

OCOM Ratgeber zum Tag der Kindersicherheit 5 Goldene Regeln für Kindersicherheit im Internet



Seit Jahren setzt sich in Deutschland der nationale Dachverband »Bundesarbeitsgemeinschaft (BAG) Mehr Sicherheit für Kinder e. V.« für die Sicherheit von Kindern ein. Seit dem Jahr 2000 veranstaltet die BAG. jedes Jahr am 10. Juni den Kindersicherheitstag mit dem Ziel, ein Bewusstsein für Gefahren jeglicher Art zu wecken. Dazu gehört auch die Medienerziehung und der Umgang mit mögliche Gefahren im Internet.

Anlässlich dieses Tages, zeigen wir Ihnen wie Sie Ihre Kinder beim Umgang mit dem Computer unterstützen können, wo Gefahren lauern und wie Sie Ihre Kinder davor schützen.

1. Interesse zeigen und aktiv begleiten

Teilen Sie mit Ihrem Kind seine Erfahrungen im Internet. Surfen Sie selbst mit Ihren Kindern, um dem Alter und den Interessen des Kindes entsprechend interessante, sichere und möglichst werbefreie Seiten zeigen zu können.

2. Sprechen Sie über Gefahren

Kinder wachsen heute mit einem nahezu unüberschaubaren Angebot des Internets heran.

Sie können ganz leicht und jederzeit auf Informationen, Bilder und Videos zugreifen, Leute kennenlernen, kommunizieren, Daten austauschen, Online-Games spielen usw. Das ist nicht nur am Computer der Fall, sondern natürlich auch auf Mobilgeräten. All diesen schönen und tollen Möglichkeiten bergen aber auch Gefahren: Pornografie, Gewalt, Cybermobbing sowie Kostenfallen sind nur einige davon.

Potentielle Gefahren und Vorgehen:

Ungeeignete Inhalte (Gewalt, Pornografie, Essstörungen, Suizide...)

Bedenken Sie, dass sich die Begegnung mit ungeeigneten Inhalten im Internet nicht völlig verhindern lässt. Technische Massnahmen wie Filter- und Spezielle Programm zum Schutz von Kindern, können nur ein Bruchteil eines gesunden Umgangs mit dem Internet darstellen. Sie ersetzen nicht das direkte Gespräch mit dem Kind.

Vorgehen:

Vor allem bei jüngeren Kindern empfiehlt es sich anfangs, für Fragen zur Verfügung zu stehen. Aktives Nachfragen durch die Eltern kann immer sinnvoll sein, wenn das Kind unbegleitet das Internet nutzt.

Preisgabe persönlicher Daten

Persönliche Daten sind ein wichtiger Bestandteil von Firmen und deren Angebote im Internet. Entsprechend interessant sind Namen, E-Mail-Adressen und die Kenntnis über persönliche Vorlieben. Kinder geben auf Social-Media- Plattformen oder bei Gewinnspielen häufig leichtfertig persönliche Daten an. Das führt meist zu einer Fülle von unerwünschten E-Mails (Spam). Solche sozialen Plattformen leben davon, dass die Nutzer möglichst viel aus ihrem privaten Leben preisgeben: Denn echten Namen, Fotos, Schule, Erlebnisse, Bewertungen o.ä. sind die Währung des Internets.

Vorgehen:

Erklären Sie Ihrem Kind, dass es sich stets unter einem Spitz- oder Fantasienamen im Internet bewegen soll. Sorgen Sie auch dafür, dass Ihr Kind eine alternative E-Mail-Adresse beim Surfen verwendet die keine Hinweise auf die tatsächliche Identität Ihres Kindes liefert; Die reguläre Adresse bleibt für den normalen E-Mail-Verkehr reserviert. Stellen Sie ausserdem sicher, dass Ihr Kind sich auch in den Sozialen-Netzwerken möglichst anonym bewegt. Oberstes Gebot: Sowenig wie möglich über die eigene Identität Preis geben.



Geldmacherei

Kinder surfen gerne auf Seiten, die im Bezug zu ihrer Lieblingssendung, ihrer Lieblingsfilme, Musikgruppen usw. steht. Manche dieser Seiten bieten Kindern auch einen echten Mehrwert. Weit häufiger jedoch geht es darum, aus Kindern längerfristig Käufer zu machen. Aggressives Merchandising, Werbung, Gewinnspiele oder Verlosungen usw. können sich als versteckte Kostenfallen herausstellen. Auch kostenlose Apps, die sich über Werbung finanzieren, können teuer werden. Wird die Werbung versehentlich angetippt, kann ein kostenpflichtiger Vertrag zustande kommen.



Vorgehen:

Erklären Sie Ihrem Kind diese Zusammenhänge von Werbungen und Gewinnspielen im Internet und vereinbaren Sie, dass es sich stets mit Ihnen berät, bevor es irgendetwas abonniert, Name und Adresse eingibt oder etwas bestellt. Achten Sie auch bei Apps von Mobiltelefonen darauf was diese genau machen, ob diese Werbung enthalten und auf persönliche Daten zugreifen. Darüber hinaus sollten Sie Ihrem Kind keine Kreditkarten-nummern zugänglich machen. Dies ist der schnellste Weg zum Bezahlen im Internet oder zum Kaufen von Apps. Achten Sie auch darauf, falls Ihr Kind Ihr Handy oder Tablet verwendet, dass keine Kreditkarte z.B. bei der Apple-ID hinterlegt ist.

Verletzung von Urheberrechten

Häufig nutzen Kinder und Jugendliche das Internet, um Filme, Spiele und Musik herunterzuladen. Dies kann ungeahnte Konsequenzen haben: Zum einen besteht die Gefahr, sich Viren oder Trojaner einzufangen, zum anderen kann es auch rechtliche Probleme geben. Denn das Urheberrecht schützt diese Werke und verbietet eine unkontrollierte Verbreitung. Vorsicht geboten ist auf jeden Fall mit Internetseiten die die die neuesten Musikhits und Videos kostenlos anbieten. Gefährlich sind auch Tauschbörsen und BitTorrents (schnelle Verteilung grosser Datenmengen). Diese Angebote sind meist illegal. Bei letzterem kommt noch verschärfend hinzu, dass man Dateien nicht nur herunterlädt, sondern gleichzeitig auch anderen Internetbenutzer anbietet.

Vorgehen:

Erklären Sie Ihrem Kind, dass es in dem Moment, in dem es z.B. ein Musikalbum über eine Tauschbörse herunterlädt, es gleichzeitig selbst allen Mitgliedern der Tauschbörse weltweit anbietet. So wird das Kind selbst zum Anbieter einer urheberrechtlich geschützten Datei. Da dies ohne Einwilligung des Urhebers geschieht, stellt das Anbieten einer solchen Datei eine Urheberrechtsverletzung dar.

Cybermobbing

Scheinbare Anonymität verleitet manch einen dazu, scheinbar lustige oder peinliche Inhalte sofort zu teilen und lassen somit jeden in Gefahr geraten, Opfer von Cybermobbing zu werden. Peinliche Fotos, beleidigende Botschaften, üble Nachrede in Foren oder sozialen Netzwerken sind die klassischen Formen von Cybermobbing. In der überwiegenden Zahl der Fälle kommen die Täter aus dem Umfeld der Kinder.

Vorgehen:

Vermitteln Sie Ihrem Kind, dass das Teilen solcher Bilder, Texte oder Kommentare kein Spass ist und anderen schadet und unglücklich machen kann. Wenn Ihr Kind selbst Opfer von Cybermobbing wird, wenden Sie sich z.B. an die Schule, falls das Mobbing von anderen Schülern ausgehen sollte. In schweren Fällen kann auch bei der Polizei Anzeige erstattet werden. Möglicher Tatbestand wäre z.B. Beschimpfung, üble Nachrede und Drohung.



Das Internet vergisst nicht

Wer etwas postet, sollte vorher nachdenken, was er veröffentlicht. Das gilt für Kinder wie auch für Erwachsene! Denn einmal veröffentlichte Inhalte verschwinden nicht. Was einmal online war, ist auch später oft noch zu finden. Zudem ist nie klar, wer einen Text oder ein Foto ohne Wissen des Urhebers bereits weiterverbreitet hat.

Vorgehen:

Strandfotos, Partybilder und peinliche Fotos haben im Internet nichts verloren. Erklären Sie Ihrem Kind, dass solche Fotos auch Jahre später noch Schaden anrichten können. Z.B. hat schon manch ein potentieller Arbeitgeber auf das Facebook-Profil eines Bewerbers

geschaut. Bedenken Sie ausserdem, dass Social-Media-Plattformen ein Tummelplatz für Perverse und Pädophile sind. Fotos von Kindern sind absolut tabu.



3. Kinderschutzkonto

Auch bestimmte Software kann Ihr Kind im Internet und mit dem Umgang mit dem Computer schützen. Dabei muss nicht eine spezielle Software angeschafft werden, ein guter Schutz ist schon in Ihrem Betriebssystem integriert. Gerne Installieren wir für Sie die entsprechende Software auf Ihrem Computer.

Windows 10:

In Windows 10 bietet Family Safety verschiedene Funktionen, um Kinder effizient zu schützen und deren PC-Verwendung zu steuern. Grundlage dafür ist, dass die Kinder sich mit einem eigenen speziellen Kinderkonto am Computer anmelden. Die Eltern können dann über die Family Safety Internetseite die verschiedenen Funktionen steuern.

Die Funktionen:

- Zeitlimits festlegen
- Internetnutzung kontrollieren und Seiten sperren oder erlauben
- Spiele und Programme kontrollieren

MacOS:

Auch auf dem Mac lassen sich einzelne Benutzerkonten so absichern, dass man sie bedenkenlos Kindern anvertrauen kann. Die Kindersicherung unter MacOS wird ähnlich wie in Windows 10 in Form eines neuen Accounts erstellt, in dem gezielt bestimmten Zugriffsrechte erteilt beziehungsweise entzogen werden können. So wird verhindert, dass Kinder oder Jugendliche auf ungeeignete Inhalte im Internet stossen oder Käufe in den verschiedenen Apple Stores tätigen. Weiterhin ist es mit der MacOS-Kindersicherung möglich, eine präzise Zeitsteuerung einzurichten. Dabei könnt ihr nicht nur die möglichen Tageszeiten, sondern auch die Dauer der Mac-Nutzung definieren.

OCOM Dienstleistung: Einrichtung Kindersicherung MacOS oder Family Safety für Windows 10 CHF 70.-

- Benutzerkonto für Kinder erstellen
- Kindersicherung aktivieren
- Einschränkungen festlegen
- Einstellungen vornehmen und dokumentieren

Verlassen Sie sich jedoch nicht allein auf solche technischen Hilfsmittel. Eine Jugendschutz-software ist nur in Kombination mit aktiver Medienerziehung sinnvoll und kann nie einen vollständigen Schutz aller bedenklichen Inhalten bieten.



4. Kindergerechte Homepages

Es gibt auch Webseiten und Suchmaschinen die speziell für Kinder geeignet sind. Richten Sie gemeinsam mit Ihren Kindern eine eigene Startseite ein. Dann hat es gleich beim Öffnen des Browsers seine Lieblingsseite und wichtige Informationen im Blick und kann das Internet sicher erkunden.

Webseiten

Webseiten für Kinder bieten nicht nur viel Spass und Unterhaltung, sondern auch wertvolle Tipps und Informationen für kleine Internet-Anfänger. Einige Beispiele für kindgerechte Seiten für Kleinkinder bis 6 Jahre:

www.internet-abc.de

Das Internet-ABC bietet Kindern und Erwachsenen Infos, Tipps und Tricks rund um das Internet – ob für Anfänger oder Fortgeschrittene. Die werbefreien Seiten sind für Kinder von fünf bis zwölf Jahren und deren Eltern gemacht.

www.kidsville.de

Die Kinderstadt fördert gemeinsames Spielen und Lernen. Gestaltung und Navigation sind sehr simpel und einfach. Einige Beispiele für kindgerechte Seiten für Schulkinder bis 12 Jahre:

www.clixmix.de

Bereitet Themen kindgerecht mit animierten Grafiken und Videos.

www.geo.de/GEOlino

Verbindet Wissen aus vielen Themenbereichen mit Abenteuern und Rätseln.

Suchmaschinen

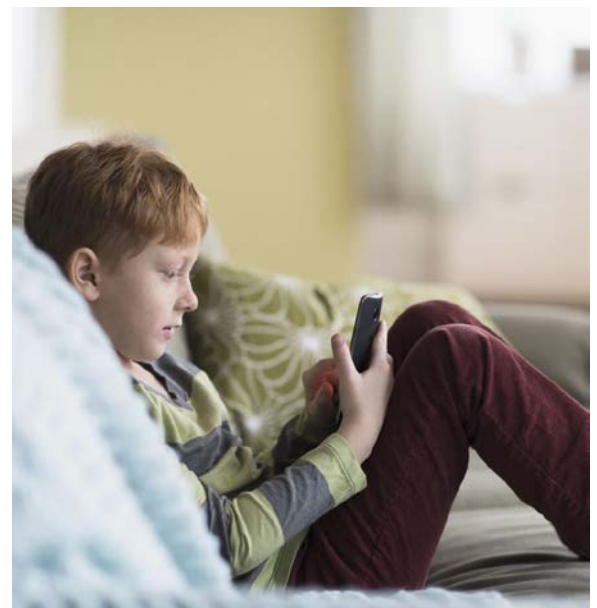
Anbieter wie „Blinde Kuh“ oder „Frag Finn“ zeigen nach der Eingabe eines Suchworts nur altersgerechte Seiten an. So können Sie sicher sein, dass keine jugendgefährdenden Seiten in der Trefferliste auftauchen.

www.blinde-kuh.de

Seit 30 Jahren sammelt die „Blinde Kuh“ schon Internetseiten für Kinder und bietet eine Stichwortsuche an. Die Verantwortlichen prüfen vorab, ob die Seiten auch wirklich für Kinder geeignet sind.

www.fragfinn.de

Diese Suchmaschine wurde im Rahmen der Initiative „Ein Netz für Kinder“ geschaffen. Das Konzept: Hier werden nur Internetseiten aufgeführt, die Medienpädagogen als sicher erachten.



5. Nützliche Tipps

Sichere Passwörter

Ein Passwort sollte nicht zu erraten sein. Auf ocom.ch/dienstleistungen/ratgeber zeigen wir Ihnen, wie Sie ganz einfach schwer zu erratende Passwörter kreieren, die Sie sich auch gut merken können.

Nutzungsdauer

Je nach Alter des Kindes oder Heranwachsenden sollten feste PC- und Internetzeiten vereinbart werden. Es geht darum, die Zeit im Internet vor allem intelligent zu nutzen. Familie, Freunde und Hobbys dürfen nicht darunter leiden. Man sollte stets für einen Ausgleich sorgen. Ausflüge in die Natur, Sport und Bewegung und Zeit mit Menschen in der wirklichen Umgebung sollten nicht zu kurz kommen.

Adressenverzeichnis anlegen

Erstellen Sie Ihrem Kind ein eigenes Verzeichnis mit Lesezeichen bzw. Favoriten im Internetbrowser, das gemeinsam gepflegt und erweitert werden kann. So sind die Lieblingsseiten immer sofort aufrufbar.

In-App-Käufe und Kreditkarte

Speichern Sie auf keinen Ihrer Geräte die in Kinderhände kommen könnten Ihre Kreditkarteninformationen. Eine grosse Gefahr geht hier vor allem von sogenannten In-App-Käufen aus. Viele Spiele lassen sich kostenlos in einem App-Store herunterladen, bieten aber neben einer Basisvariante kostenpflichtige Bonuslevel oder Gegenstände, um den Spielspass zu steigern oder schneller im Spiel vorwärts zu kommen. Diese "Freemium-Games", also kostenlose Spiele mit kostenpflichtigen Extras, sind auch bei den Browserspielen im Internet sehr verbreitet.



Handy und Tablet sicher machen

Auch ein Handy oder Tablet kann man Kindersicher machen. Denn sowohl Apple wie auch Android Geräte haben in Ihrem Betriebssystem bereits diverse Sperren und Einschränkungen integriert. Wenn Sie wissen möchten wie Sie Ihr Smartphone oder Tablet am besten für Kinder vorbereiten, helfen wir Ihnen im OCOM Store gerne weiter.



Zusätzliche Informationen zum Thema «Gefahren im Internet»

Als zusätzliche Informationsquelle hat das Bundesamt für Kommunikation BAKOM zusammen mit weiteren Partnern von Bund und Kantonen sowie Pro Juventute Schweiz die Publikation "Geschichten aus dem Internet" veröffentlicht. Die Comics zeigen gefährliche Situationen im Internet - und wie sie vermieden werden können. Die interessante Homepage finden Sie unter <http://www.thewebsters.ch/de/>

Fazit

Medienkompetenz, also das eigene Verhalten im Umgang mit dem Internet und das Festlegen von klaren Regeln verringern das Risiko, unbewusst Opfer oder Täter zu werden. Einen hundertprozentigen Schutz wird es sicherlich nie geben aber spezielle Kinderfreundliche Homepages gepaart mit technische Massnahmen wie Kinderschutzsoftware und Kinderkonten am jeweiligen Gerät, können den Umgang der Kinder mit dem Computer und dem Internet viel sicherer machen. Verbote bringen meistens nichts, zusammen das Internet erleben und besprechen, ist der beste Schutz, den Sie Ihrem Kind geben können.