugriff auf Ihre Kreditkarte oder Ihr Bank-Konto zu erhalten. Ein Beispiel: In einer Mail wird gewarnt, dass die E-Banking-Zugangsdaten nicht mehr sicher sind und man wird aufgefordert, Benutzername und Passwort zu ändern. Der im Mail genannte Link führt aber nicht auf die Internetseite der genannten Bank, sondern auf eine täuschend ähnliche Internetseite. Wenn Sie nun auf dieser Internetseite Benutzername und Passwort eingeben, übergeben Sie damit gleichzeitig den Betrügern den Zugang auf Ihr Bankkonto.

Eine weitverbreitete Art der Abzockerei ist auch, dass man jemandem etwas verkauft, ohne dass man es merkt. Der Preis ist entweder versteckt ganz unten oder wird nur in den allgemeinen Geschäftsbedingungen erwähnt. Kurze Zeit später erhält man dann eine gesalzene Rechnung. Das ist meistens nicht legal und Sie müssen diese Rechnung mit ziemlicher Sicherheit nicht bezahlen. Am besten informieren Sie sich in so einem Fall aber im Internet oder holen Rat bei Fachleuten.

Hier noch zwei Abzockerschutz-Faustregeln:

Seien Sie kritisch! Denken Sie bei Mails und Internet-Angeboten stets an die Abzock-Gefahr.

Banken und allgemein vertrauenswürdige Grossunternehmen kontaktieren Ihre Kunden in wichtigen Fragen nicht per Mail.

Weitere Risiken und Gefahren

Leider gibt es im Internet noch mehr Gefahren. So wird z.B. die „Internet-Abhängigkeit“ immer mehr zu einem Problem. So bezeichnet man die übermässige Nutzung des Internets, welche Gesundheit und Persönlichkeit schädigen kann. Folgen einer derartigen krankhaften Internet-Nutzung sind Realitätsflucht, soziale Isolation, Vereinsamung, Vernachlässigung normaler Lebensgewohnheiten und lebenswichtiger Bedürfnisse (wie Nahrungsaufnahme und Schlaf).

Wenn Kinder im Internet statt auf dem Spielplatz spielen, fehlen ihnen auch die sozialen Kontakte mit Gleichaltrigen und sie verpassen wichtige Erfahrungen im zwischenmenschlichen Bereich (z.B. wie man mit Meinungsverschiedenheit umgeht).

Das Internet ist aber auch aus anderen Gründen kein geeigneter Ersatz-

Spielplatz. Sie würden Ihre Kinder sicher nicht auf einem Spielplatz unbeaufsichtigt spielen lassen, wenn Sie wüssten, dass sich in der Nähe Pädophile und politische Extremisten treffen, die ab und zu auch auf dem Spielplatz vorbeischauen. Genau das ist aber im Internet der Fall, denn Ihr Kind ist nur einen Mausklick entfernt von Neo-Nazi- oder Sex-Webseiten oder von einem Chat, wo Pädophile lauern. Deshalb müssen Sie diesen Spielplatz unbedingt beaufsichtigen!

Cybermobbing

Schliesslich möchte ich auch noch eine Gefahr erwähnen, die oft auch von Kindern und Jugendlichen selbst ausgeht: Cybermobbing. So bezeichnet man den Missbrauch elektronischer Kommunikationsmittel (z.B. Chat, E-Mail oder Handy), um einen Mitmenschen fertig zu machen. In der Schule gibts Cybermobbing von SchülerInnen gegen SchülerInnen, aber auch von SchülerInnen gegen LehrerInnen. Dabei verbreiten die Mobber hinter dem Rücken des Gemobbten anonym ein Gerücht oder stellen echte oder gar manipulierte Fotos oder Filme ins Internet, welche MitschülerInnen oder Lehrpersonen in entwürdigenden oder blossstellenden Situationen zeigen.

Cybermobbing unterscheidet sich in einigen Punkten von Mobbing und ist noch gravierender:

Cybermobbing kann rund um die Uhr geschehen.

Das Publikum ist im Internet viel grösser und die Verbreitung der Information erfolgt viel schneller.

Da das Internet nichts vergisst, ist es schwierig Cybermobbing-Inhalte zu beseitigen.

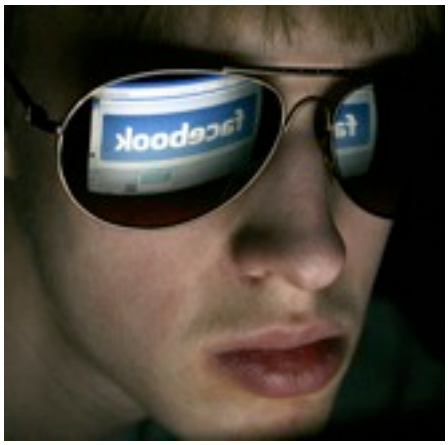
Cybermobbing kann komplett anonym passieren. Das verunsichert die Opfer zusätzlich und die Täter fühlen sich in Sicherheit.

Die Reaktionen des Opfers sind für den Täter nicht sichtbar. Der Täter merkt so möglicherweise nicht oder zu spät, was er seinem Opfer wirklich antut.

Leider handelt es sich beim Cybbermobbing nicht um Einzelfälle. Gemäss Untersuchungen hat heute bereits rund jeder fünfte Jugendliche eigene Cybermobbing-Erfahrungen gesammelt, sei es als Täter oder als Opfer oder gar als Täter und Opfer.

(K)eine Privatsphäre im Internet

Viele Menschen gehen im Internet sehr sorglos um mit ihrer Privatsphäre. Ohne Bedenken werden Email-Adresse, Handy-Nummer oder Geburtstag angegeben, man veröffentlicht private Fotos, schildert Eheprobleme oder Liebeskummer und beschwert sich über den Chef. Dies alles im Irrglauben, man sei mehr oder weniger anonym und/oder man habe ja nichts zu verbergen. Anonym ist man sicher nicht. Im Gegenteil, die ganze Welt schaut zu! Und auch wenn man nichs zu verbergen hat, sollte man vorsichtig sein mit privaten Angaben.



Die Sonnenbrille schützt vor der Sonne, aber nicht die Privatsphäre im Internet... (Foto: escapetowisconsin/flickr)

Erstens vergisst das Internet nichts. Alles, was einmal veröffentlicht wurde, bleibt gespeichert. Zudem kann man einmal veröffentlichte Informationen oft nicht mehr löschen. Zweitens weiss niemand - und schon gar nicht ein Kind - wie die eigene Zukunft aussehen wird. Eine öffentliche Aussage, die man als unproblematisch betrachtet, kann später Schwierigkeiten bereiten. Drittens kann man nicht abschätzen, was mit den privaten Angaben im Internet geschehen wird. Was einmal im Internet ist, kann rund um die Welt gesehen, weitergegeben, (in anderen Zusammenhängen) verwendet und weiterverarbeitet werden. So können auch harmlose Infos unerwartete Folgen haben. Hier einige Beispiele:

Ihre Daten werden für unerwünschte Mail-Werbung missbraucht oder um ein Konsumprofil zu erstellen.

Personen mit bösen Absichten machen Name und Wohnort von Kindern ausfindig, z.B. indem sie Angaben auf einer Website mit dem elektronischen Telefonbuch verknüpfen.

Bilder von Ihnen werden zweckentfremdet verwendet. Zwei erfundene, aber durchaus realistische Beispiele:

Beispiel 1: Ein peinliches Bild - bspw. von Ihrem Polterabend - gelangt Jahre später aus dem Zusammenhang gerissen in die Hände jenes Personalchefs, der über Ihre Einstellung entscheiden muss.

Beispiel 2: Ein Kollege stellt Bilder vom letzten Betriebsfest auf seine Website. Eine Bilder-Serie zeigt, wie Sie bei einem Gesellschaftsspiel ausrutschen und von einem Kollegen aufgefangen werden. Ein Neider stellt das letzte Bild, das sie in den Armen des Kollegen zeigt und damit einen falschen Eindruck erweckt, mit einem gemeinen Untertitel ins Internet.

Fazit: Seien Sie im Internet vorsichtig mit persönlichen Angaben aller Art, v.a. auch mit Fotos und Videos! Alles, was Sie nicht auf ein riesiges Plakat auf dem Dorfplatz schreiben würden, gehört nicht ins Internet. Das gilt insbesondere für Jugendliche, da es hier noch besondere Bedrohungen gibt (bspw. Pädophile).

Übrigens gilt diese Vorsicht noch verstärkt für Angaben über Dritte: Private Angaben über andere darf man nicht ohne deren Einverständnis machen. Auch mit der Veröffentlichung von Fotos muss man vorsich-

tig sein. Man sollte keine Fotos von Drittpersonen ohne Erlaubnis veröffentlichen und Fotos nie mit Namen beschriften.

Urheberrechte gelten auch im Internet!

Genauso wie das Recht auf Privatsphäre und das eigene Bild gilt im Internet auch das Urheberrecht. Hier muss man unterscheiden zwischen Download (Inhalte wie Text, Bilder, Musik, Filme oder Software aus dem Internet auf dem eigenen Computer speichern) und Upload (Inhalte ins Internet stellen).

Zuerst zum Download: Rechtlich gesehen darf man in der Schweiz im Internet Inhalte für den Eigengebrauch downloaden und muss nach geltender Rechtsprechung ziemlich sicher auch dann keine rechtlichen Konsequenzen befürchten, wenn es sich beim runtergeladenen Inhalt um Raubkopien handelt.

Obwohl es nicht verboten ist, gibt es gute Gründe auf Raubkopien von Filmen, CDs und Software zu verzichten. Erstens steigt damit das Sicherheitsrisiko. Raubkopien sind oft ein wahrer Schädlingshort. Zweitens entsteht durch Raubkopien ein volkswirtschaftlicher Schaden in Milliardenhöhe mit entsprechenden Folgen (geringere Steuereinnahmen, gefährdete Arbeitsplätze etc.). Drittens stellen sich auch moralische Fragen: Darf man ein Produkt gratis erwerben, das die Erzeuger verkaufen wollen, um sich damit ihren Lebensunterhalt zu verdienen? Sind Musik und/oder Filme wertlos?

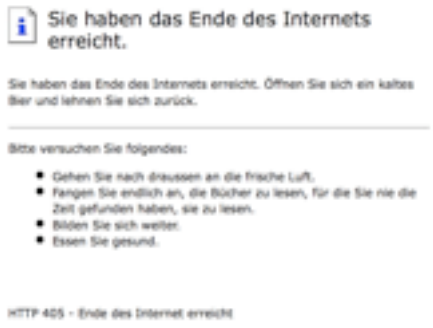
Im Bereich Upload/Veröffentlichung ist der rechtliche Spielraum kleiner. Grundsätzlich darf man im Internet nur Inhalte veröffentlichen, die man selber erschaffen hat oder für die man die erforderlichen Veröffentlichungsrechte hat. Diese Rechte erwirbt man sich übrigens mit dem Kauf einer CD / eines Filmes nicht. Und auch wenn ein Inhalt im Internet oder sonstwo bereits veröffentlicht worden ist, ist dieser geschützt und darf nicht in eigenen Veröffentlichungen verwendet werden.

Wie gehen wir damit um?

Wie sollen wir Erziehende (Eltern, Lehrpersonen etc.) aber nun mit dieser Situation umgehen? Ich möchte es mit einem Vergleich veranschaulichen: Jährlich werden tragischerweise viele Mitmenschen auf den Strassen verletzt oder gar getötet. Durch Strassen entstehen Unkosten, auf ihnen werden Abgase produziert und es wird gegen Gesetze verstossen. Da wir aber die vielen Vorteile der Strassen zu schätzen wissen, streben wir dennoch kein Verbot an, sondern versuchen mit Massnahmen (Schulung, Gesetze, Katalysatoren etc.) die negativen Folgen so klein wie möglich zu halten.

Dieselbe Denk- und Sichtweise brauchen wir auch fürs Internet. Wie bei den Strassen müssen wir uns mit den negativen Folgen auseinandersetzen und versuchen diese möglichst klein zu halten. Zu diesem Zweck müssen wir unser Wissen übers Internet und seine Risiken verbessern und ständig aktualisieren. Zudem müssen wir auch lernen, wie wir unseren Kindern einen verantwortungsvollen Umgang mit dem Internet beibringen. Grundlegend hierfür ist die Vermittlung von Grundwerten. Nur wenn die Kinder wissen, was richtig oder falsch ist, können sie in schwierigen Situationen richtig entscheiden. Zusätzlich müssen wir die Kinder und Jugendlichen aber auch konkret auf die Risiken und Gefahren des Internets vorbereiten und uns - vor allem bei jüngeren Kindern - auch überlegen, ob wir den Gebrauch zeitlich und inhaltlich einschränken und gewisse Regeln festlegen wollen.

Kontraproduktiv sind Internet-Verbote. Damit schützt man die Kinder allenfalls kurzfristig, aber mittelfristig schadet man ihnen. Man verhindert sie damit zu lernen, wie man mit dem Internet verantwortungsvoll und gekonnt umgeht. Das führt angesichts der grossen und zunehmenden Bedeutung des Internets in Beruf und Privatleben in eine Sackgasse. Zudem ist es zweifellos besser, wenn die Kinder das Internet mit seinen Risiken zu Hause und unter angepasster Aufsicht entdecken als irgendwo mit irgendwem.



Das Internet hat zwar kein Ende, aber frische Luft, Bücher und gesundes Essen sind sicher empfehlenswerte Internet-Alternativen. (Quelle: http://www.ende.li)

Kleine Linksammlung

Auf der Website www.schule-escholzmatt.ch finden Sie unter „Treffpunkt Schule“ eine kleine Sammlung von Links zum Thema Internet und Sicherheit.

Haben Sie Fragen zum Thema?

Haben Sie eine Anmerkung zu diesem Artikel oder oder eine Frage zum Thema, auf die Sie in den angegebenen Links keine Antwort finden? Schreiben Sie mir eine Email (juerg.bieri@edulu.ch). Und falls ich Ihnen nicht selber antworten kann, schreibe ich Ihnen wenigstens, wer oder was Ihnen weiterhelfen kann.