Leitfaden für Eltern

Schützen Sie Ihre Kinder online

Deutsche Version unterstützt von:

Unterstützt von:

INHALT

A. Anwendung dieser Broschüre

Wenn Sie für ein Jahr planen, pflanzen Sie Reis.
Wenn Sie für zehn Jahre planen, pflanzen Sie einen Baum.
Wenn Sie für ein ganzes Leben planen, erziehen Sie Ihr Kind.

Chinesisches Sprichwort

Liebe Eltern und PädagogInnen,

Sie halten das e-Sicherheits-Kit für Familien mit Kindern zwischen 6 und 12 Jahren in Händen. Dieses Material wurde in dem festen Glauben erstellt, dass neue Technologien die Generationen nicht trennen, sondern ganz im Gegenteil die Kluft zwischen ihnen überbrücken helfen. Es wurde mit dem Fachwissen von Insafe zusammengestellt, dem paneuropäischen Netzwerk nationaler Kontaktzentren, die an der Förderung des Bewusstseins für Themen im Bereich einer sichereren Nutzung des Internets arbeiten. Die Entwicklung und Herstellung dieses e-Sicherheits-Kits wurde von UPC unterstützt.

Genau wie das Spielen auf dem Spielplatz oder das Überqueren einer Straße gefährlich sein kann, wenn man nicht aufpasst, kann die Nutzung des Internets und der mobilen Technologien Gefahren für unachtsame Nutzer mit sich bringen. Glücklicherweise gibt es Hilfsmittel, um den InternetnutzerInnen die nötigen Kenntnisse über die Vorteile und Risiken des Web zu vermitteln.

Anhand dieses neuen Kits können Sie Ihren Kindern dabei helfen, die sichere und effiziente Nutzung des Internets zu lernen. Das Kit bietet über 50 Sicherheitstipps und Übungen, die Ihnen dabei helfen werden, Ihren Kindern die e-Sicherheit auf amüsante, ansprechende und nicht beängstigende Art beizubringen. Es enthält unter anderem:

- Zwei e-Sicherheits-Broschüren: eine Broschüre für die ganze Familie und einen Leitfaden für Eltern
- Goldene Regeln
- Ein Familienzertifikat
- Aufkleber
- 12 Situationskarten zum Ausschneiden für die Kinder

Sowohl die Familien- als auch die Elternbroschüre sind farblich gekennzeichnet, um die vier e-Sicherheits-Themen hervorzuheben: Sicherheit, Kommunikation, Cyber-Mobbing und Unterhaltung & Herunterladen. Der Eltern-Leitfaden dient als Referenz für die Familienbroschüre: Er enthält Hintergrundinformationen, Hinweise zu den Übungen, vorgeschlagene Lösungen zu den Übungen und Situationskarten.

Die Familienbroschüre ist für die gemeinsame Verwendung von Eltern und Kindern gedacht. Die vier Themen werden anhand der Geschichte von zwei Jugendlichen, Alex und Marie, ihren Eltern und dem Informatikgenie Tina behandelt. Jedes Kapitel enthält lehrreiche Übungen, einschließlich Online-Übungen, Ratespiele, Goldene Regeln und nützliche Links.

Lesen Sie die Geschichte laut mit Ihren Kindern und führen Sie die vorgeschlagenen Übungen zusammen durch. Am Ende jedes Kapitels können Sie anhand der jeweiligen Situationskarten eine Diskussion mit Ihren Kindern anregen, um das Verständnis des Inhalts zu vertiefen.

Wenn Ihre Kinder das Kit erfolgreich durchgenommen haben, können Sie diese belohnen, indem alle gemeinsam einige Goldene Regeln festlegen und das Familienzertifikat unterschreiben. Schließlich können die Kinder die Broschüren mit Emoticon-Aufklebern verzieren.

Viel Spaß beim sicheren Surfen im Internet

wünscht Ihnen

ins@fe

1. Sicherheit

EIN COMPUTER ZU H@USE

Ein Computer zu Hause kann für die ganze Familie eine großartige Bildungsressource und Freizeitbeschäftigung sein. Wenn Sie den Computer in einem gemeinsam genutzten Raum aufstellen und bestimmte Regeln hinsichtlich der Verwendung und Benutzungsdauer festlegen, beschützen Sie damit Ihre jungen Familienmitglieder.

Denken Sie daran, dass Ihre Kinder auch bei FreundInnen, in Internetcafés usw. Zugang zum **Internet** haben. Deshalb ist es wichtig, dass Sie gemeinsam einen Verhaltenskodex festlegen, den sie immer und überall anwenden können.

SICHERUNG IHRES COMPUTERS

Sicherheit kann durch ein grundsätzliches Verständnis potenzieller Gefahren und die Kenntnis einfacher Lösungen erreicht werden. Diese Lösungen beinhalten nützliche technologische

Hilfsmittel und auch den gesunden Menschenverstand des Benutzers/der Benutzerin. Wie in allen Bereichen entwickelt sich der gesunde Menschenverstand mit dem Alter und der Praxis.

Die Sachen, die Sie und Ihre Kinder wahrscheinlich auf Ihrem Computer tun werden, wie die Verwendung von **USB-Sticks** oder **CD-ROMs**, das Öffnen von **Anhängen** und das **Herunterladen** von **Dateien**, können Gefahren bergen. Diese Risiken bestehen größtenteils aus heimtückischen **Computerprogrammen (Malware)**, die entworfen wurden, um Ihrem Computer zu schaden, persönliche Informationen zu stehlen oder Ihnen unerwünschte Werbung zu schicken.

Den Kindern werden verschiedene Arten von Malware vorgestellt – **Viren**, **Würmer**, **Trojaner** und **Spyware** – und sie erfahren, wie sie die Symptome eines infizierten Computers erkennen können. Sie lernen, wie sie einer Infektion vorbeugen können, indem sie das Internet nur auf Computern benutzen, die durch aktuelle **Anti-Virus-Programme** und **Anti-Spyware** geschützt sind. Es wird ihnen auch geraten, bei E-Mail-Anhängen von unbekannten Absendern, beim Herunterladen von Programmen aus dem Internet und bei der Benutzung von USB-Sticks oder CD-ROMs vorsichtig zu sein.

DER KAMPF GEGEN SPAM

80 Prozent der im Internet zirkulierenden E-Mails sind **Spam** (unerwünschte E-Mails), die Ihre Kinder leicht beeinflussen können. Die unachtsame Angabe einer **E-Mail-Adresse** im Web bei der Benutzung einer **News-Group**, einer **Chat**-Seite, eines öffentlichen **Forums**, einer **Social Networking Seite** oder eines **Online-Forums** kann Spam verursachen. Es gibt besondere Software, die E-Mail-Adressen aus dem Web sammelt, um Mailinglisten zusammenzustellen. Diese werden dann benutzt, um große Mengen an Spam zu verschicken. Die Gesellschaften, die sich solcher Aktivitäten bedienen, befinden sich oft in Ländern, deren Gesetzgebung unerwünschten E-Mails keinen Einhalt gebietet.

Spam-Mails stehen oft in Zusammenhang mit Pornografie, Pharmazeutika, dubiosen finanziellen Transaktionen usw. Darüber hinaus kann Spam auch die Quelle heimtückischer Programme sein. In den meisten Fällen wird Spam mit betrügerischen Absichten verschickt. Hier einige Tipps, wie Sie Ihre Familie schützen können:

- Benutzen Sie **Spam-Filter**. Ihr E-Mail-Anbieter bietet normalerweise Anti-Spam-Optionen an, die Sie in Ihrem E-Mail-Programm aktivieren können. Kontaktieren Sie Ihren E-Mail-Anbieter für weitere Informationen. Prüfen Sie regelmäßig Ihren **Junk**- oder **Spam-Ordner**, um zu sehen, ob unerwünschte E-Mails hier gelandet sind. Die Filter sind allerdings nicht hundertprozentig sicher.
- Bringen Sie Ihren Kindern bei, nie E-Mails von unbekannten Personen zu öffnen. Spam enthält meistens viel versprechende Angebote und Anhänge. Zeigen Sie ihnen, wie sie den Absender einer E-Mail blockieren können, oder bitten Sie sie einfach, verdächtige Mails zu löschen.

SURFEN IM NETZ

Sogar sehr junge Kinder können vom Surfen im Internet profitieren, um sich zu amüsieren und informative Webseiten zu besuchen. Das Internet enthält jedoch auch Inhalte, die nicht immer altersgemäß sind.

Suchmaschinen sind eine große Hilfe bei der Suche nach Inhalten im Internet. Da die Suche jedoch von einer Reihe von Stichwörtern abhängt, ist es auch sehr leicht, unerwünschte Inhalte zu finden. Ein unschuldig klingendes Stichwort könnte zu einer nicht so unschuldigen Webseite führen, die das fragliche Stichwort enthält. Hier einige Tipps, um Ihren Kindern dabei zu helfen, sicherer im Internet zu surfen:

- Erstellen Sie ein spezielles Benutzerkonto für Ihr Kind mithilfe eines **Betriebssystems** (Windows, Linux, Mac OS), in dem Sie die elterliche **Kontrolle** für dieses Konto aktivieren können.

- Machen Sie sich mit den Optionen der elterlichen Kontrolle in Ihrem **Internetbrowser** und in der Suchmaschine vertraut. Vergewissern Sie sich, dass Sie alle Möglichkeiten der **Familieneinstellungen** dieser Hilfsmittel kennen.

- Schlagen Sie den jungen InternetnutzerInnen unter Ihrer Aufsicht kinderfreundliche Suchmaschinen vor, zum Beispiel *www.fragfinn.de, www.blinde-kuh.de, www.helles-koepfchen.de, www.milkmoon.de.* Speichern Sie die Adressen der Webseiten, die Ihre Kinder am häufigsten besuchen, in ihren Favoriten- (Internet Explorer) oder Lesezeichen-Ordner (Mozilla Firefox). So ermöglichen Sie es ihnen, ihre Lieblingsseiten im **Internet** immer wieder zu besuchen, ohne eine Suchmaschine benutzen zu müssen.

Neben den familienfreundlichen Einstellungen Ihres **Browsers** und der Suchmaschine können Sie noch einen zusätzlichen **Filter** benutzen: Eine Software, die Minderjährige vor den unangebrachten Inhalten des Web schützen soll. Weitere Informationen zu Jugendschutzprogrammen finden Sie auf folgenden Internetseiten: www.kjm-online.de und www.klicksafe.de. Denken Sie aber immer daran, dass nichts die Beratung durch die Eltern und PädagogInnen ersetzen kann. Technische Hilfsmittel sind nicht hundertprozentig sicher und können manchmal ein falsches Gefühl der Sicherheit hervorrufen, wenn man nicht zusätzlich seinen gesunden Menschenverstand benutzt.

Filtersoftware kann auch so einschränkend sein, dass sogar harmlose Inhalte blockiert werden können. Sie kann zum Beispiel Kinder davon abhalten, Informationen für einen geschichtlichen Aufsatz über den Zweiten Weltkrieg zu recherchieren, weil die Suche auch zu Webseiten führt, die Gewalt beschreiben. Außerdem kann jeder Filter, der eingeschaltet werden kann, von cleveren Jugendlichen ausgeschaltet werden, die oft auch ExpertInnen der Spurenverwischung sind. Sie können dies nur herausfinden, indem Sie selber lernen, wie man den Computer und die Software benutzt.

Außer der Vermeidung von **schädlichem Inhalt** sollten Sie sich außerdem vergewissern, dass Ihre Kinder nicht alles glauben, was sie im Internet sehen oder lesen. In der Unterhaltungsbroschüre für die Familie schlagen wir vor, dass sie bei der Suche nach Informationen online immer mindestens drei Webseiten besuchen, um die Inhalte zu vergleichen. Es wird ihnen gleichzeitig auch geraten, immer systematisch die Informationsquelle zu erwähnen, wenn sie die Angaben für eine Schularbeit benutzen.

GOLDENE REGELN FÜR ELTERN SURFENDER KINDER

- Vergewissern Sie sich, dass Ihr Computer durch eine **Firewall** sowie durch Anti-Virus-Software und Anti-Spyware geschützt ist. Sorgen Sie dafür, dass diese stets auf dem neuesten Stand sind, und beachten Sie die **Warnungen**. Prüfen Sie, ob Ihr Internetanbieter Anti-Virus-Hilfsmittel und Anti-Spyware anbietet, die Sie benutzen können.

- Benutzen Sie einen Spam-Filter in Ihrem E-Mail-Programm und halten Sie Ihre E-Mail-Adresse so geheim wie möglich, indem Sie sie nicht im Web veröffentlichen. Öffnen Sie E-Mails von unbekannten Absendern nicht und **scannen** Sie die Anhänge, bevor Sie sie öffnen.

- Maximieren Sie die elterliche Kontrolle Ihrer Software: In Ihrem Betriebssystem, Ihrem Internetbrowser, Ihrer Suchmaschine und im E-Mail-Programm. Schaffen Sie getrennte **Benutzerkonten** für sich und Ihre Kinder. Versichern Sie sich, dass die Einstellungen für den Datenschutz auf dem höchsten Niveau sind (im Menüpunkt „Optionen“ bzw. “Extras” Ihres Browsers).

- Erwägen Sie die Benutzung zusätzlicher Filtersoftware.

- Kontaktieren Sie Ihren Internetanbieter oder einen Fachmann, sobald Ihr Computer ein eigenartiges Verhalten zeigt. Er könnte infiziert sein. Ihr Internetprovider sollte auch Ratschläge für Eltern geben können.

- Schicken Sie einen Bericht an Ihre nationale Internet**hotline** (siehe “Weiterführende Informationen“), wenn Sie unerwünschte Inhalte finden.

- Setzen Sie sich so oft wie möglich neben Ihre Kinder, wenn sie surfen. Dies ist eine ausgezeichnete Art, Gespräche anzuregen und das Vertrauen aufzubauen. Stellen Sie sich der Herausforderung, gemeinsam zu lernen.

- Denken Sie daran, dass diese Sicherheitsregeln sowohl für Sie als auch für Ihre Kinder gelten. Ermutigen Sie sie, es Ihnen zu erzählen, wenn sie auf eigenartige Dinge stoßen.

WEITERFÜHRENDE INFORMATIONEN

Umfangreiche Informationen zu dem Themenbereich „Sicherheit" finden Sie unter dem Menü-Punkt „Themen" der EU-Initiative klicksafe.
www.klicksafe.de

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet umfassende Informationen zu Fragen der Sicherheit im Bezug auf das Internet.
www.bsi-fuer-buerger.de

Die Kommission für Jugendmedienschutz (KJM) informiert zum Thema Jugendschutz im Internet.
www.kjm-online.de

Die beiden deutschen Meldestellen jugendschutz.net und die Internet-Beschwerdestelle bieten Onlineformulare, anhand derer illegale und jugendgefährdende Inhalte im Internet gemeldet werden können.
www.jugendschutz.net
www.internet-beschwerdestelle.de

2. Kommunikation

PUZZLESTÜCKE

Erinnern Sie sich noch, wie wichtig es für Sie war, Kontakt mit Freunden zu halten, während Sie aufwuchsen? Das Internet bietet eine Menge neuer Orte, wo man seine Freunde treffen kann, und hält neue Wege für den Selbstausdruck und das Knüpfen von Kontakten durch E-Mails, **Dateitransfer**, **Bloggen** und Soziale Netzwerke (z.B. MySpace, Facebook, schülerVZ, wer-kennt-wen.de, lokalisten.de) usw. bereit. Die Jugendlichen von heute benutzen die Technologie, um neue Dinge auszuprobieren und in einer Umgebung Kontakte zu pflegen, die sie als privat und frei von elterlicher Kontrolle ansehen.

Das Kapitel zum Thema Kommunikation führt Eltern und Kinder in das Konzept der **persönlichen Informationen**, der **Privatsphäre**, der positiven Interaktionen online und des Umgangs mit Risiken wie dem Kontakt mit Fremden ein. Die Privatsphäre online ist sehr stark mit dem Konzept der **Konten & Profile** verbunden. Ein Konto ermöglicht den Zugang zu einem Online-Service.

Außerhalb des Internets enthalten beispielsweise Mitgliedskarten für den Fitnessclub persönliche Informationen über Sie. Online-Konten und -Dienste sind ähnlich. Man kann weder das eine noch das andere benutzen, es sei denn, man liefert persönliche Daten, aus denen das „Benutzerprofil" erstellt wird. Wichtig ist, dass man die Art von Informationen, die man mitteilt, sowie die Personen, denen man sie mitteilt, selbst aussuchen kann.

Beim Schutz der Privatsphäre geht es eher darum, welche Informationen man den anderen über sich selbst preisgeben will, als darum zu lügen. Jugendliche sind begeistert von der Möglichkeit, online mit Freunden zu kommunizieren und ihr Online-Image aufzubauen. Sie sind sich jedoch oft nicht der Konsequenzen bewusst, wenn sie ihre persönlichen Daten und Informationen veröffentlichen.

ERSTELLUNG EINES PROFILS

Der erste Schritt zum Schutz der persönlichen Daten ist das Erstellen eines sicheren Profils. Hierbei sollte man gründlich über die eingefügten Informationen nachdenken und die richtigen Einstellungen für den Datenschutz anwenden.

Schaffen Sie mehrere E-Mail-Konten für verschiedene Online-Kontexte. Wenn Ihre Kinder Online-Dienste wie Chat, Sofortnachrichtenübermittlung, Bloggen usw. benutzen, raten Sie ihnen, eine neutrale E-Mail-Adresse und einen **Screen-Namen** zu benutzen. Auf diese Art benutzt Ihr Kind keine E-Mail-Adresse, die seinen ganzen Namen preisgibt.

Halten Sie **Kontenpasswörter** geheim. Vergewissern Sie sich, dass Ihre Kinder verstehen, dass sie ihre persönlichen Konten nicht mit Personen teilen sollten, die ihr Vertrauen ausnutzen könnten. So kann vermieden werden, dass Ihr Kind seinen richtigen Namen preisgibt. Andererseits sollten Sie vielleicht die Passwörter Ihrer Kinder kennen, um so ihre Konten im Auge behalten zu können – sprechen Sie mit ihnen darüber.

Denken Sie daran, die **Einstellungen für den Datenschutz** Ihres Profils/Kontos anzupassen, indem Sie die Einstellung "privat" und "nicht öffentlich" wählen. So können Sie selbst entscheiden, für wen diese Informationen zugänglich sind und mit wem Sie interagieren. Ein privates Profil bedeutet, dass Sie die Liste Ihrer Kontakte (**Kontaktliste**) verwalten können. Bringen Sie Ihren Kindern bei, nur mit Personen in Kontakt zu treten, die sie offline kennen. Wenn Ihre Kinder Chat-Räume benutzen, prüfen Sie folgende Punkte:

- Dass es richtige **Moderatoren** gibt. Falls kein Moderator anwesend ist, ist der Chat nicht sicher.
- Dass es Hilfsmittel zum Ignorieren oder Blockieren unerwünschter Kontakte gibt.
- Dass es eine Hilfs- und **Bericht**funktion auf der Webseite gibt, die sie im Problemfall benutzen können.
- Dass die Regeln der Dienstleistung klar und deutlich erklärt sind.

FOTOS UND WEBCAMS

Kinder müssen verstehen, dass ihr Foto ein fester Bestandteil ihrer Privatsphäre ist und dass digitale Bilder äußerst aussagekräftig sind. Sie können einfach verbreitet und **gefälscht** werden und sind sehr schwierig zu löschen, wenn sie einmal über einen Computer oder ein Mobiltelefon verschickt wurden – sie könnten für immer online bleiben! Webcams sollten mit Vorsicht benutzt werden und Kinder sollten **Webcams** nicht ohne Aufsicht benutzen. Webcam-Chat-Tools und **Adressbücher** können riskant sein. Sie und Ihre Kinder sollten persönliche Bilder nur Personen zeigen, die Sie kennen und denen Sie vertrauen – bitten Sie immer um Erlaubnis, bevor Sie das Foto von jemand anderem ins Internet stellen. Lassen Sie Ihre Kinder einen Computer und eine Webcam nicht allein in ihrem Zimmer benutzen.

KONTAKT MIT FREMDEN

Leute, die man online trifft, sind nicht immer ehrlich, was ihre Identität angeht. Bringen Sie Ihren Kindern bei, ihre Privatsphäre online genauso zu schützen, wie sie sie offline schützen würden. Stellen Sie Regeln auf, wie sie sich Fremden gegenüber in der „echten" Welt verhalten sollen, und erklären Sie, dass diese Regeln online genauso gelten.

Ihre Kinder bauen vielleicht eine starke Beziehung mit Online-FreundInnen auf und neigen dazu, Leuten ihr Vertrauen zu schenken, die Interesse und Verständnis zeigen, auch wenn sie sie nicht wirklich kennen. Es kann für sie also sehr verlockend sein, sich offline mit diesen neuen Freunden zu treffen, ohne Sie darüber zu informieren. Kinder sind sich der Risiken solcher Treffen oft nicht bewusst und sehen sie vielleicht als belanglos an.

Dadurch werden sie leicht Opfer des Online-**Groomings**. Untersuchungen haben ergeben, dass viele Kinder sich unbegleitet mit ihren Online-„Freunden“ treffen, ohne ihre Eltern zu informieren. Reden Sie mit Ihren Kindern darüber, um sicherzugehen, dass es ihnen nicht passiert. Kommunikation ist der Schlüssel.

NETIQUETTE

Netiquette bezieht sich auf die guten Manieren im Internet und darauf, andere Leute im Internet so zu behandeln, wie man selber behandelt werden möchte. Kinder sind sich der Tatsache vielleicht nicht bewusst, dass sie irrtümlicherweise jemanden online beleidigt haben. Leider benutzen manche Personen das Internet und/oder Mobiltelefone, um andere zu ärgern oder zu belästigen. Dies wird Cyber-Mobbing genannt und trifft in etwa auf eines von vier Kindern zu (siehe themenbezogenes Kapitel für weitere Informationen).

CHAT-SPRACHE

Beim Online-Chatten benutzen Jugendliche eine einzigartige Sprache voller **Emoticons** und **Akronyme**! Werfen Sie einen Blick auf die untenstehenden Tabellen, um sich damit vertraut zu machen. 😀

Beispielliste von Chat-Akronymen, für weitere Informationen siehe „Weiterführende Informationen“:

ggg: (engl. „giggeling“) kichern (beliebig viele g’s möglich)

grmpf: grummeln

g: grinsen

lol: engl. „laughing out loud“ – laut lachen

rofl: (engl. „rolling on floor, laughing“) sich vor Lachen am Boden wälzen

Addy: E-Mail-Adresse

afk: (engl. „away from keyboard“) bin nicht an der Tastatur

brb (engl. “be right back”): der Chatter ist gleich wieder zurück

cs: Cybersex (es kann auch das PC-Spiel „Counter Strike“ gemeint sein)

cu (engl. „see you“): Tschüss, wir sehen uns

faq (engl. “frequently asked questions”): häufig gestellte Fragen, die als Liste für Anfänger zum Nachlesen zusammengestellt werden

hdl, ild: hab dich lieb, ich liebe dich (wird auch erweitert: z. B. hdgdl – hab dich ganz doll lieb)

hp: Homepage

ka: keine Ahnung

kp: kein Plan (auch: kein Problem)

m/w: männlich oder weiblich? (auch: mow)

mom: einen Moment bitte (auch bekannt: momtel: – einen Moment, das Telefon klingelt)

n8: Nacht (lautmalerisch); auch bekannt: gn8: Gute Nacht

omg (engl. „oh my god“): Oh mein Gott! (überrascht, auch begeistert)

re (engl. „return“): wieder da

rl: Reales Leben, das „echte Leben“

thx (engl. „thanks“): Danke

ts: Telefonsex (es kann auch die Kommunikations-Software TeamSpeak gemeint sein)

we: Wochenende

Quelle: “Chatten ohne Risiko?”, www.chatten-ohne-risiko.de [Mai 2011]

Sie können Emoticons erstellen, indem Sie Satzzeichen und Buchstaben verbinden. Hier ein paar Beispiele:

Ein Smiley (mit oder ohne Nase)	:) oder : -) Doppelpunkt, (Bindestrich), Klammer
Ein trauriges Gesicht (mit oder ohne Nase)	:(oder :-(Doppelpunkt, (Bindestrich), Klammer
Ein blinzelndes Gesicht (mit oder ohne Nase)	;) oder ;-) Strichpunkt, (Bindestrich), Klammer
Ein überraschtes Gesicht (mit oder ohne Nase)	: o oder :-o Doppelpunkt, (Bindestrich), kleines o
Ein breites Lachen (mit oder ohne Nase)	:-D oder : D Doppelpunkt, (Bindestrich), großes D
Herausgestreckte Zunge (mit oder ohne Nase)	: p oder :-p Doppelpunkt, (Bindestrich), kleines p

GOLDENE REGELN

- Nehmen Sie sich die Zeit, um herauszufinden, wie Ihre Kinder ihre Zeit online verbringen, und lassen Sie sich zeigen, wie sie mit ihren Freunden kommunizieren.
- Bringen Sie ihnen bei, ihre Privatsphäre anhand folgender Tricks zu schützen:
  - Erstellung eines sicheren Profils mit eingeschalteten Einstellungen für den Datenschutz.
  - Geheimhaltung ihrer Passwörter.
  - Kontaktaufnahme und Kommunikation nur mit Leuten, die sie offline kennen.
  - Immer die elterliche Erlaubnis einholen, bevor sie Bilder von sich selbst oder ihrer Familie, ihrem Haus, ihrer Schule usw. hochladen.
  - Persönliche Informationen wie Telefonnummern, Adresse, Schule, Sportclub usw. nur Personen mitteilen, die sie im echten Leben kennen.

- Stellen Sie den Computer in einem gemeinsam genutzten Raum auf, damit Sie ihre Online-Aktivitäten im Auge behalten können.
- Vergewissern Sie sich gemeinsam, dass Sie wissen, wie:
  - man Kontakte ablehnen oder Personen auf der Kontaktliste blockieren kann,
  - man die Sicherheits- und Berichtfunktionen auf den Webseiten, die Sie benutzen, anwenden kann.
- Bauen Sie Vertrauen auf, indem Sie Ihren Kindern versichern, dass sie mit Ihnen auch über ihre Fehler sprechen können, damit Sie gemeinsam nach Lösungen suchen können! Fehler gehören zum Lernprozess dazu.

WEITERFÜHRENDE INFORMATIONEN

Ausführliche Informationen zu dem Themenbereich „Kommunikation im Internet" finden Sie unter dem Menu-Punkt „Themen" der EU-Initiative klicksafe:
www.klicksafe.de

Das Projekt „Chatten ohne Risiko?" bietet innerhalb seines Internetauftritts und in der gleichnamigen Broschüre umfangreiche Informationen zu den Themen „Chat", „Instant Messenger" und „Online-Communitys":
www.chatten-ohne-risiko.de
www.jugendschutz.net/pdf/chatten_ohne_Risiko.pdf

Auf dem Eltern-Portal des Internet ABC finden Eltern in dem Bereich „Wissen, wie's geht" Informationen zu den Themen „Chatten/Instant Messenger" und „Online-Communitys". Innerhalb der Kinderseite des Angebotes sind speziell für Kinder aufbereitete Informationen, sowie ein Surfschein für Kinder beinhaltet:
www.internet-abc.de/eltern
www.internet-abc.de/kinder

Der Window Live Messenger für Kids ist eine sichere Alternative für Kinder: bei diesem Instant Messenger geben die Eltern die Kontakte frei, mit denen ihre Kinder chatten dürfen und es gibt einen "Melde-Button":
www.kinder-messenger.de

3. Cyber-Mobbing

EIN FALL VON CYBER-MOBBING

Die Kommunikation via Internet und Mobiltelefon hat eine Menge großartiger Vorteile. Leider kann sie jedoch auch unangenehmere Seiten haben – Ihre Kinder empfangen oder versenden vielleicht Nachrichten mit Inhalten, die ihre Gefühle oder die Gefühle anderer verletzen. Es ist wichtig, Ihren Kindern ein sozial einwandfreies Verhalten beizubringen – auch unsere eigenen Kinder sind nicht immer Engel ;-)

Cyber-Mobbing besteht darin, die neuen Informations- und Kommunikationsmittel und Dienstleistungen einzusetzen, um eine Einzelperson oder eine Gruppe von Personen zu tyrannisieren, zu belästigen oder einzuschüchtern. E-Mails, Chat, Sofortnachrichtenübermittlung, Mobiltelefone oder andere digitale Geräte können hierbei eingesetzt werden. In virtuellen Spielumgebungen können die Täter den Avatar Ihres Kindes angreifen, z.B. indem sie darauf schießen, **virtuelle Besitztümer** stehlen oder den **Avatar** zwingen, ein unerwünschtes Verhalten an den Tag zu legen.

Kinder erzählen normalerweise, wenn sie Probleme in Bezug auf die Veröffentlichung persönlicher Informationen in öffentlichen Bereichen haben, wie zum Beispiel die Veröffentlichung eines Fotos oder persönlicher Informationen in einem öffentlichen Forum oder auf einer Webseite. Wie **Mobbing** in der Schule oder auf dem Spielplatz ist ein solches Verhalten unannehmbar und Eltern, PädagogInnen und Kinder sollten wachsam sein und bereit zu reagieren. Im Gegensatz zum traditionellen Mobbing kann Cyber-Mobbing das Kind sogar betreffen, wenn es sich gerade nicht mehr in direkter Interaktion mit dem Täter befindet. Die Täter können z.B. jederzeit Drohungen an die E-Mail-Adresse oder auf das Mobiltelefon versenden.

Eltern können dabei helfen, eine Umgebung zu schaffen, in der Mobbing nicht geduldet wird – bringen Sie Ihren Kindern bei, dass sie sich online nicht verantwortungslos benehmen können, auch wenn sie anonym sind. Sie müssen ihre eigenen Rechte und ihre persönliche Verantwortung kennen und die Rechte Dritter beachten.

Sagen Sie Ihren Kindern, dass sie mit Ihnen offen über alle besorgniserregenden Situationen sprechen können. Neue Technologien wie das Internet und Mobiltelefone bieten eine ausgezeichnete Gelegenheit für Diskussionen und regen zum Nachdenken an!

GOLDENE REGELN

- Beugen Sie negativen Erfahrungen vor, indem Sie gewährleisten, dass Ihre Kinder wissen, wie sie ihre Privatsphäre schützen und die Privatsphäre Dritter respektieren können.

- Bringen Sie Ihren Kindern bei, nicht auf belästigende Nachrichten zu reagieren.
- Helfen Sie Ihren Kindern zu verstehen, welche Art von Nachrichten und Verhalten anderen unangenehm erscheinen kann und wie sie diese vermeiden können.
- Vergewissern Sie sich, dass sie die Möglichkeiten kennen, wie sie einen Absender von ihrer Kontaktliste blockieren können.
- Behalten Sie beleidigende Nachrichten im Auge, Sie benötigen sie vielleicht als wichtige Beweisstücke.
- Informieren Sie sich über die Anti-Mobbing-Strategien in der Schule Ihrer Kinder. Arbeiten Sie mit anderen Eltern und LehrerInnen zusammen, um Mobbing und Cyber-Mobbing zu verhindern.
- Seien Sie in Kontakt mit dem Umfeld Ihrer Kinder; lernen Sie ihre Freunde, die Eltern ihrer Freunde, ihre LehrerInnen und Klassenkameraden kennen.
- Ermutigen Sie Ihre Kinder, Sie über alle störenden Erfahrungen offline & online zu informieren. Versichern Sie ihnen, dass Sie für sie da sind und Sie gemeinsam nach Lösungen suchen werden, auch wenn sie unvorsichtig waren.
- Vergewissern Sie sich, dass Ihre Kinder verstehen, dass es nicht ihre Schuld ist, wenn jemand sie belästigt.

WEITERFÜHRENDE INFORMATIONEN

Umfassende Informationen zum Themenbereich „Cyber-Mobbing" sowie medienpädagogische Materialien - wie beispielsweise Flyer und Unterrichtsmaterialien - sind auf dem Internetauftritt der EU-Initiative klicksafe unter dem Menü-Punkt „Themen" -> „Cyber-Mobbing" zusammengefasst.
www.klicksafe.de

Die Arbeitsgemeinschaft vernetzter Kinderseiten (www.seitenstark.de) bietet umfangreiche Informationen für Eltern und für Kinder zur Problematik des Mobbings.
www.mobbing.seitenstark.de

Rat und Hilfe können Kinder und Jugendliche bei der Nummer gegen Kummer erhalten.
Online-Beratung:
www.nummergegenkummer.de
Telefonberatung:
0800 - 111 0 333
(Mo - Sa von 14-20 Uhr)

4. Unterhaltung & Herunterladen

IM INTERNET IST NICHT ALLES GOLD, WAS GLÄNZT

Das Internet ist eine virtuelle Umgebung mit einer Menge Aktivitäten, auch kommerzieller Art. So wie Sie Ihren Kindern nicht alles kaufen, was sie im Fernsehen sehen oder was sie im Geschäft toll finden, so sollten Sie ihnen auch beibringen, nicht alles zu wollen oder zu glauben, was sie online sehen, z.B. Musik und Spiele, **Klingeltöne**, andere Accessoires und Online-Kaufdienste.

Wenn Sie gemeinsam mit Ihren Kindern im Internet surfen, haben Sie die Gelegenheit, ihnen zu erklären, dass Produkte wie Klingeltöne, **Hintergrundbilder**, **mp3s**, Avatare usw. selten kostenlos sind. Wenn Sie solche Werbungen finden, zeigen Sie ihnen das Kleingedruckte, um ihnen vorzuführen, dass sie nicht alles im **Internet** als selbstverständlich betrachten sollten.

Um sich für eine Dienstleistung anzumelden (kostenlos oder nicht), müssen Sie ein **Online-Formular** mit wichtigen persönlichen Informationen ausfüllen. Füllen Sie diese Formulare nur aus, wenn Sie wissen, wie Ihre persönlichen Daten benutzt werden, und raten Sie Ihren Kindern davon ab, solche Formulare auszufüllen, es sei denn, Sie helfen ihnen dabei.

Pop-up-Fenster werden oft benutzt, um Objekte im Internet zu verkaufen. Sie sind nicht immer schlecht – es hängt davon ab, ob sie von einer vertrauensvollen Webseite stammen oder nicht. Im Allgemeinen können Sie einem Pop-up-Fenster vertrauen, wenn Sie der Webseite vertrauen. Gewisse Pop-up-Fenster werden jedoch benutzt, um Produkte anzubieten, die unzuverlässig sind, oder sie führen zu **Online-Fragebögen**, die persönliche Daten sammeln. Bringen Sie Ihren Kindern bei, unzuverlässige Pop-ups durch einen Klick auf das Kreuz in der oberen rechten Ecke zu schließen.

ONLINE-SPIELE SPIELEN

Online-Spiele unterscheiden sich von älteren digitalen Spielen in der Hinsicht, dass sie eine **Live-Netzwerkverbindung** benötigen. Kinder können Spiele von einer CD/DVD, auf Webseiten, auf Spielkonsolen oder auf Mobiltelefonen und anderen tragbaren Geräten spielen.

Online-Spiele reichen von einfachen, bekannten Spielen wie Pacman und Tetris bis zu virtuellen Realitätsspielen, bei denen mehrere BenutzerInnen zusammen online spielen und dabei Inhalte und Geschichten erstellen. Viele solcher **Multiplayer-Spiele** verfügen über

virtuelle Gemeinschaften für die SpielerInnen. Dies kann die Kinder Risiken aussetzen, weil sie hierbei im Internet Personen treffen können, die sie nicht kennen (siehe Kapitel über Kommunikation).

Spiele sind von großer Bedeutung in der Entwicklung der Kinder, da soziale Fähigkeiten und strategisches Denken in einer Umgebung gefördert werden, die von Spielregeln bestimmt wird. Viele digitale Spiele sind attraktiv und interaktiv und werden zu pädagogischen Zwecken eingesetzt.

Nicht alle digitalen Spiele sind jedoch von guter Qualität. Sie müssen entscheiden, welche Spiele sich für Ihre Kinder am besten eignen – indem Sie Regeln festlegen, können Sie außerdem gewährleisten, dass die Zeit, die Ihre Kinder mit dem Spielen online verbringen, nicht auf Kosten anderer Aktivitäten geht.

In Deutschland sind Altersfreigaben für Computerspiele seit dem 1. April 2003 gesetzlich vorgeschrieben. Sie sollen sicherstellen, dass Kinder und Jugendliche nur Zugang zu Computerspielen haben, die für ihr jeweiliges Alter unbedenklich sind. Diese Kennzeichnung wird durch die USK (Unterhaltungssoftware Selbstkontrolle; www.usk.de) vergeben. Fünf Kategorien werden unterschieden:
- USK ab 0 Jahren freigegeben
- USK ab 6 Jahren freigegeben
- USK ab 12 Jahren freigegeben
- USK ab 16 Jahren freigegeben
- USK ab 18 Jahren freigegeben

Diese Kennzeichen geben jedoch keine Auskunft über die tatsächliche “Spielbarkeit” ab diesem Alter, ob das Kind beispielsweise die Fähigkeiten mitbringt, das Spiel zu verstehen.

GOLDENE REGELN

- Ermutigen Sie Ihre Kinder, Webseiten zu benutzen, die legale Inhalte anbieten, und erklären Sie ihnen, dass nicht alles im Internet so ist, wie es scheint.
- Erklären Sie die Risiken des unvorsichtigen Herunterladens von Material aus dem Netz.
- Versichern Sie sich, dass Ihr Computer geschützt ist, und benutzen Sie immer ein aktuelles Anti-Virus-Programm.
- Lesen Sie immer den Datenschutzhinweis und die Benutzerbedingungen, bevor Sie etwas installieren. Prüfen Sie (im Internet), ob die Software, die Sie herunterladen möchten, vertrauenswürdig ist.
- Schließen Sie unzuverlässige Pop-up-Fenster, indem Sie auf das Kreuz in der oberen rechten Ecke klicken. Klicken Sie nie in die Fenster.

KINDER & SPIELE

Wenn Ihre Kinder Online-Spiele mit mehreren BenutzerInnen spielen:

- Wählen Sie Webseiten mit strikten Regeln und echten Moderatoren.
- Ermahnen Sie Ihre Kinder, anderen Spielern keine persönlichen Daten mitzuteilen.
- Warnen Sie sie davor, andere Spieler offline zu treffen, es sei denn in Ihrer Begleitung.
- Ermutigen Sie Ihre Kinder, Ihnen von belästigenden oder bedrohlichen Nachrichten oder Schimpfworten, der Darstellung unangenehmer Inhalte oder Einladungen, sich außerhalb des Spielkontextes zu treffen, zu erzählen.
- Ziehen Sie Ihr Kind aus dem Spiel zurück oder ändern Sie die Online-Identität Ihres Kindes, wenn ein Aspekt des Spiels oder dessen Entwicklung Ihnen ein unangenehmes Gefühl bereitet.

WEITERFÜHRENDE INFORMATIONEN

Das deutsche Prüfsiegel der USK (Unterhaltungssoftware Selbstkontrolle) wird auf folgendem Internetauftritt beschrieben:
www.usk.de

Erfahren Sie mehr über Online-Spiele und das PEGI-Bewertungssystem:
www.pegi.info/de/index/id/515

In dem Themenbereich "Spiele" auf www.klicksafe.de finden sich umfangreiche Informationen und Materialien:
www.klicksafe.de/themen/spielen/index.html

Der Spieleratgeber NRW bietet für Eltern medienpädagogische Bewertungen von PC-Spielen:
www.spieleratgeber-nrw.de

Die Bundeszentrale für politische Bildung beurteilt PC-Spiele:
www.spielbar.de/neu

Das Institut zur Förderung von Medienkompetenz: Spielraum der Fachhochschule Köln fasst wissenschaftliche Texte zum Thema PC-Spiele zusammen:
www1.fh-koeln.de/spielraum

Die Verbraucherzentral Rheinland-Pfalz bietet Hilfe zum Thema "Internet-Abzocke":
www.verbraucherzentrale-rlp.de/UNIQ129232373605370/link432741A.htm

1. Sicherheit

KOMMENTIERTE ÜBUNGEN

Sucht die passenden Wörter zu den Bildern: Computergehäuse, Mauspad, Bildschirm, Lautsprecher, Webcam, Drucker, USB-Stick, Maus, CD-ROM.

Eine Aufwärmübung, um Ihre Kinder mit den verschiedenen Teilen des Computers und anderem Hardware-Material vertraut zu machen. Sie können auf die Art, die Ihnen angebracht erscheint, darauf aufbauen.

Bittet eure Eltern, euch eine E-Mail mit einem **Anhang** zu schicken, oder schickt euch selbst eine. Übt Folgendes: Klickt mit der rechten Maustaste auf den Anhang und speichert ihn auf eurem Computer-Desktop ab. Geht zum Desktop, klickt mit der rechten Maustaste auf das Dokument und klickt auf Scannen. Wenn ihr wisst, dass das Dokument ungefährlich ist, könnt ihr es öffnen. Denkt daran: Rechter Mausklick und SPEICHERN – SCANNEN – ÖFFNEN.

Schicken Sie eine E-Mail an die E-Mail-Adresse Ihres Kindes oder an Ihre eigene Adresse und hängen Sie eine Datei an. Lassen Sie Ihr Kind die Angaben der Übung befolgen, um das Dokument mit einem rechten Mausklick zu speichern, ohne es zu öffnen. Nachdem die Datei

auf dem Desktop oder in einem Computerordner wie „Meine Dokumente“ gespeichert ist, zeigen Sie Ihrem Kind, wie es mit einem weiteren rechten Mausklick das Dokument vor dem Öffnen scannen kann. So fördern Sie sichere Gewohnheiten.

Folgt Tinas Tipp und lernt, wie ihr eure E-Mail-Adresse beschreiben könnt, wenn ihr sie wirklich online veröffentlichen müsst. So könnt ihr verhindern, dass eure E-Mail-Adresse automatisch aufgegriffen und von Spammern benutzt wird.
Beispiel: cybercat.smith@mymail.com = cybercat Punkt smith at mymail Punkt com

Beschreibt als Übung die E-Mail-Adressen eurer Familie: deine E-Mail-Adresse, die E-Mail-Adresse eurer Familie, die E-Mail-Adresse deiner Mutter, die E-Mail-Adresse deines Vaters.

Um zu vermeiden, dass Ihre E-Mail-Adresse automatisch von einer Software für Spam-Verteilung aufgegriffen wird, beschreiben Sie sie, anstatt sie auszuschreiben. Lassen Sie Ihr Kind diese Technik wie oben beschrieben üben. Denken Sie jedoch daran, dass Ihre Kinder ihre E-Mail-Adresse nicht im Internet veröffentlichen sollten, und falls sie dies tun, sollten sie eine Adresse benutzen, die ihren Namen nicht verrät (siehe Kapitel „Kommunikation“).

Bevor Tina fortfährt, helfen wir Marie dabei, alles besser zu verstehen. Schaut euch die Aktivitäten in diesem Textfeld an und malt einen Kreis um die Dinge, die ihr nur tun könnt, wenn ihr eine Internetverbindung habt.

Sehr junge Kinder verstehen vielleicht nicht genau, für welche Aktivitäten eine Internetverbindung benötigt wird und für welche nicht. Um einen Text zu schreiben, muss der Computer nicht ans Internet angeschlossen sein, für das Chatten schon. Sie können anhand einer CD oder auf Ihrem Computer gespeicherter Musikdateien auf Ihrem PC Musik hören, aber Sie können auch direkt online Musik hören. Ihre Kinder sollten nur die Aktivitäten ankreuzen, für die eine Internetverbindung von wesentlicher Bedeutung ist.

Gebt zusammen mit euren Eltern www.fragfinn.de, www.blinde-kuh.de oder www.helles-koepfchen.de in euren Browser ein. Sucht nach Informationen über den Tyrannosaurus Rex und versucht herauszufinden, wann dieser Dinosaurier auf der Erde gelebt hat. Versucht auch ein gutes Bild von einem Tyrannosaurus zu finden. Vergesst nicht, die Informationen anhand verschiedener Quellen (Webseiten, Lexikon etc.) zu prüfen.

Bringen Sie Ihren Kindern gute Suchgewohnheiten bei, indem Sie sie daran erinnern, nicht alles zu glauben, was sie online sehen. Erinnern Sie sie daran, Informationen bei mindestens drei Quellen (Webseiten, Lexikon etc.) zu suchen und zu vergleichen und bei Schulaufgaben immer diese Quellen anzugeben.

Gebt zusammen mit euren Eltern www.fragfinn.de, www.blinde-kuh.de oder www.helles-koepfchen.de in euren Browser ein. Sucht dann nach einem Thema, zum Beispiel dem Tyrannosaurus Rex, und speichert die drei Webseiten, die ihr am interessantesten findet, ab, indem ihr entweder auf den Menüpunkt “Favoriten” (Internet Explorer) oder den Menüpunkt “Lesezeichen” (Mozilla Firefox) oben auf der Browserseite klickt und sie zu euren Lieblingsseiten hinzufügt. Ihr könnt auch einen eigenen Ordner anlegen.

Interessante Webseiten speichern und in den Favoriten organisieren (Option in der Browsersymbolleiste) ist eine gute Art, das Bedürfnis Ihrer jungen Kinder, im Internet nach Informationen zu suchen, zu reduzieren.

HABT IHR ES GESCHAFFT?

1: (geschützt) 2: (Virus), (unbekannten), (herunterlädt), (infizierte), (USB-Stick), (ungeschützten) 3: (komisch) 4: (Anhängen), (Titeln), (Spam) 5: (Spam) 6: (erst), (3), (vergleiche), (Jeder), (veröffentlichen) 7: (Anti-Virus-Programme), (Anti-Spyware) 8: (redet), (Eltern)

VORGESCHLAGENE LÖSUNGEN ZU DEN SITUATIONSKARTEN

SITUATION 1. Surft nie im Internet, wenn euer Computer nicht durch ein aktuelles Anti-Virus-Programm und Anti-Spyware geschützt ist. Dies würde einer Grenze ohne Grenzwächter gleichkommen; euer Computer könnte von schädlichen Programmen wie Viren, Trojanern, Würmern oder Spyware infiziert werden.

SITUATION 2. Passt auf bei E-Mails, die von Leuten kommen, die ihr nicht kennt, und Anhänge oder Texte enthalten, die „das Blaue vom Himmel" versprechen – es handelt sich sehr wahrscheinlich um Spam! Spam kann euren Computer mit schädlichen Programmen wie Viren, Trojanern, Würmern oder Spyware infizieren. Öffnet diese E-Mails nicht. Blockiert stattdessen den Absender, indem ihr mit einem rechten Mausklick auf die Mail klickt und „Absender blockieren" wählt, oder löscht diese Mails einfach.

SITUATION 3. Wenn ihr Informationen im Internet sucht, vertraut nicht der erstbesten Seite, die ihr findet. Überprüft mindestens drei verschiedene Seiten und vergleicht die Informationen, die ihr gefunden habt. Denkt daran: Jeder, der eine Internetverbindung hat, kann Informationen erfinden und im Internet veröffentlichen. Wenn ihr einen Bericht oder Aufsatz schreibt, müsst ihr immer die Quelle der Informationen und Bilder erwähnen ... so würde ein/e echte/r WissenschaftlerIn arbeiten.

2. Kommunikation

KOMMENTIERTE ÜBUNGEN

Gebt an, wie **persönlich** die folgenden Angaben für euch sind:
eure Telefonnummer, eure Haarfarbe, euer Name, das Land, in dem ihr lebt, die Schule, die ihr besucht, eure Adresse, der Name eures Haustieres, der Beruf eurer Eltern, eure E-Mail-Adresse, eure Fotos, euer Alter.

Haben Ihre Kinder die gleiche Auffassung über Privatsphäre wie Sie? Die drei Farben stellen „sehr privat" (rot), „recht privat" (orange) und „nicht so privat" (grün) dar.

Helft Marie, mit Tinas Tipps ein richtig gutes Passwort zu finden.

Gute Passwörter sollten eine willkürliche Folge verschiedener Zeichen enthalten (Zahlen, Buchstaben und Satzzeichen) und immer geheim gehalten werden.

Folgt Maries Beispiel und erstellt ein sicheres Profil. Fertigt anschließend ein Beispiel eines unsicheren Profils an.

Lassen Sie Ihre Kinder ein sicheres und anschließend ein weniger sicheres Profil erstellen, das persönliche Informationen preisgibt. Erinnern Sie Ihre Kinder daran, dass die Erstellung eines sicheren Profils nur dann sinnvoll ist, wenn sie online immer ihre Privatsphäre schützen.

Seht euch dieses Bild an und schreibt auf, was ihr über diese Person sagen könnt.

Welche persönlichen Informationen lassen sich aus einem Bild herauslesen? Kinder sind sich der Kraft von Bildern oft nicht bewusst.

Folgt Maries Idee und denkt euch 3 Ratschläge aus, die Tina „Alex, dem Rotkäppchen mit Kapuzenpulli" geben würde, um sich vor den „Wölfen des Web" zu schützen.

Prüfen Sie, ob Ihre Kinder verstanden haben, welche Risiken der Kontakt mit Fremden online mit sich bringen kann.

Wie möchtet ihr online von anderen behandelt werden? (1..... 2..... 3.....)

Vergewissern Sie sich, dass Ihre Kinder verstehen, dass sie andere so behandeln sollen, wie sie selbst behandelt werden möchten.

KNACKT DEN CODE: Findet heraus, was einige der beliebtesten Chat-Akronyme bedeuten, indem ihr sie mit ihrer Bedeutung verbindet.

Verbessern Sie Ihr Verständnis der Akronyme, indem Sie das Kapitel über Kommunikation und den darin enthaltenen Beitrag über Netiquette und Chat-Sprache lesen.

Benutzt die Tastenkombinationen, um die folgenden Emoticons darzustellen: ein Smiley, ein trauriges Gesicht, ein blinzelndes Gesicht, ein überraschtes Gesicht, ein breites Lachen, herausgestreckte Zunge.

Weitere Informationen finden Sie im Kapitel „Kommunikation/Netiquette, Chat-Sprache“.

HABT IHR ES GESCHAFFT?

1: (Profil) 2: (Privatsphäre), (verantwortlich) 3: (Fremden) 4: (Netiquette), 5: (Emoticon) 6: (Passwort), (8) (Satz-) 7: (geheim) 8: (weigere) 9: (kennst)

VORGESCHLAGENE LÖSUNGEN ZU DEN SITUATIONSKARTEN

SITUATION 4. Wenn ihr das Internet benutzt, kann euer Profil oder die Informationen, die ihr über euch preisgebt, Dutzende, Hunderte, Tausende oder sogar Millionen Leute erreichen. Deshalb ist es so wichtig, vorsichtig mit den Informationen umzugehen, die ihr über euch preisgebt. Teilt persönliche Daten nur Leuten mit, denen ihr vertraut und die ihr offline gut kennt.

SITUATION 5. Mike hat seinem Freund wahrscheinlich sein E-Mail-Passwort mitgeteilt, der dann beschloss, sich durch das Verschicken gemeiner E-Mails in seinem Namen an ihm zu rächen. Behaltet euer Passwort immer für euch, es sei denn, ihr habt nichts dagegen, wenn andere Leute eure E-Mails lesen oder in eurem Namen Dinge sagen, die ihr nie sagen würdet!

SITUATION 6. Ein Treffen mit einem Fremden ist keine gute Idee. Aber wenn ihr wirklich denkt, dass ihr einem Online-Freund vertrauen könnt, und er möchte sich mit euch treffen, dann erzählt euren Eltern davon, damit sie euch begleiten können. Kein wahrer und aufrichtiger Freund wird damit ein Problem haben. Das ist nur ein Problem für Leute, die etwas zu verstecken haben.

3. Cyber-Mobbing

KOMMENTIERTE ÜBUNGEN

Zeichnet ein Bild der Einladung, die Alex von seinen LehrerInnen erhalten hat. Stellt das Anti-Mobbing-Logo und den Slogan dar, die die Schule für die Anti-Mobbing-Woche benutzt.

Lassen Sie der Kreativität Ihrer Kinder freien Lauf und lassen Sie sie in den leeren Rahmen zeichnen.

Folgt Alex' Beispiel und gebt 5 Gründe an, für die ihr jemandem eine „rote Karte" geben würdet.

Sprechen Sie mit Ihren Kindern darüber, welche Art von Benehmen sie unannehmbar finden.

HABT IHR ES GESCHAFFT?

1: (fair), (stören) 2: (redet) 3: (GUTEN) 4: (Cyber-Mobbing) 5: (blockiere) 6: (kenne) 7: (antworten)

VORGESCHLAGENE LÖSUNGEN ZU DEN SITUATIONSKARTEN

SITUATION 7. Dies ist sicherlich keine akzeptable Art, euer Mobiltelefon zu benutzen. Verbreitet keine Botschaften, Bilder oder anderes, schädliches Material. Behandelt andere immer, wie ihr selber behandelt werden möchtet. Sprecht in solchen Situationen immer mit euren Eltern oder einer anderen erwachsenen Person, der ihr vertraut.

SITUATION 8. Alex sollte seinem Freund sagen, dass das gemeine Verhalten des anderen nicht seine Schuld ist. Er sollte auf die Botschaften nicht antworten, sondern sie als Beweis behalten und sie seinen Eltern oder LehrerInnen zeigen. Alex sollte auch mit seinen Eltern sprechen, die ihn dabei unterstützen können, seinem Freund zu helfen.

SITUATION 9. Bei der Netiquette geht es darum, die anderen im Web genau so zu behandeln, wie ihr selbst behandelt werden möchtet. Ihr habt sicherlich inzwischen genug gelernt, um Marie bei dieser Aufgabe zu helfen.

4. Unterhaltung & Herunterladen

KOMMENTIERTE ÜBUNGEN

Öffnet eure bevorzugte Suchmaschine. Tippt „kostenlose Klingeltöne“ oder „kostenlose Spiele“ ein und schaut euch die Resultate an. **Überprüft einige der Webseiten. Könnt ihr Fallen entdecken?**

Üben Sie, indem Sie eine Suche mit den angegebenen Stichwörtern durchführen, und prüfen Sie, ob Sie Marketingfallen auf den Webseiten finden können. Sehen Sie selbst, wie die Informationen im Kleingedruckten in den Werbeslogans fehlen.

Was ist euer bevorzugtes Computerspiel? Prüft, ob eure Eltern es wissen und es beschreiben können. Wenn sie keine Ahnung haben, erklärt es ihnen erst und lasst sie dann eine kleine Beschreibung aufschreiben. Haben sie es geschafft? Welche Note würdet ihr ihnen geben?

Ein Elternteil verfasst eine kurze Beschreibung des bevorzugten Spieles des Kindes, das Kind malt ein Bild davon.

Wissen Sie wirklich, welche Spiele Ihre Kinder online spielen, und kennen Sie ihre Lieblingsspiele? Lassen Sie Ihr Wissen von ihnen prüfen!

HABT IHR ES GESCHAFFT?

1: (kostenlos) 2: (Formulare) 3: (Fallen) 4: (Online-Formulare), (persönlichen) 5: (Kreuz) 6: (ignorieren) 7: (Privatsphäre) 8: (frage) 9: (Ladet), (herunter)

VORGESCHLAGENE LÖSUNGEN ZU DEN SITUATIONSKARTEN

SITUATION 10. Onlinefragebögen können sehr nützlich sein, um Reaktionen von den BenutzerInnen zu erhalten. Falls jedoch persönliche Daten gesammelt werden, sollte der Verwendungszweck deutlich angegeben sein. Raten Sie Ihren Kindern, Onlineformulare nur dann auszufüllen, wenn sie deren Zweck kennen. Selbst dann sollten sie sehr vorsichtig mit ihren persönlichen Informationen umgehen (siehe Kapitel Kommunikation).

SITUATION 11. Es gibt kostenlose Dienstleistungen im Internet, aber Klingeltöne, Hintergrundbilder, mp3s, Avatare und solche Dinge sind selten kostenlos. Wenn Alex sich die Webseite genauer ansieht, entdeckt er wahrscheinlich Kleingedrucktes, das ihm den wahren Preis dieser Dienstleistungen mitteilt. Klingeltöne, Rätsel, Spiele usw. sind ausgezeichnete Mittel, um Leute zu verlocken, so genannte "kostenlose" Dienstleistungen zu abonnieren, die sie in Wirklichkeit Geld kosten werden.

SITUATION 12. Alex sollte daran denken, seine Identität für sich zu behalten, wenn er online mit Leuten spielt, die er im wirklichen Leben nicht kennt. Er sollte keine Informationen über seinen Wohnort, seine Schule, seinen Familiennamen usw. preisgeben. Er sollte auch seine Eltern über die Spiele informieren, mit denen er sich beschäftigt, und nie ein Spiel aus dem Internet herunterladen, ohne sie vorher zu fragen, da dies dem Computer Schaden zufügen könnte.

D. Glossar

Abonnieren: Anmelden für eine Dienstleistung oder Nachrichtenaktualisierung, die direkt an das persönliche E-Mail-Postfach geschickt wird.

Akronym: Eine Abkürzung, die aus den ersten Buchstaben jedes Wortes eines Satzes oder eines Ausdrucks besteht. Akronyme werden häufig von Chattern benutzt, um schneller zu kommunizieren, zum Beispiel LoL, CU, Btw (siehe Kapitel „Kommunikation").

Anhang: Eine Computerdatei, die an eine E-Mail-Nachricht angehängt ist. Würmer und Viren werden oft in Form von E-Mail-Anhängen verbreitet. E-Mails von unbekannten Absendern mit Anhängen sollten als verdächtig angesehen werden.

Anmelden: Abonnieren eines Online-Dienstes wie Newsletter, Diskussionsforum, E-Mail, Chat-Räume usw. Normalerweise sollten die BenutzerInnen die Möglichkeit haben, sich jederzeit wieder abzumelden.

Anti-Spyware: Ein Programm, das Spyware bekämpft. Das Programm scannt alle eingehenden Daten auf Spyware und blockiert die gefundenen Gefahren oder liefert eine Liste mit verdächtigen Eingängen, die zu löschen sind.

Anti-Virus: Ein Computerprogramm, das Computerviren und andere schädliche Computersoftware zu identifizieren, zu isolieren, zu blockieren und zu eliminieren versucht.

Der Anti-Virus scannt die Dateien, um nach bekannten Viren zu suchen, und identifiziert verdächtiges Verhalten der Computerprogramme, die auf eine Infektion hindeuten.

Avatar: Das Profil eines Benutzers/einer Benutzerin, dargestellt durch einen Benutzernamen und ein Bild, ein Symbol oder eine 3-D-Figur in Online-Computerspielen und virtuellen Welten.

Benutzerprofil: Eine Reihe von Informationen, die eine/n bestimmte/n BenutzerIn einer Software, Webseite oder eines anderen technischen Hilfsmittels beschreiben. Normalerweise beinhalten die Informationen den Benutzernamen, das Passwort und andere Details (z.B. Geburtsdatum, Interessen).

Beratungsstelle: Ein E-Mail- oder auch Telefondienst, der in mehreren Ländern von Kinderhilfsorganisationen und Mitgliedern des Insafe-Netzwerks zur Verfügung gestellt wird, in Deutschland das Kinder- und Jugendtelefon der Nummer gegen Kummer (s. Weiterführende Informationen). Kinder können ihre Bedenken über illegale und schädliche Inhalte hier äußern und über unangenehme oder angsteinflößende Erfahrungen in Zusammenhang mit ihrer Benutzung von Online-Technologien berichten.

Betriebssystem: Ein Programm, das die Basisfunktionen eines Computers steuert und das Funktionieren anderer Programme ermöglicht. Bekannte Beispiele sind Windows, Linux und Mac OS.

Blog: Kurzform von Weblog. Eine Webseite, für die eine Einzelperson oder eine Gruppe Inhalte erstellt, normalerweise auf täglicher Basis, die aus Texten, Bildern, audiovisuellen Dateien und Links besteht.

Browser: Ein Programm zur Ansicht von Webseiten. Internet Explorer, Mozilla Firefox und Opera sind einige der gebräuchlichsten Browser für Windows, Safari wird häufig auf Macs benutzt. Die aktuellsten Versionen dieser Browser enthalten innovative Optionen zur elterlichen Kontrolle.

CD-ROM: Ein Akronym für Compact Disc Read-Only Memory. Es handelt sich um eine nicht beschreibbare CD mit Daten, die von einem Computer gelesen werden können. CD-ROMs werden allgemein benutzt, um z.B. Computersoftware zu verteilen.

Chat: Synchrone Kommunikation über das Internet durch geschriebene Botschaften über Chat-Anwendungen und Instant Messaging (z.B. ICQ, WLM (Windows Live Messenger)).

Chat-Raum: Öffentlicher virtueller Ort für die Kommunikation in Echtzeit. Leute aus der ganzen Welt können sich in Chat-Räumen treffen und anhand von Mitteilungen, die sie auf ihrer Tastatur eintippen, diskutieren. Wenn Kinder Chat-Räume benutzen, sollten sich die

Eltern vergewissern, dass diese ihrem Alter angepasst sind und von Aufsichtspersonen und Moderatoren überwacht werden.

Computerdatei: Ein Archiv/eine Sammlung verbundener Informationen (Dokumente, Programme usw.), die auf einem Computer unter einem eigenen Dateinamen abgespeichert sind. Computerdateien können als das moderne Gegenstück zu Papierdokumenten angesehen werden, die in Büro- und Bibliotheksdateien aufbewahrt werden.

Computerprogramm: Normalerweise als Software bezeichnet. Software besteht aus einer strukturierten Folge von Anweisungen, die von Computerprogrammierern geschrieben wurden und es einem Computer ermöglichen, Aufgaben auszuführen. Softwareprogramme werden z.B. auf CD-ROMs verkauft.

Cookie: Eine Datei, die von einer Webseite im Internetbrowser abgelegt wird. Jedes Mal, wenn die Webseite aufgerufen wird, wird das Cookie an den Server zurückgeschickt, auf dem die Webseite untergebracht ist. Cookies geben die Seiten-Vorlieben von Nutzern an und werden z.B. auf Online-Shopping-Webseiten benutzt. Die Ablehnung von Cookies kann die Nutzungsmöglichkeiten bei manchen Webseiten einschränken.

Cracker: Eine Person, die sich illegal Zugang zu einem Computersystem verschafft.

Cracken: Das illegale Kopieren von kommerzieller Software unter Verletzung des Urheberrechts.

Cyber-Mobbing: Bezieht sich auf das Mobbing durch elektronische Medien, oft durch Chats, Soziale Netzwerke oder E-Mails. Diese Nachrichten oder E-Mails können Drohungen, sexuelle Bemerkungen und abwertende Kommentare beinhalten. Täter können zum Beispiel persönliche Kontaktinformationen ihrer Opfer veröffentlichen und sogar ihre Identität annehmen und Material unter ihrem Namen veröffentlichen, um die Opfer zu diffamieren oder zu verhöhnen.

Datenschutz: Die Befähigung einer Einzelperson oder einer Gruppe, veröffentlichte Informationen über sich selbst zu kontrollieren und sich somit selektiv zu erkennen zu geben. Datenschutz steht manchmal in Verbindung mit Anonymität, dem Wunsch, in der öffentlichen Welt unerkannt zu bleiben.

Datenschutzeinstellungen: Eine Reihe spezifischer Datenschutzdetails, die der Nutzer selbst bearbeiten kann, um den Datenschutz bei der Veröffentlichung persönlicher Informationen, Cookies usw. zu erhöhen.

Dateitausch: Der Online-Austausch von Dateien zwischen Computerbenutzern. Der Begriff deckt sowohl das Anbieten von Dateien an andere Benutzer (Hochladen) wie das

Kopieren verfügbarer Dateien aus dem Internet auf einen Computer (Herunterladen) ab. Dateien werden oft über P2P(Peer-to-Peer)-Netzwerke ausgetauscht.

Dateitransfer: Der Vorgang der Übermittlung von Dateien über ein Computernetzwerk. Vom Standpunkt des Benutzers/der Benutzerin wird die Übermittlung von Dateien oft als Hoch- oder Herunterladen bezeichnet.

Digitales Spiel: Ein von Spieleentwicklern entworfenes Spiel, das z.B. auf einem Computer gespielt wird. Ein Online-Spiel ist ein digitales Spiel, das eine Live-Verbindung zum Internet benötigt, um gespielt zu werden. Online-Spiele können die Interaktion zwischen mehreren SpielerInnen fördern.

Elterliche Kontrolle: Siehe Definition für „Familieneinstellungen".

E-Mail: Ein elektronisches Mittel der geschriebenen Kommunikation, das es ermöglicht, Nachrichten mit allen möglichen Computerdateien im Anhang zu verschicken – Texte, Bilder, Audiodateien und mehr.

E-Mail-Adresse: Eine virtuelle Stelle, an die E-Mail-Nachrichten geschickt werden können. E-Mail-Adressen bestehen aus zwei Teilen, getrennt durch das @-Symbol.

Emoticon: Ein Bild, ein Symbol, wird benutzt, um Gefühle und Emotionen zu übermitteln, z.B. ein Smiley. Es kann durch die üblichen Tastaturbuchstaben und Satzzeichen oder durch vorgefertigte Zeichen symbolisiert werden, wie sie in Chat-Räumen, Spielräumen, Instant Messaging auf Mobiltelefonen usw. zur Verfügung gestellt werden.

Familieneinstellungen: Auch bekannt als elterliche Kontrolle. Die Einstellungen zum Anpassen des Browsers oder eines anderen Web-Tools an die persönlichen Vorlieben, um sie durch die Anwendung von Inhaltsfiltern, Zeitbegrenzung, Spielkontrollen usw. kinderfreundlicher zu machen.

Favoriten /Lesezeichen: Ein anpassbarer Ordner des Browsers, in dem interessante Links gespeichert werden. Diese können in Unterordner organisiert und/oder mit Stichwörtern gekennzeichnet werden, um sie einfacher zu finden.

Filter: Anwendung, die den Zugang zu Informationen oder bestimmten Internetdiensten regelt, vor problematischen Webseiten warnt, der Navigation des Benutzers/der Benutzerin nachgeht, riskante Seiten blockiert und einen Computer sogar ganz abschalten kann. Filtersysteme können auf Einzelrechnern, auf Servern, auf Telefonen mit Internetzugang usw. installiert werden.

Firewall: Hardware- und Softwarekomponenten, die den Zugriff von unbefugten Nutzern

(wie Hacker und Cracker) auf einen mit dem Internet verbundenen Computer oder ein Computernetzwerk verhindert.

Flaming: Ein feindseliger und beleidigender Austausch zwischen InternetnutzerInnen. Normalerweise spielt sich dieser in Diskussionsforen, in Chats oder sogar per E-Mail ab.

Formular (Online-Formular): Ein formatiertes Dokument mit leeren Feldern, in die man Daten eingeben kann. Das elektronische Formular kann mit freiem Text oder durch die Auswahl von Alternativen in vorher erstellten Listen (z.B. Aufklapplisten) ausgefüllt werden. Nach dem Versand werden die Daten direkt an eine Verarbeitungsanwendung geschickt, die die Informationen in eine Datenbank eingibt.

Forum: Eine Online-Diskussionsgruppe, in der TeilnehmerInnen mit gemeinsamen Interessen ihre Meinung zu verschiedenen Themen austauschen können.

Freeware und Shareware: Im Allgemeinen ist Software durch Urheberrechte geschützt und kann daher meist nicht kostenfrei heruntergeladen werden. Freeware bedeutet, dass der/die InhaberIn des Urheberrechts der Software einverstanden ist, dass die Software von jedem kostenlos benutzt wird. Shareware bedeutet, dass der/die InhaberIn des Urheberrechts jedem gestattet, die Software während einer Testperiode auszuprobieren. Nach dieser Periode muss der/die BenutzerIn eine Gebühr bezahlen, um die Dienstleistung weiterhin zu benutzen.

Grooming: Die Benutzung von Chat-Räumen durch Pädophile, um mit Kindern Kontakt zu knüpfen, indem sie behaupten, Gleichaltrige zu sein. Pädophile fangen Unterhaltungen mit möglichen Opfern an, um Informationen über deren Aufenthaltsort, Interessen, Hobbies und sexuelle Erfahrungen zu gewinnen. Diese Verbrecher benutzen verschiedene Mittel, um Kinder in Unterhaltungen sexueller Art zu verwickeln.

Hacker: Allgemein benutzter Begriff für eine Person, die sich mit Computer-Cracken beschäftigt (siehe „Cracker"). Kann in Computerkreisen auch für Personen angewandt werden, die computerbegeistert sind.

Handy: Ein elektronisches Telekommunikationsgerät, auch bekannt als Mobiltelefon, Mobile, Smartphone. Es verfügt über die gleichen Basisfunktionen wie eine normale Festnetzleitung. Die meisten Mobiltelefone verfügen heutzutage über eine Kamera und viele bieten Zugang zum Internet (gegen Bezahlung).

Hardware: Der physische Teil eines Computers, im Gegensatz zur Computersoftware, die im Inneren der Hardware agiert. Die Hardware kann sich im Computer befinden – Hauptplatine, Festplatte und RAM (oft als Komponenten bezeichnet) – oder extern sein – Bildschirm, Tastatur, Drucker usw. (auch Peripheriegeräte genannt).

Herunterladen: Bezieht sich auf den Vorgang, eine Datei von einem Online-Dienst auf einen Computer zu kopieren.

Hintergrundbild: Ein Muster, ein Bild usw., das den Hintergrund des Computerbildschirms darstellt.

Homepage: Eine Webseite, die automatisch geladen wird, wenn ein Webbrowser startet. Der Begriff wird auch für die erste Seite oder die Hauptseite einer Webseite (siehe Definition) benutzt.

Hotline: Telefonnotrufstelle oder webbasierte Dienstleistung, bei der Beschwerden über vermeintliche illegale Inhalte und/oder die illegale Nutzung des Internets eingereicht werden können. Hotlines müssen über wirksame und durchsichtige Verfahren verfügen, um mit Beschwerden umzugehen und sich die Unterstützung der Regierung, der Industrie, der Strafverfolgungsbehörden und der InternetnutzerInnen in den teilnehmenden Ländern zu sichern. Die beiden deutschen Hotlines sind jugendschutz.net und internet-beschwerdestelle.de (s. Weiterführende Informationen).

Identitätsdiebstahl: Das Stehlen persönlicher Angaben (z.B. Name, Geburtsdatum, Kreditkartennummer) und deren illegale Verwendung.

Illegale Inhalte: Online-Inhalte, die laut der nationalen Gesetzgebung illegal sind. Häufig sind solche Inhalte Bilder von Kindesmissbrauch, illegale Aktivitäten in Chat-Räumen (z.B. Grooming), volksverhetzende und fremdenfeindliche Webseiten.

Instant Messaging: Eine Form der sofortigen und simultanen elektronischen Kommunikation zwischen zwei oder mehreren BenutzerInnen (z.B. ICQ, WLM - Windows Live Messenger). Die sofortige Nachrichtenübermittlung ermöglicht es, mit einer ausgewählten Liste von Kontakten zu kommunizieren. Wenn Personen aus der Kontaktliste online sind, wird man davon unverzüglich in Kenntnis gesetzt.

Internet: Ein weltweites, öffentlich zugängliches Netzwerk von zusammenhängenden Computernetzwerken für die Übermittlung und den Austausch von Daten. Es enthält kleinere häusliche, akademische, geschäftliche Netzwerke und Regierungsnetzwerke, die zahlreiche Dienstleistungen wie Informationen, E-Mail, Online-Chat, Dateitransfer usw. anbieten.

Internetverbindung: Bezieht sich auf die Mittel, mit denen sich die BenutzerInnen mit dem Internet verbinden. Übliche Methoden für den Internetzugang beinhalten den Zugang per Telefonleitung, über WLAN, Satellit und Mobiltelefone.

Junk/Spam-Ordner: in einem E-Mail-Postfach der Ort, wo E-Mails landen, die als Spam oder Junk angesehen werden.

Junk-Mail: s. Spam

Kinderpornografie: Fälschlich verwendeter Begriff für „sexueller Missbrauch von Kindern", dargestellt auf Fotos, Filmen etc. Dazu gehören auch Darstellungen, die den Anschein von sexuellen Handlungen an Kindern erwecken. Immer mehr Länder setzen auch sogenannte „Posing-Bilder" unter Strafe.

Klingelton: Ein Mobiltelefonklang für eingehende Anrufe. Es gibt eine große Vielfalt von anpassbaren Tönen und Melodien, die MobiltelefonbesitzerInnen herunterladen können, oft gegen Bezahlung.

Kontaktliste: Eine Sammlung von Kontakten in Sofortnachrichtenübermittlungs- und E-Mail-Programmen, bei Online-Spielen, in Mobiltelefonen usw. Kontakte können hinzugefügt, abgelehnt oder gelöscht werden.

Konto: Ein Konto erlaubt es, sich zu authentifizieren, und ermöglicht, anhand eines Benutzernamens und Passworts, Online-Dienste zu benutzen. Man kann auch im eigenen Betriebssystem getrennte Benutzerkonten für jedes Familienmitglied einrichten.

Link: Eine Referenz zu einem Dokument, das online zur Verfügung steht (Webseite, Textdokument, Bild usw.). Wenn man auf den Link klickt, wird man zu einer neuen Seite oder einer anderen Webseite weitergeleitet. Textlinks sind üblicherweise z.B. farblich oder durch Unterstreichung gekennzeichnet. Auch Bilder können als Links zu anderen Webseiten dienen.

Malware: Abkürzung für schädliche Software. Es handelt sich hierbei um Software, die erstellt wurde, um in ein Computersystem einzudringen und es zu beschädigen, ohne dass der/die BesitzerIn sich dessen bewusst ist. Es gibt Computerviren, Würmer, Trojaner, Spyware, betrügerische Adware und andere heimtückische und unerwünschte Software.

Manipulieren: Der Vorgang, ein Bild, eine Datei, ein Foto oder eine Illustration auf sichtbare oder unsichtbare Art zu verändern. Heutzutage gibt es zahlreiche Tools, die benutzt werden können, um den Inhalt oder die Form der Daten zu verändern und so die Wirklichkeit verfälscht wiederzugeben.

Massively Multiplayer Game: Spiel, das eine umfangreiche 3-D-Welt anbietet, die mit Tausenden von SpielerInnen bevölkert ist. Diese nehmen die Rolle fiktiver Figuren an und konkurrieren miteinander. Rollenspiele dominieren in dieser Kategorie, in der die TeilnehmerInnen gemeinsam Geschichten erfinden und diese erleben.

Melden: Eine Funktion, die es den BenutzerInnen öffentlicher virtueller Umgebungen ermöglicht, dem/der ModeratorIn oder Webmaster ein Problem zu melden (technischer Art,

unannehmbares Verhalten eines Benutzers/einer Benutzerin, illegale Inhalte usw.).

Mobbing: Belästigung durch wiederholte Angriffe, Drohungen, sexuelle Anspielungen oder abwertende Kommentare durch eine oder mehrere Personen.

mp3: Ein Kodierungsformat für Audiodateien. Eine mp3-Datei ist zehnmal kleiner als die Originalaudiodatei, der Klang hat jedoch fast CD-Qualität. Wegen ihrer geringen Größe und der guten Tonwiedergabe sind mp3-Dateien zu einer beliebten Möglichkeit geworden, um Musikdateien auf Computern und tragbaren Geräten zu speichern.

Nachrichtengruppe: siehe Definition für „Forum".

Netiquette: Internet-Etikette für die Höflichkeitsregeln der Online-Kommunikation.

Ordner: Eine Einheit in einem Dateisystem, das eine Gruppe von Dateien und/oder andere Verzeichnisse enthält. Ordner können mehrere Dokumente enthalten und werden benutzt, um Informationen zu organisieren.

P2P-Netzwerk: Ein Peer-to-Peer(P2P)-Netzwerk erlaubt es denjenigen, die damit verbunden sind, durch Hoch- und Herunterladen Dateien auszutauschen. Dies ist nur eine von vielen Möglichkeiten, um Dateien im Internet zu teilen. Einige Dateitauschdienste sind illegal.

Papierkorb: Ein Computerverzeichnis, in dem alle gelöschten Dateien vorübergehend gespeichert werden, bevor die BenutzerInnen sie endgültig löschen. Man muss regelmäßig alte und unerwünschte Dateien aus dem Papierkorb entfernen, um etwas Platz auf der Festplatte, dem internen Speicherplatz des Computers, zu schaffen.

Passwort: Eine geheime Folge von Buchstaben, die es dem/der BenutzerIn erlaubt, Zugang zu einer Datei, einem Computer, einem Konto oder einem Programm zu erhalten, als Sicherheitsmaßnahme gegen unbefugten Zugriff (siehe Kapitel „Kommunikation").

Persönliche Daten: Alle Informationen, die mit einer Person in Verbindung gebracht werden können. Falls persönliche Daten gesammelt, verarbeitet und gelagert werden müssen, ist die Bestimmung deutlich anzugeben.

Pop-up-Fenster: Ein zusätzliches Fenster, das beim Besuch einer Website oder beim Klicken auf einen bestimmten Link erscheint. Pop-up-Fenster enthalten ein Befehlsmenü und bleiben auf dem Bildschirm, bis man einen der Befehle auswählt oder es durch einen Klick auf das Kreuz in der oberen rechten Ecke schließt.

Port: Eine Schnittstelle auf einem Computer, die dazu dient, ihn mit einem anderen Gerät

zu verbinden. Ports können entweder intern oder extern sein. Interne Ports erstellen z.B. eine Verbindung zu einem CD/DVD-Laufwerk oder einem Netzwerk, während externe Ports die Verbindung mit einem Gerät wie einem Drucker oder einer Tastatur herstellen.

Privat: Alles über eine Einzelperson oder eine Gruppe, das der Öffentlichkeit nicht preisgegeben werden soll. Wenn eine Person etwas für sich behalten möchte, handelt es sich hierbei normalerweise um besondere oder vertrauliche persönliche Informationen.

Profil: Persönliche Benutzerinformationen in Social-Networking-Plattformen, Systemen für Instant Messaging, Online-Chat-Anwendungen, Online-Spielen usw. Profile können öffentlich oder privat sein und werden von den BenutzerInnen angepasst, um sich selbst in virtuellen Umgebungen darzustellen.

Prozessor: Auch Hauptprozessor (Central Processing Unit – CPU). Er ist der Teil des Computers, der Daten verarbeitet, Kontrollsignale erzeugt und Resultate speichert. Zusammen mit dem Computerspeicher bildet er den Kern eines Computers.

Scannen: Umwandlung von gedrucktem Material in digitale Dateien unter Anwendung eines Scanners. Diese Umwandlung ermöglicht es, das Material als elektronische Dateien auf dem Computer zu speichern, zu betrachten und es online zu verbreiten.

Schädliche Inhalte: Bilder, Texte, Dokumente usw., deren Inhalt Schaden verursachen kann, z.B. Bilder, die Gewalt darstellen – sie sind ungeeignet und schädlich für Kinder und Minderjährige.

Screen-Name: Siehe Definition für „Spitzname".

Sexting: Freiwilliger Austausch von erotischem Bildmaterial des eigenen Körpers über digitale Medien.

Sicherheitseinstellungen (Profil): Eine Reihe anpassbarer Sicherheitsoptionen für das eigene Online-Profil (siehe Definition). Gewöhnlich stehen diese Optionen in Verbindung mit dem Öffnen von Bildern und Dateien, der Identifizierung vertrauenswürdiger Informationsanbieter und der Erlaubnis für erwachsene Inhalte.

Software: Siehe Definition für „Computerprogramm".

Soziale Netzwerke (Social Networking Sites): Online-Plattform für Gemeinschaften von Mitgliedern, die ähnlichen Interessen und Aktivitäten nachgehen (z.B. Facebook, werkennt-wen, schülerVZ). Die Mitglieder müssen Benutzerprofile erstellen und können Hilfsmittel gebrauchen, um Texte, Bilder und andere Dateien hochzuladen, Nachrichten in Nachrichtenforen zu veröffentlichen und an Foren teilzunehmen. Viele Social Networking

Sites sind Kindern unter 13 Jahren untersagt und bieten Sicherheitseinstellungen für das Profil.

Spam: Unerwünschte E-Mails, normalerweise kommerzieller Art und in großen Mengen verschickt. Anderen Personen Spam zu schicken ist zweifellos einer der berüchtigsten Missbräuche des Internets.

Spam-Filter: Eine Anwendung, die verhindert, dass Spam-Nachrichten im eigenen E-Mail-Posteingang landen.

Speicher-/USB-Stick: Datenspeichergerät mit einem USB(Universal Serial Bus)-Stecker. Ein USB-Stick ist üblicherweise schmal, leicht, abnehmbar und wieder beschreibbar.

Spitzname: Ein Synonym für Screen-Name und Pseudonym. Er stellt den/die BenutzerIn eines Online-Dienstes dar und wird von dem/der BenutzerIn selbst definiert. Er stellt die BenutzerInnen in der Kontaktliste, im Chat-Raum usw. dar. Spitznamen können, wenn sie gut gewählt sind, die Anonymität online bewahren.

Spyware: Malware, heimlich an aus dem Internet heruntergeladenen Dateien angehängt, die sich selbst auf dem Computer installiert und die Aktivitäten überwacht. Sie schickt Informationen an eine dritte Partei, oft Firmen, die an der Erstellung persönlicher Profile interessiert sind, um Werbung oder andere Informationen zu schicken, oder an Cracker, die sich Zugang zu privaten Informationen verschaffen möchten.

Suchmaschine: Ein Hilfsmittel für die Suche nach Informationen auf Webseiten. Bekannte Beispiele sind Google, Bing oder Yahoo. Suchmaschinen verfügen über fortgeschrittene Benutzereinstellungen, unter denen sich manchmal interessante Sicherheitseinstellungen finden. Spezielle Suchmaschinen für Kinder sind www.fragfinn.de, www.blinde-kuh.de oder www.helles-koepfchen.de. Die Recherche mithilfe dieser Suchmaschinen geschieht innerhalb einer Liste mit geprüften und für Kinder unbedenklichen Internetseiten.

Symbolleiste: Eine Reihe von Symbolen oder Schaltflächen, die Teil der Schnittstelle des Softwareprogramms sind. Symbolleisten dienen als immer zur Verfügung stehende, einfach zu benutzende Schnittstellen zur Ausführung gebräuchlicher Funktionen.

Testsoftware: Software, die man vor dem Kaufen ausprobieren kann. Testversionen enthalten gewöhnlich alle Funktionen der normalen Version, können aber nur für eine begrenzte Zeit benutzt werden.

Trojaner: Heimtückische Codes, Malware, die sich hinter harmlos aussehenden Vorgängen wie Spielen oder sogar Anti-Virus-Programmen verstecken und sich so in den Computer einschleusen. Trojaner vervielfältigen sich nicht selbst, sind aber normalerweise dazu da,

um sich Zugang zu empfindlichen Daten zu verschaffen oder Daten zu zerstören. Sie können die Festplatte löschen oder vertrauliche Informationen stehlen.

Urheber/In: Der/die SchöpferIn einer literarischen oder audiovisuellen Arbeit, einer Software usw. Urheberrechte schützen die Werke des Urhebers vor illegaler Reproduktion.

Urheberrecht: Eine Reihe exklusiver Rechte zur Regelung der Anwendung einer Idee, einer Arbeit oder einer Information. Das Urheberrecht wird durch das Symbol © dargestellt.

URL (Uniform Resource Locator): Die Adresse einer bestimmten Webseite oder Datei im Internet. Sie enthält keine Sonderzeichen oder Abstände und benutzt Schrägstriche, um die verschiedenen Verzeichnisse zu markieren. Der erste Teil der Adresse deutet an, welches Protokoll benutzt werden muss, der zweite Teil präzisiert die IP-Adresse oder den Domain-Namen, wo sich die Ressource befindet.

Verzeichnis: Eine Organisationseinheit, die der Computer benutzt, um Ordner und Dateien in einer hierarchischen Struktur zu organisieren, z.B. „Meine Dokumente“, „Meine Bilder“ usw.

Voice over Internet Protocol (VoIP): Eine Technologie, die es den BenutzerInnen ermöglicht, über Internet miteinander zu sprechen, nachdem sie eine Software heruntergeladen haben. Die Anrufe sind meist kostenlos für BenutzerInnen des gleichen VoIP-Anbieters (z.B. Skype, Voicebuster). Solche Software bietet normalerweise auch Möglichkeiten zum Chat und Dateitausch.

Virtueller Besitz: Eine Reihe von Objekten, die alle TeilnehmerInnen eines Spieles erhalten. Jede/r SpielerIn besitzt seine/ihre Objekte virtuell über ein Computerterminal, das die Objekte darstellt.

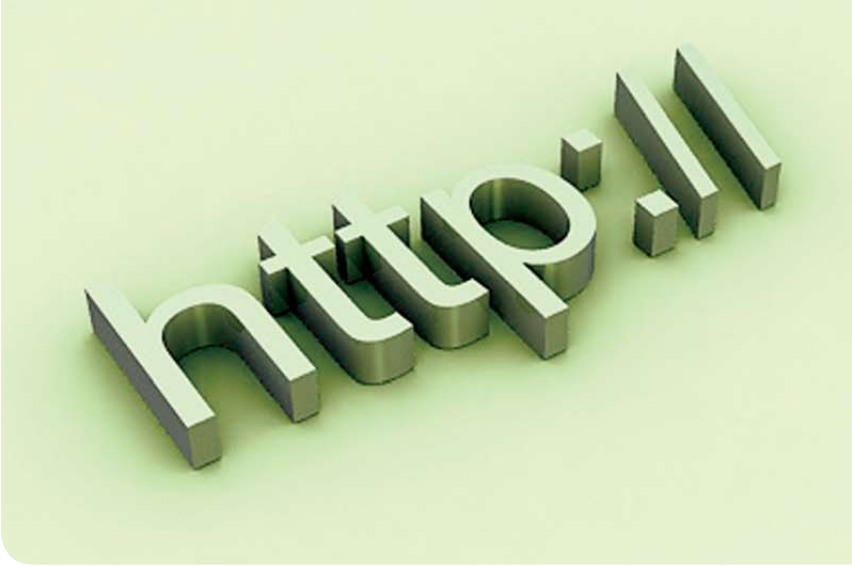
Virus: Eine Art heimtückischer Code, Malware, entworfen, um sich dank des Eingriffs der BenutzerInnen zu verbreiten. Es verbreitet sich normalerweise durch E-Mail-Anhänge, jedoch auch durch infizierte externe Speichergeräte (USB-Sticks, CD-ROMs).

Web: Kurzform von World Wide Web. Eine Sammlung von Online-Dokumenten in HTML (HyperText Markup Language), die Links zu anderen Dokumenten sowie zu Grafiken, Audio- und Videodateien enthalten. Das Web ist ein Teil des Internets.

Webseite: Ein Standort im World Wide Web. Jede Webseite enthält eine Homepage (Startseite), das erste Dokument, das beim Öffnen der Seite erscheint. Webseiten enthalten normalerweise Links zu anderen Dateien und Seiten. Webseiten gehören Einzelpersonen, Firmen oder Organisationen und werden von diesen verwaltet.

Webcam: Eine Kamera, die im Web, in Instant Messaging Programmen, in Videokonferenzanwendungen, auf Chat-Plattformen usw. senden kann. Kameras mit Zugang zum Web beinhalten eine digitale Kamera, die Bilder entweder fortlaufend oder in regelmäßigen Abständen auf einen Webserver hochlädt.

Wurm: Eine bestimmte Art von Virus, der sich selbst vervielfältigt, sich ohne das Eingreifen des Besitzers auf zahlreiche Computer verbreiten, ein Netzwerk beschädigen, einen Computer herunterfahren kann usw.



E. Weiterführende Informationen

Umfangreiche Informationen zu allen Themen rund um den Bereich Internet und Internetsicherheit finden Sie auf der Internetseite der EU-Initiative klicksafe:
www.klicksafe.de

Die beiden deutschen Meldestellen jugendschutz.net und Internet-Beschwerdestelle bieten Onlineformulare, anhand derer illegale und jugendgefährdende Inhalte im Internet gemeldet werden können:
www.jugendschutz.net
www.internet-beschwerdestelle.de

Rat und Hilfe können Kinder und Jugendliche bei der Nummer gegen Kummer erhalten:
Online-Beratung:
www.nummergegenkummer.de
Kinder- und Jugendtelefon: 0800 – 111 0 333 (Mo - Sa von 14-20 Uhr)

Auf dem Eltern-Portal des Internet ABC finden Eltern in dem Bereich „Wissen, wie's geht" bspw. Informationen zu den Themen „Chatten/Instant Messenger" und „Online-Communitys". Innerhalb der Kinderseite des Angebotes sind speziell für Kinder aufbereitete Informationen, sowie ein Surfschein für Kinder beinhaltet:
www.internet-abc.de/eltern
www.internet-abc.de/kinder

Die Webseite “Surfen ohne Risiko” des Bundesfamilienministeriums, umgesetzt von jugendschutz.net, bietet Informationen für Eltern sowie u.a. die Möglichkeit, mithilfe eines Moduls eine individuelle Startseite selbst zusammenzustellen:
www.surfen-ohne-risiko.de

INSAFE

Das europäische e-Sicherheits-Netzwerk möchte InternetnutzerInnen für die positiven Aspekte des Web und gleichzeitig für die potenziellen Risiken sensibilisieren:
www.saferinternet.org

Deutsche Version unterstützt von:

Unterstützt von:

Titel: e-Sicherheits-Kit für die Familie • Erstellt von Insafe, unterstützt von Liberty Global Inc. und UPC im Jahr 2008
Prefix: 9789078209 • Id 51950 • ISBN-NUMMER: 9789078209584 • EAN : 9789078209584

Urheberrecht: Dieses Werk ist lizenziert unter der Creative Commons Namensnennung-Keine kommerzielle Nutzung-Keine Bearbeitung 3.0 Unported. Um eine Kopie dieser Lizenz einzusehen, folgen Sie diesem Link: http://creativecommons.org/licenses/by-nc-nd/3.0