Informations-sicherheit

Leitfaden zur Informationssicherheit

für den Unterricht und zu Hause

Numéro spécial du courrier de l'Éducation Nationale

MINISTÈRE DE L'ÉDUCATION NATIONALE
ET DE LA FORMATION PROFESSIONNELLE
Service de coordination de la recherche et de l'innovation pédagogiques et technologiques

MINISTÈRE DE L'ÉCONOMIE
ET DU COMMERCE EXTÉRIEUR
Direction du Commerce électronique et de la Sécurité informatique

CASES LUXEMBOURG

Inhalt

Einleitung	**5**
1. Internet und Neue Medien – eine Chance für Kinder	5
2. Gefahren und Risiken des Internets	5
3. Vermittlung von Medienkompetenz	6
4. Informationssicherheit „made in Luxembourg“	7

Teil I - Hinweise zur Nutzung des Leitfadens	**9**
1. Idee	9
2. Ziel	9
3. Aufbau	10
4. Methodologische Empfehlungen	11
Interessen	12
Einsatz im Unterricht	13

Teil 2 - Unterrichtsmaterial	**15**
Teilziel 1 Einfache Zusammenhänge und Funktionen des Internets verstehen	15
Teilziel 2 Soziale und gesellschaftliche Verhaltensregeln im Internet beachten	24
Teilziel 3 Mit dem Internet und seinen Funktionen kritisch und vorsichtig umgehen	28
Teilziel 4 Konkrete Risiken und Gefahren erkennen und richtig darauf reagieren	35
Teilziel 5 Einfache Grundsätze der Informationssicherheit kennen und beherzigen	39

Teil 3 - Praxistipps	51
Unterrichtsideen	51
Rollenspiel: „Fang das Virus“	41
Rollenspiel: „Firewall“	52
Vereinbarung eines Vertrags „Regeln der Internetnutzung“ mit den Kindern	53
„Mein Computertagebuch“	54
Gute Geheimnisse - schlechte Geheimnisse	55
Smileys	56
Gefühlsgesichter	57
Gewaltbarometer	58
Folgen von Cyberbullying	59
Quizfragen	60
Musterformular: Zustimmung zur Veröffentlichung von Fotos	63
Links für den Unterricht	64
Weiterführende Informationen	66

Zusätzliche Dokumente	70
Bastelbögen	
Themenblätter für Kinder	

Zeichenerklärung


Teilziel


Kurztext


Kompetenz


Unterrichtsidee

Herausgeber:

Ministerium für Erziehung und Berufsausbildung

Informationssicherheitsportal CASES
des Ministeriums für Wirtschaft und Außenhandel

2009

ISBN: 978-2-87995-996-2

Vorwort

Mady Delvaux-Stehres
Ministerin für Erziehung und Berufsausbildung

Jeannot Krecké
Minister für Wirtschaft und Außenhandel

Computer und Internet sind aus dem Alltag der Kinder und Jugendlichen in Luxemburg nicht mehr wegzudenken. Die junge Generation nutzt den heimischen Computer und die vielfältigen Internetangebote oft ohne Bedenken: Kinder und Jugendliche chatten, aktualisieren ihre Homepage, laden Programme herunter oder spielen Online-Spiele. Sie sind wenig mißtrauisch und haben noch nicht die nötigen Reflexe, um sich und ihre Daten zu schützen. Das Abschätzen von Risiken, denen sie sich aussetzen, fällt ihnen noch schwer.

Angesichts dieser Situation besteht eine wichtige Erziehungsaufgabe darin, den Kindern die erforderlichen Kompetenzen und das nötige Wissen zu vermitteln, damit sie sich in der virtuellen Welt innerhalb gesicherter Grenzen bewegen können. Sie müssen lernen, Gefahren frühzeitig zu erkennen, und sich Reflexe anzueignen, um diesen Gefahren aus dem Weg zu gehen.

Der vorliegende Leitfaden führt anhand kurzer, leicht verständlicher, modular aufgebauter Texte durch die verschiedenen Themen der Informationssicherheit. Lehrpersonal und Eltern können Kindern und Jugendlichen damit das Basiswissen an die Hand geben, das eine sichere Nutzung der digitalen Welt ermöglicht. Die einzelnen Themen können dabei fächerübergreifend in den täglichen Unterricht einfließen.

Der Leitfaden baut auf den Inhalten und Erfahrungen der Schulung „Luxemburg sicher im Netz“ auf, die seit 2007 von weit über 25.000 luxemburgischen Kindern und Jugendlichen besucht wurde und auf Anfrage über www.cases.lu zugänglich ist. Zusätzlich wurden die Erfahrungen anderer europäischer Länder berücksichtigt.

Entstanden ist dieser Leitfaden als Gemeinschaftsprojekt des Ministeriums für Erziehung und Berufsausbildung und des Informationssicherheitsportals CASES vom Ministerium für Wirtschaft und Außenhandel in Zusammenarbeit mit Lehrkräften, Eltern, Kindern und Jugendlichen.

Wertvolle Ideen konnten dadurch in den Leitfaden einfließen.

Ihre Anregungen und Anmerkungen sind uns wichtig und ausdrücklich erwünscht. Sie können uns diese über www.cases.lu mitteilen.

Tragen Sie zur Informationssicherheit „made in Luxembourg“ bei.

Der Vielzahl an Personen, die mit ihren Erfahrungen, ihrem Fachwissen und ihren Ideen zur Entstehung dieses Leitfadens beigetragen haben, möchten wir an dieser Stelle ein herzliches Dankeschön sagen.

Einleitung

1. Internet und Neue Medien - eine Chance für Kinder

Internet und Computer sind inzwischen ein fester Bestandteil der kindlichen Lebenswelt in Luxemburg wie auch in anderen europäischen Ländern.

Das Internet bietet jüngeren Kindern im Wesentlichen folgende wichtige Nutzungsmöglichkeiten: spielen, sich informieren, miteinander kommunizieren sowie Daten und Dateien austauschen.

Kinder, die zu Hause über keinen Zugang zu Computer und Internet verfügen, können in Schule und Unterricht den Umgang mit dem faszinierenden neuen Medium kennenlernen. Seine zahlreichen Einsatzmöglichkeiten unterstützen das entdeckende Lernen und fördern die Medienkompetenz bereits in einem frühen Alter. Beides ist für die spätere Lebens- und Berufswelt von Vorteil.

2. Gefahren und Risiken des Internets

Wo Chancen sind, sind auch Risiken: Hinter allen Einsatzmöglichkeiten des Internets verbergen sich Gefahren, auf die Kinder schon früh aufmerksam gemacht werden müssen, da sie mit diesem neuen Medium oft auf sich allein gestellt sind.

Eine große Gefahr für Kinder ist zunächst die Anonymität des Internets. Cyberbullying, das heißt das Schikanieren und Bedrohen anderer mit Hilfe der neuen Kommunikationstechnologien, ist nur ein Beispiel für die zahlreichen unliebsamen Auswirkungen des Internets. Auch sexuelle Übergriffe durch Personen, die sich eine falsche Identität zulegen, sind an dieser Stelle zu nennen. Zudem erleichtert das Internet Kindern den Zugang zu jugendgefährdenden Inhalten wie Pornografie oder Seiten, auf denen Gewalt in all ihren Formen verherrlicht wird.

Eine weitere Gefahr sind Trickbetrüger, die Kinder durch Manipulation in finanzielle Fallen locken, die als Gewinnspiele oder Hausaufgabenhilfe getarnt sind. Obwohl Kinder in aller Regel noch nicht im Internet einkaufen können, geschieht es immer wieder, dass sie unwissentlich oder unüberlegt Verträge abschließen. Zudem haben sie häufig noch kein ausgeprägtes Verständnis für den Wert des Geldes, wie zum Beispiel astronomische Mobiltelefonrechnungen zeigen. Abgesehen von der psychologischen Belastung, die dadurch für die Kinder entsteht, müssen Erziehungsberechtigte wertvolle Zeit und teils nicht unerhebliche finanzielle Mittel aufwenden, um entstandene Probleme zu lösen. Schädliche Folgen für die körperliche und seelische Gesundheit der Kinder können zudem durch stundenlanges Sitzen vor dem Computer und ungeeignete Computerspiele auftreten.

Schließlich führt die Professionalisierung der Cyberkriminalität zu technisch ausgereiften Angriffsformen, die zu erkennen Anwender und insbesondere Kinder nicht in der Lage sind. So kann ein nicht ausreichend geschützter Computer leichte Beute von Kriminellen werden, die sich Zugriff auf alle persönlichen Daten der Kinder und ihren Computer verschaffen. Im schlimmsten Fall können sie den Computer sogar fernsteuern und ohne das Wissen der Anwender für Angriffe auf weitere Rechner benutzen.

Diese Risiken werden noch dadurch verschärft, dass sich Kinder wie auch viele Erwachsene der Gefahren im Internet nicht bewusst sind und daher die wichtigsten Sicherheitsregeln im Umgang mit dem Computer missachten.

3. Vermittlung von Medienkompetenz

Angesichts dieser Situation sollte es Aufgabe der Gesellschaft sein, den Kindern die notwendigen Kompetenzen und das erforderliche Wissen zu vermitteln, damit sie sich in der virtuellen Welt innerhalb sicherer Grenzen bewegen und den Gefahren des Internets aus dem Weg gehen können.

Aus diesem Grunde wurde der vorliegende Leitfaden zur Informationssicherheit für den Unterricht und zu Hause konzipiert. Er enthält alle notwendigen Informationen in Form leicht verständlicher Kurztexte, verschiedenster Spielideen und Anregungen für die ansprechende Gestaltung des Unterrichts sowie eine Sammlung interessanter Links zum Thema Internet.

Durch den Einsatz im schulischen Unterricht und zu Hause können Kinder anhand dieses Leitfadens zu einem kompetenten, eigenverantwortlichen und bewussten Umgang mit dem Internet angeleitet werden. Gleichzeitig sollen sie befähigt werden, Sicherheitsrisiken selbst zu erkennen und entsprechend zu handeln.

4. Informationssicherheit „made in Luxembourg“

CASES (Cyberworld Awareness and Security Enhancement Structure), die Luxemburger Initiative zur Verbesserung der Informationssicherheit und Dienststelle des Ministeriums für Wirtschaft und Außenhandel, trägt bereits seit mehreren Jahren in enger Zusammenarbeit mit dem Ministerium für Erziehung und Berufsausbildung zur Förderung der Bildung von Medienkompetenz in luxemburgischen Schulen bei. So veranstaltet CASES beispielsweise Kurse zur Informationssicherheit in Lyzeen und Primärschulen für Schüler, Erziehungsberechtigte und Lehrkräfte. Die Schulungen werden von Fachpersonal mit pädagogischer Erfahrung durchgeführt. Interessierte Schulen und Elternvereinigungen können sich über das luxemburgische Sicherheitsportal CASES www.cases.lu zu den Weiterbildungskursen anmelden.

Auf dem Sicherheitsportal **www.cases.lu** steht Internetnutzern ferner unterschiedlichstes Material zu Fragen der Informationssicherheit zur Verfügung.

Daneben bietet das von der Europäischen Komission unterstützte Portal **LuSI (Luxembourg Safer Internet), www.lusi.lu**, das sich speziell an Kinder und Eltern richtet, nützliche Informationen und Tipps für ein sicheres und medienkompetentes Verhalten im Internet an.

Neben der Website stellt LuSI eine spezielle Helpline zur Verfügung. Hier können Fragen und Probleme zu Themen der Informationssicherheit im persönlichen Gespräch diskutiert werden.

Die Helpline ist unter der Rufnummer **(+352) 26 64 05 44** erreichbar.

Illegale Webinhalte können auf **www.lisa-stopline.lu** oder über die kostenlose Telefon-Hotline **8002-6767** gemeldet werden.

Teil 1

Hinweise zur Nutzung des Leitfadens

1. Idee

Der Leitfaden ist als Lehrbehelf zur Vermittlung der Medienkompetenz konzipiert, die Schüler im Umgang mit dem Internet benötigen.

Anregungen für diesen Leitfaden bot der Best Practice Leitfaden, der von der nordrheinwestfälischen Landesregierung und den sogenannten Internauten für das Lehrpersonal in Nordrhein-Westfalen entwickelt wurde.

Im Wesentlichen stützt sich der vorliegende Leitfaden jedoch auf das von CASES und LuSI erstellte und kindgerecht aufbereitete Informationsmaterial sowie auf die praktischen Erfahrungen, die CASES im Rahmen der Arbeit mit Schulklassen in Luxemburg sammeln konnte.

2. Ziel

Der Leitfaden dürfte Sie in die Lage versetzen, den Kindern dabei zu helfen, das folgende übergeordnete Lernziel zu erreichen:

Aneignung von Schutzreflexen und Verhaltensregeln im Bereich „Sicherheit von Informationen“ und verantwortungsbewusster Umgang mit dem Internet und seinen Funktionsweisen.

Das übergeordnete Lernziel wird anhand der fünf folgenden Teilziele erreicht:

1.	Einfache Zusammenhänge und Funktionen des Internets verstehen.
2.	Soziale und gesellschaftliche Verhaltensregeln im Internet beachten.
3.	Mit dem Internet und seinen Funktionen kritisch und vorsichtig umgehen.
4.	Konkrete Risiken und Gefahren erkennen und richtig darauf reagieren.
5.	Einfache Grundsätze der Informationssicherheit kennen und beherzigen.

Diese fünf Teilziele werden schrittweise in Form von Kompetenzen mit den Kindern erarbeitet.

3. Aufbau

5 Teilziele:
Die fünf Teilziele entsprechen fünf Kapiteln. Eine Tabelle zu Beginn eines jeden Kapitels gibt einen Überblick über die behandelten Themen.

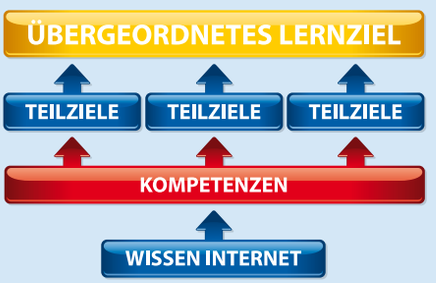
Kurztexte:
Sämtliche Themen sind in Form von Kurztexten aufbereitet, die Sie nutzen können, um die Kinder auf das Erlernen der Kompetenzen vorzubereiten. Zu zahlreichen Fachwörtern und -begriffen aus der Welt des Internets und der Computer finden Sie Analogien oder kindgerechte Beispiele kursiv und in Klammern („Beispiel"). Gegebenenfalls werden die Texte durch kursiv gesetzte Hintergrundinformationen ergänzt.

Es ist keinesfalls erforderlich, dass die Kinder die gesamten Informationen in den Kurztexten lernen!

Kompetenzen:
Im Anschluss an die Kurztexte finden Sie die einfach und regelhaft formulierten Kompetenzen. Sie bilden die Grundlage für das Erreichen des übergeordneten Lernziels: des sicheren Umgangs mit dem Internet.

Durch den modularen Aufbau dieses Leitfadens können Sie einzelne Kompetenzen herausgreifen und mit den Kindern erarbeiten.

Die folgende Grafik zeigt Ihnen die Zuordnung der Begriffe „übergeordnetes Lernziel", „Teilziele" und „Kompetenzen":



Praxistipps:
In den Praxistipps finden Sie zahlreiche Vorschläge zur abwechslungsreichen Gestaltung des Unterrichts und zur Wissensüberprüfung, wie etwa konkrete Spielideen, Kopiervorlagen mit Quizfragen sowie ausgesuchte und geprüfte Links, die Sie zu Internetseiten mit interessanten Filmen, Spielen und zusätzlichen Informationen führen.

Kinderthemenblätter:
Anhand von kindgerechten Kurzgeschichten werden hier wichtige Begriffe, Werkzeuge und nötige Verhaltensweisen der Informationssicherheit erklärt.

4. Methodologische Empfehlungen [2]

Vorbereitete Lernumgebung.

Die Bildschirme sollten so ausgerichtet sein, dass Sie sehen können, woran ein Kind arbeitet und wo es sich im Internet aufhält. [3]

Jeder Computer muss über ein Mindestmaß an Schutz verfügen: Sie sollten Ihre Programme, den Antivirusschutz und die Antispyware auf dem aktuellen Stand halten sowie die Firewall und den Spamfilter korrekt einstellen. Informieren Sie sich über die nötige Vorgehensweise und entsprechende Einstellungen unter **www.cases.lu** oder lassen Sie sich vom technischen Personal der Schule unterstützen.

Es sollten nicht mehr als 2–3 Kinder an einem Computer arbeiten.

Es empfiehlt sich, dass alle Kinder einer Gruppe über die gleichen Grundkenntnisse verfügen. Eine gewisse Lesekompetenz sollte bei allen Kindern gegeben sein.

Einbindung von Vorwissen, Erfahrungen und Interessen der Kinder

Folgende Fragen können Sie am Anfang der Unterrichtsreihe stellen, um an das bereits vorhandene Wissen der Kinder anzuknüpfen:

Vorwissen:

- Was genau kann man im Internet machen?
- Welche Gefahren können sich im Internet verbergen?

Erfahrungen:

- So nutze ich den Computer/das Mobiltelefon/das Internet.
- Das ist mir schon einmal mit dem Computer/Mobiltelefon/Internet passiert.
- Das habe ich schon mal bei meiner Freundin/meinem Freund/meinen Eltern gesehen.

[2] SIEDING (Bettina), STAPELER (Kai), Internet-Fibel, Bonn, Agentur secure-it nrw, 2006, S.7–9.

[3] Es gibt hierzu eine Bildschirmkontrolle (z. B. Schulnetzverwalter SNV, auch Freeware), die eine übersichtliche Anzeige aller Bildschirminhalte auf dem Lehrer-Bildschirm gestattet.

Interessen

- Was muss ich wissen, um mich sicher im Internet zu bewegen?
- Was muss ich wissen, um sicher mit dem Computer/dem Mobiltelefon umzugehen?

Sie können folgende drei Methoden nutzen, um die Kinder zur Diskussion anzuregen:

Methode	Schritt 1	Schritt 2
1. Stichwort-sammlung mit Karteikarten	Kinder schreiben in Gruppenarbeit oder allein Stichworte zu den Bereichen Vorwissen, Erfahrungen und Interessen auf mehrfarbige Karteikarten - ein Stichwort pro Karte.	Die Bereiche werden nun an der Tafel von links nach rechts notiert. Die Kinder lesen nacheinander ihre Stichworte vor und ordnen sie den Bereichen an der Tafel zu.
2. Plakatarbeit	Die Kinder werden in Gruppen aufgeteilt. Jede Gruppe erhält zwei Plakate, jeweils eins für das Thema „Welche Möglichkeiten kann man im Internet nutzen?“ und „Welche Gefahren können sich im Internet verbergen?“. Reihum schreibt jedes Kind ein Stichwort auf jedes Plakat.	Jede Plakatgruppe präsentiert ihre Ergebnisse.
3. Erzählkreis mit Film	Die Kinder sprechen im Erzählkreis von ihrem Vorwissen, ihren Erfahrungen und ihren Interessen.	Die Ergebnisse des Erzählkreises werden von den Lehrpersonen zusammengefasst.

Anhand des gesammelten Materials zu Vorwissen, Erfahrungen und Interessen der Kinder können die einzelnen Themenbereiche nun zusammen erarbeitet werden.

Einsatz im Unterricht

Medienpädagogische Themen können fächer- und jahrgangsübergreifend behandelt werden.

Beispiele:

1.	Die richtige Nutzung der Internetfunktionen kann in den Rahmen einer Recherche zu einem bestimmten Thema gestellt werden.
2.	Schädlinge wie das „Trojanische Pferd“ können in einem geschichtlichen Kontext behandelt werden. „Viren“ lassen sich im Naturkundeunterricht erklären.
3.	Verhaltensregeln sind in Verbindung mit Kursen zur Gewaltprävention erarbeitbar.
4.	Das Chatten im Internet lässt sich im Deutschunterricht nachspielen.

Teil 2
Unterrichtsmaterial

Teilziel 1

Einfache Zusammenhänge und Funktionen des Internets verstehen

	Interessant zu wissen	Wichtig zu können
1.1	Das Internet ist ein Zusammenschluss von vielen Millionen Computern.	Im Internet keine persönlichen Daten veröffentlichen.
1.2	Im Internet ruft man bekannte Adressen mit dem Browser auf.	Internetadressen mit Adressleiste des Browsers aufrufen.
1.3	Im Internet findet man Informationen mit der Suchmaschine.	Suchmaschinen richtig nutzen.
1.4	Im Internet gelangt man mit Links von Seite zu Seite.	Links richtig nutzen.
1.5	Im Internet werden Informationen per E-Mail verschickt.	E-Mails richtig empfangen und senden.
1.6	Im Internet findet man interessante Texte und Fotos.	Texte und Grafiken richtig kopieren.
1.7	Fremde Veröffentlichungen dürfen nicht ungefragt kopiert werden.	Bei Veröffentlichung von fremden Dateien den Autor angeben.
1.8	Fotos und Filme dürfen nur mit Zustimmung der darauf abgebildeten/aufgezeichneten Personen veröffentlicht werden.	Veröffentlichung persönlicher Fotos nur nach ausdrücklicher Zustimmung zulassen.

1.1 Das Internet ist ein Zusammenschluss von vielen Millionen Computern

In den 60er Jahren ließ die US Air Force von Forschern ein geheimes Computernetzwerk aufbauen, das zunächst nur für die Armee bestimmt war.

Später jedoch überließ die amerikanische Regierung die Kontrolle über das geheime Netzwerk den Universitäten. Die Studenten bauten es aus, und täglich wurden mehr Computer angeschlossen. Heute wird es von Millionen Menschen auf der ganzen Welt genutzt. Dieses Computernetzwerk verbindet Menschen in allen Ländern der Welt. Daher ist das Internet weder privat noch geheim, sondern öffentlich *(„Zeitung")*. Da auf den Computern des Internets alles gespeichert wird, kann nichts, was einmal veröffentlicht wurde, wirklich gelöscht werden. Das Internet vergisst daher nichts!

Ein wichtiger Teil des Internets ist das WWW oder auch World Wide Web. Das World Wide Web besteht aus vielen Internetseiten, die miteinander verbunden sind.

Wichtig zu können: im Internet keine persönlichen Daten veröffentlichen

- Veröffentliche keine persönlichen Daten, denn jeder kann sie lesen.
- Erzähle deinen Internetfreunden nur Dinge, die wirklich jeder wissen darf.

1.2 Im Internet ruft man bekannte Adressen mit dem Browser auf

Im Internet können Kinder ihre Meinung mitteilen und die Ansichten anderer Menschen kennenlernen. Sie können auch daran teilhaben, wie ihr Land regiert wird, indem sie sich z. B. die Regierungsseiten ansehen. Dazu benötigen sie aber deren genaue Adresse.

Der Browser, ein spezielles Softwareprogramm, führt zu der genauen Adresse des Computers im Internet und der damit verbundenen Internetseite. Eine Internetadresse kann bereits erste Hinweise auf den Inhalt einer Internetseite geben.

Eine Internetadresse besteht aus drei Teilen:

- Der erste Teil der Adresse lautet oft WWW (World Wide Web).
- Der zweite Teil besteht aus einem Namen. Dieser Name weist oft auf den Inhalt der Internetseite hin. Der Name wurde von demjenigen ausgesucht, der Informationen öffentlich zugänglich machen möchte.
- Am dritten Teil können wir oft erkennen, aus welchem Land die Adresse ist. Zum Beispiel steht .lu für Luxemburg. Wir können auch erkennen, wem die Seite gehört: Zum Beispiel steht .edu für Schulen und Universitäten oder .com für Unternehmen.

Die einzelnen Teile einer Internetadresse, auch URL (Uniform Resource Locator) genannt, werden als Domain bezeichnet.

Wer den Browser benutzt, muss die Internetadresse richtig in die Adressleiste eingeben, sonst findet der Browser die Seite nicht *(„Telefonbuch benutzen“)*. Dabei ist es egal, ob die Adresse groß- oder kleingeschrieben wird. Wichtig ist jedoch, die Adresse immer selbst einzugeben. Eine Adresse sollte z. B. nicht aus einer E-Mail kopiert werden, denn es besteht die Gefahr, dass Internetpiraten die Adresse gefälscht haben.

Manche Anbieter spekulieren darauf, dass Kinder sich vertippen. Kinder können auf diese Weise sehr leicht auf Seiten mit Werbung oder pornografischen sowie sonstigen extremen Inhalten landen, anstatt auf der Homepage ihres Lieblingssängers [4].
Beispiel: www.madona.com verweist auf eine Werbeseite und nicht auf die Internetseite der Sängerin Madonna.

Wichtig zu können: Internetadressen mit Adressleiste des Browsers aufrufen

1.	Kopiere nie die Internetadresse!
2.	Gib sie selbst in die Adresszeile des Browsers ein.
3.	Achte auf die korrekte Schreibweise der Adresse.
4.	Korrigiere eventuelle Fehler.
5.	Bestätige deine Eingabe mit der Bestätigungstaste.

1.3 Im Internet findet man Informationen mit der Suchmaschine

Es ist nicht einfach, Informationen im Internet zu finden. Aus diesem Grund wurden Suchmaschinen erfunden.

Die großen Suchmaschinen wie z. B. ***www.google.de*** werden automatisch aktualisiert. Daher sind sie oft unübersichtlich. Sie zeigen manchmal Seiten an, die nicht für Kinder gedacht sind, sie sogar erschrecken können.[5] Kinder sollten daher wissen, dass es speziell für sie aufbereitete und betreute Suchmaschinen gibt, die sie nutzen sollten. Empfehlenswert ist zum Beispiel die Suchmaschine auf ***www.blinde-kuh.de***. Hier werden Kinderseiten erfasst und in einer eigenen Datenbank gespeichert.

Alle von Suchmaschinen gefundenen Seiten müssen aber nochmals manuell aussortiert werden, denn nicht alle Seiten sind in Bezug auf die gesuchten Informationen nützlich *(„Detektiv spielen: Informationen suchen und auswerten“)*.

Falls mit einer Suchmaschine keine guten Ergebnisse erzielt werden oder wenn der Link auf eine falsche Seite führt, ist die Suche neu zu starten. Je genauer die Stichworte zur Suche gewählt werden, desto besser sind die Suchergebnisse!

[4] KALLWEIT Andrea, THOMAS Chris. *Ein Netz für Kinder*, Berlin, (Hg.) Bundesministerium für Familie, Senioren, Frauen und Jugend, 2007, S. 22
[5] ebda., S. 10

Wichtig zu können: Suchmaschinen richtig nutzen

In der Suchmaschine ein Suchwort eingeben:

1.	Klicke mit der Maus in das Eingabefeld.
2.	Schreibe das Wort oder eine Kombination von mehreren Wörtern hinein.
3.	Drücke die Bestätigungstaste oder klicke auf den Suchknopf.
4.	Die Ergebnisse erscheinen als Links.
5.	Klicke auf die Links, wenn sie dir nützlich erscheinen.

Neue Suche starten:

1.	Überprüfe nochmals die Rechtschreibung.
2.	Überlege dir ein anderes Wort.
3.	Gib einen allgemeineren Terminus ein.

Ein „Lesezeichen“ erstellen:

1.	Rufe eine Seite auf.
2.	Klicke mit dem Mauszeiger auf „Favoriten“ oder „Lesezeichen“.
3.	Das Lesezeichenmenü öffnet sich.
4.	Wähle „Hinzufügen“ aus.
5.	Ein Menüfenster öffnet sich.
6.	Klicke auf OK.

Eine gute Seite als Startseite festlegen:

1.	Rufe die gewünschte Seite auf.
2.	Klicke mit dem Mauszeiger auf das Zeichen vor http:// und ziehe es auf das Haus in der Menüleiste des Browsers.
3.	Ein Menüfenster öffnet sich.
4.	Klicke auf OK.

1.4 Im Internet gelangt man mit Links von Seite zu Seite

Ein Link ist eine Verbindung zu weiteren Informationen. Viele Internetseiten sind so miteinander verbunden. Mit einem Klick auf einen Link kommt man auf eine weitere Internetseite oder an eine andere Stelle der Seite, auch Hyperlink genannt. Mit Hyperlinks ist es möglich, blitzschnell von einer Internetseite zur nächsten zu gelangen. Mit den Hyperlinks sind auch E-Mail-Adressen *(„Briefkästen des Internets")* erreichbar.

Wichtig zu können: Links richtig nutzen

Links erkennen:

	Links sind oft unterstrichen, farbig markiert, in einer dickeren Schrift oder als Bilder oder Symbole dargestellt.

Links anklicken:

1.	Mit dem Mauszeiger über einen Link fahren.
2.	Der Mauszeiger verändert sich.
3.	Link anklicken.

1.5 Im Internet werden Informationen per E-Mail verschickt

Sehr interessant für Kinder ist der E-Mail-Austausch. Kinder sollten daher wissen, wie E-Mails und angehängte Dateien, etwa Fotos oder Musik, verschickt und empfangen werden.

Kinder können sich im Internet kostenlos eine E-Mail-Adresse einrichten *(„Briefkasten")*. Sie kann von jedem Computer mit Internetanschluss genutzt und von ihnen selbst verwaltet werden.

Die E-Mail-Adresse besteht aus drei Teilen:

1. Persönlicher Name - je nach Verwendung sollte hier ein Fantasiename und nicht der richtige Name verwendet werden;
2. Klammeraffe - das @-Zeichen;
3. Mail-Server-Name.

Den ersten Teil der E-Mail-Adresse kann man sich selbst aussuchen. Er sollte leicht zu merken sein und darf von niemand anderem verwendet werden.

Elektronische Post wird in einem sogenannten Mail-Server *(„Postamt“)* und dort im eigenen Briefkasten aufbewahrt.

Die E-Mails müssen auf den Computer geladen werden *(„Briefkasten leeren“)*. Hier können sie bearbeitet und beantwortet werden. Dazu ist ein E-Mail-Programm nötig.

Es gibt im Programm mehrere Ordner: Im Ordner „Posteingang“ sieht man, wann, von wem und zu welchem Thema eine Nachricht eingetroffen ist.

E-Mails sind aber wie Postkarten: Jeder im Internet kann sie lesen! Daher sollten keine zu persönlichen Dinge darin stehen.

Es ist auch möglich, E-Mails per Webmail abzurufen. Damit können die E-Mails über den Browser gelesen und versendet werden. Sie sind somit von jedem internetfähigen Computer aus zugänglich. Online-Anbieter von E-Mail-Adressen stellen solche Dienste zur Verfügung. Die Handhabung ist ähnlich wie beim E-Mail-Programm.

Wichtig zu können: E-Mails richtig empfangen und senden

1.	Öffne die Nachricht, wenn du sie lesen möchtest.
2.	Klicke auf „Antworten“, wenn du die Nachricht beantworten möchtest.
3.	Klicke auf „Löschen“, um die Nachricht aus deinem Posteingang zu entfernen.
4.	Klicke auf „Einfügen, Datei“ und wähle die Dateien aus, die du mitschicken möchtest.

Achtung: Öffne nur Nachrichten, bei denen du den Absender kennst und dir nichts eigenartig oder ungewöhnlich vorkommt.

1.6 Im Internet findet man interessante Texte und Abbildungen

Das Internet bietet für eigene Berichte oder Hausaufgaben viele Informationen, Illustrationen und Fotos. Diese Daten können durch Markieren, Herunterladen oder Kopieren in die eigenen Dokumente eingefügt werden.

Es darf dabei aber nicht vergessen werden, dass diese Datei von jemandem erstellt worden ist. Das ist der Autor oder die Autorin. Sein/ihr Name sollte immer genannt werden. Das nennt man „die Quelle angeben“.

Wichtig zu können: Texte und Grafiken richtig kopieren

Texte kopieren:

1.	Öffne ein bestehendes Textdokument, erstelle ein neues Dokument oder suche mit der Suchmaschine nach dem Thema und öffne einen Text.
2.	Markiere den Text.
3.	Klicke mit der rechten Maustaste auf den markierten Text (Ctrl + C / Strg + C oder Menü „Bearbeiten, Kopieren“ oder Symbol „Kopieren“).
4.	Setze im Dokument, in das der Text eingefügt werden soll, den Cursor an die Stelle, an der du den Text einfügen möchtest.
5.	Füge den kopierten Text ein (Ctrl + V / Strg + V oder Menü „Bearbeiten, Einfügen“ oder Symbol „Einfügen“).
6.	Gib die Quelle an und vergiss das Speichern nicht!

Grafik kopieren:

1.	Öffne ein bestehendes Textdokument, erstelle ein neues Dokument oder suche mit der Suchmaschine nach dem Thema und öffne einen Text.
2.	Markiere die Grafik.
3.	Klicke mit der rechten Maustaste auf die Grafik: Das Kontextmenü öffnet sich.
4.	Wähle „Kopieren“ oder „Bild speichern unter“.
5.	Gehe in das Dokument und dort an die Stelle, in der die Grafik eingefügt werden soll.
6.	Füge die Grafik über die Zwischenablage oder über „Einfügen, Grafik, aus Datei“ ein.
7.	Gib die Quelle an und vergiss nicht zu speichern!

1.7 Fremde Veröffentlichungen dürfen nicht ungefragt kopiert werden

Das sogenannte Urheberrecht sieht vor, dass nur solche Werke veröffentlicht werden dürfen, die man selbst geschaffen hat. Musikvideos aus den neuesten Charts gehören nicht dazu, auch keine kopierten Texte oder Fotos aus dem Internet *(„wenn man etwas von jemandem ausleiht, den Besitzer vorher fragen“)*.

Um ganz sicher zu gehen, sollte geprüft werden, ob die Homepage einen Hinweis auf das Urheberrecht enthält oder nicht. Damit zeigt man, dass man sein Bestes getan hat, die Urheberrechte des Autors zu achten.

Tipp: *Nichts ist leichter, als selbst ein Urheberrecht zu seinen Veröffentlichungen zu schreiben, wie zum Beispiel auf der eigenen Homepage. Das könnte ungefähr so klingen: „Jeder darf meine Musik benutzen. Es kostet nichts, aber bitte gebt meinen Namen und meine Homepage an. Ich möchte auch nicht, dass ihr meine Musik verfälscht oder umändert.“*

In Luxemburg ist das Urheberrecht durch das Gesetz vom 18. April 2001 geregelt: « Loi sur les droits d’auteur, les droits voisins et les bases de données ». Bei Übertretungen können Strafen zwischen 250,- bis 250.000,- EUR verhängt werden.

Wichtig zu können: bei Veröffentlichung von fremden Dateien den Autor angeben

	Gib immer den Namen des Autors an, wenn du Texte, Musik, Filme oder Fotos veröffentlichst.
	„Knacke“ keine kopiergeschützten Dateien.
	Gib keine kopiergeschützten Videos, Spiele und Ähnliches weiter.

1.8 Fotos und Filme dürfen nur mit Zustimmung der abgebildeten/ aufgezeichneten Personen veröffentlicht werden

Im Blog oder auf der persönlichen Homepage ist es möglich, selbst geschossene Fotos oder verfasste Texte zu veröffentlichen. Das ist in Ordnung, solange nur Fotos dabei sind, von denen nicht zu erwarten ist, dass sie einem jetzt oder später Probleme einhandeln, zum Beispiel, weil man darauf nur leicht bekleidet ist oder weil man mit seinen Freunden Quatsch macht. Außerdem müssen alle, die auf dem Foto zu sehen sind, vorher gefragt werden, ob sie damit einverstanden sind, dass das Foto im Internet veröffentlicht wird. Für alle Personen unter 18 Jahren ist zusätzlich noch die Genehmigung von einem Elternteil einzuholen.

Laut Artikel 8 der europäischen Menschenrechtskonvention, Artikel 14.(1) des luxemburgischen Gesetzes vom 8. Juni 2004 zur Meinungsfreiheit in den Medien sowie des Gesetzes vom 11. August 1982 zum Schutz des Privatlebens ist es nötig, vor der Veröffentlichung eines Fotos die Zustimmung der betroffenen Person einzuholen. Dies gilt bereits bei Kindern ab einem Alter von 5 bis 7 Jahren. Bis zu einem Alter von 18 Jahren ist zusätzlich die Zustimmung der Eltern oder des Vormundes der Kinder einzuholen.

Auch wenn die Zustimmung erteilt wurde, sollte darauf hingewiesen werden, dass das Bild nur im Zusammenhang mit dem speziellen Ereignis, in dessen Rahmen das Bild aufgenommen wurde, veröffentlicht wird. Zusätzlich ist festzuhalten, dass das Bild nicht in Bezug auf andere Ereignisse veröffentlicht werden darf, auch nicht zu einem späteren Zeitpunkt.

→ *Im Kapitel Praxistipps befindet sich ein Musterformular zur Erteilung der Zustimmung.*

Wichtig zu können: Veröffentlichung persönlicher Fotos nur nach ausdrücklicher Zustimmung zulassen

	Verlange von deinen Freunden, dass sie dich fragen, bevor sie Fotos veröffentlichen, auf denen du zu sehen bist.
	Frage deine Freunde, wofür dein Foto benutzt wird.
	Überlege es dir gut, bevor du einer Veröffentlichung zustimmst.

Teilziel 2

Soziale und gesellschaftliche Verhaltensregel im Internet beachten

	Interessant zu wissen	Wichtig zu können
2.1	Auch im Internet sind soziale Verhaltensregeln und Umgangsformen zu beachten.	Im Internet freundlich, höflich und respektvoll sein.
2.2	Persönliche Angriffe, Verletzungen und Schädigungen über das Internet sind verboten.	Andere im Internet nicht angreifen und bei Angriffen richtig handeln.

2.1 Auch im Internet sind soziale Verhaltensregeln und Umgangsformen zu respektieren

Auch im Internet gelten Verhaltensregeln. Es ist sehr unfair, sich im Internet zu verstecken, um andere anzugreifen oder lächerlich zu machen.

So hat jeder im Chat und bei E-Mails freundlich mit den anderen umzugehen *(„ein angenehmes Gespräch führen, niemanden anschreien, niemanden beschimpfen")*.

Kinder sollten jene Chats besuchen, die moderiert und daher kontrolliert werden.[6] Das heißt, dass alle Beiträge vor ihrer Freigabe von Erwachsenen gelesen werden. Es ist damit gesichert, dass Kinder keine unangenehmen Leute kennen lernen, die gemein zu ihnen sind oder Verbotenes tun.

Achtung: Sogenannte Kinderchats sind oft nicht moderiert! Es gibt auch Chaträume, die zwar einen kindgerechten Eindruck vermitteln, aber Gefahren bergen können. Ein Beispiel dazu: Die Vergabe von sogenannten „Knuddelpunkten" kann den Eindruck erwecken, es handele sich um einen kindgerechten Chatraum. In Wirklichkeit können sich dort jedoch Erwachsene aufhalten, die Böses im Schilde führen und im Schutz dieses Chatrooms agieren.

→ *Im Kapitel Praxistipps befindet sich eine Tabelle mit Emoticons zur Diskussion wie man Gefühle im Internet ausdrücken kann.*

Wichtig zu können: Im Internet freundlich, höflich und respektvoll sein

Im Internet, vor allem im Austausch mit anderen im Chatraum, sollst du folgende Regeln beachten:

1.	Begrüße als Erstes die Anderen im Chat, nachdem du dich eingeloggt hast.
2.	Sei freundlich zu den Anderen.
3.	Hilf denen, die sich nicht auskennen.
4.	Rede alle mit ihren Nicknames an.
5.	Schreibe kurze Sätze.
6.	Benutze keine Schimpfwörter.
7.	Benutze nicht zu viele Smileys und Großbuchstaben, denn das kann auch anstrengend sein.

[6] http://www.seitenstark.de/chat/ ist ein Beispiel eines moderierten, kindgerechten Chats

2.2 Persönliche Angriffe, Verletzungen und Schädigungen über das Internet sind verboten

Immer öfter erhalten Kinder und Jugendliche über Mobiltelefon oder E-Mail gemeine Botschaften von unbekannten Absendern, und das oft wochen- und monatelang. Die Angreifer, die man als Cyberbullys bezeichnet, veröffentlichen manchmal sogar Fotos von einem, die andere nicht sehen sollten. Es passiert auch, dass Kinder öffentlich gedemütigt und dabei gefilmt werden. Diese gemeinen Videoaufzeichnungen landen danach im Internet und können von allen gesehen werden.

Tipp: *Wenn ein Kind von einem Cyberbully angegriffen, bedroht oder schikaniert wurde und es deswegen traurig ist, sich unwohl fühlt oder Angst hat, hilft es dem Kind, mit seinen Eltern und einem guten Freund darüber zu reden. Fällt es dem Kind schwer, mit diesen Personen über den Angriff zu sprechen, kann es unter* ***(+352) 26 64 05 44*** *auch die LuSI-Telefon-Helpline anrufen.*

Es ist manchmal wichtig, einen Beweis für den Angriff zu haben. Dazu muss man nur auf der Internetseite die Taste „PrtSc"/„Druck S-Abf" drücken und dann in einem Word-Dokument den Befehl zum „Einfügen" geben, entweder über Crtl+V oder Einfügen auf der Menüleiste. Danach ist das Word-Dokument zu speichern. Die Taste„PrtSc"/„Druck S-Abf" macht ein „Foto" vom Bildschirm. Damit wird festgehalten, was auf dem Bildschirm steht.

Jeder, der auf Cyberbullying stößt, sollte darüber mit Erwachsenen reden, auch wenn er nicht direkt davon betroffen ist. Er sollte Hilfe und Unterstützung holen.

Cyberbullying ist eine besonders heimtückische Form von Schikanieren und Bedrohen. Typisch für Cyberbullying ist, dass sich die Täter die Anonymität des Internets zunutze machen, um andere zu verletzen und zu schädigen.

Charakteristisch für die Täter ist beispielsweise, dass sie ein übersteigertes und instabiles Selbstwertgefühl besitzen, wohingegen die Opfer sich eher passiv und ängstlich verhalten.

Die Folgen dieser Aggressionen für die Opfer sind häufig gravierend. Durch Cyberbullying treten sowohl akute, direkte Belastungen (sich verletzt fühlen, verängstigt sein) als auch dauerhafte Belastungen (psychische und gesundheitliche Probleme) auf.

→ *Unter Praxistipps befinden sich zwei Übungen. Mit Hilfe des Gewaltbarometers lernen Kinder, die unterschiedlichen Formen von Gewalt kennen. Sie lernen, wer bestimmt, wann Gewalt vorliegt. Der Erfahrungsbericht eines Cyberbullys hilft Kindern dabei, die Folgen von Cyberbullying zu erkennen.*

LuSi bietet zum Thema Cyberbullying über das SCRIPT zwei Kurse an: Im Grundkurs werden Informationen zum Phänomen Cyberbullying vermittelt und Möglichkeiten aufgezeigt, um sich zu schützen. Im Aufbaukurs wird erklärt, wie gegen Cyberbullying nachhaltig vorgegangen werden kann.

Wichtig zu können:
andere im Internet nicht angreifen und bei Angriffen richtig handeln

Andere nicht über Internet angreifen, bedrohen oder schikanieren:

- Mache andere nicht lächerlich.
- Greife andere nicht an.
- Bedrohe oder schikaniere andere nicht über das Internet.
- Unterstütze andere nicht dabei, jemandem wehzutun.
- Unterstütze andere nicht dabei, Schaden anzurichten.

Bei Angriffen und Bedrohungen über das Internet richtig handeln:

- Hol dir Hilfe bei Erwachsenen und rede mit ihnen darüber, wenn du Cyberbullying entdeckst, d. h. wenn du merkst, dass jemand von anderen angegriffen, bedroht oder schikaniert wird.
- Zeige, dass Du mit dem Verhalten des Cyberbullys nicht einverstanden bist.
- Sei der Person, die unter Cyberbullying leidet, ein Freund.
- Reagiere nicht auf die Nachrichten eines Cyberbullys und rede mit deinen Eltern und guten Freunden darüber.
- Fertige einen Beweis an, indem du die Internetseite kopierst und abspeicherst. Das geht ganz einfach. Erscheint die Internetseite, die du speichern möchtest, auf dem Bildschirm, drücke einfach die Taste „PrtSc“/„Druck S-Abf“.
  Öffne ein Textdokument und gib den Befehl „Einfügen“. Speichere das Textdokument als Beweis ab.
- Auf der Internetseite von LuSI ***(www.lusi.lu)*** findest du weitere Informationen zum Thema Cyberbullying.

Teilziel 3

Mit dem Internet und seinen Funktionen kritisch und vorsichtig umgehen

	Interessant zu wissen	Wichtig zu können
3.1	Im Internet gibt es sichere und unsichere Seiten.	Sichere Seiten erkennen und von unsicheren Seiten unterscheiden.
3.2	Fallen für Kinder sind oft gut versteckt.	Vor dem Klicken an die Folgen denken.
3.3	Persönliche Daten können gestohlen werden.	In E-Mails nicht auf Links klicken, sondern Links immer eigenhändig eingeben.
3.4	Kinder sollen niemandem trauen, den sie nur über Internet kennen.	Keine Internetbekanntschaften treffen und keine persönlichen Angaben machen.
3.5	Im Internet gibt es Dinge, die Kindern Angst machen.	Auf Unangenehmes nicht reagieren und mit anderen darüber sprechen.
3.6	Die übermäßige Nutzung des Computers ist ungesund für den Körper.	Computerzeit gut einteilen und auf richtig eingestellten Computerplatz achten.

3.1 Im Internet gibt es sichere und unsichere Seiten

Internetseiten, die von Zeitungen, Fernsehsendern, Gemeinden usw. gemacht sind, sind in der Regel für Kinder sicher. Es lässt sich herausfinden, wer die Seite gemacht hat, wenn man unter „Betreiber", „Kontakt", „Wir über uns" oder „Impressum" nachsieht. Ist kein solcher Hinweis zu erkennen, sollte die Seite nicht besucht werden.[7]

Es gibt Internetseiten, auf denen richtige Fallen für Kinder versteckt sind und auf denen Kinder verleitet werden, ihre Daten anzugeben oder etwas zu kaufen.

Achtung: Wenn der Computer etwas sagen will, geht ein „Menüfenster" auf. Diese Meldung ist nicht mit einem Pop-Up-Fenster zu verwechseln, das aufspringt und z.B. Werbung enthält! Was in diesem „Menüfenster" geschrieben steht, sollte immer aufmerksam gelesen werden. Wenn du dir unsicher bist, ob du den Inhalt verstanden hast, ist es wichtig, einen Erwachsenen zu fragen.

Tipp: *Wenn Kinder im Internet auf Informationssuche gehen, sollten sie am besten nur geprüfte Kinderseiten besuchen. Sie sind z. B. daran zu erkennen, dass sie keine Lockangebote enthalten und dass redaktionelle Inhalte und Werbung nicht vermischt sind.*[8]

Wichtig zu können:
sichere Seiten erkennen und von unsicheren Seiten unterscheiden

Sichere Seiten erkennst du oft so:

- Die Internetadresse oder das Feld „Betreiber", „Kontakt", „Wir über uns" oder „Impressum" zeigt, dass die Seite von Gemeinden, Zeitungen, Schulen, Universitäten usw. gemacht wird.

Unsichere Seiten erkennst du oft so:

- Sie sind knallig-bunt und haben viele blinkende Extras.
- Sie fallen durch Pop-Up-Fenster auf, die ständig aufgehen und stören.

[7] *Internet-Führerschein.* Luxemburg, Lycée Aline Mayrisch, 2007, S.13.
[8] KALLWEIT Andrea, THOMAS Chris. *Ein Netz für Kinder*, Berlin, (Hg.) Bundesministerium für Familie, Senioren, Frauen und Jugend, 2007, S. 18.

3.2 Fallen für Kinder sind oft gut versteckt

Im Internet sind viele Fallen versteckt. Solche Fallen sind zum Beispiel als Gewinnspiele oder Geschenke getarnt und richten oft großen Schaden an. So kann sich ein Gratisangebot oder Geschenk plötzlich als Abonnement oder Vertrag entpuppen, durch den Hunderte von Euro an Kosten anfallen. Falsche Gewinnspiele sind oft so aufgebaut, dass man zuerst etwas bezahlen oder teure SMS versenden muss, um an den Geldpreis zu kommen. In Wahrheit jedoch wird der Gewinn nie ausbezahlt!

Wie im wirklichen Leben gilt der Grundsatz: Wenn etwas zu schön klingt, um wahr zu sein, ist Vorsicht geboten!

Kinder klicken gern auf alles, was irgendwie ansprechend aussieht. Sie sind jedoch überfordert, wenn es darum geht, die kommerziellen Inhalte der Werbefenster zu erkennen und die Folgen für voreiliges Anklicken abzuschätzen .

Das Informationssicherheitsportal CASES des Ministeriums für Wirtschaft und Außenhandel stellt zusammen mit dem Ministerium für Erziehung und Berufsausbildung im Rahmen der Kooperation Benelux sowie der internationalen Kampagne „Fraud Prevention Month 2008" Schulen ein pädagogisch aufbereitetes Lucky Luke Comic von V. Leonardo zur Verfügung. Der Comic zeigt die wichtigsten Betrugsarten, mit denen im Internet zu rechnen ist, sowie mögliche Schutzmaßnahmen auf. Der Comic kann kostenlos über CASES bezogen werden.

Wichtig zu können: vor dem Klicken an die Folgen denken

	Klicke nicht auf Pop-Up-Fenster.
	Verwechsle Menüfenster nicht mit Pop-Up-Fenstern.
	Nimm nicht an Gewinnspielen im Internet oder über Mobiltelefon teil.
	Nimm keine Geschenke an.
	Melde dich nirgends namentlich an.

Achtung: Kinder sollen ihre E-Mail-Adresse nie in Internetformulare eingeben, da sie sonst von unerwünschten E-Mails, sogenanntem Spam, überschwemmt werden könnten.

3.3 Persönliche Daten können gestohlen werden

Datenräuber versuchen immer wieder, persönliche Daten zu stehlen. Damit können sie nämlich viel Geld machen. Um an die Daten zu gelangen, verschicken sie E-Mails mit gefälschten Links. Die Links führen auf die Internetseite der Datenräuber, die genauso aussieht wie die echte. Wenn jemand auf dieser Seite seine Daten eingibt, fallen sie den Räubern in die Hände. Dieser Trick heißt „Phishing“ (siehe 5.5).

Um Daten zu schützen, hilft es, keine Links in E-Mails anzuklicken.

Tipp: *Ein einfacher Trick, um gefälschte Links zu erkennen: Fährt man mit der Maus über den Link, ohne darauf zu klicken, so verrät der Computer die echte Adresse unten am Bildschirmrand.*

Wichtig zu können:
in E-Mails nicht auf Links klicken, sondern Links immer eigenhändig eingeben

	Klicke in E-Mails nicht auf Links.
	Kopiere keine Links in die Adresszeile des Internetbrowsers.
	Gib die Links immer manuell in die Adresszeile des Internetbrowsers ein.

3.4 Kinder sollen niemandem trauen, den sie nur über Internet kennen

Im Internet ist es leicht, sich als jemand auszugeben, der man nicht ist. Besonders im Chat sollten Kinder daher vorsichtig und misstrauisch sein. Auch wenn eine Chatfreundin erzählt, sie wäre 10 Jahre alt, kann es sich in Wirklichkeit um einen erwachsenen Mann oder eine erwachsene Frau handeln, der/die sich als jemand anders ausgibt, weil er/sie böse Absichten hat.

Kinder sollten sich niemals mit einer Internetbekanntschaft treffen, ohne die Eltern darüber zu informieren. Wenn die Eltern einverstanden sind, sollte das Treffen an einem öffentlichen Ort stattfinden, und ein Elternteil oder eine andere erwachsene Vertrauensperson sollte das Kind zum Treffen begleiten.

Aus Sicherheitsgründen sollte man niemandem die Telefonnummer, die E-Mail-Adresse, die Anschrift oder den Namen, auch nicht das Geburtsdatum, geben. Es sollte auch nicht verraten werden, ob man ein Junge oder ein Mädchen ist. Dazu gehört auch, dass man im Internet einen erfundenen Namen benutzt, einen sogenannten „Nickname“ oder Spitznamen. Dieser Name sollte weder das Alter noch das Geschlecht verraten.

Für Kinder ist es sehr verwirrend, dass es nicht als Lügen gilt, sondern dem eigenen Schutz dient, wenn sie auf Fragen zu ihrer Person nicht antworten oder sich eine falsche Identität zulegen.[9] Sie sollen daher wissen, dass es im Internet allgemein üblich ist, nicht alles von sich preiszugeben.

Sexualverbrecher lassen sich oft Monate oder Jahre Zeit, um das Vertrauen eines potenziellen Opfers zu gewinnen.

→ *Im Kapitel Praxistipps befindet sich eine Übung die Kinder dabei unterstützt, zwischen guten und schlechten Geheimnissen unterscheiden zu lernen.*

Wichtig zu können:
keine Internetbekanntschaften treffen und keine persönlichen Angaben machen

	Triff dich prinzipiell niemals mit einer Internetbekanntschaft.
	Mache keine Angaben zu deiner Person.
	Erfinde einen Namen, der nichts über dein Alter und dein Geschlecht verrät.
	Schicke niemandem Fotos von dir oder deinen Freunden.

3.5 Im Internet gibt es Dinge, die Kindern Angst machen

Im Internet herrscht Meinungsfreiheit, das bedeutet, dass jeder (fast) alles veröffentlichen kann, was er will. Gewalt und andere unangenehme Dinge gehören leider auch dazu. Oft werden sogar unerlaubte Dinge veröffentlicht, da die Polizei nicht gleich alles findet und entfernen kann.[10]

Es kann vorkommen, dass Kinder auf E-Mails oder Beiträge in Chatrooms stoßen, die zweideutig klingen, unanständig sind, hetzerisch wirken, bedrohlich scheinen oder ihnen unangenehm sind. Solche Beiträge sollten von den Kindern nicht beantwortet werden. Wenn möglich, sollten Kinder diese Beiträge auf dem Computer (siehe 2.2) speichern und sich bei Erwachsenen Unterstützung holen.

Besonders am Anfang und beim Ausprobieren neuer Möglichkeiten im Internet sollten Kinder sich immer von Erwachsenen begleiten lassen. Wenn Kinder ein unangenehmes, sonderbares oder trauriges Gefühl haben, sollten sie mit den Eltern darüber reden. Gefühlsgesichter (siehe Praxistipps) können dabei helfen, dass Kinder ihre Gefühle ausdrücken und mit den Eltern darüber reden.

Unangenehme Seiten können und sollten außerdem gemeldet werden. Hierzu steht in Luxemburg die LISA-Stopline ***(http://www.lisa-stopline.lu***) zur Verfügung.

[9] KALLWEIT Andrea, THOMAS Chris. *Ein Netz für Kinder*, Berlin, (Hg.) Bundesministerium für Familie, Senioren, Frauen und Jugend, 2007, S. 18.
[10] http://www. Internet-abc.de

Ein Erwachsener, der einen sexuellen Übergriff auf ein Kind verübt oder es zu sexuellen Handlungen auffordert, verstößt gegen gesellschaftliche Normen und Gesetze. Das gilt im Internet ebenso wie in der realen Welt. Kindern sollte dieser Zusammenhang erklärt werden.

Von leichten sexuellen Übergriffen spricht man, wenn jemand mit einem Kind über Sex reden möchte, nach dem Aussehen des Körpers des Kindes oder nach seinen sexuellen Erfahrungen fragt, beziehungsweise von seinen eigenen sexuellen Erfahrungen erzählt. Schwere sexuelle Übergriffe liegen vor, wenn jemand einem Kind Fotos von nackten Personen oder Pornofilme schickt, beziehungsweise das Kind zu sexuellen Handlungen auffordert, zum Beispiel vor der Webcam. Wenngleich Mädchen häufiger Opfer sexueller Übergriffe werden als Jungen, sind von solchen Angriffen Kinder jeden Alters betroffen. Allgemein ist die Anzahl der sexuellen Übergriffe auf Kinder im Internet sehr hoch.[11]

→ *Unter den zusätzlichen Dokumenten befindet sich ein Bastelbogen (Gefühlsgesichter) der den Kindern helfen kann, ihre Gefühle auszudrücken.*

Wichtig zu können:
auf Unangenehmes nicht reagieren und mit anderen darüber sprechen

	Beantworte in Chatrooms keine E-Mails oder Beiträge, die dir unangenehm sind.
	Speichere diese Beiträge, wenn möglich, auf dem Computer (siehe 2.2).
	Hole dir eine erwachsene Vertrauensperson zur Unterstützung, sobald du dich unwohl fühlst.

[11] *Cyberbullying: Neue Formen von Aggression und Gewalt unter Jugendlichen*, Dr. Catarina Katzer, Institut für Wirtschafts- und Sozialpsychologie, Universität Köln, 2007.

Melde unangenehme Beiträge deinen Eltern, einer Vertrauensperson oder der Polizei. Es steht dir auch die LuSI-Telefon-Helpline unter der Rufnummer (+352) 26 64 05 44 zur Verfügung.

3.6 Die übermäßige Nutzung des Computers ist ungesund für den Körper

Der menschliche Körper ist von Natur aus für Bewegung bestimmt. Langes Sitzen belastet ihn daher und tut ihm auf die Dauer nicht gut. Außerdem können manche Computerspiele süchtig machen. Besonders gefährlich sind solche Spiele, bei denen sich der Spieler ganz in eine Spielfigur hineinfühlt.

Wie leicht vergisst man beim Spielen: Das, was im Spiel gilt, gilt im richtigen Leben noch lange nicht. Wer im Spiel etwas Böses tut oder tötet, wird mit Punkten belohnt. Im wirklichen Leben ist das anders! Wenn jemand etwas Böses tut, wird er dafür nicht belohnt, sondern bestraft.

Es ist wissenschaftlich erwiesen, dass Spiele, in denen Gewalt vorkommt, zu aggressiverem Verhalten führen. Dies gilt auch für Comicspiele und Ähnliches.

Neben dem Computer sollte genügend Zeit für andere Beschäftigungen bleiben, wie z. B. Musik, Sport oder draußen mit Freunden spielen.

Gut ist es, wenn eine vorab vereinbarte „Bildschirmzeit" pro Tag nicht überschritten wird. Die Bildschirmzeit ist die Zeit, die man vor dem Computer, der Spielkonsole und dem Fernseher verbringt.

Für Kinder ist ein richtig eingestellter Computerplatz außerdem besonders wichtig. Das bedeutet, dass er der Körpergröße des Kindes angepasst ist und gutes Licht zum Arbeiten und Spielen bietet.[12]

→ *Im Kapitel Praxistipps befindet sich eine Anleitung zu einem Computertagebuch das Kindern dabei helfen soll, ihre Bildschirmzeit in gesunden Schranken zu halten.*

Wichtig zu können:
Computerzeit gut einteilen und auf richtig eingestellten Computerplatz achten

- Versuche, die vereinbarte tägliche Bildschirmzeit nicht zu überschreiten
- Frage deine Eltern und Lehrer, ob dein Computerplatz richtig für dich eingestellt ist.
- Wähle zusammen mit deinen Eltern Computerspiele aus, die gewaltfrei sind.

[12] Europaweit geregelt durch die EU-Bildschirmrichtlinie des Rates 90/270/EWG.

Teilziel 4

Konkrete Risiken und Gefahren erkennen und richtig darauf reagieren

	Interessant zu wissen	Wichtig zu können
4.1	Spam ist unerwünschte elektronische Post.	SPAM ignorieren.
4.2	„Viren" sind gefährliche Programme, die mit Hilfe eines Anwenders aktiviert werden.	Jede Nachricht kritisch prüfen.
4.3	„Würmer" sind gefährliche Programme, die ohne Hilfe aktiviert werden.	Internet nach Gebrauch ausschalten, unbekannte E-Mails löschen, Nachrichten kritisch prüfen.
4.4	„Trojanische Pferde" sind besonders gefährliche Programme, die sich heimlich auf dem Computer festsetzen.	Keine Raubkopien, günstig erworbene Programme oder fragwürdige Gratisprogramme verwenden oder installieren.

4.1 Spam ist unerwünschte elektronische Post

Nicht jede E-Mail kommt von Leuten, die man kennt. Spam ist so eine E-Mail. Spam ist unerwünschte Post. Sie wird in großen Mengen verschickt und enthält meist Werbung, ist aber auch dazu gedacht, Verwirrung zu stiften oder Viren in Umlauf zu bringen.

Damit möglichst viele Menschen Spam erhalten, müssen ihre Adressen gesammelt werden. Wenn E-Mail-Adressaten auf SPAM antworten, bestätigen sie damit, dass die Adresse wirklich existiert, und erhalten noch mehr Werbemüll.

Wichtig zu können: Spam ignorieren

- [ ] Antworte nicht auf unbekannte und verdächtige E-Mails.
- [ ] Schicke keine unbekannten und verdächtigen E-Mails weiter.
- [ ] Lösche unbekannte und verdächtige E-Mails.
- [ ] Öffne keine Anhänge unbekannter und verdächtiger E-Mails.

Kettenbriefe zählen auch als Spam.
Auf Kettenbriefe sollte prinzipiell nicht reagiert werden.

4.2 „Viren" sind gefährliche Programme, die mit Hilfe eines Anwenders aktiviert werden

Eine große Gefahr, die vom Internet ausgeht, sind Viren. Es handelt sich dabei um Programme, die in einer E-Mail oder Datei, die aus dem Internet heruntergeladen wird, in einem Film oder Video-Clip, einem Lied, Foto oder Text versteckt sind. Sie können auch als Spiel, Bildschirmschoner, Virenschutz oder etwas anderes Harmloses getarnt sein.

Viren können auf einem Computer nur dann Schaden anrichten, wenn ihnen dabei geholfen wird. Das geschieht, wenn ein Anwender zum Beispiel auf einen Dateianhang klickt, der ein Virus enthält. Das Virus kann sich dann im Computer ausbreiten und Informationen zerstören. Er kann wichtige Funktionen blockieren, sodass der Computer nicht mehr funktioniert.

Wichtig zu können: jede Nachricht kritisch prüfen

- [ ] Lösche alle verdächtigen oder unbekannten E-Mails mitsamt ihrer Anhänge.
- [ ] Traue nicht jeder Nachricht.
- [ ] Überlege, bevor du etwas anklickst.

4.3 „Würmer“ sind gefährliche Programme, die ohne Hilfe aktiviert werden

Eine weitere Gefahr aus dem Internet sind sogenannte „Würmer“.

Würmer sind gefährlicher als Viren. Sie können ganz ohne Hilfe Schaden anrichten und sich selbstständig, zum Beispiel über die Adressliste eines Computers, weiterverbreiten. Sie verschicken sich sogar im Anhang von E-Mails, die dann als E-Mail eines Freundes empfangen werden. Sie sind sehr schnell und können äußerst zerstörerisch sein.

Auch ein Mobiltelefon kann von Würmern befallen werden, zum Beispiel über „Bluetooth“. Ist ein Wurm auf dem Telefon, verschickt er sich zum Beispiel als MMS-Nachricht im Namen des Mobiltelefonbesitzers an dessen Freunde weiter.

Bluetooth ist ein Ersatz für Kabelverbindungen zwischen Geräten. Diese Technologie funktioniert über Funk und ermöglicht die Kommunikation zwischen Mobiltelefonen, Computern und sonstigen Geräten.

Wichtig zu können: Internet nach Gebrauch ausschalten, unbekannte E-Mails löschen, Nachrichten kritisch prüfen

	Schalte das Internet nach Gebrauch aus.
	Schalte auf deinem Mobiltelefon die Internetverbindung über „Bluetooth“ nach Gebrauch immer aus.
	Lösche unbekannte E-Mails und ihre Anhänge.

4.4 „Trojanische Pferde“ sind besonders gefährliche Programme, die sich heimlich auf dem Computer festsetzen

Trojanische Pferde sind Programme, die als Spiel, Bildschirmschoner oder etwas anderes Witziges oder Harmloses getarnt sein können. Sie können sich auch in einer E-Mail oder einer Datei, die aus dem Internet heruntergeladen wird, verstecken. Auch beim Surfen auf gewöhnlichen Webseiten kann ein Trojanisches Pferd auf den Computer gelangen.

Ein Trojanisches Pferd verschwindet nicht einfach, wenn es Schaden angerichtet hat. Es bleibt ständig auf dem Computer und verschafft einem Piraten Zugang zu allem, was auf dem Computer gespeichert ist. Es kann Daten verändern, das Konto plündern, Passwörter rauben, gespeicherte Adressen löschen und einen Computer wie einen Roboter zum Angriff auf andere fernsteuern.

Das Schlimme ist: Der Computerbesitzer merkt nichts davon.

Kinder sind als Zielgruppe deshalb besonders gefährdet, weil ihre Interessen wie zum Beispiel Spiele spielen, Videoclips ansehen, Lieder anhören oder Fotos herunterladen als Köder dienen.

Das Trojaner-Programm wirkt wie eine weit offene Tür im Computer. Piraten können alle Daten auf dem Computer sehen und die Aktivitäten des Anwenders verfolgen. Sie können den Computer auch fernsteuern. Der Computer wird dann zu einem Roboter, auch Bot oder Zombie-Computer genannt, mit dessen Hilfe z. B. andere Computer angegriffen, Spam-E-Mails versendet oder pädophile Inhalte im Internet verbreitet werden.

Piraten kombinieren heutzutage die technischen Eigenschaften von Viren, Würmern und Trojanischen Pferden. Daher sind technische Maßnahmen zum Schutz des Computers unerlässlich.

Wichtig zu können: keine Raubkopien, günstig erworbene Programme oder fragwürdige Gratisprogramme verwenden oder installieren

	Lade keine Gratisprogramme aus dem Internet herunter.
	Kaufe keine zu günstigen Programme.
	Lade keine Raubkopien von Spielen, Musik oder Videos herunter.

Teilziel 5

Einfache Grundsätze der Informationssicherheit kennen und beherzigen

	Interessant zu wissen	Wichtig zu können
5.1	Das bestehende Risiko kann durch Vermeidung von Schwachstellen verringert werden.	Schwachstellen vermeiden.
5.2	Vor den Gefahren im Internet schützt man sich mit Sicherheitsreflexen.	Wachsamkeit, Misstrauen, Kenntnisse und Erfahrung einsetzen.
5.3	Vor den Gefahren im Internet schützt man sich mit technischen Schutzmaßnahmen.	Technische Schutzmaßnahmen richtig einsetzen und sie immer auf dem neuesten Stand halten.
5.4	„Rechte einschränken“ ist eine technische Schutzmaßnahme.	Aus Sicherheitsgründen den Zugang zum Computer einschränken.
5.5	„Passwörter“ sind eine technische Schutzmaßnahme.	Aus Sicherheitsgründen Passwörter benutzen.
5.6	„Patches“ sind eine technische Schutzmaßnahme.	Aus Sicherheitsgründen Patches herunterladen.
5.7	„Antivirusprogramme“ sind eine technische Schutzmaßnahme.	Aus Sicherheitsgründen ein Antivirusprogramm installieren und ständig aktualisieren.
5.8	Eine „Firewall“ ist eine technische Schutzmaßnahme.	Aus Sicherheitsgründen eine Firewall installieren und richtig einstellen.
5.9	„Spamfilter“ sind eine technische Schutzmaßnahme.	Aus Sicherheitsgründen einen Spamfilter installieren und ständig aktualisieren.
5.10	„Antispyware“ ist eine technische Schutzmaßnahme.	Aus Sicherheitsgründen ein Antispyware installieren und ständig aktualisieren.
5.11	„Back-Up“ ist eine technische Schutzmaßnahme.	Von Daten regelmäßig eine Sicherheitskopie erstellen.

5.1 Das bestehende Risiko kann durch Vermeidung von Schwachstellen verringert werden

Risiko = Schwachstelle x Bedrohung x Auswirkung

Schwachstelle:	**Bedrohung:**	**Auswirkung:**
Schlüssel frei zugänglich	Einbrecher versucht einzudringen	Einbrecher stiehlt Geld, schafft Unannehmlichkeiten

Das Risiko im Internet.

Schwachstelle	Bedrohung	Auswirkung
Das Verhalten des Anwenders und technische Mängel auf dem Computer.	Eine Milliarde Menschen nutzen das Internet, darunter auch solche mit bösen Absichten.	Jeder Internetnutzer hat etwas auf dem Computer, was gestohlen werden kann. Jeder kann in seinen Gefühlen verletzt werden.
Diese Schwachstellen kann der Anwender vermeiden.	Bedrohungen sind nicht beeinflussbar.	Auswirkungen kann ein Anwender nur wenig beeinflussen.

Achtung: Ein Restrisiko bleibt immer bestehen. Auch ein Schlüssel, den man mit sich führt, kann von einem Taschendieb gestohlen werden. Es ist daher nötig, im Internet ständig aufmerksam und wachsam zu sein! *(„Straßenverkehr“)*

Wichtig zu können: Schwachstellen vermeiden

- Überlege, welche technischen Schwachstellen der Computer haben könnte.
- Überlege, welche deiner Verhaltensweisen eine Schwachstelle beim Surfen im Internet darstellt.
- Versuche aktiv, Schwachstellen zu vermeiden.

5.2 Vor den Gefahren im Internet schützt man sich mit Sicherheitsreflexen

Als Benutzer eines Computers sollte sich ein Anwender immer vor Augen halten, dass er selbst den größten Beitrag zur Sicherheit leistet *(„der Anwender ist der Chef seines Computers, und nur er bestimmt, was passiert“)*.

Ein Anwender sollte sich daher auch für das Internet bestimmte Verhaltensweisen angewöhnen *(„bei Gewitter gehen wir nicht vor die Tür“)*, sogenannte Sicherheitsreflexe. Diese Sicherheitsreflexe haben nichts mit Technik zu tun, sondern sie bedeuten, dass man wachsam, misstrauisch, informiert und erfahren sein sollte, wenn man im Internet unterwegs ist. Wenn man selbst noch keine oder wenig Erfahrung mitbringt, sollte man sich von jemandem im Internet begleiten lassen, zum Beispiel den Eltern.

Wichtig zu können: Wachsamkeit, Misstrauen, Kenntnisse und Erfahrung einsetzen

	Sei wachsam.
	Vertraue nie dem ersten Eindruck.
	Informiere dich bei erfahrenen Erwachsenen, in Zeitschriften oder im Internet.
	Lass dich bei deinen ersten Ausflügen ins Internet von erfahrenen Erwachsenen begleiten.

5.3 Vor den Gefahren im Internet schützt man sich mit technischen Schutzmaßnahmen

Das richtige Verhalten ist zwar sehr wichtig, aber es reicht nicht aus, um sich vor allen Gefahren zu schützen, die vom Internet ausgehen. Ein Anwender muss auch dafür sorgen, dass sein Computer mit technischen Mitteln geschützt ist *(„vor Kälte schützen wir uns mit geeigneter Kleidung“)*. Diese Mittel werden „technische Schutzmaßnahmen“ genannt.

Dabei ist es wichtig, alle technischen Schutzmaßnahmen richtig einzustellen und sie auf dem neuesten Stand zu halten. Das kann der Computer teilweise selbst übernehmen, wenn es ihm befohlen wird.

Die automatische Aktualisierungsfunktion (auch: Update-Funktion) eines Programms aktualisiert das Programm bei jedem Internetbesuch automatisch.

Wichtig zu können: technische Schutzmaßnahmen richtig einsetzen und sie immer auf dem neuesten Stand halten

- Informiere dich, welche technischen Schutzmaßnahmen auf deinem Computer installiert sind.
- Informiere dich, ob alle technischen Schutzmaßnahmen auf dem neuesten Stand sind.
- Bitte Erwachsene darum, alle nötigen Schutzprogramme zu installieren.
- Bitte Erwachsene darum, alle Schutzmaßnahmen richtig einzustellen.

5.4 „Rechte einschränken“ ist eine technische Schutzmaßnahme

Im Falle von Kindern bedeutet Rechte einschränken, dass ein Kind den Zugang zum Computer auf ausgewählte Personen beschränkt. Das kann zum Beispiel bedeuten, dass nur das Kind selbst das Recht hat, den Computer zu benutzen *(„ich bestimme, wen ich in mein Haus/meine Wohnung/mein Zimmer lasse“)*.

Rechte einschränken bedeutet auch, dass die Internetverbindung immer getrennt wird, sobald sie nicht mehr benötigt wird. Besonders auf dem Mobiltelefon sollte geprüft werden, ob nicht versehentlich Bluetooth eingeschaltet ist. Bluetooth funktioniert über Funk und verbindet Mobiltelefone, Computer und sonstige Geräte miteinander.

Auf dem Computer ist es möglich, Benutzerrechte zuzuteilen. Eltern oder Erwachsene sollten die Systemeinstellung „Benutzerrechte einschränken“ vornehmen, dem Kind diese Funktion erklären und mit dem Kind üben.

Wichtig zu können:
aus Sicherheitsgründen den Zugang zum Computer einschränken

- Bestimme - mit Einwilligung der Eltern - selbst, wer an den Computer darf und was damit gemacht wird.
- Wenn du Internet oder Bluetooth nicht benutzt, schalte sie aus.

5.5 „Passwörter“ sind eine technische Schutzmaßnahme

Das Passwort ist der Beweis, dass die richtige Person am Computer sitzt. Es wird beim Anmelden an einen Computer oder beim Abruf einer E-Mail eingegeben. Auch beim Chatten im Internet wird ein Passwort benötigt, sonst kann man nicht in den Chatroom hinein *(„Märchen von Ali Baba und den 40 Räubern: Das Passwort, um in die Höhle zu gelangen, ist Simsalabim“)*.

Niemand darf das Passwort kennen, auch nicht die beste Freundin oder der beste Freund. Das Passwort darf nirgendwo aufgeschrieben werden. Man sollte seine Passwörter auch mindestens alle sechs Monate ändern. Für jedes Programm oder System sollte ein anderes Passwort verwendet werden *(„unterschiedliche Schlüssel für Haustür, Briefkasten und Garagentor“)*.

Vorsicht vor Passwortdieben

Passwortdiebe wenden besonders gerne zwei Tricks an, nämlich „Phishing“ (siehe 3.3) und „Trojanische Pferde“ (siehe 4.4), um an Passwörter zu gelangen.

Ist das Passwort gestohlen worden, dann kann der Pirat zum Beispiel die E-Mails des Bestohlenen lesen oder in dessen Namen E-Mails verschicken.

Wichtig zu können: aus Sicherheitsgründen Passwörter benutzen

Passwörter erfinden:

	Benutze mindestens 8 Zeichen.
	Benutze Ziffern, Groß- und Kleinbuchstaben sowie Sonderzeichen.
	Nimm keine Wörter aus dem Wörterbuch.
	Nimm keine persönlichen Daten.

Passwörter schützen:

	Gib deine Passwörter nicht weiter.
	Tausche deine Passwörter nicht mit anderen aus.
	Wechsle deine Passwörter öfters.
	Benutze für jedes Programm ein anderes Passwort.

Tipp: *Ein gutes Passwort, das du dir leicht merken kannst, erhältst du mit einem Trick. Merke dir einen Satz und davon die Anfangsbuchstaben der Wörter sowie Zahlen und Zeichen. Beispiel: „**3** **k**leine **S**chweinchen**: P**im**, P**am **u**nd **P**um“ ergibt das sehr sichere Passwort **3kS:P,PuP**. Obwohl es sich um ein kompliziertes Passwort handelt, kannst du es dir leicht merken (Achtung! Jetzt ist das KEIN sicheres Passwort mehr).*

5.6 „Patches“ sind eine technische Schutzmaßnahme

Ein Patch ist eine Verbesserung der Programme, auch „Aktualisierung“ genannt, die man auf dem Computer benutzt („wenn Löcher in der Hose sind, müssen sie geflickt werden“).

Programme, auch Computerspiele, sollten aus mehreren Gründen aktualisiert werden: Es werden Programmfehler ausgebessert und Sicherheitslücken geschlossen. Das verhindert, dass Piraten den Computer angreifen und den Benutzer in Schwierigkeiten bringen können. Zusätzlich werden Programme durch eine Aktualisierung mit den neuesten Möglichkeiten ausgestattet und können leichter bedient werden.

Wichtig zu können: aus Sicherheitsgründen Patches herunterladen

	Sage deinen Eltern und Lehrern, dass sich der Computer vom Internet automatisch die neuesten Patches holen soll.
	Bitte sie, die nötigen Einstellungen vorzunehmen.
	Lass dir zeigen, dass die entsprechenden Funktionen aktiviert sind.

5.7 „Antivirusprogramme“ sind eine technische Schutzmaßnahme

Antivirusprogramme schützen den Computer vor Virusangriffen *(„gegen gefährliche ansteckende Krankheiten muss man sich impfen lassen“).*

Das Antivirusprogramm durchsucht Dateien, also Fotos, Texte, Musik usw., die auf dem Computer gespeichert sind, nach Viren, um zu überprüfen, ob sich ein Virus darin versteckt. Findet das Antivirusprogramm ein Virus, so macht es das Virus unschädlich.

Ein Antivirusprogramm muss immer zusammen mit einer Firewall verwendet werden. Zusammen schützen sie den Computer vor Viren, Würmern und Trojanischen Pferden. Beim Installieren des Antivirusprogramms sollten Eltern oder Erwachsene helfen.

→ *Kindern kann die Funktion eines Antivirusprogramms anhand eines kurzen Rollenspiels von 10 Minuten erklärt werden. Die ganze Klasse ist dabei beteiligt. Eine Beschreibung des Spiels findet sich im Kapitel Praxistipps.*

Wichtig zu können: aus Sicherheitsgründen ein Antivirusprogramm installieren und ständig aktualisieren

Weise deine Eltern darauf hin, dass der Computer, den du benutzt, mit einem aktuellen Antivirusprogramm geschützt sein muss.

Prüfe zusammen mit deinen Eltern oder Lehrern, ob auf dem Computer, den du benutzt, ein Antivirusprogramm installiert ist und ob dieses regelmäßig aktualisiert wird.

Es ist möglich, Dateien oder Downloads aus dem Internet, die sich auf der Festplatte befinden, vom Antivirusprogramm überprüfen zu lassen. Hierzu müssen Dateien oder Downloads mit der rechten Maustaste angeklickt werden. Anschließend kann die Antivirusüberprüfung durchgeführt werden.

Privatanwendern stellt die Industrie auch kostenlose Antivirusprogramme zur Verfügung. Eine Auswahl solcher kostenlosen Schutzprogramme und deren Testergebnisse finden sich auf dem luxemburgischen Informationssicherheitsportal ***www.cases.lu***

5.8 Eine „Firewall" ist eine technische Schutzmaßnahme

Eine Firewall funktioniert wie eine Schutzmauer rund um den Computer. So kann kein Angreifer aus dem Internet durchkommen. Sollte sich ein Trojanisches Pferd auf dem Computer festgesetzt haben, verhindert die Firewall, dass dieses Trojanische Pferd Informationen nach außen weitergibt oder den Zugang zum Computer für andere Angreifer öffnet *(„der Türsteher vor dem Haus hält alle Leute ab, die nicht erwünscht sind")*.

Tipp: *Das Antivirusprogramm und die Firewall sind immer gemeinsam zu benutzen. Zusammen schützen sie den Computer vor Viren, Würmern und Trojanischen Pferden.*

Beim Einstellen der Firewall sollten Eltern oder Erwachsene helfen.

Eine Firewall funktioniert auf Grundlage von Regeln: Alles, was nicht ausdrücklich erlaubt ist, ist verboten. Man kann selbst bestimmen, welche Arten von Informationen zum Empfang auf dem Computer oder zur Versendung zugelassen sein sollen. Die Firewall muss daher richtig eingestellt werden, damit sie ausreichenden Schutz bietet, ohne den Nutzer dabei zu sehr einzuschränken.

→ *Kindern kann die Funktion einer Firewall anhand eines kurzen Rollenspiels von 10 Minuten erklärt werden. Die ganze Klasse ist dabei beteiligt. Eine Beschreibung des Spiels findet sich im Kapitel Praxistipps.*

Wichtig zu können:
aus Sicherheitsgründen eine Firewall installieren und richtig einstellen

- Weise deine Eltern darauf hin, dass der Computer mit einer richtig eingestellten Firewall geschützt sein muss.
- Prüfe mit deinen Eltern oder Lehrern, ob eine Firewall auf deinem Computer installiert ist.
- Bitte deine Eltern darum, die Einstellung der Firewall zu prüfen.

Privatanwendern stellt die Industrie auch kostenlose Firewalls zur Verfügung. Nähere Informationen zu diesen Schutzprogrammen finden sich auf ***www.cases.lu***

5.9 „Spamfilter" sind eine technische Schutzmaßnahme

Bei Spam handelt es sich um E-Mails, die dazu gedacht sind, falsche Informationen, Chaos und Viren zu verbreiten. Um sich davor zu schützen, kann man einen Spamfilter installieren, der solche E-Mails im Vorfeld aussortiert *(„mit dem Aufkleber „Keng Reklamm w.e.g." auf dem Briefkasten verhindern wir, dass wir unerwünschte Werbebriefe erhalten")*.

Beim Einstellen eines Spamfilters sollten Eltern oder Erwachsene helfen.

Wichtig zu können:
aus Sicherheitsgründen einen Spamfilter installieren und ständig aktualisieren

- Prüfe zusammen mit deinen Eltern, ob der Spamfilter auf deinem Computer aktiviert ist und welche Spams gefiltert werden.

5.10 „Antispyware“ ist eine technische Schutzmaßnahme

Antispyware ist ein Schutzprogramm, das Spionageprogramme vom Computer fernhält oder sie vom Computer entfernt *(„der Geheimagent James Bond deckt Spione auf und verhindert, dass sie wichtige Geheimnisse verraten“)*.

Es gibt verschiedene Spionageprogramme:

Eine **Spyware** ist ein Programm, das einen Anwender bei allem, was er im Internet macht, ausspioniert. Das Ergebnis wird Computerpiraten geschickt. So erfahren diese, welche Webseiten der Anwender besucht oder wem er E-Mails schreibt.

Eine **Adware** ist eine andere Art von schädlicher Software. Sie verursacht das ständige Aufgehen von unerwünschten Werbefenstern, sogenannten Pop-Up-Fenstern.

Wenn sich der Computer nach dem Herunterladen eines Programms oder Spiels eigenartig verhält, sei es, dass sich Fenster mit Werbung öffnen, der Computer ungewöhnlich langsam ist oder manche Programme nicht funktionieren, dann hat sich vielleicht ein Spionageprogramm auf dem Computer festgesetzt.

Gratisprogramme oder günstige Angebote, wie zum Beispiel Spiele, die aus dem Internet heruntergeladen werden können, sollten gemieden werden. Es gibt im Internet ganz legale und risikofreie Möglichkeiten, Demoversionen von Spielen oder Programmen direkt von der Internetseite der Hersteller herunterzuladen.

Wichtig zu können:
aus Sicherheitsgründen eine Antispyware installieren und ständig aktualisieren

	Weise deine Eltern darauf hin, dass dein Computer regelmäßig mit einer aktualisierten Antispyware überprüft werden muss.
	Prüfe zusammen mit deinen Eltern oder Lehrern mit einer Antispyware, ob sich auf dem Computer Spione verstecken.
	Aktualisiere die Antispyware von Zeit zu Zeit und lasse sie regelmäßig den Computer überprüfen.

5.11 „Back-Up“ ist eine technische Schutzmaßnahme

Ein Back-Up ist eine Sicherheitskopie von Dateien (Texte, Fotos, Videoclips, Musik, Programme usw.).

Stürzt ein Computer ab oder vernichtet ein Virus die darauf gespeicherten Daten, dann kann man mithilfe der Sicherheitskopie die Informationen wieder herstellen. Ist keine Sicherheitskopie erstellt, können alle Daten für immer verloren sein.

Daten können auf verschiedenen Datenträgern gesichert werden, zum Beispiel auf einer CD-ROM, einer externen Festplatte oder auf einem Memory-Stick.

Wichtig zu können: Daten regelmäßig als Sicherheitskopie speichern

	Speichere zusammen mit deinen Eltern deine Daten regelmäßig auf Datenträgern.
	Bewahre die gespeicherten Daten immer getrennt vom Computer, also in einem anderen Raum, auf.

Teil 3
Praxistipps

Unterrichtsideen

Rollenspiel: „Fang das Virus“

Dauer: 10 Minuten

Beschreibung:

Ein Kind wird ausgewählt. Es soll das Antivirusprogramm darstellen. Der Lehrer/die Lehrerin erklärt ihm, seine Aufgabe bestünde darin, die in der Klasse vorhandenen Viren zu erkennen, die von anderen Kindern dargestellt werden. Das Kind soll diese Viren durch Berührung unschädlich machen. Die anderen Kinder sitzen auf ihren Plätzen. Es werden dabei keine weiteren Erklärungen abgegeben.

Das Kind wird nun fragen: „Aber woher weiß ich denn, wer die Viren sind?“ Diese Frage ist der Schlüssel zur ersten Erkenntnis: Nur ein Antivirusprogramm, das mit Informationen versorgt wird, also regelmäßig aktualisiert wird, kann richtig funktionieren. Erst jetzt gibt der Lehrer/die Lehrerin beliebige Hinweise wie zum Beispiel, dass alle Kinder mit einem roten T-Shirt Viren sind, dann zusätzlich alle Kinder mit einem blauen T-Shirt und so weiter. Das Kind sucht nach den Merkmalen und geht nacheinander zu jenen Kindern, die es als Viren erkannt hat. Es berührt diese Kinder.

Die aktive Suche des ausgewählten Kindes nach den Viren ist der Schlüssel zur zweiten Erkenntnis: Ein Antivirusprogramm sucht den Computer aktiv nach Viren ab und macht diese unschädlich.

Rollenspiel: „Firewall“

Rollenspiel: Schütz den Computer mit einer Mauer
Dauer: 10 Minuten

Beschreibung:

Ein Kind wird ausgewählt und kommt an die Tafel. Es soll den Computer darstellen. Weitere 5 - 6 Kinder werden ausgewählt. Sie stellen sich im Kreis um den Computer. Dabei halten sie sich an den Händen. Sie sollen eine Schutzmauer, also eine Firewall, darstellen. Die restlichen Kinder verkörpern das Internet.

Als Lehrer/in gibt man der Klasse die Information, dass alle Kinder mit einer spezifischen Kennzeichnung zum Computer dürfen, zum Beispiel alle Schüler mit grünen Pullovern. Es sollte immer eine Kennzeichnung gewählt werden, die nicht auf übermäßig viele Kinder zutrifft. Die Kinder, die die Firewall bilden, lassen normalerweise automatisch alle Kinder mit entsprechender Kennzeichnung zum Computer durch. Dies ist der Schlüssel zur ersten Erkenntnis: Die Firewall lässt nicht jeden durch. Als Lehrer/in nennt man den Kindern eine neue Kennzeichnung, zum Beispiel alle Kinder mit einem orangefarbenen Pullover. Auch diese Kinder gehen zum Computer und werden von der Firewall durchgelassen.

Danach gibt man als Lehrer/in die Information, dass die Kinder einer Kennzeichnung, zum Beispiel die Kinder mit orangefarbenem Pullover, den Computer wieder verlassen dürfen. Die Kinder mit orangefarbenem Pullover werden von der Firewall durchgelassen und dürfen sich setzen. Dies ist der Schlüssel zur zweiten Erkenntnis: Die Firewall ist nach Regeln eingestellt.

Meistens hat ein Kind, das Kind X, eine zweideutige Kennzeichnung, steht aber beim Computer. Es wurde von den Kindern, die die Firewall bilden, zum Computer durchgelassen. Als Lehrer/in gibt man diese Feststellung an alle Kinde weiter. Danach dürfen alle Kinder mit eindeutig grünem Pullover den Computer verlassen. Kind X gehört nicht dazu. Dies ist der Schlüssel zur dritten Erkenntnis: Nicht jeder darf aus dem Computer heraus und ins Internet.

Auf diese Art und Weise funktioniert die Firewall. Die Kinder gelangen zu der Erkenntnis, dass die Firewall eine Schutzmauer um den Computer bildet. Sie erkennen, dass es wichtig ist, die Firewall richtig einzustellen. Nur so kann genau geregelt werden, wer in den Computer darf und wer den Computer verlassen darf. Bei einer Firewall kommt zum Beispiel ein Trojanisches Pferd (Kind X) vielleicht in den Computer rein, aber es kann nachher nicht nach außen kommunizieren.

Alle Kinder dürfen sich setzen.

Vereinbarung eines Vertrags „Regeln der Internetnutzung“ mit den Kindern

Zusammen mit den Kindern kann ein Vertrag aufgesetzt werden, um die Verhaltensregeln im Internet festzuhalten. Da die Kinder am Vertrag mitarbeiten, werden Schutzregeln sowie Erlaubtes und Verbotenes für die Kinder besser ersichtlich. Sanktionen bei bewusstem Fehlverhalten werden von den Kindern besser verstanden und akzeptiert.[13]

Beispiel für einen Vertrag:

Regeln der Internetnutzung

1. *Ich mache nur jene Aufgaben und besuche nur jene Internetseiten, die ich im Unterricht von meinen Lehrern erhalte.*
2. *Bin ich nicht sicher, ob eine Internetseite für Kinder gut ist, frage ich meine Lehrer oder Eltern oder einen anderen Erwachsenen.*
3. *Was ich im Internet, mit dem Computer oder dem Mobiltelefon mache, darf niemand anderem schaden. Ich unterstütze auch niemand anderen dabei, Schaden zu verursachen.*
4. *Ich bin im Internet immer freundlich und höflich.*
5. *Ich verrate im Internet nichts über mich, keinen Namen, kein Alter, keine Adresse, keine Telefonnummer, kein Passwort und keine E-Mail-Adresse. Ich stelle auch keine Fotos von mir oder anderen ins Internet, auch nicht auf meine Homepage.*
6. *Bevor ich etwas anklicke, überlege ich genau, ob das für mich und andere gut ist.*
7. *Ich prüfe jede Nachricht kritisch, ob sie wahr ist.*
8. *Ich schütze mich zusätzlich mit folgenden technischen Mitteln: eingeschränktem Zugang, Passwörtern, aktualisierten Programmen, Antivirusprogramm, Firewall und Antispyware.*
9. *Bei Problemen oder wenn ich ein ungutes Gefühl habe, wende ich mich an meine Lehrer, Eltern oder an eine andere erwachsene Vertrauensperson.*

Unterschrift:

[13] Weitere Empfehlungen für die Nutzung von Computern im Unterricht unter http://wir-in-berlin.de/wss/mml/regeln/index.htm

„Mein Computertagebuch“

Mit Hilfe eines Computertagebuchs erhalten Kinder einen Überblick über die Stunden, die sie am Computer, an der Spielkonsole oder dem Mobiltelefon verbringen. Sie lernen, diese Zeit in gesunden Schranken zu halten.

Führe ein Computertagebuch und notiere dir zwei Wochen lang, wie viele Stunden pro Tag du am Computer, der Spielkonsole und mit dem Mobiltelefon verbringst.

Denke auch über folgende Fragen nach:

- Welche Spiele hast du in den letzten zwei Wochen gespielt, und wie viele Stunden hast du damit verbracht?
- Wieso gefällt dir ein Spiel besonders gut und was lernst du aus dem Spiel?
- Wie könntest du die Zeit, die du vor dem Computer verbringst, sonst verbringen?

Andere Ideen:

- Spiele mit deinen Eltern zusammen eines deiner Computerspiele. Wie ist das für dich?
- Versuche jede Stunde vor dem Computer und mit dem Mobiltelefon durch eine Stunde Bewegung auszugleichen. Gelingt dir das?
- Versuche, zwei Tage ohne Computer/Mobiltelefon auszukommen. Überlege, wie du dich fühlst.

Gute Geheimnisse – schlechte Geheimnisse

Kinder schämen sich oder fühlen sich schuldig, wenn sie belästigt und angegriffen werden. Die meisten sprechen daher über solche Vorkommnisse nicht.

Um Kindern zu vermitteln, dass es Dinge gibt, über die sie sprechen sollten, auch wenn es ihnen schwer fällt oder von jemandem untersagt wurde, kann man den Unterschied zwischen guten und schlechten Geheimnissen thematisieren.[14]

Gute Geheimnisse	Schlechte Geheimnisse
In drei Tagen hat deine Lehrerin Geburtstag. In der Klasse macht ihr aus, dass jeder eine Blume mitbringt. Niemand darf vorher etwas verraten.	Auf dem Schulweg wirst du von einem älteren Jungen bedroht. Er will einen Euro von dir. Du sollst aber niemandem davon erzählen. Du hast große Angst.
Das Telefon klingelt, deine Tante meldet sich: „Bitte miss die Größe eures Tisches im Esszimmer für mich aus. Ich möchte deiner Mama eine Tischdecke schenken. Aber nichts verraten!“	Du hast mit dem Fahrrad ein parkendes Auto gestreift. Am Kotflügel ist ein Kratzer. Du überlegst: „Soll ich es zu Hause erzählen?“
Dein Bruder hat im Diktat mehrere Fehler gemacht. Du hast sein Heft entdeckt und versprichst, den Eltern nichts zu verraten.	Du beobachtest, wie ein Kind im Kaufhaus heimlich eine CD in die Tasche steckt. Als es merkt, dass du es beobachtet hast, droht es: „Wenn du mich verrätst, passiert was!“

[14] http://kinderportal.anti-kinderporno.de/

Smileys [15]

Getippter Text ist oft sehr unpersönlich und trocken. Daher werden gerne Smileys oder Emoticons benutzt. Emoticon ist ein zusammengesetztes Wort aus dem Englischen: „Emotion» heißt Gefühl und „Icon" bedeutet so viel wie Zeichen. Also ein Gefühlszeichen!

Kinder lieben es, im Chatroom Smileys zu benutzen. Zur Veranschaulichung des Themas „Gefühle, die man im Internet haben kann" können die folgenden Smileys mit den Kindern diskutiert werden.

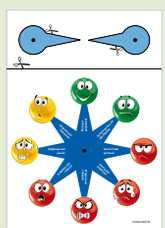
:-)	Das **Grundmodell eines Smileys**. Man benutzt es, um Freude zum Ausdruck zu bringen.
:-))))))	Dieser Smiley drückt **noch größere Begeisterung** aus als der darüber. Je mehr Klammern, also lachende Münder, desto glücklicher ist derjenige, der ihn benutzt.
;-)	**Zwinker-Smiley** Er soll ausdrücken: „Nimm mir nicht übel, was ich gerade gesagt habe." Man benutzt ihn bei scherzhaften, lustigen oder nicht ganz ernst gemeinten Bemerkungen.
:-(	**Saures Gesicht** ...ist böse, sauer, traurig, stinkig.
:-<	...ist sehr traurig.
-)	Halber Smiley. Wird bei scherzhaften Bemerkungen benutzt.
:-))	...zeigt ganz große Freude!
:-/	...zeigt ein schiefes Gesicht, verzieht das Gesicht.
:-I	..sagt: „Ist mir gleichgültig!"
:->	...ist besonders ironisch oder sarkastisch.
>:->	...macht eine teuflische Bemerkung.

[15] http://www.Kidsville.de

Gefühlsgesichter [16]

Gefühlsgesichter helfen ähnlich wie Smileys, Gefühle im Internet einzuordnen. Sie können Kindern dabei helfen, zur Sprache zu bringen, wie sie sich bei Chatgesprächen oder in Bezug auf gelesene und gesehene Informationen fühlen.

	froh, glücklich, gut gelaunt, zufrieden, stolz	**1**
	erleichtert, uninteressiert, gleichgültig	**2**
	schlecht drauf, mürrig, genervt, gestresst, müde, lustlos, beleidigt	**3**
	traurig, trostlos, enttäuscht, einsam, allein	**4**
	böse, wütend, verletzt, genervt, verärgert, unmutig	**5**
	ängstlich, verloren, krank	**6**
	aufgeregt, nervös, erregt, verliebt, empört	**7**
	erstaunt, erwartungsvoll, neugierig, gespannt, überrascht, ungeduldig	**8**



Ein Bastelbogen zum Thema finden Sie unter «Zusätzliche Dokumente»

Gesicht 3 bis 6: Mit den Eltern oder anderen Erwachsenen über das Erlebte reden und Unterstützung holen.

Gesicht 7 bis 8: Mit den Eltern oder einem anderen Erwachsenen darüber sprechen, welche Nachricht oder Tätigkeit dieses Gefühl bei dir verursacht hat.

[16] Vorlage: Madeleine Faber, Religionslehrerin in Mamer

Gewaltbarometer

Dauer: 45 Minuten

Beschreibung: Die Kinder sitzen im Stuhlkreis um einen Kreppstreifen auf dem Boden. Der Kreppstreifen kennzeichnet mit seinen Endpunkten „Gewalt“ und „keine Gewalt“ ein Barometer. Jedes Kind zieht eine Karte mit einer Situationsbeschreibung. Dies ist der Schlüssel zur ersten Erkenntnis: Es gibt unterschiedliche Formen von Gewalt. Die entsprechenden Karten mit mehr oder weniger gewalttätigen Situationen werden im Vorfeld von der unterrichtenden Person angefertigt.

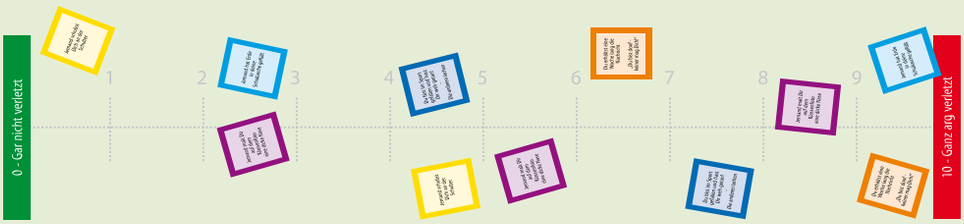
Das Kind liest laut vor. Danach ordnet das Kind die Karte auf dem Barometer ein. Für seine Einordnung gibt das Kind eine Begründung. Andere Kinder können die Karte umordnen. Sie begründen, warum sie denken, dass die Situation mehr oder weniger Gewalt beinhaltet. Dies ist der Schlüssel zur zweiten Erkenntnis: Es gibt unterschiedliche Einschätzungen dazu, ab wann Gewalt vorliegt.

Ein Bastelbogen zum Thema finden Sie unter «Zusätzliche Dokumente»

Die Kinder halten schriftlich fest, welche Formen von Gewalt sie kennen, zum Beispiel verbale Gewalt oder körperliche Gewalt. Jetzt ordnen die Kinder die Situationskarten den einzelnen Gewaltformen zu.

Aus der Diskussion über konkrete Situationen kann eine gemeinsame Definition von Gewalt hergeleitet werden. Was ist Gewalt? Gewalt ist eine gezielte, absichtliche Handlung, um einem Menschen Schaden zuzufügen.

Es lässt sich diskutieren, wer bestimmt, ob ein Verhalten gewalttätig ist oder nicht. Die Kinder lernen, dass am Ende das Opfer entscheidet, ab wann Gewalt vorliegt.



Folgen von Cyberbullying

Dauer: 30 Minuten

Der beigefügte Erfahrungsbericht eines Cyberbullys wird vorgelesen. Die Kinder erarbeiten in Gruppen die Auswirkungen von Cyberbullying auf das Opfer, den Täter und das Umfeld.

Danach werden die Ergebnisse zusammengetragen und diskutiert. Wie fühlt sich das Opfer des Cyberbullyings? Wie fühlt sich der Täter des Cyberbullyings? Tut dem Täter sein Verhalten leid? Fühlt er mit dem Opfer? Wie reagiert das Umfeld?

Die Kinder werden für die Folgen von Cyberbullying sensibilisiert.

Erlebnisbericht Cyberbullying

Hallo, ich bin ein Junge, bin 12 Jahre alt, treibe viel Sport, habe gute Noten usw. Aber es gibt da etwas, was ich euch nie empfehlen würde: „Cyberbullying". Ich will euch erzählen, wie es dazu kam und was für Folgen es hatte.

An einem schönen Samstagnachmittag ging ich nach dem Training zu einem guten Freund. Wir hatten den ganzen Nachmittag viel Spaß. Wir spielten Fußball, blödelten mit dem Hund, rauften und taten alles, was man mit seinen Freunden eben so tut.

Schließlich setzten wir uns an den Computer, um im Internet zu surfen. Das hätte ich verhindern sollen. Ihr habt bestimmt alle MSN. Wir loggten uns in meinen MSN-Account ein, und plötzlich loggte sich ein guter Freund aus dem Sportverein ebenfalls ein.

Wir fingen an mit „Hey, wie geht's" usw., und dann plötzlich waren wir irgendwie nervös, wütend. Irgendetwas war in uns, keine Ahnung was und warum! Wir machten unseren Freund runter, beschimpften ihn, sagten schlechte Sachen zu ihm usw. Wir dachten uns nichts dabei. Es war Spaß.

Was wir nicht wussten, war, dass unser Freund alles speicherte und es seinem Vater zeigte.

Die Folgen:

Ich flog fast aus dem Sportverein. Ich entschuldigte mich in aller Form beim Vorstand und dem Trainer und flog Gott sei Dank letzten Endes doch nicht raus.

Meine 15 Jahre alte Schwester wurde von den größeren Jungs aus meinem Sportverein, die davon Wind bekommen hatten, im Gymnasium gemobbt. Die anderen Eltern redeten nicht mehr mit meinen Eltern. Das war schlimm.

Ich erhielt 4 Wochen Trainingsverbot von meinem Trainer. Meine Sportkollegen beachteten mich nicht mehr. Zusätzlich wurde ich deswegen beinahe nicht in die Sportschule aufgenommen, die ich besuchen wollte.

Heute weiß ich auch, dass mein Freund, den wir über Internet beschimpft hatten, sehr traurig war und viel weinte. Er verstand nicht, wieso ich ihm das angetan hatte. Er war doch im Verein mein bester Freund. Auch Worte können sehr verletzen ...

Inzwischen ist alles wie immer. Ich habe wieder meine Freunde. Auch die Sportschule hat mich angenommen. Ich bin wieder glücklich.

Das alles kostete Disziplin, Zeit und Arbeit. Deshalb: Tut so was niemals!!

Quizfragen

Quiz 1

1. ***Ich kann viele verschiedene Sachen auf dem Computer machen, z. B. chatten, E-Mails verschicken und spielen. Wie gehe ich am besten mit den Passwörtern um?***

- ☐ Um mir die Sache zu vereinfachen, benutze ich immer das gleiche Passwort.
- ☐ Ich habe für jeden Dienst ein eigenes Passwort und wechsele es regelmäßig.
- ☐ Ich benutze immer das gleiche Passwort. Ich wechsele es nie, sonst vergesse ich es.

2. ***Was ist denn eigentlich ein Computervirus?***

- ☐ Ein Programm, das sich in Filmen, Musik, Texten und so weiter versteckt. Klickt man darauf, verbreitet es sich. Dabei kann es eine zerstörerische Kraft haben.
- ☐ Das jüngste Spiel. Jeder hat es, und deswegen nennt man es Virus.
- ☐ Etwas, das die Festplatte zerstören kann. Es ist aber kein Programm.

3. ***Jeder sagt, ich soll meine Programme und Spiele immer auf den letzten Stand bringen. Warum ist das so wichtig?***

- ☐ Jeder macht es, und ich will nicht als Einziger dumm dastehen.
- ☐ Damit bekomme ich neue Bildschirmschoner, und meine Spiele laufen schneller.
- ☐ Dadurch werden Programmfehler ausgebessert.

4. ***Warum muss man immer eine Firewall und ein Antivirusprogramm benutzen?***

- ☐ Das Antivirusprogramm braucht die Firewall, um an bestimmte Dateien zu kommen.
- ☐ Die Firewall verhindert, dass der Computer andauernd abstürzt.
- ☐ Die Firewall analysiert ein- und ausgehende Daten des Computers, und das Antivirusprogramm wehrt Viren ab.

5. ***Seit ich ein Spiel auf meinem Computer installiert habe, das ich im Internet gefunden hatte, ist mein Computer viel langsamer als sonst. Außerdem gehen dauernd Pop-Ups auf, die Werbung anzeigen. Ich denke:***

- ☐ Ich habe wohl gleichzeitig mit dem Spiel eine Spyware installiert. Das ist ein Programm, das mich beim Surfen im Internet ausspioniert.
- ☐ Das hat nichts zu bedeuten und ist normal, wenn man auf Werbeseiten surft.
- ☐ Keine Ahnung, was das bedeutet. Bei dem Spiel wurde nichts von Werbung gesagt.

6. ***Eine Freundin, die gar nicht gut Französisch kann, schickt mir eine französische E-Mail mit einer angehängten Datei. In der Betreffzeile steht in Großbuchstaben: WICHTIG. Wie reagiere ich?***

- ☐ Ich mache den Anhang auf, es ist sicher etwas sehr Wichtiges.
- ☐ Ich schicke es gleich an alle Freunde weiter, da es anscheinend wichtig ist.
- ☐ Ich lösche die E-Mail, weil mir das Ganze sonderbar vorkommt. Zusätzlich erkundige ich mich bei meiner Freundin, ob sie mir wirklich ein E-Mail geschickt hat.

7. ***Ich habe nicht viel Taschengeld, deswegen geben mir meine Freunde Kopien von ihren Computerspielen. Ich lade auch manche Spiele aus dem Internet herunter. Was kann passieren?***

- ☐ Das ist gefährlich. Ich kann mir damit Schädlinge auf den Computer holen.
- ☐ Nichts, das ist erlaubt, solange ich kein Geld damit verdiene.
- ☐ Meine Eltern freuen sich, weil ich so sparsam bin.

Lösung Seite 58

Quiz 2

1. ***Ich habe eine Menge Fotos von Schulfreunden. Wir lachen uns immer kaputt, wenn wir sie uns ansehen. Was könnte ich damit machen?***

- ☐ Die Fotos meiner Freunde auf meinem Blog oder meiner Webseite veröffentlichen, zusammen mit den Namen, dem Alter und den Adressen von allen.
- ☐ Die Fotos veröffentlichen, zusammen mit witzigen Spottnamen.
- ☐ Meine Freunde vorher fragen, bevor ich einige Fotos auf meinem Blog oder meiner Webseite veröffentliche.

2. ***Stell dir vor, du bist ein Mädchen, heißt Nina und bist 10 Jahre alt. Welchen Nickname soll ich mir idealerweise im Chatroom geben?***

- ☐ Tina10
- ☐ Prinzessin
- ☐ Ratatouille

3. ***Ich chatte oft mit jemandem, den ich noch nie wirklich getroffen habe. Seit einigen Tagen stellt er mir Fragen über mich und meine Familie. Er will sogar, dass ich ihm Fotos von mir schicke. Was soll ich tun?***

- ☐ Ich fühle mich nicht wohl dabei. Ich spreche nicht mehr mit der Person und erzähle meinen Eltern gleich davon.
- ☐ Ich fühle mich nicht ganz wohl dabei, schicke ihm aber trotzdem ein paar Fotos.
- ☐ Wir haben uns immer so gut unterhalten. Ich denke, es ist normal, dass er mich näher kennenlernen will. Ich schicke ihm ein paar Fotos von mir.

4. ***Seit einigen Wochen chatte ich mit einem Gleichaltrigen, den ich noch nie getroffen habe. Er will jetzt, dass wir uns treffen, um ein paar CDs auszutauschen. Was soll ich machen?***

- ☐ Ich vertraue ihm/ihr, weil es ein Internetfreund ist.
- ☐ Ich erzähle meinen Eltern davon und bitte sie, mich zu begleiten.
- ☐ Ich gehe alleine hin, es ist ganz in der Nähe und wird nicht lange dauern.

5. ***Ich bin ein Fan von Videospielen, Filmen und Musik. Manchmal kaufe ich sie, aber oft lade ich sie aus dem Internet herunter. Ich gebe sie sogar meinen Freunden weiter. Darf ich das überhaupt?***

- ☐ Nein. Das ist verboten. Ich verletze damit die Autorenrechte.
- ☐ Ja, das ist erlaubt, solange ich kein Geld damit verdiene.
- ☐ Die Polizei wird schon nichts sagen, es sind ja nur zehn Spiele und ein paar CDs.

6. ***Ein älterer Freund von mir will, dass ich ihn mit seinem Handy filme, während er einen anderen auf der Straße hänselt. Er sagt, er will es nur seinen Freunden zeigen. Ich denke:***

- ☐ Ist nicht so schlimm, ist ja nur zum Spaß. Es bleibt ohnehin unter uns.
- ☐ Das mag ich gar nicht, aber ich muss wohl mitmachen.
- ☐ Das ist gemein. Ich mache nicht mit und sage es den anderen. Gemeinsam gehen wir zu unserer Lehrerin und bitten sie, uns zu helfen.

Lösung Seite 58

Lösungen Quiz 1

1. ***Ich kann viele verschiedene Sachen auf dem Computer machen, z. B. chatten, E-Mails verschicken und spielen. Wie gehe ich am besten mit den Passwörtern um?***

   Ich habe für jeden Dienst ein eigenes Passwort und wechsele es regelmäßig.

2. ***Was ist denn eigentlich ein Computervirus?***

   Ein Programm, das sich in Filmen, Musik, Texten und so weiter versteckt. Klickt man darauf, verbreitet es sich. Dabei kann es eine zerstörerische Kraft haben.

3. ***Jeder sagt, ich soll meine Programme und Spiele immer auf den letzten Stand bringen. Warum ist das so wichtig?***

   Dadurch werden Programmfehler ausgebessert.

4. ***Warum muss man immer eine Firewall und ein Antivirusprogramm benutzen?***

   Die Firewall analysiert ein- und ausgehende Daten des Computers, und das Antivirusprogramm wehrt Viren ab.

5. ***Seit ich ein Spiel auf meinem Computer installiert habe, das ich im Internet gefunden hatte, ist mein Computer viel langsamer als sonst. Außerdem gehen dauernd Pop-Ups auf, die Werbung anzeigen. Ich denke:***

   Ich habe wohl gleichzeitig mit dem Spiel eine Spyware installiert. Das ist ein Programm, das mich beim Surfen im Internet ausspioniert.

6. ***Eine Freundin, die gar nicht gut Französisch kann, schickt mir eine französische E-Mail mit einer angehängten Datei. In der Betreffzeile steht in Großbuchstaben: WICHTIG. Wie reagiere ich?***

   Ich lösche die E-Mail, weil mir das Ganze sonderbar vorkommt. Zusätzlich erkundige ich mich bei meiner Freundin, ob sie mir wirklich ein E-Mail geschickt hat.

7. ***Ich habe nicht viel Taschengeld, deswegen geben mir meine Freunde Kopien von ihren Computerspielen. Ich lade auch manche Spiele aus dem Internet herunter. Was kann passieren?***

   Das ist gefährlich. Ich kann mir damit Schädlinge auf den Computer holen.

Lösungen Quiz 2

1. ***Ich habe eine Menge Fotos von Schulfreunden. Wir lachen uns immer kaputt, wenn wir sie uns ansehen. Was könnte ich damit machen?***

   Meine Freunde vorher fragen, bevor ich einige Fotos auf meinem Blog oder meiner Webseite veröffentliche.

2. ***Stell dir vor, du bist ein Mädchen, heißt Nina und bist 10 Jahre alt. Welchen Nickname soll ich mir idealerweise im Chatroom geben?***

   Ratatouille

3. ***Ich chatte oft mit jemandem, den ich noch nie wirklich getroffen habe. Seit einigen Tagen stellt er mir Fragen über mich und meine Familie. Er will sogar, dass ich ihm Fotos von mir schicke. Was soll ich tun?***

   Ich fühle mich nicht wohl dabei. Ich spreche nicht mehr mit der Person und erzähle meinen Eltern gleich davon.

4. ***Seit einigen Wochen chatte ich mit einem Gleichaltrigen, den ich noch nie getroffen habe. Er will jetzt, dass wir uns treffen, um ein paar CDs auszutauschen. Was soll ich machen?***

   Ich erzähle meinen Eltern davon und bitte sie, mich zu begleiten.

5. ***Ich bin ein Fan von Videospielen, Filmen und Musik. Manchmal kaufe ich sie, aber oft lade ich sie aus dem Internet herunter. Ich gebe sie sogar meinen Freunden weiter. Darf ich das überhaupt?***

   Nein. Das ist verboten. Ich verletze damit die Autorenrechte.

6. ***Ein älterer Freund von mir will, dass ich ihn mit seinem Handy filme, während er einen anderen auf der Straße hänselt. Er sagt, er will es nur seinen Freunden zeigen. Ich denke:***

   Das ist gemein. Ich mache nicht mit und sage es den anderen. Gemeinsam gehen wir zu unserer Lehrerin und bitten sie, uns zu helfen.

Musterformular: Zustimmung zur Veröffentlichung von Fotos

Ich die/der Unterzeichnende,.....
(Name des Elternteils)

Mutter/Vater/erziehungsberechtigte Person

von.....(Name des Kindes)

gebe meine Zustimmung, dass von meinem Kind während der Veranstaltung

.....(Bezeichnung der Veranstaltung) am

.....(Datum)

ein Foto aufgenommen werden darf und dass dieses Foto in der Presse oder zu einem sonstigen nicht kommerziellen Zweck, der in direktem Zusammenhang mit dem entsprechenden Ereignis steht, aber nicht mit einem Entgelt verbunden ist, veröffentlicht wird.

Unterschrift:

Unterschrift des Kindes:

.....(Vorname, Name),

.....(Datum)

Unterschrift des Erziehungsberechtigten:

.....(Vorname, Name),

.....(Datum)

Links für den Unterricht

CASES-Themenblätter für Kinder zu den Themen „Internet", „E-Mail" „Viren", „Würmer", „Trojanische Pferde", „Passwort", „Patch", „Antivirusprogramm" und „Firewall" sowie ein sehr anschaulicher Zeichentrickfilm über Viren, Würmer und Trojanische Pferde finden sich auf **www.cases.lu**

Internetführerschein für Kinder auf **https://pwws.cases.lu**

Fragen- und Lernblöcke der CASES E-Learning-Plattform auf **https://elearning.cases.lu**

Inhalt der luxemburgischen Schulungen zur Informationssicherheit für Kinder, Jugendliche, Eltern und Lehrpersonal sowie Illustrationen zu den Gefahren des Internets auf **www.cases.lu** und **www.lusi.lu.**

Auf **www.saferinternet.org**, dem europäischen Sensibilisierungsnetzwerk InSafe, finden sich europäische Projekte und Inhalte rund um die Informationssicherheit. Diesem Netzwerk gehören 28 Mitglieder an, unter anderem LuSI.

Das europäische Unterrichtsportal **www.teachtoday.eu** zeigt Möglichkeiten zur Gestaltung einer Unterrichtsstunde für Kinder und Jugendliche mit Ideen zu Themen wie „Suche im Internet", „Gesundheit und Wohlbefinden", „Internet- und Mobiltelefonbullying", „Datenschutz und persönliche Sicherheit" auf. Das Unterrichtsportal ist eine Initiative der Internet-, Mobilfunk- und sozialen Netzwerkanbieter in Zusammenarbeit mit dem Europäischen Schoolnet.

Klicksafe-Lehrerhandbuch: **www.klicksafe.de**. Praxisnahe Einführung in das Internet mit vielen Tipps, Unterrichtsübungen und umfangreicher Beschreibung. Die einzelnen „Bausteine" können aus dem Internet heruntergeladen oder als Handbuch über Klicksafe.de bestellt werden.

Englischer Film für ältere Kinder über die Folgen der Veröffentlichung privater Daten im Internet **www.safesocialnetworking.com/**

Alle Domain-Namen der Welt auf **www.united-domains.de**

Kinderseiten : **www.blinde-kuh.de · www.fragfinn.de · www.kindernetz.de www.scoolz.de · www.die-maus.de · www.kidsville.de · www.oliswildewelt.de www.kinder-tierlexikon.de**
Weitere Klicktipps gibt es unter **www.cases.lu / www.lusi.lu**

Spiel des Europarates zur Verdeutlichung der Gefahren im Internet für Kinder von 6 bis 10 Jahren auf **www.webwoods.org**

Weiterführende Informationen

Luxemburgisches Informationssicherheitsportal CASES des Ministeriums für Wirtschaft und Außenhandel mit praktischen Tipps und Informationen: **www.cases.lu**

Von der Europäischen Komission unterstütztes luxemburgisches Portal zur Informationssicherheit speziell für die Zielgruppen Kinder, Eltern und Lehrpersonal: **www.lusi.lu**

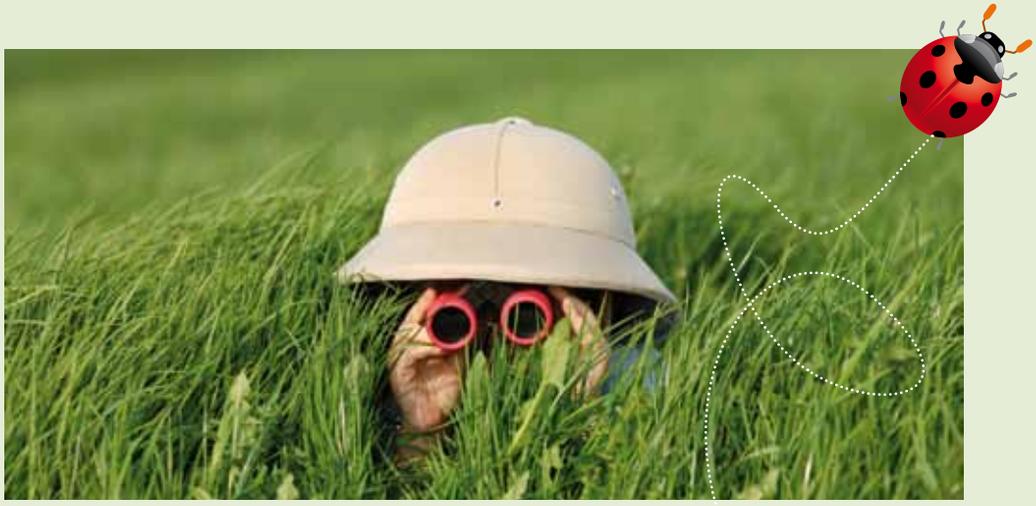
Luxemburgische Internetseite über die illegale Inhalte im Internet anonym gemeldet werden können: **www.lisa-stopline.lu**

Von der Europäischen Kommission unterstütztes europäisches Portal zur Informationssicherheit für Eltern und Lehrpersonal: **www.saferinternet.org**

Gesetz zur Regelung des Urheberrechts in Luxemburg: **http://www.eco.public.lu/documentation/legislation/lois/2004/04/Loi_modifiee_du_18_avril_2001_.pdf**

Internetseite der Direction de la Propriété Intellectuelle: **http://www.eco.public.lu/attributions/dg2/d_propriete_intellectuelle/index.html**

Internetseite der Sacem (Société des auteurs, compositeurs et éditeurs musicaux) für Autorenrechte von Musikstücken: **www.sacem.lu**



Zusätzliche Dokumente

ISBN : 978-2-87995-996-2

www.cases.lu
2009