Was tun bei Dialern, Spam und Viren?

Internetsicherheit
Technische Tipps
E-Mail
Chat
Internet und Recht
Handy

Weitere Broschüren des BMFSFJ und der GMK zur Medienkompetenz:

Geflimmer im Zimmer

Medienkompetenz in Theorie und Praxis

Alles nett im Chat?

Der richtige Dreh im WWW

Gefördert durch:

Information Society
European Commission
Bundesministerium für Familie, Senioren, Frauen und Jugend

s@ferinternet

GMK
Gesellschaft für Medienpädagogik und Kommunikationskultur

Was tun bei Dialern, Spam und Viren?

Tipps zum sicheren Internetgebrauch in Familien

Das Internet ist auf vielfältige Art gegenwärtig:

Wir werfen online einen Blick auf das aktuelle Kinoprogramm, bestellen Bücher, sind auf Schnäppchenjagd bei Online-Auktionen oder buchen das Ferienhaus für den nächsten Urlaub. Nur wenige Klicks und wir können mit Menschen auf der ganzen Welt kommunizieren, Informationen austauschen, online spielen oder nach Material für den Schulunterricht suchen.

Aber der bunte Marktplatz Internet hat auch unangenehme Seiten, auf die jede Nutzerin und jeder Nutzer stoßen kann. Würmer, Viren, Spam, Dialer* - das ist nur eine kleine Auswahl der Gefahren, die uns im Umgang mit dem Internet begegnen. Kinder und Jugendliche sind im Internet durch ihre Unerfahrenheit besonderen Risiken ausgesetzt. Beispielsweise bietet eine Hausaufgabenseite Informationen, aber im Gegenzug wird ein Dialer auf dem heimischen Computer installiert, der pro Minute zwei Euro kassiert, manchmal auch deutlich mehr. Chat-Räume, bei Mädchen und Jungen gleichermaßen beliebt, werden auch von Pädophilen genutzt, um Kontakt zu Kindern und Jugendlichen aufzunehmen.

Technische Lösungen wie Filter oder Virenschutzprogramme bieten nur begrenzten Schutz. Zusätzlich sollten sich die Internetnutzerin und der Internetnutzer fragen: Kann ich dem Internetanbieter vertrauen, wenn er für die Teilnahme an einem Preisrätsel die Angabe meiner persönlichen Daten fordert? Wer ist der Betreiber der Internetseite, auf der ich mich informiere? Dient die Seite der objektiven Information, einem kommerziellen Zweck oder werden falsche Informationen verbreitet?

Das Internet erschließt neue Chancen und Möglichkeiten auch für Kinder und Jugendliche. Doch viele Eltern machen sich Sorgen über den richtigen Umgang ihrer Kinder mit dem Internet. Die vorliegende Broschüre beantwortet die wichtigsten Fragen zur Internetsicherheit und zum sicheren Umgang mit Handy und SMS. Sie gibt Tipps und Empfehlungen, wie Sie sich und Ihre Kinder in der Online-Welt schützen können. Zusätzlich finden Sie Links zu interessanten Internetseiten.

Die Broschüre entstand im Rahmen des Projekts SafeBorders, das europaweit Kinder und Familienrechte im Internet stärken möchte. Auf der Homepage der Kampagne *www.safernet.info* finden sowohl Eltern, Erzieherinnen und Erzieher als auch Kinder und Jugendliche viele weiterführende Informationen zu Fragen, die in dieser Broschüre behandelt werden.

Wir haben Fragen von Kindern und Eltern und Antworten darauf in dieser Broschüre zusammengestellt.

Die Homepage www.safernet.info bietet Eltern, Kindern, Jugendlichen und pädagogischen Fachkräften viele weiterführende Informationen.

* gelb gekennzeichnete Begriffe werden im Glossar am Ende der Broschüre und auf der Seite www.mediageneration.net/glossar/index.php erläutert.

Inhalt

s@ferinternet

Inhalt

Sind Seiten aus Deutschland sicherer als Seiten aus dem Rest der Welt?

Deutschland hat teilweise strengere Gesetze zur Regulierung des Internets als die meisten anderen Länder. Zum Beispiel sind bei uns rechtsradikale, pornografische Inhalte und solche, die gegen die Menschenwürde verstoßen verboten, die in anderen Ländern durch die Garantie der Meinungsfreiheit geschützt werden. Aber der deutsche Gesetzgeber kann nicht alle deutschsprachigen Webseiten kontrollieren und belangen, denn der Server, auf dem die Daten gespeichert sind, kann überall auf der Welt stehen.

Warum werden jugendgefährdende Seiten nicht verboten? Welche Jugendschutzmaßnahmen gibt es in Deutschland?

Es wäre wünschenswert, dass Kinder und Jugendliche völlig ungefährdet die Online-Welt erkunden könnten. Aber im Internet gibt es Angebote für Menschen aller Alters- und Interessengruppen und aus allen Teilen der Welt. In anderen Ländern gelten andere Regeln.
Was in Deutschland verboten ist, kann anderswo erlaubt sein, so dass Verbote sich nicht weltweit durchsetzen lassen. Auch wenn es eine gesetzliche Verpflichtung für eine Altersfreigabe aller Seiten geben würde, wäre das nicht überprüfbar. Die deutsche Kontrollmöglichkeit endet an den deutschen Grenzen. Versuche, einen Jugendschutz für das Internet durchzusetzen, können sich somit nur auf Inhalte von deutschen Servern beschränken. Da aber Seiten aus der ganzen Welt empfangen werden können, ist das nur eine sehr eingeschränkte Regulierung.
In Deutschland gibt es seit April 2003 den Jugendmedienschutz-Staatsvertrag. Die zentrale Aufsichtsstelle der Länder, die Kommission für Jugendmedienschutz (KJM), wacht darüber, dass keine Angebote auftauchen, die Gewalt verherrlichen, pornografisch sind oder gegen die Menschenwürde verstoßen. Kinder und Jugendliche sollen somit vor Inhalten im Internet geschützt werden, die sich negativ auf ihre Entwicklung oder Erziehung auswirken. Der Jugendmedienschutz-Staatsvertrag wendet sich dabei an die Anbieter von Webseiten. Die Anbieter von Seiten, die nur für Erwachsene geeignet sind, sollen beispielsweise durch entsprechende Verfahren sichern, dass niemand unter 18 Jahren auf diese Internetangebote gelangen kann. Wenn eine Webseite gegen die Bestimmungen verstößt, drohen strafrechtliche Konsequenzen oder Bußgelder.

Problematisch bleibt jedoch, dass diese Regelungen nur für Seiten auf deutschen Servern anwendbar sind.

s@ferinternet
Allgemeines zur Sicherheit im www

Es wäre wünschenswert, dass Kinder und Jugendliche völlig ungefährdet die Online-Welt erkunden könnten.

Beschwerdestellen und weitere Informationen:

www.bundespruefstelle.de
(für die Indizierung von Medien)

www.alm.de
(Kommission Jugendmedienschutz / KJM)

www.jugendschutz.net
(angegliedert an die KJM, mit Beschwerde-Hotline für illegale Webseiten-Inhalte)

www.fsm.de
(Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V., mit Beschwerde-Hotline für illegale Webseiten-Inhalte)

Welche Kinder- und Jugendseiten sind empfehlenswert?

Alle empfehlenswerten Kinderseiten können wir hier sicher nicht aufführen. Die Seiten verändern sich, neue kommen dazu und andere fallen weg. Zum Einstieg empfehlen wir daher *www.seitenstark.de*, einen Zusammenschluss renommierter deutschsprachiger Kinderseiten im Internet. Alle hier gelisteten Seiten sind für Kinder oder Jugendliche interessant.

www.kidsville.de

www.sowieso.de

www.milkmoon.de

www.blinde-kuh.de

www.wasistwas.de

www.hanisauland.de

www.geolino.de

www.kindersache.de

www.wolf-kinderclub.de

s@ferinternet
Allgemeines zur Sicherheit im www

www.tk-logo.de

www.zzzebra.de

www.vuz-web.de

www.rossipotti.de

www.alws.de

www.jolinchen.de

www.klasse-wasser.de

www.kidnetting.de

Weitere empfehlenswerte Websiten finden Sie unter:
www.mediageneration.net/kinderseiten/index.php

Welche Seiten sind als Hausaufgabenhilfen zu empfehlen?

Wenn Kinder sich mit einem bestimmten Thema beschäftigen, können sie wie Erwachsene auch über eine Suchmaschine Informationen finden. Leider sind die bekanntesten dieser Service-Angebote wie *www.google.de* oder *www.altavista.com* gar nicht oder nur teilweise für Kinder geeignet. Die Ergebnisse der Suchabfragen stellen alles wahllos nebeneinander: Wichtige Informationen neben Werbung, neben Sexangebote usw. Eine Vorauswahl für kindgerechte Seiten gibt es nicht. Für Kinder ist daher die Spezial-Suchmaschine *www.blinde-kuh.de* empfehlenswert, die nur Seiten anzeigt, die redaktionell von Pädagogen gesichtet und geprüft wurden. Gelungen ist auch die Suchmaschine von *www.wasistwas.de*. Hierüber lassen sich viele Texte finden, die beispielsweise bei Hausaufgaben hilfreich sein können. Neben einem umfangreichen Archiv zu den Themen Geschichte, Technik, Wissenschaft, Natur und Tiere gibt es auf der Startseite auch aktuelle Berichte.

Der „Schulfachnavigator“ von *www.internet-abc.de* gibt viele nützliche Tipps rund um das Thema Hausaufgaben. An Beispielen wird Kindern gezeigt, wie sie am besten Informationen finden. Die Suche im Internet ist nur eine von vielen Strategien, die beschrieben werden. Auch die Struktur einer Arbeit sowie die Nutzung anderer Quellen werden leicht verständlich erklärt.

Hilfreich ist oft der Austausch mit anderen. Bei *www.eeqoo.de* kann jeder zu verschiedenen Schulfächern und Themen Fragen stellen, die dann von anderen Nutzerinnen und Nutzern der Webseite beantwortet werden.

Natürlich kommt es zu keinerlei Lerneffekten, wenn Schülerinnen und Schüler Texte einfach nur kopieren, ohne dass sie sich selbst mit dem Thema beschäftigen.

Warnung: Etliche Hausaufgaben-Seiten werden von unseriösen Geschäftsleuten angeboten, deren Nutzung die Installation eines teuren Dialer-Programmes erfordert. Die wichtigste Regel lautet: Bevor Sie etwas anklicken oder durch eine Eingabe bestätigen, vorher immer die Nutzungsbedingungen von Online-Quellen lesen. Anbieter von Dialer-Programmen sind in Deutschland dazu verpflichtet, ihre Kundinnen und Kunden über die Kosten zu informieren. Oft sind die wichtigen Kosteninformationen aber versteckt (beispielsweise hinter „Anbieterinformation“) oder sehr klein geschrieben. Deswegen ist Vorsicht geboten. Weitere Hinweise hierzu finden Sie in dieser Broschüre im Kapitel über Dialer.

s@ferinternet
Allgemeines zur Sicherheit im www

Wo gibt es die besten Spiele im Netz?

Viele Seiten bieten kostenlose Spiele an. Es gibt Software, die Sie auf dem Computer speichern können oder kleinere Spielchen, die direkt online laufen. Die Auswahl ist groß und wenn Sie mit Ihren Kindern im Internet suchen, finden Sie schnell eine Vielzahl von Angeboten. Aber Vorsicht vor unseriösen Anbietern! Auch hinter manchen Spiele-Seiten stehen Firmen oder Einzelpersonen, die die Besucherinnen und Besucher dazu bringen wollen, einen teuren Dialer zu installieren.

Unter folgendem Link lassen sich immer ein paar gute und kostenlose Spiele finden:

www.kidstation.de
Ein umfangreiches Angebot für Kinder mit mehreren Dutzend Spielen. Ob Actionspiele, Geschicklichkeitsprüfungen oder Denksportaufgaben gesucht werden, hier wird jeder fündig. Zum Hüpfspiel „Super-Climber“ gibt es sogar einen virtuellen Baukasten, mit dem sich eigene Levels (Schwierigkeitsstufen) erstellen lassen.

Screenshot vom Hüpfspiel „Super-Climber“

USB-Stick, Diskette und CD sind optimale Medien, um wichtige oder persönliche Dateien vor Übergriffen aus dem Internet zu schützen.

Wie sicher sind die Daten auf dem Computer?

Wenn Ihr Computer ungeschützt ist, können andere, die es darauf anlegen und das nötige Computerwissen mitbringen (so genannte Hacker oder Cracker), auf Ihren Rechner zugreifen. Die Daten, die Sie auf der Festplatte Ihres Computers speichern, sind also ungeschützt und theoretisch für viele Menschen einsehbar. Vermitteln Sie dies auch Ihren Kindern. Besonders sensible Daten, wie zum Beispiel Konto-Passwörter, sollten Sie auf keinen Fall auf ihrem Rechner abspeichern. Es gibt aber Möglichkeiten, die Daten vor dem Zugriff durch andere zu sichern, beispielsweise durch eine Firewall.

Wie kann ich meinen Computer vor Hackern und Crackern schützen?

Es gibt verschiedene Strategien, um den Computer und Ihre persönlichen Daten vor Fremden abzuschirmen. Die einfachste Methode Ihren Computer und Ihre persönlichen Daten vor fremden Zugriffen zu schützen ist eine Firewall. Es gibt im Internet einige kostenlose Firewalls zum Download. Diese Filter verhindern unberechtigte Zugriffe auf Rechner oder Netzwerke. Wenn Sie ganz sicher

s@ferinternet
Technische Tipps

gehen wollen, dass wichtige oder persönliche Dateien vor Übergriffen aus dem Internet geschützt sind, sollten Sie diese auf eine CD brennen oder auf Diskette speichern, anstatt sie auf der Festplatte zu hinterlegen.

Wie stelle ich die Firewall auf dem Computer richtig ein?

Der beste Schutz ist, zu Beginn die höchste Sicherheitsstufe einzustellen und jedes Mal nachzubessern, wenn ein Programm nicht funktioniert oder wenn Sie Probleme mit dem Aufrufen einer Seite haben. Dies ist vielleicht etwas unkomfortabel, aber sehr wirksam. Einzelne Programme und Verbindungen können der Firewall hinzugefügt werden, damit sie jederzeit ohne Einschränkungen nutzbar sind.

Download Firewall Zonealarm unter: *www.zonelabs.de*

Was ist ein Dialer, wie arbeitet er und wie kann ich mich davor schützen?

Dialer sind kleine Einwahlprogramme, die bereits bestehende Internetverbindungen auf dem Rechner unterbrechen und einen neuen Zugang einrichten, für den erhöhte Kosten anfallen. Gedacht sind diese Programme zur einfachen Abrechnung von Dienstleistungen, allerdings werden sie häufig von unseriösen Internetanbietern missbraucht.

Das ist die Gesetzeslage: **INFO!**

- Obwohl die Nutzung eines Dialers erst ab 18 Jahren erlaubt ist, wird die Halterin oder der Halter des Telefonanschlusses für entstandene Kosten zur Kasse gebeten (das sind oft die Eltern), auch wenn Kinder die Dialer genutzt haben. Viele Dialer kosten zwei Euro pro Minute. Neue Gesetze erschweren es den Anbietern, an das Geld der Internetnutzerinnen und -nutzer zu kommen. So muss ein Dialer-Programm klar erkennbar sein. Seit Dezember 2003 darf die Einwahl nur über die Nummer 09009 erfolgen. Sie müssen dem Herunterladen der Datei, der Installation des Dialers auf Ihrem Rechner und dem Verbindungsaufbau einzeln zustimmen. Ihre Zustimmung geben Sie meist durch die Eingabe eines OKs. Eine Minute darf nicht mehr als zwei Euro kosten und nach einer Stunde erfolgt automatisch eine Verbindungstrennung. Allerdings beträgt der gesetzlich festgelegte Höchstpreis für eine Einwahl 30 Euro. Seit dem Dialer-Gesetz vom August 2003 sind daher viele Abzocker dazu übergegangen, von vornherein für die einmalige Einwahl 30 Euro zu berechnen, unabhängig von der Verweildauer.

INFO! **Das sind die Probleme bei Dialern:**

- Dialer können enorm hohe Telefonrechnungen verursachen.
- Webseiten werden zunehmend mit Dialern versehen, auch solche, die als Zielgruppe Kinder haben. (Beispiele: Malvorlagen, Hausaufgabenhilfen)
- Viele Dialer-Betreiber sitzen im Ausland und entziehen sich so deutschen (Verbraucherschutz-) Gesetzen.
- Einige Dialer sind auf Ihrem Desktop oder in der Taskleiste nicht zu erkennen. Das heißt, Sie merken gar nicht, dass Sie über einen Dialer verbunden sind.

INFO! **Daran können Sie erkennen, ob sich ein Dialer auf Ihrem Rechner installiert hat:**

- Überprüfen Sie im DFÜ-Netzwerk die eingetragenen Verbindungen.
- Überprüfen Sie, ob auf Ihrem Desktop oder in der Taskleiste neue unbekannte Symbole auftauchen.
- Beobachten Sie die Aktivitäten Ihres Modems oder Ihrer ISDN-Karte.
- Weitere Hinweise auf einen Dialer können eine neue Startseite sein, die nicht von Ihnen ausgesucht wurde, sowie Pop-Up-Fenster, die sich beim Starten des Browsers selbstständig öffnen.

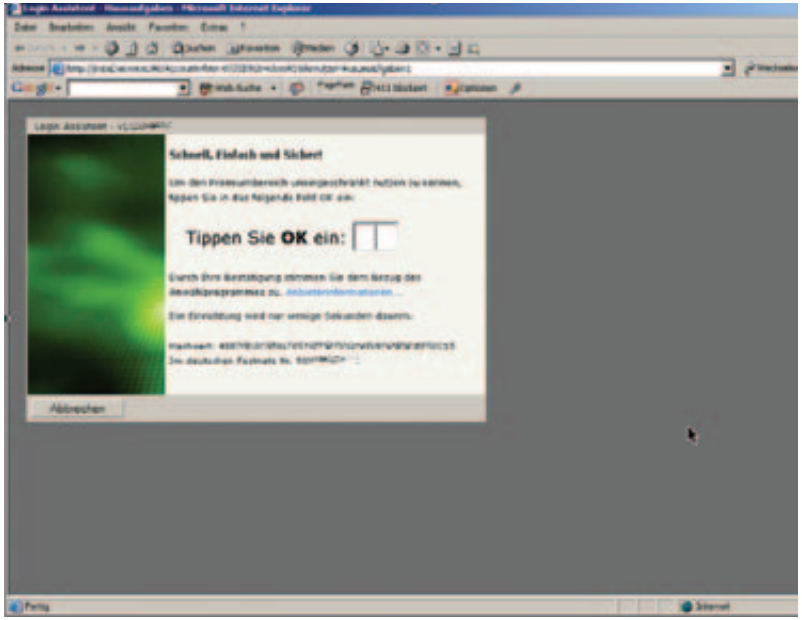
INFO! **Gefährliche Nummern sperren lassen:**

- Eine Nummernsperre des Telefonanbieters ist eine weitere Schutzmöglichkeit. Die Telekom bietet zum Beispiel ein Sicherheitspaket an, mit dessen Hilfe Sie gegen eine geringe Gebühr bestimmte Vorwahlen sperren lassen können. Wenn die Nummern 0190, 0192, 0193, 0900 und diverse Auslandsvorwahlen gewählt werden, wird keine Verbindung mehr aufgebaut, allerdings auch nicht zu anderen Service-Nummern, die mit diesen Zahlen beginnen.

INFO! **Wenn Sie aufgefordert werden OK/oder Ja oder ähnliches einzugeben:**

- Lesen Sie sich alle Dialogfenster gründlich durch, bevor Sie sich mit etwas einverstanden erklären und ein „OK“ eintippen. Oft sind die Geschäftsbedingungen in einem weiteren Fenster versteckt, das sich erst öffnet, wenn farblich hervorgehobene Punkte wie „weitere Informationen“ oder „Anbieterinformationen“ angeklickt werden.

s@ferinternet
Technische Tipps



Screenshot von Dialer-Einwahl

- Die richtige Einstellung des Internet-Browsers: Beim Internet-Explorer (unter Extras/Internetoptionen) sollte zum Beispiel die Software Active-X deaktiviert werden. Bei allen Browsern ist die Abschaltung von JavaScript ein guter Schutz vor vielen Dialern. Leider sind danach viele Webseiten nicht mehr voll funktionsfähig. Besonders kleine Internet-Spiele oder Animationen benötigen diese Programme oft, um zu funktionieren.
- Benutzen Sie Dialerschutz-Programme, empfehlenswerte sind beispielsweise a2, AdAware oder Spybot.
- Es gibt verschiedene Methoden, Ihren heimischen Computer zu schützen. Internet-Abzocker denken sich immer neue Methoden aus, darum ist es wichtig, sich auf dem Laufenden zu halten: Aktuelle Informationen zu Dialern und Beschwerde-Musterschreiben finden Sie auf: *www.dialerschutz.de*

Erste Schritte, wenn Sie befürchten, Opfer eines Dialers geworden zu sein: **INFO!**

- Haben Sie eine überhöhte Telefonrechnung? Fragen Sie alle Nutzerinnen und Nutzer des Computers, ob jemand diese Gebühren verursacht hat.

- Fordern Sie einen Einzelverbindungsnachweis von Ihrem Telefonanbieter. Beantragen Sie ihn besser sofort.
- Sichern Sie Beweise: Suchen Sie den Dialer und kopieren Sie ihn auf eine Diskette.

Illegale Dialer können der Hotline der Regulierungsbehörde (*www.regtp.de*) gemeldet werden: 01805 – 342537 (12 Cent / Minute)

Weitere Infos und Tipps auch online unter
www.mediageneration.net/dialer/index.php

INFO! **Was kann ich gegen Pop-Ups machen?**

So genannte Pop-Ups, Werbefenster, die sich selbstständig öffnen, können den Spaß am Surfen verderben. Doch es gibt Gegenmaßnahmen:

- Wenn Sie einen neueren Browser, z.B. Mozilla Firefox nutzen, können Pop-Ups über den eingebauten Pop-Up-Blocker direkt unterdrückt werden.

Screenshot vom Browser Mozilla Firefox.

- Es gibt auch Pop-Ups, die sich nicht durch den Besuch bestimmter Internetseiten öffnen, sondern in unregelmäßigen Abständen von Programmen auf Ihrem Computer aktiviert werden.
- Wenn Sie häufig die gleiche Werbebotschaft erhalten, obwohl Sie sich auf ganz unterschiedlichen Seiten im Netz aufhalten, ist die Wahrscheinlichkeit recht hoch, dass sich auf Ihrer Festplatte so genannte „Adware“ eingenistet hat, die häufig als Teil einer anderen Software heruntergeladen wird. Wenn Sie die störende Werbung loswerden möchten, ist „Ad-Aware“ ein Programm, das Ihren Rechner durchsucht und einen Großteil der Verursacher von Pop-Ups findet. Anschließend werden die Programme unschädlich gemacht. Dieses Tool finden Sie unter:
www.lavasoftusa.com.

Was sind Viren?

Ein Virus ist ein Programm oder Teil eines Programms, der sich in der Regel schädlich auf seine Umgebung auswirkt (zum Beispiel Dateien auf Ihrem Computer zerstört). Da sich ein Computervirus genau wie ein Grippevirus vermehren kann, immer mehr Dateien befällt und sich auch auf andere Systeme ausbreitet, kann Ihr Rechner schnell die Arbeit einstellen, abstürzen oder den Virus weiter verbreiten. Die Folgen können von kleinen Problemen mit Ihrem Betriebssystem oder Abstürzen bis zum vollständigen Löschen der Festplatte reichen. Aktuelle Informationen zu Viren, Würmern, Trojanern und Hoaxes gibt es unter:
www.sophos.de
www.hoax-info.de

Beschreibungen der bekanntesten Virenarten finden Sie auf:
www.mediageneration.net/viren/index.php

Wie können Viren auf den Computer gelangen?

Wenn Daten von außen auf Ihren Rechner kommen, können theoretisch jedes Mal Viren enthalten sein. Es ist egal, ob Sie eine Datei aus dem Internet herunterladen, eine CD-ROM benutzen, eine E-Mail öffnen, einen Text von einer Diskette kopieren oder eine andere Quelle (USB-Stick, Memory Cards usw.) an Ihren Computer anschließen - die Gefahr ist immer vorhanden. Sie sollten also darüber nachdenken, wie sicher die Daten sind, die Sie auf Ihrem Rechner speichern und benutzen. Wenn eine Bekannte oder ein Bekannter einen aktuellen Virenscanner benutzt und Ihnen ein Bild per E-Mail schickt, ist das in der Regel relativ sicher. Wenn Sie einen Anhang einer E-Mail von jemandem öffnen, den

Sie überhaupt nicht kennen, ist das Virenrisiko sehr groß. Eine Original-CD-ROM ist weniger riskant als ein Programm von einer Seite im Internet. Eine absolute Sicherheitsgarantie gibt es aber nie. Selbst große Software-Firmen haben schon versehentlich Produkte veröffentlicht, die virenverseucht waren.

INFO! Wie kann ich den Computer vor Viren schützen?

- Der beste Schutz ist, aufmerksam zu sein und vorsichtig mit Programmen umzugehen. Installieren Sie nicht einfach jede Software, sondern denken Sie erst darüber nach, ob Sie das Programm tatsächlich benötigen und woher es kommt.
- Prüfen Sie, ob eine Seite vertrauenswürdig und sicher ist, bevor Sie dort Dateien herunterladen. Öffnen Sie nicht unbedacht die Anhänge jeder E-Mail. Besonders misstrauisch sollten Sie sein, wenn Sie die Absenderin oder den Absender nicht kennen oder Ihnen der Inhalt oder die Betreff-Zeile einer E-Mail merkwürdig vorkommt.
- Manchmal werden die Namen von bekannten Firmen, Kinderseiten oder Einzelpersonen als Absender zum Verschicken von Viren verwendet (Microsoft, Deutsche Bank, Blinde Kuh, Kidsville). Wer Viren in Umlauf bringt, will damit oft möglichst viel Schaden anrichten und sorgt deshalb häufig dafür, dass die E-Mail unauffällig wirkt. Darum werden als Absender bekannte Namen gewählt, denen Vertrauen entgegengebracht wird. Hier hilft es, auf merkwürdige Betreffs zu achten, die nichts mit den tatsächlichen Inhalten der vermeintlichen Absender zu tun haben.
- Vorsicht ist auch geboten, wenn Sie direkt aufgefordert werden, einen Anhang zu öffnen oder auf einen Internet-Link zu klicken und Ihnen gedroht wird oder Versprechungen (z.B. Geldgewinne) gemacht werden.

Ein Virenscanner ist ein nützliches Werkzeug, um den Computer vor Angriffen durch gefährliche Programme zu schützen. Sie können Virenscanner im Internet herunterladen oder im Handel kaufen. Es gibt verschiedene Angebote, zum Beispiel Freeware, die nichts kostet, aber auch kostenpflichtige Programme (z.B. für große Firmen). Manche können befallene Dateien „reinigen“ oder wieder herstellen, während andere alles sofort löschen, was Viren enthält. Manche Virenscanner sind ständig aktiv und informieren Sie, falls ein Virus versucht, auf Ihren Computer zuzugreifen. Andere Programme müssen Sie immer wieder selbst starten, damit sie Ihren Rechner auf Viren überprüfen.
Ein gutes Programm, das Sie kostenlos auf einem privaten Rechner installieren dürfen, ist AntiVir Personal Edition. Auf *www.free-av.de* finden Sie Links zur aktuellen Version. Neue Viren, Würmer, Trojaner und andere Schädlinge werden fast täglich im Internet verbreitet; daher muss selbst der beste Virenscanner regelmäßig (mindestens alle zwei Wochen) aktualisiert werden. Nur wenn Ihre

Schutz-Software auf dem neuesten Stand ist, sind Sie optimal gegen Attacken geschützt. Informationen über die neuesten Viren gibt *www.sophos.de*. Eine umfangreiche Liste mit Virenscannern inklusive Beschreibung finden Sie unter: *www.heise.de/security/dienste/antivirus/links.shtml*.

Was kann ich tun, wenn sich bereits Viren auf meinem Computer befinden?

Wenn Sie sicher sind, dass Ihr Rechner bereits von einem Virus befallen ist, gehen Sie folgendermaßen vor:

1. Starten Sie ein aktuelles Anti-Viren-Programm und überprüfen Sie die Dateien auf Ihrer Festplatte.

2. Informieren Sie sich im Internet über die aktuellen Gefahren und überprüfen Sie, ob es Tipps gibt, wie sich der Virus entfernen lässt. Viele Seiten beschäftigen sich mit dem Thema Viren. T-Online hat zum Beispiel einen eigenen Computer-Bereich, der auch eine Rubrik namens „Viren und Sicherheit“ beinhaltet (*http://oncomputer.t-online.de/*). Auch Suchmaschinen können Ihnen bei der Lösung Ihrer Probleme helfen. Falls Ihnen der Name des Virus oder einige unverwechselbare Merkmale bekannt sind, nutzen Sie diese Informationen, um Nachforschungen anzustellen. Die größte deutschsprachige Viren-Datenbank finden Sie unter: *www.percomp.de/virinfo-f.php*

3. Wenn Sie allein nicht dazu in der Lage sind, den Virus zu entfernen, wenden Sie sich an Experten in Ihrem Bekanntenkreis oder in einem Computer-Fachgeschäft.

4. Die komplette Löschung und Formatierung Ihrer Festplatte ist glücklicherweise nur in sehr seltenen Fällen erforderlich. Bei extremem Virenbefall und völliger Zerstörung wichtiger Dateien ist diese Maßnahme aber manchmal das letzte wirksame Mittel.

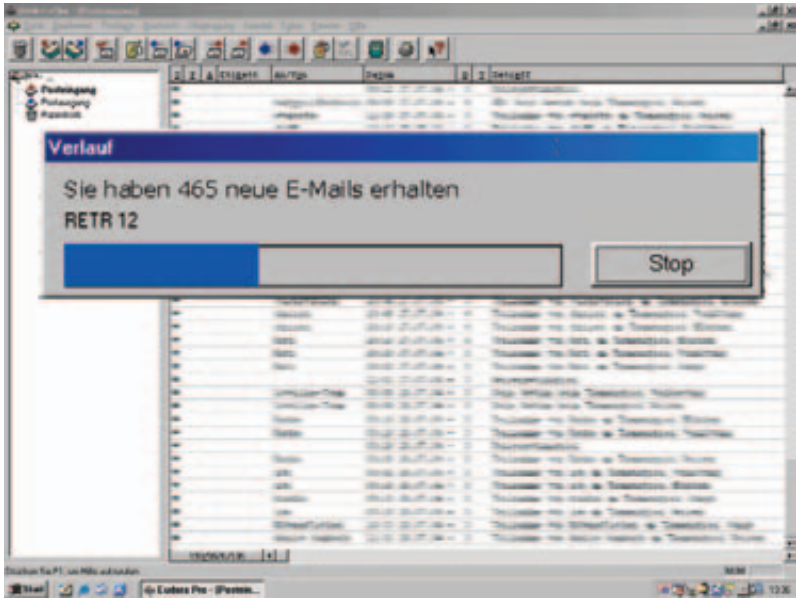
Da es keinen absoluten Schutz vor Viren, Würmern und anderen schädlichen Programmen gibt, sollten Sie wichtige Daten sichern. Wenn in Ihrem Computer ein CD-Brenner eingebaut ist, sichern und kopieren Sie alle wichtigen Dateien in regelmäßigen, von Ihnen für sinnvoll erachteten Abständen auf eine CD-ROM. Wenn es zu einem Notfall kommt und Sie wegen eines Virus oder eines anderen technischen Problems Ihre Festplatte löschen müssen, ist das zwar ärgerlich und zeitraubend, aber wenigstens bleibt Ihnen ein Backup mit den wichtigsten Daten. Wenn nur ein paar Texte (zum Beispiel die gesammelten Hausaufgaben der Kinder) gesichert werden sollen, reicht auch eine Diskette.

Woran kann es liegen, wenn der Computer ständig abstürzt?

Computertechnik ist komplex und verschiedene Ursachen können zu unterschiedlichen Fehlern führen, so dass es leider keine allgemein gültige Antwort auf diese Frage gibt.

Wodurch die Probleme entstehen, lässt sich oft nur sagen, wenn verschiedene Möglichkeiten überprüft werden. Manchmal hilft es bereits den Rechner neu zu starten. Für Probleme können Viren, Überlastung, Systemfehler und viele andere Auslöser verantwortlich sein.

Wenn ein Rechner so oft abstürzt, dass Arbeiten und Spielen beinahe unmöglich wird, sollte eine Expertin oder ein Experte den Rechner überprüfen. Selten sind Hardware-Defekte (z.B. eine kaputte Festplatte); häufiger solche Abstürze, die beispielsweise durch Viren verursacht werden. Wenn Sie sich damit nicht auskennen, sollten Sie auf keinen Fall selbst versuchen, den Computer zu reparieren.



Wo können sich Internetnutzer über SPAM-Mails beschweren?

Was tun, wenn die SPAM-Mails (unerwünschte Werbung per E-Mail) bereits den Weg ins eigene Postfach gefunden haben? INFO!

- Senden Sie auf keinen Fall eine Beschwerde-Mail an die Absenderin oder den Absender, denn damit wird die Richtigkeit Ihrer E-Mail-Adresse bestätigt. Als Folge könnte noch mehr Werbung im Postfach landen.
- Nur wenn es sich bei dem Absender um eine größere und bekannte Firma handelt, können Sie direkten Kontakt aufnehmen und darum bitten, die Zusendung von Werbung zu stoppen.
- Seriöse Firmen bieten in Werbe-Mails an, durch das Anklicken eines Links oder das Abschicken einer Nachricht die eigene Adresse aus dem Werbeverteiler zu entfernen. Doch auch hier ist Vorsicht geboten, da manchmal auf diese Weise versucht wird, potenzielle Kundinnen und Kunden auf Internetseiten zu locken: Das Werbebombardement erfolgt weiter.
- Wenn ein Postfach immer wieder mit Werbung von einer Adresse überflutet wird, die offensichtlich einen kostenlosen, webbasierten E-Mail-Service nutzt (wie *hotmail.com*, *web.de*, usw.), kann sich die Kontoinhaberin oder der Kontoinhaber auch direkt an diesen Dienst wenden und die störenden E-Mails an eine Beschwerdestelle weiterleiten.

Wie lässt sich SPAM verhindern?

INFO!

Es ist inzwischen nahezu unmöglich, Werbe-Mails komplett zu vermeiden. Listen mit E-Mail-Adressen werden oft innerhalb kürzester Zeit zwischen Versenderinnen und Versendern von SPAM ausgetauscht. Einige Schutzmaßnahmen können Sie und Ihre Kinder dennoch ergreifen:

- Verbreiten Sie Ihre eigene Adresse nicht überall, sondern geben Sie sie nur Personen, deren E-Mails auch wirklich erwünscht sind.
- Wenn Ihre E-Mail-Adresse auf Ihrer eigenen Homepage steht, kann diese auch für Werbesendungen missbraucht werden..
- Wer viel im Netz einkauft und dabei persönliche Informationen hinterlässt, muss damit rechnen, dass viele SPAM-Nachrichten den Weg ins eigene Postfach finden. Es ist sinnvoll, für solche Zwecke eine zweite E-Mail-Adresse bei einem kostenlosen Anbieter im Internet einzurichten. Seiten wie *hotmail.com*, *gmx.de* und *web.de* bieten nicht nur ein webbasiertes Postfach, das von jedem Computer mit Internetzugang aufgerufen werden kann; sie bieten oft hilfreiche Zusatzfunktionen, wie SPAM- und Virenfilter, die in regelmäßigen Abständen aktualisiert werden, so dass die Internetnutzerin und der Internetnutzer mit minimalem Aufwand gut geschützt ist.
- Einige Anbieter besitzen für E-Mail-Konten zusätzliche Sicherheitsvorkehrungen für Kinder.

Einen einfachen Weg, um SPAM-Mails auch vom lokalen Postfach des eigenen Computers fernzuhalten, gibt es leider nicht. Aber mit einem aktivierten Filter lässt sich die Anzahl der störenden E-Mails auch dort reduzieren.

Welchen Schutz gibt es vor Belästigungen und Beleidigungen im Internet?

In der Gemeinschaft der Internetnutzer wird es immer schwarze Schafe geben. Manche Nutzerinnen und Nutzer lassen ihre Wut oder ihre Frustration per E-Mail an anderen Menschen aus. Es gibt keine perfekten Möglichkeiten, sich vor Belästigungen im Netz zu schützen. Wichtig ist: cool bleiben und die Nachrichten ignorieren. Eltern sollten darauf drängen, dass Kinder, wenn sie das Ziel von E-Mail-Attacken sind, das Gespräch mit den Eltern oder den pädagogischen Fachkräften suchen.
Kinder nehmen Beleidigungen oft sehr ernst und es fällt ihnen manchmal schwer, Ruhe zu bewahren. Manche Leute wollen provozieren und legen es auf eine Auseinandersetzung per E-Mail an. Wenn die oder der Angeschriebene nicht reagiert, wird die Belästigung in der Regel schnell aufhören. Geht sie dennoch weiter, bietet ein Filter, der die Absender-Adresse blockt, guten Schutz vor

In der Gemeinschaft der Internetnutzer wird es immer schwarze Schafe geben.

solchen E-Mails. Standard-E-Mail-Programme wie Outlook Express oder Thunderbird (E-Mail-Client von Mozilla) bieten Filterfunktionen.

Die meisten Anbieter von kostenlosen E-Mail-Konten im Internet besitzen inzwischen ebenfalls Filterfunktionen. Sie ermöglichen, E-Mail-Adressen zu sperren, von denen Nachrichten unerwünscht sind. Filterprogramme, die Sie selbst installieren können, sind im Handel erhältlich, im Internet gibt es aber auch kostenlose Angebote.

Das Internet ist kein rechtsfreier Raum. Bedrohungen und Belästigungen können bei der Polizei angezeigt werden. Dazu ist es wichtig, die E-Mails als Beweismittel aufzubewahren.

Weitere Informationen finden Sie unter
www.mediageneration.net/eMail/index.php

Ab welchem Alter können Kinder chatten?

Ab welchem Alter können Kinder chatten?

Die meisten Chats schreiben kein Mindestalter vor. Viele sind allerdings für Kinder ungeeignet. Interessant sind Chats für jüngere Internetsurferinnen und Internetsurfer erst dann, wenn sie moderierte Bereiche, die für ihre Altersgruppen reserviert sind, anbieten. Dort wird darauf geachtet, dass niemand belästigt oder beleidigt wird, und die Regeln eingehalten werden. Wenn eine Moderatorin oder ein Moderator fit ist, geht es in solchen Chats oft viel entspannter, höflicher, lustiger und vor allem auch sicherer zu als in unmoderierten Chats. Ein Qualitätsmerkmal für einen Chat kann auch ein Hinweis der Anbieter auf eine geltende Netikette sein.

Es gibt eine ganze Reihe von Fan-Seiten zu Zeichentrick-Serien, Computerspielen, Hausaufgabenhilfen oder anderen Themen, die für Kinder attraktiv sind und oft einen eigenen Chat haben. Allerdings ist ständige Moderation durch kompetente Personen eher die Ausnahme. Darum ist es für Eltern empfehlenswert, zunächst gemeinsam mit ihren Kindern nach der passenden Kommunikationsplattform zu suchen und darüber zu reden, was an einzelnen Angeboten

interessant ist. Um die Entscheidung zu erleichtern, sollten Sie gemeinsam chatten und die anderen Besucherinnen und Besucher ein wenig über die vorherrschende Kommunikationskultur ausfragen. Gerade junge Kinder, die im Lesen und Schreiben unsicher sind, werden eine solche Maßnahme nicht als Bevormundung, sondern als willkommene Hilfestellung empfinden.

Sollte man im Chat „ehrlich“ bleiben und echte Namen / richtiges Alter / tatsächliches Geschlecht angeben?

Wenn der echte Name nicht genannt wird, bedeutet das nicht, dass Chat-Teilnehmerinnen und -teilnehmer lügen oder auf andere weniger vertrauenswürdig wirken. Im Internet ist es normal, Fantasienamen in Chats und Foren zu nutzen. Oft verraten diese so genannten „Nicknames“ sogar etwas über die Interessen einzelner Besucherinnen und Besucher. Wenn zum Beispiel ein „Harry Potter“ im Chat auftaucht, ist jedem sofort klar, dass es sich höchstwahrscheinlich um einen Fan der Bücher oder Filme handelt und dass sich die Person sicherlich gern über dieses Thema unterhalten würde.

Ob es für Ihre Kinder sinnvoll ist, ihr wahres Alter oder ihr Geschlecht zu verraten, muss situationsabhängig entschieden werden. In Chats für Kinder lassen sich leichter Gesprächspartnerinnen und -partner mit ähnlichen Interessen finden, wenn ein paar Details bekannt sind. Schließlich unterhalten sich z.B. siebenjährige Jungs im Chat über andere Themen als 15-jährige Mädchen.

Wenn aber jemand nach dem richtigen Namen, der Adresse oder Telefonnummer fragt, ist Vorsicht geboten. Der sorgfältige Umgang mit vertraulichen Daten ist für Chatter aller Altersstufen wichtig. Häufig ist unklar, wer die Chat-Partnerin oder der Chat-Partner wirklich ist und welche anderen Menschen mitlesen.

Lässt sich herausfinden, ob jemand im Chat lügt? Oder: Kann ich wirklich wissen, mit wem ich chatte?

Ob die Internetnutzerinnen und -nutzer in Chat-Räumen die Wahrheit sagen oder nicht, lässt sich nie nachprüfen. Es ist auch nicht verboten, sich eine neue Identität auszudenken. Vielleicht haben Sie auch selbst schon einmal mit dieser Möglichkeit experimentiert und gemerkt, dass so etwas reizvoll sein kann. Die Anonymität in Chats kann sogar von Vorteil sein. Beispielsweise für kontaktscheue Menschen, die sich dort frei und ohne Ängste unterhalten können. Allerdings treten manche Erwachsene selbst als Kinder auf, um sich das Vertrauen von Kindern zu erschleichen.

Der Unterschied zwischen Online-Bekanntschaften, über die außer ihrem Spitznamen nichts bekannt ist, und Freundinnen und Freunden aus der Schule oder dem Sportverein muss Kindern deutlich gemacht werden. Wenn eine Person aus dem Internet die Adresse, Telefonnummer oder andere persönliche Informationen haben möchte, kann eine falsch empfundene Vertrautheit mit einer Chat-Partnerin oder einem Chat-Partner zu vorschnellen Antworten Ihrer Kinder führen. Unangenehme Anrufe oder sogar unaufgeforderte Besuche sind zwar selten, aber dennoch eine nicht zu unterschätzende Gefahr.

Kann Chatten gefährlich werden?

Pädophile nutzen Chats und andere Bereiche des Internets, um mit Kindern Kontakt aufzunehmen. Mindestens seit dem Jahr 2000 gibt es in Deutschland dokumentierte Fälle von sexuellem Missbrauch durch Chat-Bekanntschaften. Folgende Vorsichtsmaßnahmen helfen, Ihre Kinder vor den Gefahren zu bewahren.

Was können Sie tun, um Ihren Kindern ungefährdetes Chatten zu ermöglichen? INFO!

- Wichtigste Regel: Kinder müssen wissen, dass die Weitergabe von persönlichen Informationen wie Adresse, tatsächlicher Name und Telefonnummer erhebliche Risiken mit sich bringt und niemals unbedacht erfolgen sollte. Sollten Ihre Kinder persönliche Daten weitergeben, dann nur in Absprache mit Ihnen.
- Wenn Kinder sich unbedingt mit Chat-Bekanntschaften treffen wollen, geht das nur mit folgenden Sicherheitsmaßnahmen: Nie sollten sie alleine zu einem Treff mit Bekannten aus dem Chat gehen. Unbedingt sollten sie eine erwachsene Person mitnehmen, der sie vertrauen. Das Treffen sollte an einem sicheren öffentlichen Ort stattfinden, wie beispielsweise in einem Jugendzentrum.
- Informieren Sie sich über die Internetgewohnheiten Ihrer Kinder. Lassen Sie sich von den Online-Bekanntschaften Ihrer Kinder berichten und geben Sie Tipps. Surfen Sie gemeinsam und diskutieren Sie über positive und negative Aspekte der besuchten Seiten.
- Empfehlen Sie Ihren Kindern, E-Mail-Adressen und Nicknames (Fantasienamen für Chats, Foren, usw.) zu verwenden, die keine Hinweise auf Alter, Geschlecht, Wohnort oder den richtigen Namen enthalten.
- Vermitteln Sie Ihren Kindern, warum sie keine digitalen Fotos von sich versenden sollen. Auch Bilder können im Internet grenzenlos verbreitet werden; sie können von jedem kopiert, weitergegeben, manipuliert und in neue Zusammenhänge gebracht werden. Darum gilt: Vorsicht mit Bildmaterial, besonders wenn es sich um Fotos von Kindern handelt!
- Klären Sie Ihre Kinder darüber auf, dass sie einen Chat-Raum verlassen oder einen Dialog sofort beenden sollten,
  - wenn sie zu Handlungen aufgefordert werden, die ihnen falsch oder auch nur komisch vorkommen;
  - wenn ihnen Fragen gestellt werden, die sie nicht beantworten wollen.

Durch Beachtung dieser Regeln werden viele Gefahrenquellen ausgeschaltet.

Was kann mein Kind tun, wenn es im Chat beleidigt wird oder wenn über Sachen geredet wird, die unangenehm sind? INFO!

- Eine Lösung ist, den Chat sofort zu verlassen. Es gibt viele Orte im Internet, um sich zu unterhalten; eine Ausweichmöglichkeit ist leicht zu finden. Wenn einer der liebsten Online-Aufenthaltsorte eines Kindes beeinträchtigt wird und es nur wegen eines störenden Menschen nicht darauf verzichten will, die Seite zu besuchen, ist die Lösung des Problems etwas komplizierter.

- Erklären Sie Ihrem Kind, dass die Belästigungen nur „virtuell“, also unpersönlicher Natur und deswegen zwar ärgerlich, aber nicht real bedrohlich sind (sofern keine persönlichen Angaben wie richtiger Name, Telefonnummer, Adresse, etc. weitergegeben wurden).
- Verdeutlichen Sie, warum es im Internet anders als im „wirklichen Leben“ möglich ist, Belästigungen einfach zu ignorieren oder sich zurückzuziehen.

Manche Chats bieten auch technische Lösungen bei Problemen. So lassen sich zum Beispiel Listen mit Teilnehmerinnen und Teilnehmern erstellen, die ignoriert werden sollen. Dann sind keine Nachrichten mehr sichtbar, die von diesen Personen geschrieben wurden. Am besten sehen Sie auf den Seiten des entsprechenden Anbieters nach, ob es eine Gebrauchsanleitung für den Chat gibt und mit welcher Methode sich Ihre Kinder gegen Belästigungen wehren können.

Gute Chat-Bereiche bieten eine Kontakt-E-Mail-Adresse, an die sich alle Besucherinnen und Besucher wenden können, um Beschwerden vorzubringen. Dafür ist es sinnvoll, einen Screenshot (Bild von dem, was auf dem Monitor zu sehen ist) als Beweis für die Beleidigungen zu machen und ihn zusammen mit einer Beschreibung der Probleme an die Verantwortlichen für den Chat zu schicken. Wenn Sie auf Ihrer Tastatur die Tasten „Alt“ und „Druck“ gleichzeitig drücken, wird das gesamte Bild auf Ihrem Bildschirm als .jpg-Datei zwischengespeichert. Danach öffnen Sie ein Programm, das solche Bilder verarbeiten kann (Word, Paint, Photoshop und viele andere). Durch das Drücken der Tasten „Strg“ und „V“ fügen Sie das im Speicher befindliche .jpg ein, wodurch es sich anschließend als Datei abspeichern lässt.

Moderierte Chats für Kinder finden Sie unter:
www.br-online.de/kinder
www.kindersache.de
www.seitenstark.de/chat

Ausführliche Chat-Empfehlungen, Alternativen und weitere Informationen zu diesem Thema finden Sie auf: *www.mediageneration.net/chat/index.php*

Sind Instant Messenger Programme für Kinder besser geeignet als Chat-Räume?

Instant Messaging Programme bieten eine ähnliche Kommunikationsatmosphäre wie Chats, haben aber einige Vorteile, die vor allem für jüngere Computernutzerinnen und -nutzer interessant sein können. Im Gegensatz zu den meisten Chats erlauben kostenlose Programme wie ICQ, MSN Messenger oder AOL Messenger private Gespräche zwischen Einzelpersonen. Das ist übersichtlicher als ein Chat und vereinfacht den Umgang besonders für Personen,

Instant Messaging Programme bieten Übung im Umgang mit der Tastatur.

die nicht viel Übung im Umgang mit einer Tastatur haben. Außerdem lässt sich die Software so konfigurieren, dass nur Personen Kontakt aufnehmen können, die durch die Benutzerin oder den Benutzer dazu berechtigt werden. In einer Liste können Sie die Namen von Bekannten und Verwandten speichern. Sobald ein gespeicherter Kontakt online ist und die Software gestartet ist, zeigt der Instant Messenger dies an. Durch einen Klick lässt sich ein Live-Chat-Fenster öffnen. Ein Nachteil dieser Programme ist, dass sie immer mehr zu Werbezwecken missbraucht werden und dass sie auch von anderen Nutzern belästigt werden können. Gehen Sie daher sorgfältig mit diesen Programmen um:
- Kommunizieren Sie nur mit Ihnen bekannten Personen.
- Reagieren Sie nicht auf unbekannte Absender und weisen Sie diese ab.

Ist es riskant, bei Preisausschreiben im Internet mitzumachen?

Ja, denn oft werden Preisausschreiben nur veranstaltet, um an E-Mail-Adressen oder andere Informationen von Internetnutzerinnen und -nutzern zu kommen. Bevor Ihre Kinder oder Sie an einem Gewinnspiel teilnehmen, sollten Sie immer nachlesen, was der Veranstalter mit den gespeicherten Informationen macht. Wenn zu diesem Thema keine Angaben zur Verfügung stehen, ist von der Teilnahme abzuraten.

Gerade im wenig überprüftbaren Internet ist fraglich, ob es bei einigen dieser Aktionen überhaupt etwas zu gewinnen gibt. Kinder lassen sich schnell mit Versprechen locken und geben dann unbedacht ihre persönlichen Daten an. Wenn die Adresse eingegeben wird, kann es passieren, dass immer wieder Werbung von der Firma verschickt wird, die das Preisausschreiben veranstaltet hat. Da es einen regen Handel mit Kundendaten gibt, werden eventuell auch andere Firmen aufmerksam und bewerben ihre Produkte mit Hilfe der gewonnenen Daten sowohl per E-Mail als auch mit der normalen Post.

Damit Ihre private E-Mail oder die Ihrer Kinder nicht mit nervender Werbung überflutet wird, nachdem Sie bei einem Internet-Rätsel oder Preisausschreiben mitgemacht haben, können Sie sich eine zweite E-Mail-Adresse einrichten (siehe Kapitel über E-Mails). Wenn Unsicherheit darüber herrscht, ob ein Veranstalter eventuell nur Werbung verschicken will, können Sie die zweite Adresse benutzen, wenn eine Eingabe gefordert wird. Falls dann eines Tages zu viel SPAM (Werbung) bei dieser Zweitadresse landet, kann sie einfach gelöscht und eine neue eingerichtet werden.

Welche rechtlichen Risiken bestehen, wenn Musik oder Filme aus dem Internet heruntergeladen werden? Können auch Kinder bestraft werden?

Es drohen zivilrechtliche Klagen der Musik- und Filmindustrie, die nicht nur Verbreiter von Dateien treffen, sondern auch Nutzerinnen und Nutzer, die geschützte Werke herunterladen, auch wenn dies keine Straftat darstellt. Wie hoch die Geldstrafen sind, hängt von der Menge des Materials und davon ab, wie hoch der entstandene Schaden eingeschätzt wird. Kinder unter 14 Jahren können sich laut deutscher Gesetzgebung nicht strafbar machen. Zivilrechtliche Schritte der Musik- und Filmindustrie sind aber dennoch zu befürchten und treffen möglicherweise die Eltern, die zumindest bei einem nachweislichen Verstoß gegen die Aufsichtspflicht belangt werden können.
Seit dem 13. September 2003 existiert ein neues Gesetz zu diesem Thema, das allerdings aufgrund der nicht eindeutigen Formulierung einige Fragen offen

s@ferinternet
Internet und Recht

Eltern haften für ihre Kinder!

lässt. Kopierschutzmaßnahmen digitaler Werke für kommerzielle Zwecke zu umgehen oder zu knacken sowie das öffentliche Anbieten von Dateien mit geknacktem oder übergangenem Kopierschutz sind inzwischen Straftatbestände. Damit sind auch Musik- und Filmdateien gemeint, die mit Hilfe von Internet-Tauschbörsen anderen Nutzerinnen und Nutzern zur Verfügung gestellt werden.

Unter folgendem Link finden Sie eine ausführliche Erklärung des neuen Urheberrechts und eine Sammlung von häufig gestellten Fragen und Antworten, die sich ausschließlich mit diesem Thema beschäftigt:
www.recht-im-internet.de/themen/urheber

Ist es immer illegal, Filme oder Lieder aus dem Internet herunterzuladen?

Nein, es gibt auch viele Seiten, von denen die Internetnutzerin oder der Internetnutzer ganz legal und völlig kostenlos Videos und Musik herunterladen kann. Manche Bands stellen auf ihren Webseiten einzelne Lieder zur Verfügung, die Sie und Ihre Kinder auf Ihrem Computer speichern können, ohne dafür etwas bezahlen zu müssen. Es ist auch erlaubt, Internet-Radiosendungen zu hören und gleichzeitig im MP3-Format aufzuzeichnen. Auf den offiziellen Homepages von Filmen gibt es oft Download-Bereiche, in denen Sie Ausschnitte oder Vorschauen finden. Verschiedene Firmen vermarkten ihre Filme oder ihre Musik auch als Dateien über das Internet. Gegen eine Gebühr können Sie dort komplette Spielfilme oder Musik-Alben herunterladen. Lohnenswert ist das aber nur, wenn Sie einen schnellen Internet-Zugang haben.

CNet, eine Firma, die schon seit langer Zeit die Seite *download.com* betreibt und dort kostenlose Software anbietet, hat kürzlich ein weiteres Portal gestartet, von dem Musik im MP3-Format heruntergeladen werden darf. Dank der Verpflichtung unabhängiger Künstlerinnen und Künstler ist auch dieser englischsprachige Service kostenlos:
http://music.download.com

Links zu vielen Internet-Radiostationen:
www.radiosites.de, www.surfmusik.de, www.shoutcast.com (Englisch)

Links zu legalen MP3-Angeboten:
www.tonspion.de

„Video On Demand"-Angebot von T-Online:
www.vision.t-online.de/c/10/56/45/1056454,pt-nopopup.html

Kostenpflichtige Musik-Downloads von Bild-T-Online (in der linken Leiste „Kino & Musik" anklicken, danach „Musik-Downloads"):
www.bild.t-online.de/BTO/index.html

Welche Risiken bestehen bei Internetauktionen? Wie können wir uns dagegen schützen?

Personen unter 18 Jahren sollten gar nichts selbstständig bei Internetauktionen ersteigern. Nach den allgemeinen Geschäftsbedingungen der Online-Auktionshäuser *eBay.de* und *hood.de* ist die Anmeldung nur „unbeschränkt geschäftsfähigen natürlichen Personen erlaubt. Insbesondere Minderjährigen ist eine Anmeldung untersagt".

s@ferinternet
Internet und Recht

Wichtig ist, den Text zu der angebotenen Ware genau durchzulesen.

Wenn Kinder oder Jugendliche also etwas bei eBay sehen, was sie gerne ersteigern möchten, müssen sie ihre Eltern fragen, ob sie das Geschäft in Vertretung und mit voller Übernahme der elterlichen Verantwortung durchführen dürfen. eBay ist die größte und eine der sichersten Auktionsseiten im Internet. Zwar besteht das Risiko, an eine unseriöse Person zu geraten, doch Sie können größere Schäden vermeiden: Am sichersten ist es, den Treuhandservice von eBay zu nutzen: Dann fließt Ihr Geld erst, wenn Sie die Ware erhalten haben. Wenn Sie etwas gekauft haben, die Verkäuferin oder der Verkäufer aber nicht liefert, können Sie Anzeige erstatten. In einem solchen Fall sollten Sie allerdings nachweisen können, dass die Zahlung auch wirklich stattgefunden hat. Niemals sollten Sie Geld in einem Briefumschlag bar versenden. Eine Überweisung ist da schon sicherer.

Wichtig ist, den Text zu der angebotenen Ware genau durchzulesen, um Mogelpackungen auf die Spur zu kommen.

Können über das Internet kostenlos SMS verschickt werden?

Ja, aber mittlerweile gibt es nur noch wenige Anbieter mit einem kostenlosen SMS-Service im Internet. Vorsicht ist geboten bei Seiten, die mit Gratis-Angeboten locken. Eventuell entstehen Kosten durch Downloads von Klingeltönen oder Ähnlichem. Seien Sie vorsichtig, wenn Sie zuerst aufgefordert werden, persönliche Daten (Name, Adresse, Telefonnummer) einzugeben. Vermitteln Sie Ihren Kindern, dass sie diese persönlichen Angaben auf keinen Fall preisgeben, um gratis SMS zu verschicken. Wahrscheinlich ist der Anbieter vor allem daran interessiert, Daten von potenziellen Kunden zu sammeln.

Einige wenige Internetseiten verlangen keine persönlichen Daten und ermöglichen trotzdem Gratis-Nachrichten ins Handy-Netz. Oft finanzieren sich diese Seiten durch Werbung. Das bedeutet, dass fast immer Pop-Ups auf Ihrem Bildschirm erscheinen, sobald die Angebote genutzt werden. Manchmal wird Werbung auch direkt an die SMS angehängt, die verschickt wird. Wenn Ihre Kinder sich für Internet-SMS-Dienste interessieren, aber noch wenig Erfahrung im Umgang mit Computern haben, sollten Sie bei der Suche und Nutzung helfen, damit es nicht zur Weitergabe persönlicher Daten kommt oder unerwartete Kosten entstehen.

Empfehlenswert ist der SMS-Dienst in der Werkstatt der Kinderseite des Internet-ABC's (*www.internet-abc.de*). Nachdem ein kleines SMS-Rätsel gelöst wurde, können die Kinder mehrere SMS mit 140 Zeichen versenden, ohne weitere Angaben machen zu müssen.

INFO! Was können meine Kinder und ich gegen SMS-Werbung tun?

- Das Wichtigste ist, die Handy-Nummer nicht jedem mitzuteilen. Ohne die Eingabe der Handy-Nummer im Internet und den Eintrag ins Telefonbuch ist es für Versender von Werbung sehr viel schwieriger, Werbung zu schicken.
- Bleiben Sie und Ihre Familie informiert über die neuen Tricks der Firmen. Wenn Sie eine SMS von einer 0190er-Nummer erhalten, sollte diese ungelesen gelöscht werden. Oft locken die Nachrichten mit unseriösen Behauptungen, zum Beispiel, dass die Empfängerin oder der Empfänger der SMS bei einem Gewinnspiel gewonnen hätte. Eine Antwort genügt angeblich, um den Gewinn zu erhalten. In Wirklichkeit kostet die Antwort aber mehrere Euro und der Gewinn bleibt aus. Es ist nicht immer leicht zu erkennen, ob eine Nachricht oder ein entgangener Anruf ein Lockangebot ist. Wichtig ist ein Blick auf die Vorwahl, denn der Rückruf führt eventuell ins Ausland oder zu einer teuren Service-Hotline. Auch Kinder können erkennen, ob eine Nummer verdächtig ist, wenn sie entsprechend von Ihnen informiert wurden.

Das Wichtigste ist, die Handy-Nummer nicht jedem mitzuteilen.

- Es ist sinnvoll, Nummern von Unbekannten gleich nach dem Erhalt einer SMS zu löschen. Wenn ein Handy mit Werbe-SMS überflutet wird, kann die Besitzerin bzw. der Besitzer auch die Handynummer ändern lassen. Leider ist das nicht kostenlos und sollte daher der letzte Ausweg sein.

Was mache ich, wenn in der Familie ein Handy abhanden gekommen ist? INFO!

- Nach Verlust des Handys sollte umgehend der Netzanbieter informiert werden. Falls das Handy mit einer PrePaid-Karte betrieben wurde, hält sich der Schaden in Grenzen. Sobald das Guthaben auf der Karte abtelefoniert ist, fallen für die Besitzerin oder den Besitzer keine weiteren Kosten an.

- Bei einem Handy mit Vertrag müssen Handy und SIM-Karte so schnell wie möglich gesperrt werden, denn bis zur Sperrung kann auf Kosten der Handy-Besitzerin oder des -Besitzers telefoniert werden. Einige Firmen bieten eine Haftungsgrenze für solche Fälle an, die sehr hohe Kosten verhindert. Ein Teil des Schadens muss jedoch immer selbst bezahlt werden. Sichern Sie sich und Ihre Kinder dagegen ab! Es ist wichtig, den PIN-Code für Ihre Karte nicht zu deaktivieren. Die Benutzung einer Zahlenkombination bietet Schutz vor unberechtigtem Zugriff auf Ihr Handy.
- Aktuelle Mobiltelefone bieten oft mehrere Sicherheitsmöglichkeiten an. Jede Handy-Nutzerin und jeder Handy-Nutzer sollte mit diesen Funktionen vertraut sein und möglichst viele Sicherheitseinstellungen nutzen. Reden Sie mit Ihren Kindern über den Sinn und Zweck solcher Schutzmechanismen und erklären Sie, warum es wichtig ist, Nummerncodes nicht zu deaktivieren, obwohl so die Bedienung vereinfacht wird.
- Bewahren Sie Unterlagen des Handys auf. Vor allem die IMEI-Nummer (International Mobile Equipment Identifier) ist wichtig, wenn Sie das Telefon sperren lassen möchten oder als gestohlen melden müssen. Diese IMEI-Identifikationsnummer steht oft auch unter dem Akku oder Sie geben folgende Kombination ein, um sie zu erhalten: *#06#

Wie kann ich verhindern, dass die Handykosten meiner Kinder zu hoch ausfallen?

Besonders im Handy-Bereich gibt es viele kostenpflichtige Dienstleistungen, die für Kinder faszinierend sind z.B das Verschicken von SMS oder das Herunterladen von Bildern und Klingeltönen. Nehmen Sie diese Interessen der Kinder ernst. Diskutieren Sie darüber und sprechen Sie nicht vorschnell Verbote aus, selbst wenn der Nutzen solcher Angebote nicht immer nachvollziehbar ist.

- Informieren Sie sich und Ihre Kinder genau über die Preise und reden Sie über überhöhte Kosten. Wenn Ihre Kinder noch kein ausreichendes Gefühl für den Umgang mit Geld entwickelt haben, können Sie die Preise für Handy-Dienste in Relation zu anderen Waren setzen, um zu verdeutlichen, wie teuer manche Angebote sind. Treffen Sie feste Abmachungen mit Ihren Kindern, um die Kosten gering zu halten. Denkbar ist eine klare Regelung der Anzahl von SMS-Mitteilungen, die pro Woche verschickt werden dürfen. Oder Sie legen eine Euro-Obergrenze für die Handy-Nutzung fest.
- Auch eine PrePaid-Karte ohne Vertragsbindung ist eine Überlegung wert. Zwar ist das Telefonieren mit solchen Karten teurer, aber da das Euro-Limit nicht überzogen werden kann, ist diese Variante empfehlenswert, wenn Ihre Kinder Probleme haben, die Kosten selbstständig zu überblicken.

s@ferinternet
Handy

- Ihre Kinder sollten grundsätzlich teure 0190/0900er-Nummern meiden, die auch häufig genutzt werden, um Angebote wie Klingeltöne oder Logos abzurechnen. Vorsicht ist auch bei 0137er- und 0180er-Nummern geboten, da diese manchmal neue Verbindungen zu 0190/0900er-Nummern herstellen können. Ein neuer Klingelton ist häufig sehr teuer, wenn man ihn herunterlädt und sollte deshalb eine Ausnahme sein, wie der Kauf einer CD, auch wenn diese Handyfunktion unter Kindern oft einem Statussymbol gleichkommt. 0190/0900er-Nummern lassen sich auch sperren. Wünschenswerter ist aber, dass Ihre Kinder selbst kompetente Entscheidungen in diesem Bereich treffen können und sich an getroffene Vereinbarungen halten.
- Dies betrifft auch den Umgang mit Premium SMS-Nummern. Premium SMS-Dienste bieten Angebote und Dienstleistungen wie Klingeltöne, Chats, Spiele-Downloads oder Teilnahme an Gewinnspielen. Bezahlt wird dabei mit dem

Versenden einer SMS an eine fünfstellige Nummer. Die Preise lagen bisher zwischen 0,29 und 3 Euro. In naher Zukunft können diese Dienste auch bis zu 50 Euro pro SMS kosten.
An der SMS-Servicenummer selbst ist nicht erkennbar, welche Kosten sie verursachen. Verstärkt nutzen auch unseriöse Geschäftsleute die SMS-Servicenummern für ihre Zwecke und versuchen mit Tricks, Handybesitzer zum Versand möglichst vieler teurer SMS zu bewegen – Kinder und Jugendliche sind wegen ihrer Arglosigkeit besonders beliebte Opfer.

- Das Verschicken von SMS und das Telefonieren sind oft deutlich günstiger, wenn die Teilnehmerinnen und Teilnehmer das gleiche Netz nutzen. Informieren Sie sich also darüber, bei welchen Anbietern die Freundinnen und Freunde Ihrer Kinder sind und wechseln Sie eventuell selbst das Netz, um die Kosten gering zu halten. Reden Sie auch mit anderen Eltern über günstige Tarife.

Weitere Informationen finden Sie unter
www.mediageneration.net/handy/index.php

3G / UMTS
Die neueste Art von Handys. 3G ist eine Abkürzung für dritte Generation und beschreibt den derzeitigen Entwicklungsstand der mobilen Geräte. UMTS ist die Kurzform für „Universal Mobile Telecommunications System“. UMTS erlaubt es der Benutzerin und dem Benutzer, immer in Verbindung zum Internet zu bleiben und große Dateien, wie zum Beispiel Videos, an andere Handys zu verschicken. Sicher werden mit der zunehmenden UMTS-Verbreitung neue Jugendschutzprobleme auf uns zukommen.

ActiveX
ActiveX ist eine von Microsoft eingeführte Technologie, die in aktuellen Versionen des Microsoft Internet Explorers integriert und für Netscape als Erweiterung zum Herunterladen erhältlich ist. Durch ActiveX, das als Konkurrenzprodukt zu JavaScript gedacht ist, können Programmabläufe in Internetseiten eingebunden werden. Das ermöglicht kleine Internet-Spiele, Chats, Animationen und andere Inhalte. Allerdings stellt diese Zusatzfunktion auch eine Sicherheitslücke dar, die es Hackern erlaubt, auf fremde Computer zuzugreifen. Es empfiehlt sich, ActiveX zu deaktivieren, wenn keine Seiten genutzt werden, die diese Technologie benötigen.

Anti-Viren-Programme
Programme, mit denen Sie alle Dateien und E-Mails auf dem Computer auf Viren untersuchen können. Gute Anti-Viren-Programme überwachen den Rechner ständig, warnen vor verseuchten Dateien und sind in der Lage, Viren zu entfernen. Anti-Viren-Programme müssen regelmäßig aktualisiert werden.

Backup
Mit Backup wird eine Sicherheitskopie eines Datenbestandes bezeichnet. Bei Datenverlust, Zerstörung oder Virenbefall ermöglicht sie die Wiederherstellung der Daten.

Browser
Programm, mit dem Sie sich Webseiten ansehen können. Die bekanntesten Browser sind der Internet Explorer und Netscape. Immer mehr Computernutzerinnen und Computernutzer verwenden auch Mozilla, Firefox oder Opera, also Browser, die nur wenige Sicherheitslücken haben und keine Werbefenster zulassen.

Chat
Kommunikation zwischen Internetbesucherinnen und -besuchern, die in Echtzeit (live) abläuft. In der Regel wird in Chats via Tastatur kommuniziert. Es gibt auch die Möglichkeit, direkt mit anderen zu sprechen, diese Variante nennt sich Voice-Chat.

Cracker
Jemand, der sich in böser Absicht unautorisierten Zugriff auf ein Rechnersystem verschafft, um dort Daten zu manipulieren oder auch die Lizenzierungsfunktion von Software „auszuschalten".

Konfiguration
Wenn man bestimmte Einstellungen innerhalb eines Programms vornimmt, um es beispielsweise besser an die eigenen Bedürfnisse anzupassen, nennt sich diese Tätigkeit Konfiguration.

Cybertrail
Cybertrail sind die Spuren, die die Nutzerin oder der Nutzer hinterlässt, wenn sie oder er das Internet nutzt. Daten wie Uhrzeit, Datum und IP-Adresse eines Computers werden auf dem Server in einem so genannten Logfile (Datei, die Aktivitäten eines Computers protokolliert) gespeichert.

Desktop
Bezeichnung für die Arbeitsoberfläche auf dem Bildschirm, die nach der Anmeldung beim Betriebssystem erscheint.

Dialer
Ein Einwahlprogramm, das eine Verbindung zum Internet unterbricht und einen neuen Internetzugang einrichtet, für den in der Regel hohe Kosten anfallen.

Dialogfenster
Ein Dialogfenster wird eingeblendet, wenn Sie die Wahl zwischen verschiedenen Optionen haben oder wenn weitere Angaben gemacht werden müssen.

Download
Herunterladen von Dateien oder Programmen aus dem Internet auf den eigenen Computer.

DSL
Die Abkürzung DSL steht für „Digital Subscriber Line". Mit Hilfe dieser Technik, die ein spezielles Modem voraussetzt, sind wesentlich schnellere Verbindungen zum Internet möglich. Durch das Aufsplitten der Bandbreite in unterschiedliche Kanäle und die Nutzung mehrerer Frequenzbereiche wird die Geschwindigkeit des Datentransfers über Kupferkabel erhöht.

E-Mail
Electronic mail (deutsch: elektronische Post) zum Versenden und Empfangen von Nachrichten über das Internet.

Encryption (Verschlüsselung)
Um eine sichere Übermittlung zu gewährleisten, werden Daten verschlüsselt („encrypted") verschickt. Das bedeutet, dass man ein Passwort oder einen Code benötigt, um die Daten wieder benutzen bzw. lesen zu können. Unverschlüsselte Daten nennt man „plain text" (normaler Text), verschlüsselte Daten nennt man „cipher text". Die Aufschlüsselung wird als „decryption" bezeichnet.

Firewall
Programme, die dafür sorgen, dass sich niemand unberechtigten Zugang zu einem Computer verschaffen kann. Sie überprüfen jede eingehende und verschickte Nachricht. Wenn eine nicht ausdrücklich genehmigte Verbindung hergestellt wird, informiert die Firewall die Nutzerin oder den Nutzer. Absolute Sicherheit bietet auch eine Firewall nicht. Sie schützt beispielsweise nicht vor Dialern.

Forum
Eine Kommunikationsplattform im Internet, die im Gegensatz zu Chats nicht in Echtzeit abläuft. Textbeiträge werden gespeichert und können auch nach langer Zeit noch von anderen Forumsbesucherinnen und -besuchern gelesen und beantwortet werden.

Freeware
Software, die ohne Schutzgebühr aus dem Internet heruntergeladen werden darf oder auf anderen Datenträgern (CD-ROM, Diskette) gespeichert ist.

Hacker
Expertinnen und Experten für Programmiersprachen oder Computersysteme, die sich unerlaubt Zugang zu Computern verschaffen, um Daten zu stehlen oder zu zerstören.

Header
Der oberste Teil einer E-Mail, in dem die IP-Adresse der Absenderin oder des Absenders und der Name der Empfängerin oder des Empfängers steht.

Hoax (dt.: schlechter Scherz)
Hoax sind falsche Warnungen vor bösartigen Computerprogrammen, die angeblich Festplatten löschen, Daten ausspionieren oder anderweitig Schaden auf den Rechnern der Betroffenen anrichten sollen. Sie richten Schaden an, wenn Personen den Anweisungen dieser Falschmeldungen folgen und Systemdateien oder Ähnliches von ihrem Computer löschen, um angeblich entstehende Schäden zu verhindern.

HTML
HTML (Hypertext Markup Language) ist die Programmiersprache für die meisten Seiten im World Wide Web. Der Browser liest diese Sprache und setzt die darin enthaltenen Informationen (wie zum Beispiel Schriftart und Größe) zur entsprechenden Darstellung auf dem Monitor um. HTML bietet die Möglichkeit, Verweise auf andere Seiten im Netz zu integrieren (Links), die durch einen Mausklick aktiviert werden können.

Instant Messaging
Instant Messaging Programme (zum Beispiel ICQ) übermitteln ohne nennenswerte Wartezeiten Texte, wenn die Empfängerin oder der Empfänger gleichzeitig online sind. Auch der Austausch von Dateien ist über solche Dienste möglich.

IP-Adresse (Internet Protocol)
Jedem Computer, der online ist, wird eine IP-Adresse zugeordnet. Diese IP-Adresse dient dazu, einen einzelnen Rechner zu identifizieren. (Beispiel für IP-Adresse: 127.32.8.191)

Internet Service Provider
Ein ISP (Internet Service Provider) ist eine Firma, die den Zugang zum Internet ermöglicht.

JavaScript
Ähnlich wie ActiveX ist auch JavaScript ein Zusatz für den Browser und ermöglicht weitere Funktionen auf Webseiten. Kleine Spiele, Animationen und andere Programmabläufe werden durch JavaScript ermöglicht. Allerdings stellt diese Technologie auch eine Sicherheitslücke dar, die es Hackern erlauben könnte, auf fremde Computer zuzugreifen, wenn nicht die nötigen Sicherheitsmaßnahmen ergriffen wurden. Aus diesem Grund empfiehlt es sich, JavaScript zu deaktivieren, wenn keine Seiten besucht werden, die diesen Zusatz benötigen.

JPEG / .jpg
Diese Abkürzung steht für „Joint Photographic Experts Group“. Diese Gruppe hat ein Kompressionsverfahren für digitales Bildmaterial entwickelt. Bilder im .jpg-Format werden, genau wie .gif-Dateien, oft im Internet verwendet, da sie wenig Speicherplatz benötigen und deshalb schnell laden.

Emoticon
Zeichen, die aus dem normalen Zeichensatz einer Tastatur zusammengesetzt sind und dazu dienen, Gefühle auszudrücken. Die meisten Emoticons bestehen aus zwei bis vier Zeichen und oft wird ein Gesicht dargestellt. Beispiele: :-) (lustig), :-((traurig), :-O (geschockt)

Lesezeichen (Bookmarks)
Eine im Browser hinterlegte persönliche Liste wichtiger Internetadressen oder häufig besuchter Seiten. Damit genügt ein Klick auf die gewünschte Adresse, um auf deren Seite zu gelangen, ohne dass die gesamte Internetadresse selbst eingetippt werden muss.

Moderierter Chat-Raum
Ein Chat-Raum, der von einer einzelnen Person oder einer Gruppe überwacht wird. Die so genannten Moderatorinnen oder Moderatoren haben die Möglichkeit, Nachrichten zu blockieren oder Besucherinnen und Besucher auszuschließen, wenn diese gegen bestimmte Regeln (zum Beispiel die Netikette) verstoßen.

Netstat
Ein kleines Programm, mit dem die IP-Adresse von anderen Internet-Nutzerinnen und -nutzern herausgefunden werden kann.

Netikette / Netiquette
Das Wort Netikette steht für die Regeln der Höflichkeit im Internet. Es gilt zum Beispiel als unhöflich, einen Text in Großbuchstaben zu schreiben, da dies im Cyberspace als Schreien angesehen wird. Es gibt mehrere Varianten der Netikette, allerdings hat sie ursprünglich keine feste Form, sondern basiert auf unausgesprochenen Regeln.

Netzwerk (engl.: network)
Miteinander verbundene Computer, deren Daten untereinander ausgetauscht werden können.

Nickname (dt.: Spitzname)
Pseudonyme, die von Internetbesucherinnen und -besuchern statt ihrer tatsächlichen Namen verwendet werden. Diese Spitznamen werden in Foren, Chats und Instant Messaging Systemen eingesetzt und sind manchmal auch in E-Mail-Adressen integriert.

Patch
Eine Datei, die genutzt wird, um Fehler oder Sicherheitslücken in einem Programm zu beseitigen. Patches können ein Programm in bestimmten Bereichen verändern oder erweitern.

Peer-to-Peer (P2P)
„peer" - englisch - bedeutet „Gleichgestellter" oder „Ebenbürtiger". Peer-to-Peer Netzwerke sind Netzwerksysteme, in denen alle Rechner gleichberechtigt agieren. Eine Datenverbindung besteht dabei immer direkt von einem Teilnehmer zum anderen, ohne Zwischenschaltung eines Netzwerk-Servers. Durch die Peer-to-Peer-Technik können Internetnutzerinnen und -nutzer direkt auf die Datenbanken bzw. freigegebenen Ressourcen anderer Nutzerinnen und Nutzer bzw. ihrer Rechner zugreifen. Beliebte Einsatzgebiete sind deshalb auch Tauschbörsen.

Pop-Up (-Fenster)
Pop-Ups, die meist zu Werbezwecken verwendet werden, sind Internetseiten bzw. Bilder oder Nachrichten die meist selbsttätig als zusätzliches (Aufklapp-) Fenster aufgehen. Bedingt Abhilfe bieten sogenannte Pop-Up-Blocker, die solche Fenster unterdrücken, allerdings auch die gutgemeinten.

Profil (Englisch: Profile)
In einem Chat-Room versteht man unter dem Begriff „Profil“ eine Art Steckbrief mit Informationen über einzelne Besucherinnen und Besucher. Das Profil wird von der Nutzerin oder dem Nutzer selbst auf der Chat-Seite eingegeben. Manchmal ist es sinnvoll, Alter oder Hobbys einzugeben, um Chatter zu treffen, die sich über ähnliche Themen unterhalten wollen.

Server
Ein meist leistungsfähiger Computer, der bestimmte Aufgaben für andere Rechner in einem Netzwerk ausführt.

Shareware
Programme die man für bestimmte Zeit kostenlos benutzen darf, für die aber später gezahlt werden kann oder muss, wenn man sie weiter verwenden möchte.

SPAM (Werbemüll)
Unerbetene ektronische Nachrichten, die Werbung für Produkte oder Internetseiten enthalten.

Spyware

Glossar

Das Wort Spy heißt übersetzt Spion. Spyware kann unbemerkt mit einer anderen Datei aus dem Internet geladen werden und gibt bestimmte Informationen über die eigenen Computeraktivitäten an Dritte weiter.

Suchmaschine
Programme, mit deren Hilfe Sie im Internet Dokumente zu Themen finden. Zusätzlich können Sie Internetseiten nach bestimmten Wörtern durchsuchen. Wenn die Suche beendet ist, werden die Resultate gezeigt.

URL
Eine URL (Abkürzung für Uniform Resource Locator) ist eine Internet-Adresse und wird vom Browser benötigt, um eine bestimmte Webseite im Netz zu finden.

Virenscanner
Programm, das Dateien auf Virenbefall überprüft und der Computernutzerin/dem Computernutzer anschließend Meldung über gefundene Viren erstattet. Anti-Viren-Programme enthalten in der Regel sowohl einen Virenscanner als auch Werkzeuge zum Entfernen oder Reinigen von betroffenen Dateien.

Virus
Programm oder ein Teil eines Computercodes, das/der sich unbemerkt auf einem Rechner installiert und ungewollt verschiedene Prozesse in Gang setzen kann. Ein Virus kann zum Beispiel dafür sorgen, dass ein Rechner abstürzt oder dass Dateien beschädigt werden.

WWW
Das World Wide Web (weltweites Netz) ist ein System von Servern, das es den Benutzerinnen und Benutzern ermöglicht, Verknüpfungen von einer Internetseite zu einer anderen zu erstellen und zu nutzen.

Wurm
Ein Virus, der sich über ein gesamtes Netzwerk ausbreitet, indem er sich meist selbst verschickt. Würmer können zu einem Computerabsturz führen.

Impressum

Herausgeber: GMK

Autoren: Dagmar Kerschbaumer, Tim Beckmann

Idee, Konzept, Endredaktion: Dagmar Kerschbaumer

Redaktion: Slim Florian Bacha, Tim Beckmann, Kathleen Gerber, Jürgen Lauffer, Kirsten Mattheis, Bianca Post, Barbara Rathert, Renate Röllecke, Lajos Speck sowie Anke Hildebrandt und Kristina Schottka

Grafisches Konzept: Sigrid Zinser, Mane Huchler

Grafik-Design: Pia Castrup, Visart

Fotos: Markus Faust, Visart

Fotocopyright: Visart 2005, www.visart.de /
Schwarzes Schaf - (c) Detlef Nerstheimer www.net-photo.de

Gefördert durch die Information Society der Europäischen Union
und das Bundesministerium für Familien, Senioren, Frauen und Jugend

Druck: AJZ-Druck & Verlag, Bielefeld, 2005

Bezug und Information:

GMK
Gesellschaft für
Medienpädagogik und Kommunikationskultur

Gesellschaft für
Medienpädagogik und Kommunikationskultur (GMK)
Körnerstraße 3
33602 Bielefeld
Tel: 0521-67787
Fax: 0521-67727
www.gmk-net.de
www.mediageneration.net
www.safernet.info
gmk@medienpaed.de