Leitfaden für Eltern

Schützen Sie Ihre Kinder online!

BEE SECURE

ins@fe

LIBERTYGLOBAL

INHALT

A. Gebrauchsanweisung für dieses Kit

Planst du für ein Jahr, so pflanze Reis.
Planst du für zehn Jahre, so pflanze einen Baum.
Planst du für ein ganzes Leben, so erziehe ein Kind.
Chinesisches Sprichwort

Liebe Eltern/Pädagogen,

Sie halten das e-Sicherheits-Kit für Familien mit Kindern zwischen sechs und zwölf Jahren in den Händen. Dieses Kit 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 Schärfung des Bewusstseins für Themen im Bereich einer sichereren Benutzung des Internets arbeiten. Die Entwicklung und Herstellung dieses eSicherheits-Kits wurde von folgenden Partnern unterstützt: CASES du Ministère de l'Economie et du Commerce Extérieur, le Guichet Unique, Ministère de l'Education et de la Formation Professionnelle, Ministère de la Famille et de l'Intégration, Ministère de la Santé und dem Service National de la Jeunesse.

Genau wie das Spielen auf dem Spielplatz oder das Überqueren einer Straße gefährlich sein können, wenn man nicht aufpasst, kann die Benutzung des Internets und der mobilen Technologien Gefahren mit sich bringen, wenn man sich unvorsichtig verhält. Glücklicherweise gibt es Hilfsmittel, um den InternetbenutzerInnen die nötigen Kenntnisse über die Vorteile und Risiken des Internets zu vermitteln.
Mit diesem neuen Kit können Sie Ihren Kindern beibringen, das Internet sicher und nutz-

bringend anzuwenden. Das Kit bietet über fünfzig Sicherheitstipps und Übungen, die Ihnen dabei helfen werden, Ihren Kindern die e-Sicherheit auf amüsante, ansprechende und unaufdringliche Art nahezubringen, einschließlich:

- zwei e-Sicherheitsbroschüren: eine Broschüre für Spaß im Netz mit der ganzen Familie und ein Leitfaden für Eltern;
- goldenen Regeln;
- ein Familienzertifikat;
- Aufkleber;
- zwölf Situationskarten zum Ausschneiden für die Kinder.

Sowohl die Familien- als auch die Elternbroschüre sind farblich gekennzeichnet, um die vier e-Sicherheitsthemen hervorzuheben: Sicherheit, Kommunikation, Unterhaltung & Downloads, Cybermobbing und Gesundheit. Der Leitfaden für die Eltern dient als Referenz für die Familienbroschüre: Er enthält Hintergrundinformationen, Hinweise zu den Aktivitäten, Lösungsvorschläge zu den Übungen und Situationskarten.

Die Familienbroschüre ist für die gemeinsame Benutzung durch Eltern und Kinder bestimmt. Die vier Themen werden durch die Geschichte von zwei Jugendlichen, Pit und Claire, ihren Eltern und dem Informatikgenie Laura behandelt. Jedes Kapitel enthält Lernaktivitäten, einschließlich Online-Übungen, Ratespiele, goldene Regeln und nützliche Links.

Lesen Sie die Geschichte laut mit Ihren Kindern und machen Sie zusammen die vorgeschlagenen Übungen. 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 anschließend alle gemeinsam einige goldene Regeln festlegen und das Familienzertifikat unterschreiben. Schließlich können die Kinder die Broschüren mit Emoticon-Aufklebern verzieren.

Ihr Feedback ist für uns sehr wertvoll. Zögern Sie nicht, bei Fragen oder Kommentaren Ihr lokales Insafe-Zentrum (www.bee-secure.lu) zu kontaktieren. Wir wünschen Ihnen und Ihrer Familie viel Spaß mit dem Kit „Internet? – Aber sicher!“

Sicheres Surfen wünscht

BEE SECURE insafe

1. Schutz bringt Sicherheit

EIN COMPUTER ZU H@USE

Ein Computer zu Hause kann für die ganze Familie eine großartige Wissensquelle und Freizeitbeschäftigung sein. Wenn Sie den Computer in einem gemeinschaftlichen Raum aufstellen und bestimmte Regeln hinsichtlich der Bedingungen und Nutzungsdauer festlegen, schützen Sie Ihre jungen Familienmitglieder.
Denken Sie daran, dass Ihre Kinder auch bei Freunden, in Internetcafés, über Handy usw. Zugang zum **Internet** haben. Deshalb ist es wichtig, dass Sie gemeinsam einen sicheren 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. Zu den Lösungen zählen nützliche technologische Hilfsmittel und auch der gesunde Menschenverstand des Benutzers. 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 Benutzung von **Speichersticks** oder **CD-ROMS**, das Öffnen von **Anhängen** und das **Herunterladen** von **Dateien**, können Gefahren bergen. Diese Risiken bestehen größtenteils aus heimtückischen **Computerprogrammen** (sogenannte Schadprogramme), die entworfen wurden, um Ihrem Computer zu schaden, persönliche Informationen zu stehlen oder Ihnen unerwünschte Werbung zu schicken.
Den Kindern werden verschiedene Arten von Schadprogrammen vorgestellt – **Viren**, **Würmer**, **Trojanische Pferde** und **Spionageprogramme** – 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-** und **Anti-Spionage-Programme sowie eine richtig eingestellte Firewall** 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 % 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 Internet bei der Benutzung einer **Nachrichtengruppe**, einer **Chat**-Seite, eines öffentlichen **Forums**, einer **Social-Networking-Plattform** oder eines **Online-Forums** kann Spam verursachen. Es gibt eigenständige Programme, die E-Mail-Adressen aus dem Internet sammeln, 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 im Zusammenhang mit Pornographie, Pharmazeutika, dubiosen Finanzgeschäften usw. Darüber hinaus kann Spam auch heimtückische Programme enthalten. In den meisten Fällen wird Spam mit betrügerischen Absichten verschickt. Hier einige Tipps, wie Sie Ihre Familie schützen können:

- Benutzen Sie „**Spamfilter**“. 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 **Spamordner**, um zu sehen, ob keine E-Mails darin gelandet sind, die Sie eigentlich gerne gelesen hätten. Die Technologie ist nicht unfehlbar.
- Bringen Sie Ihren Kindern bei, nie E-Mails von unbekannten Absendern 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 beim Surfen im Internet Spaß haben und pädagogisch wertvolle Seiten 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 auf einer Reihe von Stichwörtern basiert, stößt man auch sehr leicht auf unerwünschte Inhalte. Ein unschuldig klingendes Stichwort kann zu einer nicht so unschuldigen Internetseite führen, die das fragliche Stichwort enthält. Hier einige Tipps, um Ihren Kindern dabei zu helfen,

sicherer im Internet zu surfen:

- Erstellen Sie mit Hilfe Ihres **Betriebssystems** (Windows, Linux, Mac OS) für Ihr Kind ein spezielles Benutzerkonto, für das Sie die **Kindersicherung** aktivieren können.
- Machen Sie sich mit den Kindersicherungsoptionen Ihres **Internet-Browsers** und der Suchmaschine vertraut. Vergewissern Sie sich, dass Sie alle Möglichkeiten der **Familieneinstellungen** dieser Hilfsmittel kennen.
- Schlagen Sie den jüngsten InternetbenutzerInnen unter Ihrer Aufsicht kinderfreundliche **Suchmaschinen** wie *www.blinde-kuh.de* vor.
- Speichern Sie die Adressen der Internetseiten, die Ihre Kinder am häufigsten besuchen, in entsprechenden Ordnern als **Favoriten bzw. Lesezeichen** (eine Option des Browsers). So ermöglichen Sie es ihnen, ihre Lieblingsseiten im **Netz** immer wieder zu besuchen, ohne eine Suchmaschine benutzen zu müssen.

Außer der Kindersicherung Ihres Browsers und der Suchmaschine können Sie noch einen zusätzlichen **Filter** benutzen, eine Software, die Minderjährige vor unangebrachten Inhalten des Internets schützen soll. Fragen Sie Ihren Händler um Rat oder suchen Sie im Internet nach **Demosoftware**. Denken Sie daran, dass nichts die Beratung durch Eltern und BetreuerInnen ersetzen kann. Technische Hilfsmittel sind nicht unfehlbar und können manchmal ein falsches Gefühl von Sicherheit hervorrufen, es sei denn, man benutzt seinen gesunden Menschenverstand.
Filtersoftware kann so einschränkend sein, dass 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 zu Internetseiten führt, die Gewalt beschreiben. Außerdem kann jeder Filter, der aktiviert werden kann, von cleveren Jugendlichen, die oft auch Experten der Spurenverwischung sind, deaktiviert werden. Sie können dies nur herausfinden, indem Sie selber lernen, wie man den Computer und die Software benutzt.
Besuchen Sie die Internetseite von **SIP-Bench** (siehe nützliche Links). Diese von der Europäischen Kommission unterstützte Studie testete 30 Hilfsmittel für die elterliche Kontrolle und die Bekämpfung von Spam, um deren Wirksamkeit zum Schutz von Kindern zwischen 6 und 16 Jahren gegen schädliche Inhalte in verschiedenen Internetanwendungen zu bewerten: **Surfen**, E-Mails schreiben, **Dateitransfer**, Chat-Seiten und **-Programme**.
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 beiliegenden Unterhaltungsbroschüre für die ganze Familie wird geraten, bei der Suche nach Informationen online immer mindestens drei Internetseiten zu 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

- Vergewissern Sie sich, dass Ihr Computer durch eine richtig eingestellte **Firewall** sowie durch Anti-Virus- und Anti-Spionage-Software geschützt ist. Sorgen Sie dafür, dass diese Schutzprogramme stets auf dem neuesten Stand sind, und beachten Sie die **Warnungen**.

• 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 Internet veröffentlichen. Vermeiden Sie E-Mails von unbekannten Absendern und **scannen** Sie die Anhänge, bevor Sie sie öffnen.

• Sorgen Sie durch die Einstellung der Kindersicherungsoptionen Ihrer Software auf folgenden Ebenen für ein Höchstmaß an Sicherheit: Betriebssystem, Internet-Browser, Suchmaschinen und E-Mail-Programm. Legen Sie separate **Benutzerkonten** für Ihre Kinder an. Versichern Sie sich, dass die Einstellungen für den Datenschutz auf dem höchsten Niveau stehen (begeben Sie sich zum Menüpunkt „Optionen" Ihres Browsers).

• Erwägen Sie die Anwendung zusätzlicher Filterprogramme.

• Kontaktieren Sie Ihren Internetanbieter oder einen Fachmann, sobald Ihr Computer ein eigenartiges Verhalten zeigt, das vermuten lässt, er könnte infiziert sein. Ihr Internetanbieter sollte auch Ratschläge für Eltern geben können.

• Schicken Sie einen Bericht an Ihre nationale Internet-**Hotline** (siehe nützliche Links), wenn Sie unerwünschte Inhalte finden.

• Setzen Sie sich so oft wie möglich neben Ihre Kinder, wenn diese 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.

NÜTZLICHE LINKS

Um sicher surfen zu können, ist Wissen Trumpf: Informieren Sie sich über die Risiken und die Möglichkeiten, sich zu schützen und vieles mehr. Weitere Details befinden sich auf der BEE SECURE-Internetseite:
www.bee-secure.lu

Aktuelle Informationen, praktische Tipps (z. B. Einstellung der Firewall) und Links rund um die Online-Sicherheit erhalten Sie ebenfalls auf dem luxemburgischen Informationssicherheitsportal:
www.bee-secure.lu

Sollten Sie während des Surfens im Internet auf Inhalte stoßen, die Sie für illegal halten (Darstellungen sexuellen Missbrauchs von Kindern, Rassismus ...), schicken Sie bitte eine Meldung an die luxemburgische Stopline:
www.lisa-stopline.lu

SIP-Bench, eine von der EU-Kommission unterstützte Studie über 30 Hilfsmittel für die elterliche Kontrolle und die Bekämpfung von Spam:
www.sip-bench.eu

2. Kommunikation

PUZZLESTÜCKE

Erinnern Sie sich noch daran, wie wichtig es für Sie als Jugendlicher war, den Kontakt mit Freunden zu halten? Das Internet bietet eine Menge neuer Orte, wo man seine Freunde treffen kann. Es hält neue Wege für die Selbstdarstellung und das Knüpfen von Kontakten durch E-Mails, Chatten, **Dateitransfer**, **Bloggen** und Social-Networking-Plattformen (z. B. MySpace, Facebook, Hi5, Habbohotel usw.) bereit. Die Jugendlichen von heute benutzen die Technologie, um neue Dinge auszuprobieren und in einer Umgebung Kontakte zu knüpfen, 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 Online-Interaktionen 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 enthält ein Busabonnement, eine Karte für den Fitnessclub oder eine Mitgliedskarte persönliche Informationen über Sie. Online-Konten und -Dienste sind ähnlich. Auch solche Dienste kann man nur benutzen, wenn man persönliche Informationen liefert, aus denen das „Benutzerprofil" erstellt wird. Wichtig ist, dass man die Art von Informationen, die man mitteilt, sowie die Personen, denen man sie mitteilt, selber aussuchen kann.

Beim Schutz der Privatsphäre geht es vielmehr darum, welche Informationen man den anderen über sich selbst preisgeben will. Jugendliche finden es toll, online mit Freunden zu kommunizieren und ihr Online-Image aufzubauen. Sie sind sich jedoch oft nicht der Folgen bewusst, welche die Veröffentlichung ihrer persönlichen Informationen haben kann.

ERSTELLUNG EINES PROFILS

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

Schaffen Sie mehrere E-Mail-Konten für verschiedene Online-Kontexte. Wenn Ihr Kind Online-Dienste wie Chat-Seiten oder -Programme, Blogs usw. benutzt, raten Sie ihm, eine neutrale E-Mail-Adresse und einen neutralen **Benutzernamen (Nickname)** zu verwenden. Auf diese Art benutzt Ihr Kind keine E-Mail-Adresse, aus der sich sein richtiger Name ableiten lässt.

Halten Sie **Passwörter** geheim. Vergewissern Sie sich, dass Ihre Kinder verstehen, dass sie ihre persönlichen Passwörter auch nicht mit Freunden teilen sollten. Achtung: Kinder tauschen Passwörter gerne als Vertrauensbeweis untereinander aus.

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. Bedenken Sie, dass **Soziale Netzwerke** zum einen von Unternehmen mit kommerziellem Interesse betrieben werden und zum anderen oft Sicherheitslücken aufweisen, die von Dritten mit unlauteren Absichten ausgenutzt werden können. Bringen Sie Ihren Kindern bei, nur mit Personen in Kontakt zu treten, die sie auch im realen Leben kennen.

Wenn Ihre Kinder Chat-Räume benutzen, prüfen Sie folgende Punkte:

- Gibt es **Moderatoren**? Falls kein Moderator anwesend ist, ist der Chat nicht sicher.
- Gibt es Hilfsmittel zum Ignorieren oder Blockieren unerwünschter Kontakte?
- Gibt es eine Hilfs- und **Melde**funktion auf der Internetseite, die im Problemfall genutzt werden kann?
- Sind die Regeln der Dienstleistung klar und deutlich erklärt?

FOTOS UND WEBCAMS

Kinder müssen verstehen, dass ein Foto von ihnen fester Bestandteil ihrer Privatsphäre ist und dass digitale Bilder äußerst aussagekräftig sind. Sie können einfach verbreitet und **gefälscht** werden. Fotos sind nicht mehr zu löschen, wenn sie einmal über einen Computer oder ein Mobiltelefon verschickt wurden – sie können für immer online bleiben! Webcams sollten mit Vorsicht benutzt werden, besonders Kinder sollten **Webcams** nicht ohne Aufsicht benutzen. Webcam-Chat-Tools 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 ein Foto von jemand anderem ins Internet setzen. Bei Personen unter 18 Jahren ist zusätzlich immer die Erlaubnis der Eltern einzuholen. 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. Sie als Eltern stellen Regeln auf, wie Ihre Kinder sich Fremden gegenüber in der echten Welt benehmen sollen. Wieso sollten Kinder nicht die gleichen Regeln auch online befolgen!?

Ihre Kinder bauen vielleicht eine starke Beziehung mit Online-Freunden auf. Sie können dazu neigen, Leuten ihr Vertrauen zu schenken, die Interesse und Verständnis zeigen, auch wenn sie diese 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 von Online-**Grooming**. 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 sicher zu gehen, dass es ihnen nicht passiert. Kommunikation ist der Schlüssel.

NETIQUETTE

Netiquette bezieht sich auf die guten Manieren im Internet und darauf, andere Leute im Netz so zu behandeln, wie man selber behandelt werden möchte. Kinder sind sich vielleicht dessen nicht bewusst, dass sie irrtümlicherweise jemanden online beleidigt haben. Leider benutzen manche Personen das Internet und/oder Handys ganz bewusst, um andere zu ärgern oder zu belästigen. Dies wird Cybermobbing genannt und betrifft etwa eins von vier Kindern (siehe Kapitel „Cybermobbing“ 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:

121: one to one

AFK: away from keyboard

A/S/L: age, sex, location (oder “ASL”)

BBB: bye bye baby

B4N: bye for now

BBL: be back later

BF: boyfriend or best friend

BFF: best friends forever

C: see?

Comp: computer

CU: see you

CUL: see you later

CYO: see you online

EGBOK: everything going to be ok

F2F: face to face

G2G or GTG: got to go

JJ: just joking

K: all right /ok

KFY/K4Y: kiss for you

KISS: keep it short and simple

KPC: keeping parents clueless

L8R: later

IRL: in real life

LMIRL: let’s meet in real life

LOL: laughing out loud, lots of love

LY4E: love you forever

NE1: anyone

NP: no problem/ noisy parents

OIC: oh, I see

OLL: online love

PAL: parents are listening

PAW: parents are watching

<G>: grinsen

GF: girlfriend

GFN: gone for now

GL: good luck

GM: good morning /good match

HAND: have a nice day

^5: High 5

H2G: have to go

HDOP: help delete online predators

IDK: I don't know

ILU/ILY: I love you / I like you

PIR: parent in room / people in room

PLZ/PLS: please

POS: parent over shoulder

RL: real life

S^, S'UP: what's up?

TTYL: talk to you later

TY: thank you

WB: welcome back/ write back

WDYT: what do you think

WTGP: want to go private?

WYCM: will you call me?

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

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

GOLDENE REGELN

• Nehmen Sie sich die Zeit, um herauszufinden, wie Ihre Kinder ihre Zeit online verbringen und lassen Sie sich von Ihren Kindern zeigen, wie sie mit ihren Freunden kommunizieren.

• Bringen Sie Ihnen bei, sowohl die eigene Privatsphäre als auch die von anderen mit Hilfe folgender Sicherheitsreflexe 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 um die elterliche Erlaubnis bitten, bevor sie Fotos oder Videos von sich selbst oder Ihrer Familie, Ihrem Haus, ihrer Schule usw. hochladen
- Fotos oder Videos, auf denen andere Personen zu sehen sind, dürfen nur mit deren Erlaubnis veröffentlicht werden. Bei Personen unter 18 Jahren müssen zusätzlich die Erziehungsberechtigten ihr Einverständnis geben.
- Persönliche Informationen wie Telefonnummern, Adresse, Schule, Sportverein usw. nur Personen mitteilen, die sie im echten Leben kennen

• Stellen Sie den Computer in einem gemeinschaftlichen Raum auf, damit Sie die Online-Aktivitäten Ihrer Kinder im Auge behalten können.

• Vergewissern Sie sich gemeinsam mit Ihren Kindern wie:

- man Kontakte ablehnen oder Personen auf der Kontaktliste blockieren kann
- man die Sicherheits- und Berichtfunktionen auf Internetseiten und bei sonstigen Anwendungen benutzt.

• Bauen Sie Vertrauen auf. Versichern Sie Ihren Kindern, dass sie mit Ihnen über Erlebtes oder Fehler sprechen können, um gemeinsam nach Lösungen zu suchen! Erfahrungen und Fehler gehören zum Lernprozess.

NÜTZLICHE LINKS

Praktische Hinweise zum Absichern Ihrer Online-Aktivitäten, beispielsweise die Sicherheitseinstellungen auf Facebook und MSN oder die Rechte am eigenen Bild, erhalten Sie auf:
www.bee-secure.lu

Die Europäische Kommission organisiert jedes Jahr eine Umfrage über die Benutzung des Internets durch Kinder. Konsultieren Sie die Studie Eurobarometer 2008 – „Towards a safer use of the Internet for children in the EU – a parents' perspective":
ec.europa.eu/information_society/activities/sip/surveys/index_en.htm

3. Cybermobbing

EIN FALL VON CYBERMOBBING

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 – sogar unsere eigenen Kinder sind nicht immer Engel ;-)

Cybermobbing besteht darin, die neuen Informations- und Kommunikationsmittel einzusetzen, um eine Einzelperson oder eine Gruppe von Personen zu tyrannisieren, zu belästigen oder einzuschüchtern. Dabei werden E-Mails, Chat-Seiten oder -Programme, Handys oder andere digitale Geräte benutzt.

Wie **Mobbing** in der Schule oder auf dem Spielplatz ist ein solches Verhalten unannehmbar, und Eltern, PädagogInnen und Kinder sollten wachsam und reaktionsbereit sein. Kinder erzählen oft nicht, wenn sie Opfer von Cybermobbing werden. Im Gegensatz zum traditionellen Mobbing ist das Opfer 24 Stunden am Tag, 7 Tage die Woche jeglicher Art von Angriffen ausgesetzt. Täter können z. B. jederzeit Drohnachrichten an die E-Mail-Adresse zu Hause oder auf das Handy 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.

Reden Sie immer offen mit Ihren Kindern, damit Sie über alle besorgniserregenden Situationen sprechen können. Neue Technologien wie das Internet und Handys 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.

• Bringen Sie ihren Kindern bei, wie sie einen Kontakt blockieren können.

• Speichern Sie beleidigende Nachrichten als mögliche 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 Cybermobbing zu verhindern.

• Bleiben Sie in Kontakt mit der Umgebung Ihrer Kinder; lernen Sie deren Freunde, die Eltern ihrer Freunde, ihre LehrerInnen und KlassenkameradInnen kennen.

• Ermutigen Sie Ihre Kinder, Sie über alle störenden Erfahrungen offline und 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.

NÜTZLICHE LINKS

Auf der BEE SECURE-Seite findet man weitere Informationen und Lösungsvorschläge zum Umgang mit dieser Problematik:
www.bee-secure.lu

Auf der Internetseite Mobbing – Schluss damit! finden Sie Informationen und Tipps zum Thema Mobbing für Kinder, Eltern und LehrerInnen:
www.mobbing.seitenstark.de/

Kinder, die Opfer von Cybermobbing sind, können sich an das luxemburgische Kanner-Jugendtelefon wenden:
116 111

Eltern finden Beratung und Hilfe beim Elterntelefon (26 64 05 55) oder der BEE SECURE -Helpline
26 64 05 44

4. Unterhaltung & Downloads

IM INTERNET IST NICHT ALLES GOLD, WAS GLÄNZT

Das Internet ist eine virtuelle Umgebung mit einer Menge Aktivitäten, auch kommerzieller Art. Wenn 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. Spiele und Musik, **Klingeltöne**, andere Accessoires und Online-Dienste.

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 oder oft teurer als auf den ersten Blick zu erkennen.

Um sich im Internet für einen Dienst anzumelden (kostenlos oder nicht), müssen Sie in der Regel ein **Online-Formular** mit 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 Waren im Internet zu verkaufen. Im Allgemeinen können Sie einem Pop-up-Fenster vertrauen, wenn die Internetseite vertrauenswürdig ist. Gewisse Pop-up-Fenster werden jedoch benutzt, um unseriöse Produkte anzubieten, Schadprogramme zu verbreiten oder **Online-Fragebögen** zu verbreiten, die persönliche Daten sammeln. Bringen Sie Ihren Kindern bei, unseriöse Pop-ups durch einen Klick auf das rote Kreuz in der oberen rechten Ecke zu schließen.

SPIELE AM COMPUTER

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. Kinder können Spiele auf einer CD/DVD, auf Internetseiten, auf Spielekonsolen oder auf Handys und anderen tragbaren Geräten spielen.

Nicht alle digitalen Spiele sind jedoch von guter Qualität. Sie müssen entscheiden, welche Spiele sich für Ihre Kinder am besten eignen.
Es gibt ein paneuropäisches Bewertungssystem für interaktive Spiele, **PEGI**, das Spiele nach

Alter und Inhalt bewertet. Das System wird von mehreren Herstellern, unter anderem PlayStation, Xbox und Nintendo, sowie von Herausgebern und Entwicklern interaktiver Spiele in ganz Europa unterstützt. Beachten Sie diese Angaben auf der Verpackungsrückseite der Spiele, die Sie für ein Kind kaufen, aber denken Sie daran, nicht alle Kinder einer Altersgruppe sind auf dem gleichen Entwicklungsstand.

Online-Spiele sind vergleichbar mit Computerspielen, sie benötigen jedoch zusätzlich eine Internetverbindung. Sie reichen von einfachen, bekannten Spielen wie Pacman und Tetris zu virtuellen Realitätsspielen, in denen mehrere BenutzerInnen zusammen online spielen und dabei Inhalte schaffen und Geschichten erstellen. Viele solcher Multiplayer-Spiele verfügen über virtuelle Gemeinschaften von SpielerInnen. Hiermit sind Risiken für die Kinder verbunden, da sie hierbei im Internet auf unbekannte Personen treffen können. (Zu den speziellen Schutzreflexen in Chats, siehe Kapitel „Kommunikation".) Da das PEGI-System für Online-Spiele noch im Aufbau ist, gibt es in diesem Bereich kaum gute Orientierungshilfen für Eltern.

Tipp: Ob Computer- oder Online-Spiele – legen Sie für die Kinder Nutzungsregeln fest. Damit können Sie gewährleisten, dass die Zeit, die Ihre Kinder online mit dem Spielen verbringen, nicht auf Kosten anderer Aktivitäten geht.

DATENTAUSCH & URHEBERRECHTE ©

Das Internet ist eine Fundgrube für Filme, Musik und Spiele zum Herunterladen, Spielen, Ansehen und Hören. Besonders Kinder und Jugendliche laden oft Material über **Peer-Netzwerke** herunter, ohne sich dessen bewusst zu sein, dass die Originalwerke der Künstler, **Autoren** oder anderer Urheber durch **Urheberrechte** geschützt sind. Dieses beinhaltet auch Werke wie Texte, Videos, Lieder, Bücher, Software und Bilder.

Ist es illegal?

Im Allgemeinen ist das **Hoch-** und Herunter**laden** von Musik und Filmen ohne die Erlaubnis des **rechtlichen Eigentümers** in der ganzen Welt illegal (obwohl jedes Land sein eigenes Urhebergesetz hat). Als Faustregel gilt, dass der Dateitausch von Musik und Filmen als illegal angesehen und mit **Peer-to-Peer**-Anwendungen vorsichtig umgegangen werden muss. Der Dateitausch ist dann legal, wenn es sich um den Tausch von Dateien handelt, die Sie selber erstellt haben.

Ist es riskant?

Dateitausch gefährdet Ihren Computer, da hierdurch schädliche Programme und Schadsoftware auf den Computer gelangen können. Es ist auch möglich, dass andere Personen sich Zugang zu Ihren persönlichen Daten verschaffen oder die Kontrolle über Ihren Computer übernehmen, z. B. zum Versand von Spam oder illegalen Inhalten.

Wo kann ich legale Musik finden?

Es gibt Hunderte von Internetseiten auf der ganzen Welt, die Musik legal zum Verkauf anbieten, manchmal sogar kostenlos! Es gibt zum Beispiel Internetseiten, wo die Fans die Arbeit ihrer Lieblingsmusiker beurteilen und mehr über Konzerte und Alben erfahren können.

GOLDENE REGELN

- Vergewissern Sie sich, dass Sie eine legale Webseite benutzen, um Musik und Filme aus dem Internet herunterzuladen.
- Ermutigen Sie Ihre Kinder, Internetseiten zu benutzen, die legitime 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.
- Schützen Sie Ihren Computer: Aktualisieren Sie regelmäßig alle Programme und benutzen Sie immer ein aktuelles Anti-Virus-Programm. Achten Sie auf eine richtig eingestellte Firewall.
- Bringen Sie Ihren Kindern bei, grundsätzlich jede neue Datei vor dem Öffnen mit dem Anti-Virus-Programm zu scannen.
- Lesen Sie immer den Datenschutzhinweis und die Benutzerbedingungen, bevor Sie etwas installieren. Prüfen Sie anhand mehrerer Quellen, ob die Software, die Sie herunterladen möchten, vertrauenswürdig ist.
- Schließen Sie unseriöse Pop-up-Fenster, indem Sie auf das rote Kreuz in der oberen rechten Ecke klicken. Klicken Sie nie in die Fenster.

KINDER & SPIELE:

- Legen Sie Regeln fest, wie lange Ihre Kinder spielen dürfen.
- Lassen Sie sie in einem gemeinschaftlichen Raum spielen, wo Sie sie im Auge behalten können.
- Behalten Sie die Spielgewohnheiten Ihrer Kinder im Auge – Sie begleiten sie auf den Spielplatz, wieso also nicht auch beim Spielen in virtuellen Umgebungen?
- Reden Sie über den Inhalt des Spiels, über die Aspekte, die wie im wirklichen Leben sind, und über jene, die es nicht sind. Lassen Sie sich zeigen, was ihren Kindern am meisten Spaß macht.

- Bevor Sie Ihrem Kind ein Spiel kaufen, vergewissern Sie sich, dass der Inhalt altersgemäß ist (paneuropäisches Bewertungssystem PEGI oder ein nationales Bewertungssystem). Nehmen Sie sich die Zeit, sich Spiele von Ihren Kindern zeigen zu lassen. Es lohnt sich!

Wenn Ihre Kinder Online-Spiele mit mehreren Benutzern spielen:

- Wählen Sie Internetseiten mit strikten Regeln und echten Moderatoren.
- Ermahnen Sie sie, 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, einem vertrauenswürdigen Erwachsenen von belästigenden Nachrichten oder Drohbotschaften sowie Fluchworten, der Darstellung unangenehmer Inhalte oder Einladungen, sich außerhalb des Spielkontextes zu treffen, zu erzählen.
- Falls es zu problematischen Vorfälle kommt, nutzen Sie die Meldemöglichkeiten innerhalb des Spiels und wenden Sie sich gegebenenfalls an die BEE SECURE-Helpline.

NÜTZLICHE LINKS

Weitere Informationen zu den Themen Online-Shopping und Spiele sowie Informationen und praktische Tipps zu diesem Themenbereich, z. B. Unterbinden von Pop-up-Fenstern oder Urheberrecht, erhalten Sie auf:
www.bee-secure.lu

Online-Shopping und Online-Betrug gehören ebenfalls zu den Themen der Union Luxembourgeoise des Consommateurs (*www.ulc.lu*) oder dem Centre Européen des Consommateurs Luxembourg
www.cecluxembourg.lu

Weiterführende Informationen über Online-Spiele und das PEGI-Bewertungssystem erhalten Sie unter:
www.pegi.info/de

1. Schutz bringt Sicherheit

KOMMENTIERTE AKTIVITÄTEN

Sucht die passenden Wörter zu den Bildern: Computergehäuse, Mauspad, Bildschirm, Lautsprecher, Webcam, Drucker, USB-Stick (oder Speicherstick), Maus, CD-Rom.

Eine Aufwärmübung, um Ihre Kinder mit den verschiedenen Teilen des Computers und anderem Hardware-Material vertraut zu machen.

Bittet eure Eltern, euch eine E-Mail mit einem **Anhang** zu schicken, oder schickt euch selber eine. Übt Folgendes: Klickt mit der rechten Maustaste auf den Anhang (aber nicht öffnen!) und speichert ihn auf eurem Computer-Desktop ab. Geht zum Desktop, klickt mit der rechten Maustaste auf das Dokument und scannt das Dokument mit dem Anti-Virus-Programm. Wenn ihr wisst, dass das Dokument ungefährlich ist, könnt ihr es speichern und 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 die Sicherheitsreflexe.

Folgt Lauras 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 Spamverteilung 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 Laura fortfährt, helfen wir Claire 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 Computer Musik hören, aber Sie können auch direkt online Musik hören. Ihre Kinder sollten nur die Aktivitäten ankreuzen, für die eine Netzwerkverbindung von wesentlicher Bedeutung ist.

Gebt zusammen mit euren Eltern www.blinde-kuh.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 auf drei verschiedenen Internetseiten 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 auf mindestens drei Internetseiten zu suchen und zu vergleichen und bei Schulaufgaben immer ihre Quellen anzugeben.

Gebt zusammen mit euren Eltern www.blinde-kuh.de in euren Browser ein. Sucht dann nach einem Thema, zum Beispiel dem Tyrannosaurus Rex. Speichert die drei Seiten, die ihr am interessantesten findet, ab. Klickt dazu auf den Menüpunkt Favoriten bzw. Lesezeichen oben auf der Browserseite und fügt sie zu euren Lieblingsseiten hinzu. Ihr könnt auch einen eigenen Ordner anlegen.

Interessante Seiten speichern und in den Favoriten oder Lesezeichen organisieren (Option in der Browsersymbolleiste) hilft dabei, eine sichere Internetumgebung für Kinder zu schaffen.

HABT IHR GUT AUFGEPASST?

1: (geschützt) 2: (Virus), (unbekannt), (herunterlädt), (infizierte),(Speicherstick), (ungeschützten) 3: (komisch) 4: (bekannt), (Anhängen), (Titeln), (Spam) 5: (einzigen), (Spam) 6: (erst), (drei), (vergleiche), (jeder), (veröffentlichen) 7: (Anti-Virus-), (Anti-Spionage-Programme) 8: (redet), (Eltern) 9: (Informiert)

LÖSUNGSVORSCHLÄGE ZU DEN SITUATIONSKARTEN

SITUATION 1. Surft nie im Internet, wenn euer Computer nicht aktualisiert und durch ein aktuelles Anti-Virus-Programm sowie eine richtig eingestellte Firewall geschützt ist. Dies würde einer Grenze ohne Grenzwächter gleichkommen; euer Computer könnte von schädlichen Programmen wie Viren, Trojanischen Pferden, Würmern oder Spionageprogrammen infiziert werden.

SITUATION 2. Gebt Acht bei E-Mails, die von Leuten kommen, die ihr nicht kennt, und die 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, Trojanischen Pferden, Würmern oder Spionageprogrammen infizieren. Öffnet diese E-Mails nicht. Blockiert stattdessen den Absender, indem ihr mit einem rechten Mausklick auf die Mail klickt und „Absender blockieren“ wählt und 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 echter Wissenschaftler arbeiten.

2. Kommunikation

KOMMENTIERTE AKTIVITÄTEN

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, Fotos von euch, euer Alter, Informationen darüber, ob ihr eine Freundin oder einen Freund habt

Haben Ihre Kinder die gleiche Auffassung von Privatsphäre wie Sie? Mit den drei Farben wird der Privatheitsgrad dargestellt: rot bedeutet sehr privat, orange recht privat und grün nicht so privat.

Helft Claire, mit Lauras Tipps ein richtig gutes Passwort zu finden:

Gute Passwörter sollten eine willkürliche Folge verschiedener Zeichen enthalten (Zahlen, große und kleine Buchstaben sowie Satz- oder Sonderzeichen). Wichtig! Sie sollten immer geheim gehalten werden.

Folgt Claires Beispiel und erstellt ein sicheres Profil. Legt anschließend als Beispiel ein unsicheres Profil 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 sie nur beschützt, wenn sie auch ihre Privatsphäre online schützen. Sie sollten daher keine privaten Daten online kommunizieren.

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

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

Folgt Claires Idee und denkt euch drei Ratschläge aus, die Laura Pit, „dem Rotkäppchen mit Kapuzenpulli“ geben würde, um sich vor den „Wölfen des Webs“ 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 in einem Chat-Programm darzustellen: *ein Smiley – ein trauriges Gesicht – ein blinzelndes Gesicht – ein überraschtes Gesicht – ein breites Lachen – eine herausgestreckte Zunge*

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

HABT IHR GUT AUFGEPASST?

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

LÖSUNGSVORSCHLÄGE 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. Überlegt gut, ob es wirklich nötig ist, persönliche Daten wie Namen, Adresse, Geburtsdatum, Fotos usw. online weiterzureichen

SITUATION 5. Mike hat seinem Freund wahrscheinlich sein E-Mail-Passwort mitgeteilt, der dann beschlossen hat, sich durch das Verschicken gemeiner E-Mails in seinem Namen an ihm zu rächen. Behaltet euer Passwort immer für euch, sonst können 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 sich mit euch treffen möchte, 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. Cybermobbing

KOMMENTIERTE AKTIVITÄTEN

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

Geben Sie Ihren Kindern Gelegenheit, ihrer Kreativität freien Lauf zu lassen, und lassen Sie sie in den leeren Rahmen zeichnen.

Folgt Pits Beispiel und gebt fünf Verhaltensweisen an, für die ihr jemandem eine „rote Karte" geben würdet.

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

HABT IHR GUT AUFGEPASST?

1: (fair), (stören) 2: (redet) 3: (GRUND) 4: (Cybermobbing) 5: (blockiere) 6: (kenne) 7: (antworten)

LÖSUNGSVORSCHLÄGE 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 Situation immer mit euren Eltern oder einem anderen Erwachsenen, dem ihr vertraut

SITUATION 8. Pit 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. Pit 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 Internet genau so zu behandeln, wie ihr selbst behandelt werden möchtet. Ihr habt sicherlich inzwischen genug gelernt, um Claire bei dieser Aufgabe zu helfen.

4. Unterhaltung & Downloads

KOMMENTIERTE AKTIVITÄTEN

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

Üben Sie, indem Sie eine Suche mit den angegebenen Stichwörtern durchführen, und prüfen Sie, ob Sie Marketingfallen auf den Internetseiten finden können. Sehen Sie selbst, wie sich wichtige Informationen im Kleingedruckten verstecken oder Werbeslogans falsche Eindrücke vermitteln.

Wie heißt euer Lieblingscomputerspiel? Prüft, ob eure Eltern es kennen und beschreiben können. Wenn sie keine Ahnung haben, erklärt es ihnen erst und lasst sie dann eine kleine Beschreibung verfassen. Haben sie es geschafft? Wie viele Punkte von höchstens zehn würdet ihr ihnen geben? …/10 Ein Elternteil verfasst eine kurze Beschreibung des Lieblingsspiels 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 GUT AUFGEPASST?

1: (kostenlos) 2: (Formulare) 3: (Fallen) 4: (illegale) 5: (Kreuz) 6: (ignorieren) 7: (Privatsphäre) 8: (tauschen), (selbst) 9: (Ladet) (herunter)

LÖSUNGSVORSCHLÄGE ZU DEN SITUATIONSKARTEN

SITUATION 10. Die meisten Lieder und Filme, die man im Internet findet, sind illegale Kopien. Außerdem sind die Internetseiten, auf denen Leute Musik und Filme austauschen, normalerweise voller schädlicher Programme, wie zum Beispiel Viren, Trojanische Pferde, Würmer und Spionageprogramme. Die beste Lösung wäre, wenn Claire Option b oder c wählt. Das Herunterladen ihres Lieblingsliedes von einer zuverlässigen Seite mit legaler Musik kostet natürlich viel weniger als die ganze CD. Sie sollte ihre Eltern nach deren Meinung fragen und sie um ihre Erlaubnis bitten.

SITUATION 11. Es gibt kostenlose Dienstleistungen im Internet, aber Klingeltöne, Hintergrundbilder, MP3s, Avatare und solche Dinge sind selten kostenlos. Wenn Pit sich die Internetseite genauer ansieht, entdeckt er wahrscheinlich Kleingedrucktes, in dem ihm zusätzliche Kosten dieser Dienstleistungen mitgeteilt werden. Klingeltöne, Rätsel, Spiele usw. sind ausgezeichnete Mittel, um Leute zu verleiten, diese sogenannten „kostenlosen" Dienste zu abonnieren, die in Wirklichkeit Geld kosten. Achtung! Das Herunterladen von Liedern, Fotos oder Klingeltönen per Handy kann sehr teuer werden.

SITUATION 12. Pit 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. Pit sollte nie ein Spiel aus dem Internet herunterladen, ohne seine Eltern vorher zu fragen. Solche Spiele können Schadsoftware enthalten. Dies kann dem Computer schaden. Außerdem erhalten Cyberpiraten so die Möglichkeit, Pit und seine Familie auszuspionieren.

D. Glossar

Abonnieren: Das freiwillige Anmelden bei einem Online- oder Info-Dienst, der aktuelle Nachrichten direkt an das persönliche E-Mail-Postfach schickt.

Akronym: Eine Abkürzung, die aus den ersten Buchstaben der Wörter 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: Newsletter, Diskussionsforum, E-Mail, Chat-Räume usw. Normalerweise sollten 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 gefährliche Daten 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 auf der Suche nach bekannten Viren und identifiziert verdächtige Verhaltensweisen bei Computerprogrammen, 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 virtu-

ellen Welten.

Benutzername: Er verkörpert den/die BenutzerIn eines Online-Dienstes 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. Synonyme: Nickname, Username.

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

Beratungsstelle: Ein E-Mail- oder auch Telefondienst, der in mehreren Ländern von Kinderhilfsorganisationen und Mitgliedern des Insafe-Netzwerks zur Verfügung gestellt wird. Kinder können ihre Bedenken über illegale und schädliche Inhalte hier äußern und über unangenehme oder angsteinflößende Erfahrungen in Zusammenhang mit ihrer Nutzung 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 (Internet-Tagebuch). Eine Internetseite, für die eine Einzelperson oder eine Gruppe, normalerweise auf täglicher Basis, Inhalte erstellt und die aus Texten, Bildern, audiovisuellen Dateien und Links besteht.

Bloggen/Blogging: Das Schreiben oder die Aktualisierung eines Blogs.

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

Browsen: Die Benutzung eines Browsers zur Ansicht von Internetseiten oder zum Surfen im Netz.

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 kann. CD-ROMs werden allgemein benutzt, um Computersoftware zu verteilen.

Chat: Synchrone Kommunikation über das Internet durch geschriebene Botschaften über Chat-Programme (z. B. MSN, Skype, ICQ etc.).

Chat-Raum: Öffentlicher virtueller Ort für die Chat-Kommunikation in Echtzeit. Leute aus der ganzen Welt können sich in Chat-Räumen treffen und anhand von Mitteilungen, die sie per Tastatur eintippen, diskutieren. Wenn Kinder Chat-Räume benutzen, sollten sich die Eltern vergewissern, dass diese ihrem Alter angepasst sind und von Aufsichtspersonen und ModeratorInnen überwacht werden.

Computerdatei: Dokumente oder Anwendungen, die sich auf Datenträgern wie Festplatten, CDs o. ä. befinden, z. B. ein Word-Dokument, eine MP3-Datei, ein Video usw.

Computerprogramm: Bezeichnet normalerweise Software. Software besteht aus einer strukturierten Folge von Anweisungen, die von Computerprogrammierern geschrieben wurden und es einem Computer ermöglichen, Aufgaben auszuführen. Softwareprogramme werden auf CD-ROMs (siehe Definition) verkauft, einem physischen Träger zum Ablegen von Programmen, oder, wie immer häufiger üblich, über das Internet heruntergeladen.

Cookie: Eine Datei, die von einer Internetseite auf der lokalen Festplatte abgelegt wird. Jedes Mal, wenn die Internetseite aufgerufen wird, wird das Cookie an den Server zurückgeschickt, auf dem die Internetseite untergebracht ist. Cookies geben die Site-Vorlieben von UserInnen an und werden bspw. auf Online-Shopping-Seiten benutzt. Wenn man Cookies ablehnt, funktionieren manche Internetseiten nicht mehr richtig. Trotzdem Vorsicht: Cookies können auch Schaden anrichten.

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

Cracken: Das illegale Enfernen des Kopierschutzes von kommerzieller Software und damit eine Verletzung des Urheberrechts.

Cybermobbing: auch Cyberbullying genannt, bezieht sich auf das Mobbing durch elektronische Medien, normalerweise durch Sofortnachrichten und E-Mails. Diese Nachrichten oder E-Mails können Drohungen, sexuelle Bemerkungen und abwertende Kommentare beinhalten. Cybertyrannen 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, den Informationsfluss 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 kontenspezifischer Datenschutzdetails, die der/die UserIn selbst bearbeiten kann, um den Datenschutz gegen die Veröffentlichung persönlicher Informationen, Cookies usw. zu erhöhen.

Dateitausch: Der Online-Austausch von Dateien zwischen ComputernutzerInnen. Der Begriff deckt sowohl das Anbieten von Dateien an andere BenutzerInnen (Hochladen) als auch 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/der BenutzerIn wird die Übermittlung von Dateien oft als Hoch- oder Herunterladen (bzw. Up- oder Download) bezeichnet.

Digitales Spiel: Ein von SpieleentwicklerInnen entworfenes Spiel, das auf einem Computer gespielt wird. Ein Online-Spiel ist ein digitales Spiel, das eine Live-Verbindung zum Netzwerk 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 oder ein Symbol, das benutzt wird, 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, bei Instant-Messaging-Diensten, 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: Ein anpassbarer Ordner des Browsers, in dem interessante Links/Lesezeichen gespeichert werden. Die Lesezeichen können in Unterordner organisiert und/oder mit Stichwörtern gekennzeichnet werden, damit sie einfacher wiedergefunden werden können.

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

Firewall: Hardware- und Softwarekomponenten, die den Zugriff von unbefugten BenutzerInnen (wie Hacker und Cracker) auf einen mit dem Internet verbundenen Computer oder ein Computernetzwerk verhindern.

Flaming: Ein feindseliger und beleidigender Austausch zwischen InternetnutzerInnen. Normalerweise spielen sich diese in Diskussionsforen, im Chat oder sogar per E-Mail oder Handy 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 (Aufklapplisten) ausgefüllt werden. Nach dem Versand werden die Daten direkt an eine Verarbeitungsanwendung geschickt, die die Informationen in eine Datenbank einspeist.

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

Freeware und Shareware: Im Allgemeinen ist Software durch Urheberrechte geschützt und kann daher nicht 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 den Dienst weiter in Anspruch zu nehmen.

Grooming: Annäherungs- und Verwicklungsprozesse von Sexualstraftätern, um mit Kindern in Kontakt zu kommen und deren Vertrauen zu erschleichen. Diese Täter sind sehr auf die

eigene Sicherheit bedacht. Das Internet bietet ihnen dazu optimale Bedingungen (Anonymität, falsche Identität, viele virtuelle Zugriffsorte usw.). Pädophile fangen z. B. Unterhaltungen mit möglichen Opfern an, um Informationen über deren Aufenthaltsort, Interessen, Hobbys und sexuelle Erfahrungen zu gewinnen. Grooming kann sich über Monate oder Jahre erstrecken, bevor der Täter zuschlägt.

GSM: Ein elektronisches Telekommunikationsgerät, auch bekannt als Mobiltelefon, Handy, 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).

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

Handy: siehe GSM

Hardware: Der physische Teil eines Computers, im Gegensatz zur Computersoftware, die im Inneren der Hardware agiert. Die Hardware kann sich im Inneren des Computers 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.

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

Homepage: Eine Internetseite, die automatisch geladen wird, wenn ein Webbrowser startet. Der Begriff wird auch für die erste Seite oder die Hauptseite einer Internetseite (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 InternetbenutzerInnen in den teilnehmenden Ländern zu sichern.

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

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), Online-Hass und fremdenfeindliche Internetseiten.

Instant Messaging (Sofortige Nachrichtenübermittlung): Eine Form der sofortigen und simultanen elektronischen Kommunikation zwischen zwei oder mehreren BenutzerInnen. 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 Heimnetzwerke, akademische und 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, Wi-Fi, Satellit und Handy.

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

Junk-Mail: Unerwünschte E-Mail-Nachrichten, die über die eigene E-Mail-Adresse an Personen verschickt werden. Da das Internet öffentlich ist, kann man nur wenig tun, um Junk-Mails und Spam zu vermeiden.

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 HandybesitzerInnen herunterladen können, oft gegen Bezahlung.

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

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

Link: Ein Verweis auf ein Dokument, das online zur Verfügung steht (Internetseite, Textdokument, Bild usw.). Wenn man auf den Link klickt, wird man zu einer neuen Seite oder einer ganz anderen Internetseite weitergeleitet. Textlinks sind normalerweise blau und unterstrichen, können aber auch jede andere Farbe annehmen und nicht unterstrichen sein. Auch ein Bild kann als Link dienen.

Malware: siehe Schadprogramm

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 zu verformen.

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.).

MMORPG (Massively Multiplayer Online Role Playing 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.

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

Mobiltelefon: siehe GSM

MP3: Ein audiospezifisches Kodierungsformat. 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".

Netz: Abkürzung für Internet.

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

Nickname: Englisch für Spitzname. Siehe Definition für „Benutzername".

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

Peer-to-Peer-Netzwerk: siehe P2P-Netzwerk

P2P-Netzwerk: Ein Peer-to-Peer(P2P)-Netzwerk erlaubt es jenen, die damit verbunden sind, durch Hoch- und Herunterladen Dateien auszutauschen (siehe Definition). Dies ist nur eine von vielen Möglichkeiten, um Dateien im Internet zu teilen. Meist verstößt der Dateitausch gegen das Urheberrecht und ist damit strafbar. Außerdem sind viele Dateien gefährlich, da mit Schadprogrammen (Viren, Trojanische Pferde …) infiziert.

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 unbefugte BenutzerInnen (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 Fenster, das plötzlich beim Besuch einer Internetseite oder beim Drücken auf einen bestimmten Knopf 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 stellen eine Verbindung zu einem CD/DVD-Laufwerk oder einem Netzwerk her, 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 höchst vertrauliche persönliche Informationen.

Profil: Persönliche Benutzerinformationen in Social-Networking-Plattformen, Instant-Messaging-Systemen, 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). Der Teil des Computers, der Daten verarbeitet, Kontrollsignale erzeugt und Resultate speichert. Zusammen mit dem Computerspeicher bildet er den Kern eines Computers.

RPG (Role Playing Game): siehe MMORPG

Schadprogramm: Es handelt sich hierbei um Software, die erstellt wurde, um ein Computersystem zu infiltrieren oder 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.

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.

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 Erwachseneninhalte.

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 betrachten und es online zu verteilen.

Second Life: Eine bekannte 3-D-Webgemeinschaft, angeboten von der Firma Linden Labs, mit Sitz in den USA. Die BenutzerInnen können auf virtuelle Art anhand eines Avatars interagieren (siehe Definition), Häuser und verschiedene Umgebungen einrichten, Handel treiben und virtuelles Geld verdienen usw. Siehe www.secondlife.com

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

SIP-Bench: Eine von der Europäischen Kommission unterstützte Studie, die 30 Kontroll- und Anti-Spam-Tools getestet hat, um ihre Wirksamkeit beim Schutz der Kinder gegen schädliche Inhalte im Internet zu bewerten.

Social Networking Sites (Soziale-Netzwerke-Plattform): Virtuelle Plattform für Gemeinschaften von Mitgliedern, die ähnlichen Interessen und Aktivitäten nachgehen. Die Mitglieder müs-

sen 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.

Social Networking oder auch Soziale Netzwerke: Online-Gemeinschaften von Mitgliedern, die ähnlichen Interessen und Aktivitäten nachgehen und online durch die Anwendung geeigneter Software und Dienste (siehe „Social Networking Sites“) interagieren und Kontakte knüpfen.

Software: Siehe Definition für „Computerprogramm“.

Suchmaschine: Eine Anwendung für die Suche nach Informationen im Internet. Die bekanntesten sind Google, Yahoo und MSN Search. Suchmaschinen verfügen über fortgeschrittene Benutzereinstellungen, unter denen sich auch Sicherheitseinstellungen befinden. Für Kinder wird empfohlen, auf spezielle Kindersuchmaschinen zurückzugreifen.

Spam: Unerwünschte E-Mails, die normalerweise kommerzieller Art sind und in großen Mengen verschickt werden. Anderen Personen Spam zu schicken ist zweifellos eine der berüchtigtsten Formen von Missbrauch des Internets.

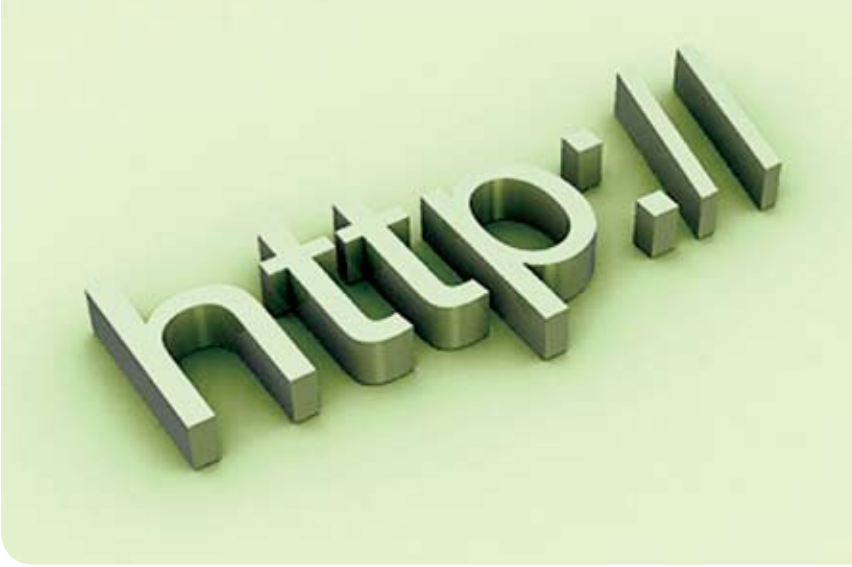
Spam-Filter: Eine Anwendung, die verhindert, dass Spam-Nachrichten in der eigenen E-Mail-Inbox landen.

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

Spyware: Schadprogramm, heimlich an heruntergeladenen Dateien angehängt, das sich selbst auf dem Computer installiert und die Aktivitäten überwacht. Es 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.

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

Username: Siehe Definition für „Benutzername“.



E. Nützliche Adressen

BEE SECURE – DAS LUXEMBURGISCHE SENSIBILISIERUNGSZENTRUM

Die luxemburgische Seite zur Internetsicherheit innerhalb des europäischen Insafe-Netzwerks. BEE SECURE bietet Informationen, Ratschläge und Hilfsmittel für Kinder, Eltern und Pädagogen und fördert einen sicheren und verantwortungsvollen Umgang mit den neuen Technologien. *www.bee-secure.lu*

BEE SECURE-HELPLINE

Die BEE SECURE-Helpline ist ein wichtiger Teil des BEE SECURE-Projekts und bietet sowohl Kindern und Jugendlichen als auch Eltern und Erziehern Beratung bei Problemen mit dem Internet. Wer sich telefonisch beraten lassen möchte, kann dies unter folgender Nummer tun: 26 64 05 44

www.bee-secure.lu

help@bee-secure.lu oder über die Telefonnummer 26 64 05 44

LISA STOPLINE

Melden Sie Internetinhalte, die Sie für illegal oder bedenklich halten, bei der LISA-Stopline online.

www.lisa-stopline.lu

CASES

Das luxemburgische Informationssicherheitsportal des Ministeriums für Wirtschaft und Außenhandel stellt Anwendern praktische Tipps und Informationen zum Thema Informationssicherheit sowie zum Ausbau der nötigen Sicherheitskompetenzen zur Verfügung.

www.cases.lu

KANNER-JUGENDTELEFON

Die kostenfreie landesweite Telefonnummer gegen Kummer bietet Beratung und Hilfe natürlich auch bei Problemen in der digitalen Welt: 116 111 *www.12345kjt.lu*

SONSTIGE

CEC –CENTRE EUROPÉEN DES CONSOMMATEURS

Das Europäische Verbraucherzentrum informiert die VerbraucherInnen über europäisches Verbraucherrecht und europäische Verbraucherpolitik, gibt Ratschläge und unterstützt die VerbraucherInnen im Zusammenhang mit ihren konkreten grenzüberschreitenden Aktivitäten. Hier findet der Bürger auch Formulare und Musterbriefe, um sich gegen Betrug zu wehren. *www.cecluxembourg.lu*

ELTERESCHOUL

Informations- und Weiterbildungsangebote für Eltern. *www.kannerschlass.lu/eltereschoul*

ERWUESSEBILDUNG

Informations- und Weiterbildungsangebote für Erwachsene. *www.erwuessebildung.lu*

GUICHET UNIQUE

Der virtuelle Schalter, der den Zugang zu den öffentlichen Diensten erweitert. Ziel ist die schrittweise Integration der Behördengänge in ein Internetportal. *www.guichet.public.lu*

INSAFE

Das europäische e-Sicherheits-Netzwerk zur Sensibilisierung möchte alle Anwender ermuntern, die positiven Aspekte des Internets zu nutzen und leichzeitig die potenziellen Risiken zu vermeiden. BEE SECURE ist Mitglied des Insafe-Netzwerks.
www.saferinternet.org

INHOPE

Inhope ist das europäische Netzwerk von Internet-Hotlines, die auf nationaler Ebene operieren, Inhope unterstützt die effiziente und direkte Behandlung von Meldungen illegaler Inhalte weltweit. BEE SECURE ist Mitglied des Inhope-Netzwerks. *www.inhope.org*

LIFELONG LEARNING

Portal für berufliche Weiterbildung. *www.lifelong-learning.lu*

MINISTÈRE DE LA FAMILLE ET DE L'INTÉGRATION, DIVISION IV – ENFANCE, FAMILLE ET JEUNESSE

Luxemburgisches Ministerium für Familie und Integration. *www.mfi.public.lu*

PORTAIL SANTÉ

Luxemburgisches Informationsportal zum Thema Gesundheit. *www.sante.public.lu/fr*

SNJ – SERVICE NATIONAL DE LA JEUNESSE

Der SNJ ist ein öffentliches Verwaltungsorgan, das einerseits selbst Projekte mit und für Jugendliche durchführt, und andererseits die Jugendorganisationen bei deren Projekten unterstützt. *www.snj.lu*

ULC – UNION LUXEMBOURGOISE DES CONSOMMATEURS

Die luxembugische Beratungszentrale zum Schutz der Verbraucher. *www.ulc.de*

WEHR DICH GEGEN CYBERMOBBING!

Diese Internetseite der Europäischen Kommission bietet in allen EU-Sprachen Anregungen für Jugendliche zu einer sichereren und verantwortungsbewussten Nutzung von Social-Networking-Plattformen wie Facebook, MySpace, YouTube usw. *www.keepcontrol.eu*

Titel: e-Sicherheits-Kit für die Familie • Erstellt von Insafe/Liberty Global-UPC im Jahr 2008
Präfix: 9782959974 • Id 51950 • ISBN-NUMMER: 9782959974045 • EAN: 9782959974045