



schutzraum

MEDIENKOMPETENZ INTERNET

Begleitheft zur
Informationsveranstaltung

»Unsere Kinder sicher im Internet«



Sehr geehrte Damen und Herren,

in den folgenden Abschnitten finden Sie ergänzende Informationen zum Thema „Unsere Kinder sicher im Internet“, die Sie für sich nutzen können.

Freundliche Grüße

Ihr Hanno Lenz

Internet: www.schutzraum-medienkompetenz.de
Mail: info@schutzraum-medienkompetenz.de

Hinweis: Diese Broschüre enthält Links zu Webseiten Dritter, auf deren Inhalte ich keinen Einfluss habe. Deshalb kann ich für diese fremden Inhalte auch keine Gewähr übernehmen. Für die Inhalte der angegebenen Internetseiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich.

Icons für Hinweise und Beiträge : CCO 1.0 Universal Public Domain Dedication by IconsDB.com



Informationsseiten für Eltern und Lehrer

www.schau-hin.info	Interessante und umfassende Informationen zur Medienerziehung. Es sind auch Hilfen zu Spielsucht zu finden. Hier können Sie auch Ihr Medienwissen unter Beweis stellen
www.klicksafe.de	Informationen für Kinder, Jugendliche, und Eltern über Sicherheit und Entwicklung
www.internet-abc.de	Spielerischer, werbefreier Ratgeber rund um das Internet mit einem Bereich für Eltern und für Kinder
www.seitenstark.de	Informationen für Eltern und Kinder rund um das Internet. Bewertungen von kindgerechten Internetangeboten Extraseite zu Cybermobbing: http://mobbing-schluss-damit.de .
www.sicherheit-macht-schule.de	Eine Initiative von Microsoft für Eltern und Lehrer zum Thema Medienkompetenz, auch für höhere Jahrgangsstufen
www.surfen-ohne-risiko.net	Unterstützung der Eltern bei der Medienerziehung ihrer Kinder (surfen, chatten, spielen)
www.chatten-ohne-risiko.net	Tipps für Eltern und Lehrkräfte rund um das Thema chatten
www.bsi-fuer-buerger.de	Das Bundesamt für Sicherheit bietet umfassende Informationen rund um die Sicherheit im Netz, am PC etc.
www.usk.de	Internetseite mit Beschreibungen und Bewertungen aktueller Spiele
www.kinderserver-info.de	Der KinderServer bietet Sicherheit für Kinder im Netz. Das Besondere: Mit einem Klick werden Computer und mobile internetfähige Geräte schnell und leicht in einen kindgerechten, sicheren Surfmodus geschaltet
www.handysektor.de	Ein Ratgeber über Sicherheit in mobilen Netzen
www.klicksafe.de/facebook/	Soziale Netzwerke: hier Facebook Hier werden alle wesentlichen Informationen für Eltern und Jugendliche gebündelt auf mehreren Seiten und in Broschüren zum Download zur Verfügung gestellt



www.jugendschutz.net

jugendschutz.net recherchiert seit Jahren nach Risiken und Schutzmöglichkeiten im Internet. Um Eltern bei der Medienerziehung zu unterstützen, gibt jugendschutz.net diese Erfahrungen in praxisnahen Hilfestellungen weiter.

An jugendschutz.net können Sie sich auch wenden, wenn Sie den Eindruck haben, dass bestimmte Internetangebote illegal, jugendgefährdend oder entwicklungs-beeinträchtigend sind. Auch bei Mobbing über das Internet (Cybermobbing) können Sie sich an die Hotline wenden.

Quellen (Seite 4 und 5):

- Broschüre „Ein Netz für Kinder“, Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ)
- Internet www.bsi.de, Bundesamt für Sicherheit in der Informationstechnologie
- Internet www.schau-hin.info
- Internet www.klicksafe.de
- Internet www.handysektor.de



Internetseiten für Kinder

Geeignete Startseiten	www.meine-startseite.de www.internet-abc.de www.helles-koepfchen.de www.blinde-kuh.de www.internauten.de
Geeignete Suchmaschinen	www.blinde-kuh.de www.fragfinn.de www.helles-koepfchen.de www.klick-tipps.net
Was ist das Internet? Hier wird es erklärt...	www.internauten.de www.internet-abc.de/kinder/computer-internet.php www.kidsville.de/internautenstation www.toggo.de www.wildwebwoods.org
Kindgerechte Chaträume	www.seitenstark.de/chat www.tivi.de www.kindersache.de
Geeignete E-Mail-Adressen / Postfächer	www.mail4kidz.de www.grundschulpost.de
Kindernachrichten und Politik	www.baerenblatt.de www.tivi.de www.sowieso.de www.hanisauland.de www.kindersache.de www.boeser-wolf.schule.de www.politikzumanfassen.de
Internetführerschein für Kinder	www.internet-abc.de

Quellen:

- Broschüre „Ein Netz für Kinder“, Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ)
- Internet www.bsi.de, Bundesamt für Sicherheit in der Informationstechnologie
- Internet, Jugendschutz.net, www.chatten-ohne-risiko.net



Vereinbarungen treffen — Eltern

Ich achte darauf, mit wem und wo mein Kind online ist!	Problematische Seiten melde ich an jugendschutz.net!
Ich richte eine kindgerechte Startseite ein!	Ich installiere Schutzsoftware!
Ich richte eine kindgerechte Suchmaschine ein!	Ich unterstütze das Kind in der Nutzung des Internets!
Ich vereinbare Surfzeiten!	Ich lege einen Benutzeraccount für jedes Kind an!

Vereinbarungen treffen — Kinder

Ich gebe nie persönliche Informationen weiter!	Ich bin freundlich und fair zu anderen Menschen im Netz!
Bevor ich etwas runter-lade od. einkaufe spreche ich mit den Eltern!	Mein Passwort ist geheim, für jeden!
Ich erzähle meinen Eltern ab und zu, was ich im Internet mache!	Ich gebe vor Freunden nicht mit Sex- oder Gewaltseiten an!
Was mir unbehaglich erscheint, zeige ich meinen Eltern!	Mit Cyber-Freunden treffe ich mich nicht!

Quellen:

- Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ), www.surfen-ohne-risiko.de



Soziale Medien und Tipps zum Umgang

Die digitale Vernetzung der Kinder, Jugendlichen und Erwachsenen nimmt stetig zu. Diese findet vor allem über Apps (App = Application = Anwendung, Programm) auf dem Smartphone statt. Soziale Netzwerke bestimmen einen sehr großen Teil unseres Lebens im und mit dem Internet. Hier ein paar Beispiele, die weiter unten noch näher erklärt werden.



Es gibt eine Vielzahl sozialer Medien, die den Prinzipien der oben dargestellten Plattformen und Diensten folgen.

Folgende Hinweise sollen Ihnen und Ihren Kindern den Umgang mit den sozialen Medien erleichtern:

1. Bitte gehen Sie mit den Informationen, die Sie oder Ihre Kinder in sozialen Netzwerken darstellen, sorgsam um, denn viele Plattformen, wie Facebook, Instagram oder Snapchat, haben nach den eigenen allgemeinen Geschäftsbedingungen (AGB) das Nutzungsrecht aller Informationen, Fotos etc., die dort dargestellt werden. Eine wesentliche Frage ist, ob man wirklich alle Informationen einem möglicherweise breitem Publikum zur Verfügung stellen will?
2. Durch das Darstellen von Informationen, wie zum Beispiel Bilder aus dem Urlaub oder von dem neuen Smartphone, entsteht oft – gerade bei Kindern und Jugendlichen – Neid und Missgunst. Dies bildet dann sehr häufig die Grundlage für Mobbing über das Internet. Hier sollte sehr darauf geachtet werden, was man unbedingt im Internet publizieren sollte.
3. Achten Sie auf die Altersbeschränkungen für das Einrichten eines eigenen Accounts (z. B. Facebook: 13 Jahre, WhatsApp: 16 Jahre). Falls Ihr Kind sich einen Account anlegen darf, begleiten Sie es bei der Einrichtung oder besser noch, richten Sie sich auch einen Account ein, und achten Sie sehr auf Ihre Privatsphäre-Einstellungen und die Ihres Kindes. Dort regeln Sie, wer welche geposteten Inhalte sehen darf. Begleiten Sie Ihr Kind anfangs bei der ersten Nutzung.
4. Besprechen Sie mit Ihrem Kind, dass die eigenen Daten Privateigentum sind und eher nicht preisgegeben werden sollten. Ins Internet sollte nur das gepostet werden, was ein Schüler auch freiwillig über sich an das schwarze Brett der Schule hängen würden.
5. Achten Sie auf die Zeiten, die Ihr Kind in sozialen Netzen verbringt. Schnell kann eine Art Sucht entstehen, dass die Kinder immer und überall über alles aus dem Freundeskreis informiert sein wollen.

Weiterhin bilden soziale Netzwerke auch Nährboden für Cybermobbing!



Facebook

ist ein Dauerbrenner eines sozialen Netzwerks. Mit Facebook kann man sich auf der ganzen Welt mit anderen Menschen vernetzen. Nach der Registrierung bei Facebook können Freunde gefunden werden oder man kann selbst entdeckt werden. So wächst langsam ein privates Netzwerk zusammen mit den Menschen, mit denen man auch virtuell befreundet sein will. Facebook ist eine Plattform im Internet, also ein moderner Treffpunkt, wo viele Informationen ausgetauscht werden können, wenn man will. Hier besteht die Möglichkeit, seinen eigenen Status anzugeben oder zu beschreiben, was man gerade so macht oder wo man sich gerade aufhält. Diese Informationen können als Text, Bild oder Video dargestellt und kommentiert werden.

Die virtuellen Freunde können dann diesen Status beim nächsten Aufruf von Facebook sehen und darauf reagieren. Hier können „likes“ oder andere Reaktionen angeklickt werden. Zusätzlich besteht die Möglichkeit, dass Freunde den eigenen Status kommentieren.

Es entsteht eine interaktive Plattform, auf der man sehen kann, was Freunde oder Bekannte so machen. Zusätzlich können beispielsweise auch die eigenen Pop-Idole, Fußballstars oder Institutionen „geliked“ werden. Dann bekommt man auch über diese Plattform weitere Informationen.

Facebook kann man sowohl über den Internetbrowser oder eine Smartphone-App aufrufen.



Youtube

ist ein Online-Videoportal und gehört zu Google. Youtube kann über einen Internetbrowser oder über die Youtube-App beispielsweise auf Smartphones aufgerufen werden. Nutzer von YouTube können Videos anschauen oder selbst hochladen. Das Videoportal ist kostenfrei und innerhalb des Portals können die Nutzer unterschiedliche Kanäle (Channel) abonnieren, die sie interessieren (z. B. Sport, Spiele etc.).

Das Angebot von Filmen und Videos scheinen unbegrenzt zu sein. Die Nutzer können auch interagieren, in dem sie die geschauten Videos bewerten. Diese Bewertungen haben in bestimmten Kanälen Auswirkung auf die Medienwirksamkeit und das Sponsoring einzelner Darsteller. Die Helden der heutigen Zeit für die Jugendlichen sind sogenannte YouTuber, die sich in unterschiedlichen YouTube-Channeln befinden, wie zum Beispiel, Beauty, Let's play oder Comedy.

Einige der beliebtesten Youtuber sind (Quelle: www.klicksafe.de):



- **Gronkh** – ein „Let's Player“, der viele Spiele filmt und unterhaltsam kommentiert
- **Y-Titty** – Erfolg durch kreative Songparodien oder Eigenkompositionen
- **Kontor.TV** – Marketing-Kanal für elektronische Musik, die von Kontor produziert wird
- **LeFloid** – Bekannt wurde er durch seine Rubrik LeNews, in denen er alltägliche Geschehnisse und Nachrichten aufgreift
- **Bibi** – mit BibisBeautyPalace gibt sie Kosmetiktipp für jugendliche Mädchen, sie hat inzwischen ein eigenes Beauty-Label



Instagram

ist ein Onlinedienst, der es den Nutzern ermöglicht, Bilder und Videonachrichten zu erstellen und zu verbreiten. Instagram ist eine kostenlose App, die auf allen gängigen Smartphone-Betriebssystemen installiert werden kann. Instagram ist auch über einen Internetbrowser aufrufbar.

Instagram gehört, wie auch WhatsApp zu Facebook!

Ähnlich wie bei Twitter kann ich als Anwender anderen Personen folgen und deren Bild- und Videobotschaften empfangen. Andere Nutzer können einem selbst auch folgen (wenn Sie es zulassen!).

Instagram agiert plattformübergreifend, sodass alle Informationen auch direkt bei Facebook oder Tumblr (einem weiteren Bloggingdienst) dargestellt werden.



WhatsApp

ist ein sogenannter Instant Messenger und gehört zu Facebook. Mit WhatsApp kann man über die Internetverbindung des Smartphones mit anderen Nutzern chatten, also Nachrichten über das Internet austauschen, oder sogar telefonieren. Über den geschriebenen Text können auch Fotos, Videos oder Tonaufnahmen verschickt werden. Es ist möglich mit einer einzelnen Person oder in Gruppen, wie zum Beispiel in Klassenchats, zu kommunizieren.

Jeder Anwender von WhatsApp muss bei der Einrichtung die Rufnummer seines Handys eingeben. Parallel greift WhatsApp (wenn es vom Nutzer zugelassen wird) auf die Kontaktdaten im Adressbuch des Mobiltelefons zu, um in der App anzuzeigen, wer von den Kontakten schon WhatsApp nutzt.



Eine einfache WhatsApp-Nachricht ist mit einer SMS vergleichbar. Man kann jedoch nur WhatsApp-Nachrichten an Personen schicken, die ebenfalls das Programm auf ihrem Smartphone nutzen. Das Verschicken von Nachrichten mit WhatsApp ist kostenlos. Dabei werden die Nachrichten über die mobile Internetverbindung oder über WLAN genutzt. Das heißt, wer unterwegs WhatsApp-Nachrichten empfangen oder verschicken will, benötigt einen entsprechenden Datentarif für sein Smartphone.

WhatsApp-Nachrichten werden nun auch verschlüsselt übertragen, das heißt grundsätzlich, dass kein unbefugter Dritter die versandten Nachrichten lesen kann. Das Thema Datensicherheit und Datenschutz ist bei WhatsApp jedoch unklar. Auch wenn die Kommunikation zwischen zwei Nutzern verschlüsselt sein mag, heißt das nicht, dass ggf. alle Informationen aus dem persönlichen Adressbuch bei WhatsApp gespeichert werden.

Vergleichbare Instant Messenger sind Threema und Facebook Messenger (unverschlüsselt!)



Twitter

ist ein Onlinedienst, der es auf der einen Seite einem Nutzer ermöglicht, Meldungen mit maximal 140 Zeichen zu veröffentlichen. Die Meldungen erreichen die Personen, die dem Nutzer folgen. Auf der anderen Seite empfängt der Nutzer Meldungen von Personen, Institutionen, Pop- oder Fußballstars,

Nachrichtenanstalten o. ä. denen er selbst folgt. Anders als bei E-Mail werden die Meldungen an die Personen gesendet, die einem folgen. Die Personen, die jemandem folgen heißen Follower. Twitter heißt „Gezwitscher“ und der Onlinedienst dient dazu viele Kurznachrichten an eine breite Masse zu versenden.

Es gibt für viele Menschen viele Dinge, die sie gern mitteilen wollen, aber diese Meldungen nicht so wichtig sind, sie beispielsweise als E-Mail zu versenden. Die Meldungen, die bei Twitter gepostet werden, nennt man Tweets. Ein Retweet ist ein Antworttweet auf einen Tweet. Also dient Twitter auch einer einfachen Kommunikation über das Internet.

Häufig werden Tweets mit einem „#“, einem sogenannten Hashtag, gekennzeichnet. Dieser Hashtag verdeutlicht den Lesern, auf welches Thema sich der Tweet gerade bezieht, wie zum Beispiel #BVB09, #GNTM oder #9/11.

Mit einem „@“ können Tweets auch direkt adressiert werden. Dies findet häufig zur interaktiven Gestaltung von Fernsehsendungen statt, wie zum Beispiel @eurovisionsongcontest. Twitter kann man sowohl in einem Browser oder über eine Twitter-App aufrufen.

Hinweis: Um immer auf dem Laufenden zu sein, gibt es viele Kinder und vor allem aber Jugendliche, die einem Idol folgen, wie beispielsweise einem Popstar, Youtuber oder einem Sportler. Sie folgen oftmals nicht nur dem Idol auf Twitter, sondern auch noch vielen anderen Fans dieser Person. Wenn nun das Idol über sich selbst und jeder Fan auch noch etwas zu dieser Person twittert,



entsteht in einer Art Schneeballeffekt eine riesige Informationsflut im Internet. Man muss sich darüber bewusst sein, dass hier eine Abhängigkeit zu den sozialen Netzen entstehen kann, da immer wieder neue Nachrichten beispielsweise auf dem Bildschirm des Smartphones auftauchen und den Nutzer anregen, „mal eben“ das Smartphone in die Hand zu nehmen und „kurz“ nach den Nachrichten zu schauen.



SnapChat

ist ein Instant-Messenger, also ein Nachrichtendienst, der von Jugendlichen zurzeit sehr gern genutzt wird. Dieser Dienst läuft – ähnlich wie Instagram – als App auf Smartphones und Tablets. Auch hier folgt man einzelnen Personen bzw. kann eigene Follower, als Personen, die einem folgen, haben.

Bei Snapchat können Kinder und Jugendliche Fotos von sich posten, die nach ein paar Sekunden nach dem Anschauen auf den Smartphones der adressierten Nutzer „verschwinden“. Durch das scheinbar nur sehr kurze Darstellen von eigenen Bildern bei auf dem Smartphone/Tablet andere Menschen senkt sich die Hemmschwelle der Nutzer, freizügigere Bilder von sich zu posten. Viele Jugendliche nutzen diese App zum Sexting (gegenseitige sexuelle Erregung über das Internet).

Die Gefahren, die hierbei bestehen sind, dass es sehr einfach ist, von diesen Bildern Screenshots, also Bildschirmaufnahmen zu machen, die dann auf anderen Wegen öffentlich gemacht werden. Weiterhin denken viele Anwender, dass diese Bilder wirklich gelöscht werden. Das ist NICHT der Fall.



Was man noch wissen sollte...

„Cybergrooming“ – was ist das?

Immer mehr Kinder und Jugendliche werden über soziale Netze von fremden Personen sexuell belästigt. Cybergrooming heißt das und steht für „anbahnen“ oder „vorbereiten“. Hierbei suchen die Täter gezielt Kontakt zu den Kindern und Jugendlichen. Sie bauen Vertrauen auf und fordern dann die Zielpersonen auf, Nacktaufnahmen von sich zu machen oder sich sogar mit den Fremden zu treffen. Alle sozialen Netzwerke, die eine Chatmöglichkeit bieten, werden hier genutzt. Die Täter geben sich meist als eine andere Person aus, um einerseits nicht erkannt zu werden und auf der anderen Seite dem Opfer ein anderes Alter und Aussehen vorzugaukeln.

Sobald ein Kind oder eine jugendliche Person Kontakt zu dem Täter aufgenommen hat, werden sie sehr leicht erpresst und dann aufgefordert, weiteres erotisches Bildmaterial zur Verfügung zu stellen oder sich beispielsweise über eine Webcam zu präsentieren.

Die Bereitschaft der Kinder und Jugendlichen, sich mit Internet-Bekanntschaften zu treffen nimmt zu. Durch Dating- und Foto-Apps, sinkt die Hemmschwelle, sich im Internet zu präsentieren und sich dann mit fremden Personen zu treffen. Zusätzlich kommt es häufig vor, dass die Privatsphäre-Einstellungen in den Apps nicht ausreichend aktiviert sind, sodass es sehr leicht zur Kontaktaufnahme durch Unbekannte kommen kann.

Eltern können hier unterstützen, indem sie regelmäßig hinterfragen, was das Kind online macht und zugleich immer wieder auf die Gefahren aufmerksam machen. Zusätzlich sollten Eltern darauf achten, dass die Privatsphäre-Einstellungen in den einzelnen Apps auch ausreichenden Schutz bieten.

„Sexting“ hat viele Risiken

Unter Sexting („sex“ und „texting“) versteht man vor dem Hintergrund der aktuellen Medienlandschaft erotische Kommunikation mit Text und Bildern des eigenen Körpers als pornografische Selfies. Verbreitete Apps sind WhatsApp und Snapchat.

Gerade bei Snapchat ist die Versuchung groß, „mal eben“ ein erotisches Selfie zu verschicken, da viele Jugendliche denken, dass die Bilder, wenn sie nach ein paar Sekunden verschwinden, für immer gelöscht sind.

Viele Jugendliche suchen im Rahmen ihrer Persönlichkeitsentwicklung nach sexueller Orientierung. Das erleben sie auch bei vielen Idolen, die sich freizügig im Internet präsentieren. Manchmal wird das Verschicken von Nacktbildern auch als Mutprobe gesehen. Oft werden diese Bilder, zum Beispiel auch nach einem Beziehungsende, für Cybermobbing verwendet und entsprechend im Internet verbreitet.

Aus rechtlicher Sicht ist Sexting auch problematisch, da das Versenden und Speichern von pornografischen Bildern ab dem 14. Lebensjahr strafrechtlich verfolgt wird, gerade, wenn die Aufnahmen von Kindern oder Jugendlichen sind. Es gibt noch weitere rechtliche Aspekte, die hierbei betroffen sind.



Begleiten Sie Ihr Kind bei der ersten Nutzung von Messaging Apps und klären Sie die Kinder über die Risiken auf. Zeigen Sie Interessen an der Mediennutzung Ihres Kindes und stehen Sie für Fragen und zur Beratung stets zur Verfügung. Weiterhin hilft es, Regeln für den Gebrauch von Smartphones etc. zu vereinbaren. Hierbei ist nicht nur die zeitliche, sondern auch die inhaltliche Nutzung wichtig. Machen Sie sich mit den Funktionen der einzelnen Apps vertraut, um die Sicherheitseinstellungen kennen zu lernen und aktivieren zu können.

Phishing und Vishing

Jeden von uns erreichen immer wieder SPAM-Mails mit unerwünschten Inhalten. Oft werden diese Art von E-Mails auch dazu verwendet, um persönliche Informationen von dem Adressaten zu bekommen. Das nennt man Phishing (abgeleitet aus „Password Fishing“). Meist geht es um Informationen zu Anmeldedaten im Internet, Bank- oder Geburtsdaten.

Das Problem ist, dass die Qualität dieser E-Mails inzwischen schon so gut ist, dass sich das Design von diesen gefälschten E-Mails kaum noch von denen seriöser Anbieter unterscheiden. Wichtig ist hierbei, dass es kaum Unternehmen gibt, die per E-Mail zum Beispiel Passworte oder Banktransaktionsnummern erfragen. Hier ist also Vorsicht geboten und eine Weitergabe von persönlichen bzw. vertraulichen Informationen sollte vermieden werden. Am besten sollten solche E-Mails einfach ungelesen gelöscht werden.

Neben dem Phishing gibt es neuerdings auch Vishing. Vishing ist das Fishing von Informationen über „Voice“ – Voice Fishing. Hier wird über automatisierte Telefonanrufe versucht, die angerufene Person zu verwirren und an persönliche Informationen wie Passworte und Kreditkarteninformationen zu gelangen. Hier ist es am sichersten, gar nicht auf den Anruf zu reagieren.

Was ist FOMO? Hast Du FOMO?

FOMO steht für „fear of missing out“. Damit bezeichnet man einen Angstzustand etwas zu verpassen. Hier im Speziellen geht es um die Angst eine soziale Interaktion zu verpassen, die sich in verschiedenen Symptomen äußert. Diese Angst bezieht sich sehr stark auf die Nutzung digitaler Medien, wie Handys oder Computer in Verbindung mit sozialen Netzwerken.

FOMO bezeichnet das Verlangen eines Menschen, immer dabei sein zu wollen – in diesem Fall in den jeweiligen sozialen Netzen, wie Facebook, Twitter und Co – bzw. nicht abwarten zu können, was andere Personen stets aktuell in diesen Netzwerken posten. Dieses Phänomen ist noch nicht medizinisch anerkannt, spiegelt aber schon die Zustände viele Menschen wider.

Symptome können beispielsweise Traurigkeit sein, zu wissen, dass sich Freunde treffen können, ohne dass man selbst dabei ist. Angst kann auch hervorgerufen werden, zum Beispiel dann, wenn es anderen Menschen besser geht, als einem selbst. Dadurch wird auch Neid erzeugt. Zudem kann sich ein sehr starkes Mitteilungsbedürfnis entwickeln, dass alles aktuell Erlebte mit anderen virtuell geteilt werden muss. FOMO kann auch Konzentrationsschwächen durch permanentes abgelenkt sein erzeugen.

All' diese Dinge können die Abhängigkeit zu Mobiltelefonen und sozialen Plattformen verstärken. Dies ist eine erkannte Gefahr!



Kettenbriefe auf dem Handy, wie schütze ich mich?

Immer häufiger erreichen Kettenbriefe die Nutzer von Messagingdiensten, wie zum Beispiel WhatsApp. Was wir als Eltern als belanglosen Blödsinn löschen, beschäftigt jedoch häufig die Kinder. Manche Kettenbriefe gehen sogar so weit, dass mit dem Tod der Mutter oder des Vaters gedroht wird wie zum Beispiel:

„Schicke diese Nachricht an 10 Freunde weiter, sonst wird in der nächsten Woche Deine Mama sterben“

Oft wird in diesen Kettenbriefen auch auf Links verwiesen (z. B. notwendige Software-Updates), auf die man Klicken soll. Entweder wird damit eine Schadsoftware aktiviert oder gar ein Abo-Vertrag abgeschlossen. Dessen Kosten sind dann auf der nächsten Telefonrechnung zu sehen.

Unterschiedliche Dinge sollten unternommen werden:

1. Aufklärung

Reden Sie mit Ihrem Kind, dass es diese Art von Nachrichten geben kann. Klären Sie auf, dass das Nicht-Befolgen dieser Nachrichten keine negativen Folgen haben wird. Dadurch geben Sie Ihrem Kind Sicherheit.

2. Drittanbietersperre

Wir haben schon einmal über die Drittanbietersperre berichtet. Diese Sperre dient dazu, dass KEINE unerwünschten Werbe-Abos abgeschlossen werden. Hierzu reicht in der Regel ein einfacher Anruf bei dem Telefonanbieter aus. Der Verbraucherschutz bietet auch ein Formular an, das man dem Anbieter zusenden kann.

Wie schütze ich mein Kind und mich vor unerwünschten Werbe-Abos bei bestimmten Apps auf meinem Smartphone?

Viele Anbieter, vor allem von kostenlosen Apps auf Smartphones, finanzieren sich durch Werbung. Ab und zu tauchen dann Werbebanner meist am unteren Bildschirmrand des Handys auf. Bei vielen, meist unseriösen Anbietern, reicht ein ungewollter Fingertipp auf das Banner und schon hat man ein Abonnement oder Ähnliches abgeschlossen. Das ist nicht nur ärgerlich, sondern in vielen Fällen auch teuer.

WAS MUSS ICH TUN? Es ist eigentlich ganz einfach! Ich kann bei den meisten Mobilfunkanbietern anrufen und direkt am Telefon – ohne lästigen Schreibkram – eine Drittanbietersperre einrichten lassen. Dadurch wird eine bestimmte Bezahlungsfunktion (WAP-Billing) für den Mobilfunkvertrag deaktiviert. Laut Gesetz sind die Mobilfunkanbieter dazu verpflichtet bei Meldung des Verbrauchers diese Sperre einzurichten.

„CYBERMOBBING“! Wie gehe ich damit um?

Bei Cybermobbing werden Personen über das Internet, beispielsweise in sozialen Netzwerken, über SMS- oder Messenger-Dienste oder per Handy beleidigt. Man wird bloßgestellt oder sogar bedroht.



Durch die Nutzung des Internets sind die Möglichkeiten, Anderen zu schaden, vielfältiger und anonymer.

CYBERMOBBING IST ERNST ZU NEHMEN!!!

Eltern können helfen, indem sie eine gute und solide Vertrauensbasis zu ihrem Kind aufbauen. Dies sollten sie schon beim ersten Umgang des Kindes mit dem Internet angehen, in dem die Eltern mit dem Kind das Internet gemeinsam entdecken, für alle Fragen offen sind und auch Fehler des Kindes zulassen. Weiterhin ist wichtig, dass Cybermobbing als Thema in der Schule behandelt wird, damit diese Art von Konflikt und dessen Auswirkungen mit möglichen Opfern und Tätern besprochen werden kann. Falls ein Kind über das Internet gemobbt wird, können rechtliche Schritte gegen die Täter eingeleitet werden. Auch wenn sich der Täter in der Anonymität des Internets sicher zu fühlen scheint, kann in den meisten Fällen ein Täter ausfindig gemacht werden.

Es ist hilfreich, wenn das geschädigte Kind oder die Eltern so viele Beweise sammeln, wie es geht. Man kann sich jederzeit an die Polizei wenden oder weiteren Rat im Internet, beispielsweise unter www.jugenschutz.net, finden.

Was zockt mein Kind da eigentlich?

Immer wieder erlebt man in Diskussionen, dass Eltern dem Spielen der Kinder an Konsolen, auf dem Handy oder an dem Computer rat- und tatenlos gegenüberstehen.

Hier ein paar Tipps für einen kindgerechten Umgang mit Spielen:

1. Eltern sollten sich – gerade bei Spielanfängern – über das Spiel informieren und es auch mal selbst gespielt haben.
2. Auf den Internetseiten www.usk.de (Unterhaltungssoftware Selbstkontrolle) oder www.spielbar.de können Eltern sich über altersgerechte Spiele für ihre Kinder schlau machen.
3. Spiele mit gewaltverherrlichenden Spieleffekten sollten in den ersten Jahren vermieden werden.
4. Lassen Sie sich regelmäßig (am Anfang mehr, später weniger) von Ihrem Kind zeigen, was es da so spielt. Zeigen Sie Interesse an den Lieblingsspielen Ihrer Kinder und lassen Sie sie nicht allein.
5. Vereinbaren Sie Spielzeiten! Für Kinder, wie auch für Erwachsene ist das „Loslassen“ bei spannenden Sachen nicht einfach. Hier sollten Sie eine Regelung finden.
6. Achten Sie bei Spielen auf versteckte Gebühren oder Onlineauktionen, wie zum Beispiel In-App-Käufe bei Spielen auf dem Handy. Hier können sehr schnell hohe Beträge anfallen, die Sie erst bemerken, wenn es zu spät ist. Bei den meisten Smartphones können In-App-Käufe deaktiviert werden.



Sicherheitseinstellungen

Viele Kriminelle versuchen stets unbefugten Zugang zu unseren Computern, Smartphones oder Tablets zu bekommen.

Es gibt unterschiedliche Arten von Bedrohungen. Kriminelle nutzen ungeschützte oder zu schwach geschützte Computer um Schadsoftware zu installieren, um damit zum Beispiel

- Daten zu löschen,
- Daten zu verschlüsseln und anschließend dem Besitzer den Entschlüsselungsschlüssel zu verkaufen (Ransomware),
- Identitätsdiebstahl bzw. Abfischen von persönlichen oder vertraulichen Informationen durchzuführen,
- in Onlineshops Waren in Ihrem Namen zu kaufen oder
- Zugang zu Ihren Bankkonten zu bekommen.

An Computern, wie auch bei Smartphones und Tablets können Sicherheitseinstellungen vorgenommen werden. Auf der einen Seite können die Geräte vor Schadsoftware aus dem Internet geschützt werden. Auf der anderen Seite kann man sich selbst oder seine Kinder beispielsweise vor moralisch verwerflichen oder unsicheren Internetseiten oder Spielen schützen.

Um diesen Bedrohungen entgegen zu wirken sind folgende Schutzmaßnahmen bei Computern sinnvoll:

- Installation eines Virenschutzprogramms
- Anlegen von Benutzerkonten mit eingeschränkten Rechten für jeden Benutzer → die wenigsten Benutzer benötigen Administrationsrechte
- Regelmäßige Installation von Systemupdates
- Installation einer Firewall zum Schutz von Angriffen aus dem Internet
- Sicherheitseinstellungen in den Web-Browsern vornehmen
- Nutzung sicherer Passwörter
- Durchführen von regelmäßigen Datensicherungen, zum Beispiel auf separate Festplatten

Bei Smartphones oder Tablets sind die Bedrohungen sehr ähnlich, aber der Weg der Kriminellen, um an Daten zu gelangen, kann oft ein anderer als bei den Computern sein. Dies hängt schon damit zusammen, dass das Smartphone von Menschen fast jeden Alters zum ständigen Begleiter geworden ist und viele Aufgaben im täglichen Leben erfüllen soll.

Bei Smartphones und Tablets sind folgende Punkte zu beachten:

- Zugangsschutz durch Vergabe einer PIN oder ähnlichem Zugangsverfahren (Mustereingabe oder Fingerabdruck)
- gerätespezifische Sicherheitseinstellungen vornehmen
- Öffentliche Hotspots (öffentliches WLAN) nicht für kritische Funktionen wie Online.-Banking o. ä. nutzen
- Private WLAN-Verbindung nur mit Verschlüsselung (WPA/WPA2) nutzen
- Aktuelle Sicherheitsupdates zeitnah installieren
- Apps nur aus vertrauenswürdigen Quellen installieren
- Deaktivieren der Ortungsdienste
- Deaktivieren der InApp-Käufe und Einrichten einer Drittanbietersperre
- Regelmäßige Backups der Daten



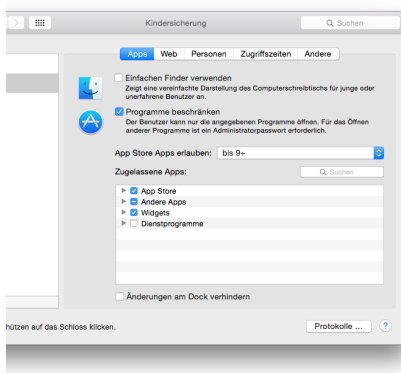
Einstellen einer Kindersicherung am Computer

In den einzelnen Betriebssystemen (z. B. MS Windows oder OSX von Apple) können Kindersicherungen eingestellt werden. Hierzu benötigt das Kind einen eigenen Account, der von dem Administrator (z. B. Elternteil) eingerichtet werden kann. Hier sind die wesentlichsten Schritte für die Einstellung der Kindersicherung auf einem Computer (in diesem Fall OSX von Apple) aufgeführt:

1. Systemeinstellung aufrufen
2. Benutzer & Gruppen aufrufen
3. Account des Kindes aufrufen

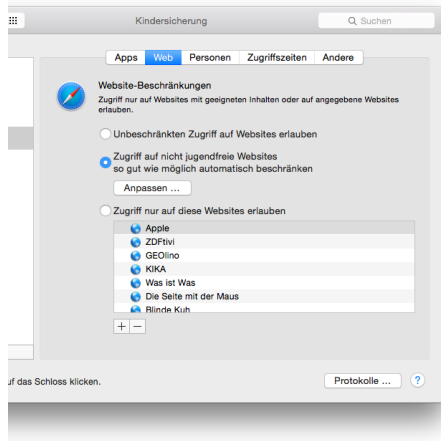


4. Button „Kindersicherung öffnen“ klicken

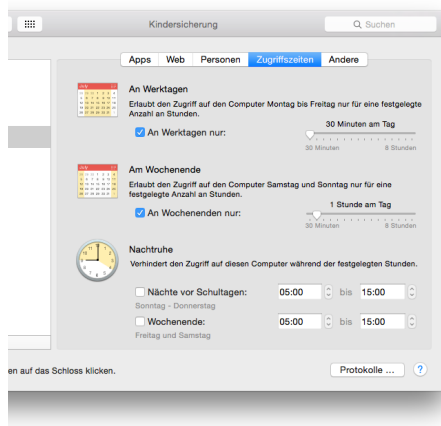




5. Hier können Einstellungen für die spezielle Nutzung für Anwendungen getroffen werden
6. Im Reiter „Web“ können die Zugriffe auf Internetseiten geregelt werden



7. Im Reiter „Zugriffszeiten“ können die Zeiten der Computernutzung geregelt werden



Weitere Hinweise zu Sicherheitseinstellungen bei den mobilen Betriebssystemen Android und iOS finden Sie auf der Schutzraum-Homepage: www.schutzraum-medienkompetenz.de



www.schutzraum-medienkompetenz.de / info@schutzraum-medienkompetenz.de

Abonnieren Sie doch den NEWSLETTER auf der Internetseite.