ELTERN, MACHT EUCH MEDIENFIT!

KFS
Katholischer
Familienverband
Südtirol

IMPRESSUM
2015 Bozen

Herausgeber:
Katholischer Familienverband Südtirol (KFS)
Wangergasse 29 · 39100 Bozen
Tel. 0471 974 778 · Fax 0471 973 823
info@familienverband.it · www.familienverband.it

Grafik: Effekt! GmbH
Druck: Ferrari Auer

Über diese Broschüre

Digitale Medien haben den Alltag erobert. Die Verwendung von Smartphone, Tablet, PC, Internet, sozialen Netzwerken und Co. gehört mittlerweile einfach dazu. Kinder und Jugendliche wachsen heute mit den neuen Medien auf (Digital Natives) und gehen ganz selbstverständlich damit um. Für Eltern ist es nicht immer leicht, Schritt zu halten und stellt sie vor eine große Herausforderung. Dennoch ist der verantwortungsvolle Umgang mit den neuen Medien eine wichtige Erziehungsaufgabe der heutigen Zeit. In der Informationsreihe „Digitale Medien" beschäftigte sich das Redaktionsteam der Verbandszeitung des Katholischen Familienverbandes Südtirol zwei Jahre lang mit der digitalen Welt. Die wichtigsten Inhalte, zusammen mit Tipps und interessanten Links, sind in dieser Broschüre zusammengefasst.

Die Beiträge wurden in Zusammenarbeit mit Fachleuten verfasst, denen wir auf diesem Wege für ihre wertvolle Unterstützung danken möchten: Dipl. Ing. Alexander Wallnöfer *(Vizedirektor Raiffeisen OnLine)*, Dipl. Ing. Robert Hartner *(Leiter IT Sicherheit Raiffeisenverband)*, Dr. Michael Reiner *(Psychologe, Leiter Young+Direct)*, Dr. Deborah Visintainer *(pädagogische Leiterin KFS, Mobbing- und Konfliktberaterin)*, Stefan Kontschieder *(Deutsche Berufsbildung)*, Manuela Kastl und Marion Thöni. Ein Dank geht an alle Beratungsstellen, insbesondere an die Südtiroler Verbraucherzentrale, das Europäische Verbraucherzentrum Bozen und die Postpolizei für ihre Mitarbeit, sowie in besonderer Form an die Südtiroler Raiffeisenkassen und Raiffeisen OnLine für die finanzielle Unterstützung.
Das Redaktionsteam der FiS wünscht eine interessante Lektüre.

Inhalt

Wie **schütze** ich PC, Smartphone und Tablet?

VIREN
Würmer und Trojaner sind Schadprogramme, mit denen sich Kriminelle Zugang zu ihrem Computer verschaffen. Vor diesen Schädlingen schützen Antivirus- und Firewallprogramme.

FIREWALL-PROGRAMME
Eine aktuelle Firewall-Software verhindert, dass jemand Zugriff auf den Rechner erhält, um Daten auszuspionieren (z. B. Passwörter), E-Mail-Adressen zu sammeln oder fremde Computer als ferngesteuerte Roboter zu verwenden (z. B. zum Versand von Spam-Mails).

Wer das Internet nutzt, ist mit Millionen Menschen in der Welt verbunden. Das bedeutet umgekehrt aber auch, dass Millionen von Rechnern theoretisch Zugriff auf Ihr Gerät erhalten. Um sich vor den Gefahren zu schützen, die dadurch entstehen, sollten Sie unbedingt folgende Tipps berücksichtigen.

Firewall und Antivirus

Jedes Computerprogramm enthält Fehler. Kriminelle nutzen sie als Hintertürchen, um in die Computer ihrer Opfer einzudringen. Halten Sie daher sowohl das Betriebssystem als auch alle anderen Programme (z.B. Adobe Reader) immer auf dem aktuellen Stand. Je neuer die Windows-Version desto sicherer!

Eine aktuelle Firewall-Software verhindert, dass jemand Zugriff auf den Rechner erhält. Die Installation eines Antivirusprogramms ist daher unter Windows ein Muss! Kostenlose Antivirusprogramme bieten einen guten Basisschutz, kommerzielle Varianten gehen darüber hinaus. Auch Besitzer von Smartphones und Tablets sollten ein Antivirusprogramm installieren (S. 11).

Die Gefahr lauert in E-Mails und auf Webseiten

Wenn Sie ohne eine Schutzsoftware ins Netz gehen, müssen Sie davon ausgehen, dass sich bereits nach kurzer Zeit ein Virus oder Wurm auf Ihrem Gerät breitmacht.
Aktivieren Sie den Webfilter Ihres Antivirusprogramms. Ein solcher Filter warnt vor gefährlichen Seiten. Meiden Sie diese Seiten, da hier ein erhöhtes Risiko besteht. Außerdem ist ein Webfilter hilfreich für den Kinder- und Jugendschutz.
Vergewissern Sie sich vor dem Download von Programmen, ob die Quelle vertrauenswürdig ist. Gehen Sie direkt auf die Webseite des Herstellers, dies gilt besonders für Sicherheitssoftware wie Antivirusprogramme. Lassen Sie besondere Vorsicht beim Öffnen von E-Mail-Anhängen

walten. Schadprogramme werden oft über Dateianhänge in E-Mails verbreitet. Im Zweifelsfall fragen Sie beim Absender nach, ob die E-Mail oder der Anhang tatsächlich von ihm stammt. Klicken Sie keine Links in Mails an, sondern nutzen Sie für wichtige Webadressen – wie die Ihrer Bank – die gespeicherten Lesezeichen.

Ein PC für mehrere Benutzer

Benutzen mehrere Familienmitglieder denselben Computer, dann sollten Sie **unterschiedliche Benutzerkonten** einrichten. So kann jeder seine E-Mails unabhängig abrufen, und die Privatsphäre bleibt gewahrt. Besonders wichtig ist es, dass Sie während der normalen Benutzung des Computers nicht mit einem Administratorenkonto arbeiten, sondern mit einem normalen Benutzerkonto. Das verhindert, dass Schadsoftware, automatisch den Zugriff auf den gesamten Computer erhält, und der Schaden kann in vielen Fällen begrenzt werden.

Daten sichern

Kommt es trotz aller Schutzmaßnahmen zu einer Infektion des PCs, können alle Daten verloren gehen. Erstellen Sie deshalb regelmäßig Sicherungskopien auf externen Festplatten oder einem anderen Computer.

Getrennte Geräte nutzen

Nutzen Sie getrennte Geräte für unterschiedliche Zwecke: einen „Unterhaltungs-PC“ für Spiele, Musik oder Softwaretests und ein streng geschütztes Gerät für ernsthafte Anwendungen wie Online Banking oder Verwaltungsaufgaben. Für alle Geräte gilt: Je sicherer ein System sein soll, desto weniger Programme oder Apps dürfen dort installiert sein. Jedes zusätzliche Programm birgt neue Risiken.

Drahtlose Netze verschlüsseln

Wenn Sie Funkverbindungen (Wireless LAN, WiFi) nutzen, achten Sie auf die Verschlüsselung Ihrer Kommunikation. Zu Hause sollte jeglicher Datenverkehr nach dem Standard WPA2 verschlüsselt sein. Bei Nutzung von öffentlichen Hotspots sollten Sie zum Abrufen Ihrer E-Mails und beim Anmelden auf einer Webseite nur verschlüsselte Protokolle wie IMAPS oder HTTPS einsetzen. Nur so können Sie verhindern, dass jemand Ihre Passwörter mitliest.

Robert Hartner
Alexander Wallnöfer

TIPP!

Benutzen Sie Windows 7 oder 8, aber nicht Windows XP oder ältere Versionen, denn hier werden keine Sicherheitslöcher mehr gestopft.

Sicher **Einkaufen**

PHISHING
Beim Phishing (engl. für Password angeln) werden über gefälschte Internet-Seiten, E-Mails oder Kurznachrichten die Daten eines Internet-Benutzers geklaut, mit dem Ziel ein Konto zu plündern, online bis ans Kartenlimit einzukaufen oder der Person zu schaden.

Online-Shopping wird immer beliebter. Wenn man einige Richtlinien beachtet, steht dem Einkaufsgenuss vom Sofa aus nichts mehr im Weg. Ein großer Unterschied besteht zwischen professionellem Verkäufer und Privatverkäufern. Bei Transaktionen mit Privatverkäufern ist der Konsument weniger geschützt.

Den Anbieter genau überprüfen

- Vollständiger Name und Adresse des Anbieters;
- Informationen zur schnellen Kontaktaufnahme (Telefon, Fax, E-Mail)
- In welchem Staat hat das Unternehmen seinen Sitz?
- Sind allgemeine Geschäftsbedingungen (AGB) verfügbar und transparent aufgelistet?
- Gibt es Angaben zu Rücktritt- und Gewährleistungsrecht und zur Kaufpreisrückerstattung?
- Übermäßig niedrige Preise im Vergleich zum Marktdurchschnitt könnten ein Hinweis auf Betrug sein.

Vorsicht mit der Kreditkarte

Die gängigste Form der Bezahlung ist die Kreditkarte. Der Käufer hat die Möglichkeit, bei nicht versendeter Ware eine Rückbuchung bei seiner Kreditkartengesellschaft (charge back) zu erwirken.

Zahlung über Bezahlsystem-Anbieter

Alternativ kann man ein Bezahlsystem (z.B. PayPal) nutzen – so muss man nicht bei jeder Transaktion die sensiblen Daten angeben. Konto eröffnen, Daten eingeben und Bankverbindung oder Kreditkartendaten hinterlegen. Unterstützt ein Online-Shop ein Bezahlsystem, wird man bei der Auswahl der Zahlungsart auf die Seite des Systems weitergeleitet.

Verschlüsselungstechniken

Alle Daten, die an einen Online-Shop übermittelt

werden, sollen verschlüsselt werden: Dies erkennt man an Meldungen wie „Sie sind im Begriff, sich Seiten über eine sichere Verbindung anzeigen zu lassen…“. Außerdem erscheint bei einer verschlüsselten Datenverbindung ein **„s“ hinter den Buchstaben „http“** in der Adresszeile. Bei vielen Browsern erscheint im unteren Bereich oder in der Adresszeile ein kleines, geschlossenes Vorhängeschloss.

Auch die Bestätigung gibt Aufschluss darüber, wieviel Wert auf Datenschutz und Datensicherheit gelegt wird: Einige Stellen der Bank- oder Kreditkartendaten sollten durch den Buchstaben „X“ ersetzt und nicht vollständig zu lesen sein.

Nicht ködern lassen!

Beim Datendiebstahl, dem sogenannten **„Phishing“**, werden User durch eine vertrauenswürdig erscheinende Mail zur Dateneingabe aufgefordert oder auf eine gefälschte Website gelockt. Meist werden Daten wie Kreditkartennummer, Kontodaten, Zugangsdaten zum Online-Banking, Kennwörter, E-Mail-Kontodaten oder andere persönliche Daten abgefragt.
Wenn Zweifel bestehen:

- **NIE** E-Mail-Formulare mit vertraulichen Daten ausfüllen.
- Nicht auf Links oder Verknüpfungen in E-Mails klicken.
- Nicht antworten und Mail löschen.
- Beim Absender nachfragen, ob er diese E-Mail senden wollte. Dazu die Telefonnummer benutzen, die man direkt vom Unternehmen erhält, nicht jene aus der E-Mail.

Kontrolle ist größte Sicherheit

Absolute Sicherheit gibt es nicht. Darum sollte man gut auf die Zugangsdaten zum Benutzerkonto achten und regelmäßig die Vorgänge auf dem Konto kontrollieren. Bei unbekannten Transaktionen sofort Kontakt mit dem Anbieter aufnehmen.

Bankkonto und Kreditkarte im Blick behalten! Viele Banken bieten den Service „Kontobenachrichtigung per SMS“.

Das Europäische Verbraucherzentrum (EVZ) hilft bei Verbraucherproblemen im EU-Ausland (S. 23).

TIPPS!

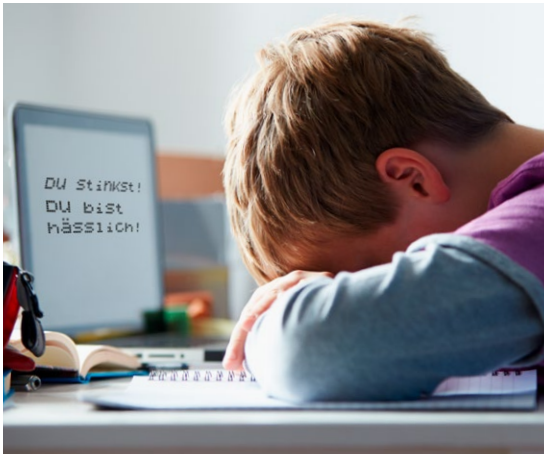
- **Kundenbeurteilungen** in Foren lesen. Namen des Shops und das Wort „Problem, Beschwerde, Betrug “ in Suchmaschine eingeben.
- Vom **Bestellvorgang** einen Screenshoot machen
- Bei der Zahlung per Kreditkarte darauf achten, dass die **Kreditkartendaten** nur **verschlüsselt** übermittelt werden und **Kreditkartenauszug kontrollieren**.

Mobbing
Die Schikane im Netz

Die mutwillige und systematische Demütigung eines Menschen ist kein Kavaliersdelikt. Cybermobbing ist das dauerhafte, gezielte Beleidigen, Bedrohen oder Bloßstellen mit Hilfe von Handy oder Internet.

Beim **Cybermobbing** (Cyberbullying) werden gefälschte Online-Profile erstellt, verletzende Nachrichten und Bilder versendet oder gemeine Kommentare veröffentlicht. Was ins Rollen gebracht wurde, kann nicht mehr kontrolliert werden. Die Hemmschwelle ist niedrig, der Täter nimmt die Betroffenheit des Opfers meist nicht wahr. Die Anonymität des Netzes kann jeden zum Mobber im Internet machen. Dem Opfer wird der Rückzugsraum genommen, da die virtuelle Attacke über PC oder Smartphone bis ins Zimmer kommt und das Opfer überall hin verfolgt.

Die Folgen sind schwerwiegend. Da der Bully (Täter) meist aus dem näheren Umfeld stammt, setzen sich die Attacken im Alltag fort. Das Opfer wird aggressiv und ist verzweifelt, hilflos, isoliert sich. Die schulischen Leistungen verschlechtern sich. Auch Schlaflosigkeit, Kopf- oder Bauchschmerzen können eintreten. Hinzu kommt der psychische Leidensdruck: Das Selbstbewusstsein sinkt, das Opfer wird depressiv, ängstlich und ist sogar selbstmordgefährdet.



Ein Cybermobbing-Opfer ist nicht leicht zu erkennen. Eltern sollen beobachten, ob sich das Verhalten verändert: Sind die Kinder beim Empfangen von Nachrichten ängstlich oder nervös? Wirken sie bedrückt oder angespannt und möchten nicht darüber reden, was sie am PC machen? Ein weiterer Indikator ist der Rückzug aus dem sozialen Leben. Suchen Sie das Gespräch, beruhigen Sie die Situation um das Opfer zu stärken und sichern Sie das Beweismaterial.

Prävention durch Aufklärung
Kinder und Jugendliche gehen recht sorglos mit den Infos um, die sie veröffentlichen. Eltern können über eine Suchmaschine (Namen, E-Mail-Adresse oder Handynummer eingeben) abfragen, was das Kind online mitgeteilt hat. Gemeinsam kann man das Ergebnis bewerten

und fragen, ob die Daten noch anderswo veröffentlicht wurden.

Vertrauen schaffen

Kinder und Jugendliche sollten grundsätzlich wissen, was Mobbing bzw. Cybermobbing ist und brauchen im Fall von Belästigung Ansprechpartner. Nur so kann der Täter zur Verantwortung gezogen werden. Wenn etwas passiert ist, nicht mit Internetverbot oder anderen Verboten drohen: Wenn sich die Kinder schuldig fühlen, verschließen sie sich, anstatt die Eltern zu Rate zu ziehen.

Mein Kind ist Opfer

Zunächst gilt zu erfahren, wie das Kind aus der Anonymität heraus attackiert und geplagt wird. Ist klar, wer hinter den Angriffen steht, oder ist das Mobbing nicht mehr kontrollierbar? Nicht selbst das Gespräch mit dem Täter oder den Eltern suchen, sondern Distanz bewahren. Mit dem Klassen- oder Vertrauenslehrer gemeinsam konkrete Schritte planen und einen Zeitrahmen vereinbaren. Bleibt dies ohne Ergebnis, folgt das Gespräch mit der Schulleitung oder Beratungsstellen.

Hilfe suchen

Professionelle Beratungsstellen (Seite 23) können abschätzen, wann Anzeige erstattet werden soll. Zunächst alle Beleidigungen und Angriffe sammeln. E-Mail Adresse und Handynummer des Kindes ändern, sowie alle Nicknames (Spitzname in der Onlinewelt) in Communities und Chaträumen. Daten des Täters den Betreibern melden und diese auffordern, die beleidigenden Inhalte zu entfernen.

Mein Kind ist Täter

Reagieren Sie! Das Kind muss wissen, dass Online-Angriffe massiv schaden können und dass es auch strafbar sein kann. Gemeinsam konkrete Schritte überlegen, z.B. eine Entschuldigung oder ein persönliches Gespräch.

Nicht wegschauen!

Cybermobbing lebt auch von stillschweigenden Mitwissern. Kinder müssen verstehen, dass Mobbing nicht cool ist und sollen Eltern auch von Fällen berichten, die andere betreffen. Nur so kann Cybermobbing gestoppt werden. Erwachsene heranzuziehen hat nichts mit Verrat zu tun, sondern mit Mut. Dem Mut, „Stopp!“ zu sagen.

Deborah Visintainer

Handy und Smartphone sicher nutzen

WLAN
Kabelloses lokales Netzwerk zwischen Computern und anderen Geräten. PC, Tablet oder Mobiltelefon können so eine drahtlose Verbindung zum Internet herstellen.

FLATRATE
Für einen festgelegten Grundbetrag steht die Internetverbindung grenzenlos zur Verfügung.

INSTANT MESSENGER
Software, mit der in Echtzeit kommuniziert wird.

CHAT
Der Begriff bedeutet „plaudern"; Meist über Instant Messenger wie Whatsapp, Skype oder Facebook Messenger.

ANDROID, **IOS** oder **WINDOWS PHONE** sind die gängigsten Betriebssysteme für Handys.

Für Kinder und Jugendliche ist das Mobiltelefon fester Bestandteil des Alltags: Für Eltern ist es nicht immer einfach, dies nachzuvollziehen. Das Smartphone bietet gegenüber dem Handy eine Reihe von zusätzlichen Nutzungsmöglichkeiten und ist die am häufigsten genutzte, multimediale Kommunikationsplattform.
Neben rein praktischen Dingen erfüllt es v.a. soziale Funktionen: Es dient der Anerkennung, der Pflege von Netzwerken und Freundschaften und der Organisation des Alltags. Unzählige Formen der Selbstdarstellung sind möglich.

Sichere und verantwortungsvolle Handynutzung

Über klare Absprachen und verbindliche Regeln erlangen die Kinder mehr Eigenverantwortung:

- Eltern sind **Vorbild**, z.B. bei der Einhaltung handyfreier Zeiten.
- Mit dem Kind die Handynutzung besprechen und sich selbst etwas beibringen lassen – Das Kind freut sich über die **Expertenrolle** und eine gute Gesprächsbasis wird geschaffen.
- Geheime Kontrollen können zu einem Vertrauensbruch führen – Kinder haben ein **Recht auf Privatsphäre!**
- Mögliche **Risiken** (Kostenfallen, Belästigungen) ansprechen und Auswege aufzeigen.
- **Regeln für die Nutzung** festlegen und vereinbaren, wer die Kosten für Zusatzdienste übernimmt (Apps, In-App-Käufe, usw.).
- **Respektvoller Umgang** in der Öffentlichkeit (leise reden, keine laute Musik, Tastentöne deaktivieren). Wie kann ein Diebstahl verhindert werden?
- **Ein Verbot** führt meist dazu, dass sich die Kinder bei möglichen Problemen nicht an die Eltern wenden.

Einfaches Handy oder Smartphone?

Kinder sollten für den Anfang ein Handy ohne Internetzugang erhalten. So ist ganz klar, was der Sinn des Gerätes ist: telefonieren.

Eine Altersgrenze zu ziehen ist schwierig, aber ein Smartphone muss im Grundschulalter nicht sein. Im Alter von 13, 14 Jahren kann es dann auch ein Smartphone sein. Als Sicherheitsausstattung für Notfälle eignet sich ein einfaches Handy – ohne Internetzugang.

Telefonkosten im Griff

Wir wird das Gerät verwendet? Wird vor allem telefoniert oder auch das Internet genutzt? Wie sollte die Qualität der Fotos sein? So kann das zweckdienlichste Gerät und der beste Mobilfunkanbieter gewählt werden. Ein Vergleich der verschiedenen Kosten lohnt sich. Als Einstieg eignen sich aufladbare Wertkartenhandys (Pre-Paid), da ein genauer Überblick über die Kosten gegeben ist. Wenn die Kinder einen Teil der Kosten selbst übernehmen, bekommen sie ein Gefühl für die Kosten.

Ganz schön teuer

Zusatzdienste (Klingeltöne, Chats, Apps) werden oft unbedacht oder versehentlich installiert und zusätzlich über die Handyrechnung verrechnet. Vor allem Kinder müssen genau informiert und aufgeklärt werden - aber die Abzocke trifft Jung wie Alt. Die Südtiroler Verbraucherzentrale, der Beirat für Kommunikationswesen oder die Postpolizei helfen bei Problemen weiter.

Apps – kleine Helfer für das smarte Telefon

Apps (Kurzform von Applications) sind spezielle Programme, die über eigene Shops (Google Play Store, App Store oder Windows Phone Store) bezogen und direkt auf dem Gerät installiert werden. So nützlich Apps manchmal sein können, bergen sie auch Risiken wie die unbemerkte Übertragung persönlicher Daten, mitgelieferte Schadsoftware oder finanzielle Abzocke. Auch hier ist also Vorsicht geboten!

Manuela Kastl
Marion Thöni

TIPP!

Fit für das mobile Telefon:
Machen Sie mit Ihrem Kind den **Handyquiz** auf **www.klicksafe.de**

Top-Ten-Apps laut Jim-Studie 2014 des Medienpädagogischer Forschungsverbundes Südwest
1. WhatsApp 2. Facebook 3. Instagram 4. YouTube 5. Clash of Clans 6. Skype 7. Quizduell 8. Google 9. Snapchat 10. Candy Crush Saga

APPhängig von WhatsApp?

Die Erfolgsgeschichte der SMS in den 90er wird übertroffen vom Boom der sozialen Anwendungen auf Smartphones (Social-Apps). Diese ermöglichen es, Text- und Bildnachrichten kostenlos über das Internet auszutauschen (chatten), wobei auch Gruppengespräche und Telefonieren möglich sind.

Für die Kinder gehören Chats zum Kommunikationsalltag wie für die Generation der Eltern das SMSen per Handy.

SocialApps

Im mobilen Bereich setzen sich immer mehr SocialApps durch. Die aufstrebendste davon ist **WhatsApp** mit über 900 Millionen Nutzern. Sie weist aber Schwächen im Datenschutz bzw. eklatante Sicherheitslücken auf. Es wird zwar seit dem Herbst 2014 eine End-to-End-Verschlüsselung eingesetzt, was bedeutet, dass Unterhaltungen zwischen Chattern vom Anbieter nicht einfach mitgelesen werden können; Aber das gilt nur zwischen Android-Benutzern. Schaltet sich nun ein iOS-Nutzer in einem Gruppenchat dazu, dann ist die Verschlüsselung ausgehebelt. Außerdem wurden Nutzerkonten „gehackt" und ganze Gesprächsverläufe im Internet für alle frei einsehbar gemacht. Zusätzlich überträgt die App die eigenen Telefonbucheinträge ohne eigene Zustimmung oder der betroffenen Dritten zu WhatsApp. Sogar Google-Konten oder PayPal wurden über WhatsApp ausspioniert.

Alternativen

Wer vor Schnüfflern sicher sein will, sollte nach Alternativen Ausschau halten. An erster Stelle steht hier die Schweizer App **Threema**. Diese (wie auch der indische Hike Messenger) setzt auf Sicherheit und Datenschutz. Bei diesen Apps kann nicht einmal der Anbieter die Chats mitlesen. Die gute Nachricht: Südtirols Jugendliche nehmen zunehmend eine gesunde, kritische Haltung gegenüber Datenschutz und Privacy ein. Sie überlegen mittlerweile genauer, welche Inhalte sie von sich im Internet preisgeben.

Die beliebtesten Apps

Applications aus dem Bereich der Social Communities (Facebook) sind, gefolgt von Instant-Messeging-Anwendungen wie WhatsApp oder Skype und diversen Spielen am beliebtesten.
Wichtig: Vor dem Installieren sollten die allgemeinen Geschäftsbedingungen (AGBs) und Zugriffsrechte sorgfältig gelesen werden. Man sollte auf Apps aus alternativen App-Stores verzichten und Anwendungen von den großen Plattformen vorziehen, da diese zumindest oberflächlich mittels eines automatisierten Verfahrens überprüft werden. Außerdem sollte man in Erfahrung bringen, welche Zugriffsrechte für die jeweilige App von Nöten sind. Wenn die App bereits installiert ist, kann man z. B. bei Android unter „Einstellungen" – „Anwendungen" – „Anwendungen verwalten"... die Berech-

tigungen der jeweiligen App erfragen und ändern. Nach dem Herunterladen sollte man bei den Einstellungen prüfen, ob sich Akkuverbrauch, Rechenzeit oder Datentransfer verändert haben. Falls dies so ist, sollte man die App entfernen, da möglicherweise ungewollt Daten weitergegeben werden.

Virenschutzprogramme

Auch für mobile Betriebssysteme gibt es Virenschutzprogramme, wie beispielsweise:

- **APEFS = Android Permission Filter System** (Android, kostenlos): Fungiert als Filter zwischen App-Store und Endgerät und zeigt an, welche Berechtigungen sich eine App beschaffen möchte. Auch bereits installierte Apps können nach diesen Berechtigungen durchsucht werden.
- **Lookout Security & Antivirus** (iOS und Android, kostenlos): Das Programm scannt jede Anwendung, die herunter geladen wird sowie die bereits auf dem Smartphone befindlichen Apps auf Schadprogramme. Automatisch werden Updates der Software durchgeführt und die auf dem Gerät befindlichen Dateien gesichert. Im Fall des Verlustes des Geräts, kann dieses mittels des Programms geortet werden.
- **Avast Mobile Security** (iOS und Android, kostenlos): Das Programm durchsucht das Gerät nach Viren, warnt vor gefährlichen URLs und schützt das Gerät durch eine Firewall. Bei Verlust des Smartphones ist es u.a. möglich, Daten zu löschen, eine Telefonsperrung zu aktivieren und das Smartphone zu lokalisieren.

Stefan Kontschieder

TIPPS!

- Gemeinsam festlegen, welche Apps es wirklich braucht oder man probieren möchte.
- Apps selbst testen und jene, die den Kriterien nicht entsprechen, gleich wieder löschen.
- Bei vielen Apps kann man beim erstmaligen Verwenden wichtige Einstellungen vornehmen. Die Einstellung „Aktuellen Ort verwenden“ macht nur Sinn, wenn es sich um eine Navigationsanwendung (z. B. Routenplaner) handelt, ansonsten deaktivieren. Bei Pop-Up-Fenstern sollten die Kinder immer nachfragen, bevor sie eine Auswahl treffen.
- Die meisten Apps verbinden sich mit dem Internet. Ein unbegrenztes Datenvolumen und Daten-Roaming können hier schnell zu hohen Kosten führen.
- Es empfiehlt sich Apps regelmäßig auszumisten und das zu löschen, was nicht mehr benötigt wird.

Downloaden & tauschen: Ist alles erlaubt, was möglich ist?

Es besteht ein großer Unterschied darin, ob man zu Hause eine Musik-CD brennt oder man dieselben Musikstücke im Internet zur Verfügung stellt - kurz gesagt: Nicht alles, was machbar ist, ist auch erlaubt!

Up- und Download

Als Download bezeichnet man das Empfangen und Speichern von Daten (Bilder, Musik, Videos, Textdateien oder Programmen) über ein Netzwerk auf dem eigenen Computer. Das Gegenteil ist das Uploaden. Dabei werden Daten vom eigenen Computer auf einen Server, eine Webseite oder einen PC übertragen.

Filesharing-Plattformen

Über Tauschbörsen (Vuze, eMule, Ares) kann man online Musik, Filme oder Software tauschen und teilen. Je mehr Personen an einer solchen Tauschbörse teilnehmen, desto mehr Dateien kursieren. Wie in den meisten europäischen Ländern ist auch in Italien noch immer nicht gänzlich geklärt, ob das alleinige Herunterladen einer urheberrechtlich geschützten Datei illegal ist.

Geschützte Inhalte zum Download anbieten

Beim Upload ist die Gesetzeslage klar: Die Vervielfältigung oder Verteilung einer urheberrechtlich geschützten Datei ohne Erlaubnis ist illegal. Besonders die Musik- und die Computerspielindustrie überwacht die gängigen Tauschbörsen systematisch und verschickt Abmahnungen. Urheber ist, wer ein Werk schafft (Text, Foto, Film, Musiktitel, Computerprogramm). Er entscheidet ob, wann oder wo sein Werk veröffentlicht wird.

Streaming: Nutzung von Videoportalen

Videos anschauen auf legalen Plattformen: Ein Video bei **YouTube** oder **MyVideo.de** anzuschauen, ist unbedenklich. Aber auch solche Videos enthalten teilweise Urheberrechtsverletzungen, denn viele Videos wurden z. B. aus dem Fernsehen aufgenommen oder kopiert: Rechtlich eine Grauzone. Der Unterschied ist, dass hier keine dauerhaften Kopien auf dem Rechner gespeichert werden. Generell ist es rechtlich unproblematisch, sich auf legalen Plattformen Videos anzuschauen, auch wenn sie nicht rechtmäßig hochgeladen wurden, denn Verantwortung und Kontrolle liegen bei den Portalen.

Videos anschauen auf illegalen Plattformen: Plattformen wie **kinox.to** oder **movie4K.to** haben meist einen fragwürdigem Hintergrund. Schon allein die Tatsache, dass die neuesten Filme, die gerade erst im Kino anlaufen, kostenlos zur Verfügung stehen, zeigt, dass die Betreiber nicht die erforderlichen Rechte dazu haben können. Aber auch hier ist noch nicht geklärt, ob das alleinige Betrachten erlaubt ist oder nicht. Abgesehen von der Verletzung des Urheberrechtes, ist von der Nutzung solcher Portale eher abzuraten, denn diese schütten die Nutzer sprichwörtlich mit Müll zu.

Videos oder Musik von legalen Plattformen herunterladen: Mittlerweile nehmen Jugendliche bevorzugt das Angebot von legalen Plattformen in Anspruch, das Interesse an illegalen Ablegern sinkt. Solche Downloads sind erlaubt, sofern sie für den privaten Gebrauch sind. Wird die dadurch „erworbene" Musik in einer Bar oder einem Restaurant verwendet, ist dies eindeutig illegal – genauso wie die Weitergabe derselben auf Tauschbörsen oder Webseiten.

Videos einbetten

Über die Videoportale kann man Videos in die eigene Webseite einbetten (embedding). Das ist nicht nur erlaubt, sondern von den meisten Betreibern der Portale gewünscht, denn es ist eine Werbung. Auch wird das Video von der Originalquelle abgespielt, ohne das eine Kopie gemacht wird.

Es ist spannend, die vielseitigen Möglichkeiten des Netzes zu nutzen und zu genießen, es wäre aber ratsam, sich dabei eine gute Portion Skepsis und Vorsicht zu bewahren, sich so gut es geht über die Gesetzeslage zu informieren. Im Zweifelsfall lieber mal etwas sein lassen!

Michael Reiner

Onlinespiele
Chance oder Gefahr?

Es handelt sich dabei um PC - oder Konsolen-Spiele (Sony Play Station, Nintendo Wii, etc), die entweder direkt über den Webbrowser online gespielt werden oder um normale Computerspiele, mit denen man, über das Internet verbunden und, falls gewünscht, gleichzeitig mit bzw. gegen andere Spieler spielen kann.

Über den PC und das Internet tauchen die Spieler in teils fantastische, faszinierende Welten ein. Man verlässt die „normale" Welt, kann eigene Charaktere erfinden und weiterentwickeln. Im Austausch mit anderen Spielern werden Aufgaben und Konflikte gelöst. Jugendliche sind gerade in Zeiten der Pubertät sehr verletzlich und stehen sich oft selbst im Weg. In den Fantasiewelten können sie dagegen Figuren erstellen, die Eigenschaften aufweisen, die sie im realen Leben selbst gerne hätten (mutig, draufgängerisch, extrovertiert...) oder die im realen Leben von der Gesellschaft nur schwer geduldet werden (aggressiv, grausam, mächtig...). Eine dabei häufig genutzte Spieleform sind sogenannte MMORPG-Spiele (dt: Massen Mehrspieler Online Rollen Spiel) wie World ofWarcraft oder Everquest.

Gründe, warum Computer und Onlinespiele auch gut sein können

Seit ihrem Aufkommen in den frühen 80er Jahren hält sich der Vorwurf, dass Computerspiele negative Auswirkungen haben. Besonders sogenannte Ego-Shooter bzw. First-Person-Shooter (Schießspiele) und Gewaltspiele waren immer wieder im Fadenkreuz der Kritik: Kaum ein Amoklauf, ohne dass auch die Medien und Computerspiele dafür verantwortlich gemacht werden. Diese würden Kinder aggressiv machen und isolieren, so die Kritiker. Bis heute konnte dies weder eindeutig bestätigt noch widerlegt werden.

Doch Gamen hat auch positive Auswirkungen

Die Entdeckungsfreudigkeit steigt: Die Spieler bilden Hypothesen, die laufend bestätigt oder wieder verworfen werden und experimentiert in einer risikofreien Umgebung. Wird ein Spielabschnitt beim ersten Versuch nicht gelöst, muss eine neue Strategie gewählt werden. Dies fördert das Durchhaltevermögen und das Frustrationspotenzial, das den Kindern auch im realen Leben zu Gute kommt.

Computerspiele fördern die Kreativität: Besonders Simulations- bzw. Echtzeitstrategiespiele fördern durch die Aufgabenstellung die Kreativität. Ziel bei diesen Spielen ist meistens, aktiv an der Gestaltung der Spielwelt mitzuarbeiten, indem gebaut, gefördert und weiterentwickelt wird. Somit sind der Fantasie kaum Grenzen gesetzt.

Computerspiele fördern strategisches und abstraktes Denken: Viele Spiele sind sehr ausgeklügelt gestaltet und lassen sich nur

mit einer Kombination aus abstraktem und strategischem Denken lösen: Welche Aufgabe muss zuerst gelöst werden? Welche Werkzeuge und Hilfsmittel braucht es? Nur wer vorausschauend denkt und strategisch plant, kommt zum Ziel.

Computerspiele machen Kinder schneller: Wer mit Computerspielen aufwächst, zeigt in der Regel eine deutlich verbesserte Reaktionsfähigkeit sowie Augen-Hand-Koordination auf. Wenn Spieler beim Ausführen einer Aufgabe erfolgreich sind und mit dem nächsten Level belohnt werden, wird das Glückshormon Endorphin ausgeschüttet, das als erneuter Ansporn dient.

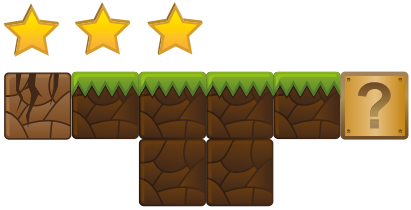
Computerspiele und soziale Kompetenzen: Auch das Onlinespielen macht in der Gruppe mehr Spaß.

Doch es lauern auch Gefahren

So wie bei fast jeder Art von Konsum lauern auch hier Gefahren. Anders als bei Substanzen (Drogen, Alkohol...) handelt es sich bei der Computerspielsucht aber um eine reine Verhaltenssucht.
Folgenden Merkmale lassen sich oft beobachten:

- Computerspiele werden zum Lebensmittelpunkt und dominieren die Alltagsstruktur.
- Der Spieler verliert den Überblick über die Spielzeiten und kann sich nicht vom Bildschirm losreißen.
- Der Spieler weist Entzugserscheinungen auf und ist abseits vom Spielen nervös, unruhig, unkonzentriert, zittert oder schwitzt.
- Der Spieler vernachlässigt allmählich Schule/Arbeit, Freunde, Familie, Ernährung und Hygiene.
- Der Spieler verdrängt zunehmend seine Probleme und flüchtet sich in die virtuelle Welt, um den Alltag zu vergessen.

Michael Reiner



Zeitvorgaben beim Onlinegamen

- 4-6 Jahre: ca. 20 min/ Tag, in Begleitung der Eltern
- 7-10 Jahre: ca. 45 min/ Tag
- 11-13 Jahre: ca. 60 min/Tag

(aus: „Computerspiele Tipps für Eltern, **www.klicksafe.de**)

Problematische Inhalte und Gefahren

Die Sexualität junger Menschen hat sich in ihren Grundsätzen in den letzten Jahrzehnten kaum verändert. Für Jugendliche sind in einer Beziehung nach wie vor dieselben Werte wichtig. Dennoch haben digitale Medien großen Einfluss auf die sexuelle Entwicklung, was gleichzeitig eine Herausforderung darstellt: Einerseits finden Jugendliche im Netz schnelle Antworten auf brennende Fragen, andererseits ist der leichte Zugang zu - auch sehr extremem - pornografischem oder gewaltverherrlichendem Material problematisch.

Was ist Posing?
Jugendliche präsentieren sich mit Profilen, Bildern, Kommentaren, aber auch mit eigenen Filmen und Musik. Musikvideos und Werbung beeinflussen die Art, wie Jugendliche ihre Fotos und Filme gestalten. Fotos spielen bei der Selbstdarstellung im Netz die größte Rolle. Dabei reicht ein einfaches Foto manchmal nicht mehr aus, Aufmerksamkeit und Auffälligkeit sind gefragt. Mit sexuell aufreizenden Posen oder entsprechend leichter Kleidung geht das umso leichter. Mit der Handykamera selbstgemacht, sind die Fotos schnell online gestellt. Die **Selfie-Funktion** (Selbstportrait) erfreut sich dabei zunehmender Beliebtheit. Mögliche negative Folgen bleiben unbedacht oder werden ausgeblendet. Erwachsene können hier unterstützen und auf die Grenzen hinweisen.

Was ist Sexting?
Die Wortkreation setzt sich aus „Sex“ und „Texting“ zusammen und meint das gegenseitige Tauschen von anzüglichen Fotos oder Nachtaufnahmen. Die erotischen Bilder oder Nacktaufnahmen werden vorerst als Liebes- oder Freundschaftsbeweis oder zum Flirten verschickt. Im schlimmsten Fall landen die Aufnahmen auf diversen Handys und werden im Web oder zur Erpressung oder zum Cybermobbing verwendet.
Sind solche Bilder einmal in Umlauf, kann deren Verbreitung nicht mehr gestoppt werden. Schnell geraten die Fotos in die falschen Hände. So können einmal verbreitete Aufnahmen auch Jahre später wieder auftauchen und den Abgebildeten schaden (z.B. Jobsuche, Beziehungen).

Was ist Grooming?
Die Gefahr vor sexueller Anmache ist eine der Schattenseiten der Nutzung von sozialen Netzwerken. Zu den negativen Erfahrungen zählen etwa unerwünschte Anmache oder die Aufforderung von Unbekannten, intime Informationen oder Foto von sich zu schicken. Beim Grooming erschleichen sich Erwachsene im Internet das Vertrauen von

Kindern und Jugendlichen – mit dem Ziel der sexuellen Belästigung und des Missbrauchs und geben sich - manchmal - auch als Gleichaltrige aus. Zunehmend versuchen Männer die Annäherung durch einschmeichelnde Kommentare.
Die Täter bauen Vertrauen auf, um Nacktbilder zu erhalten. In der Folge wollen sie weitere Fotos und verschicken dazu auch selbst Bilder und Kommentare. Möchten die betroffenen Kinder den Kontakt lösen, schüchtern die Täter ihre Opfer mit Drohungen und Erpressungen ein: „Du wolltest das ja auch, du hast ja mitgemacht."

Wie können Eltern Ihre Kinder stärken?

- Oft ist auf den ersten Blick nicht erkennbar, wer im Internet das tatsächliche Gegenüber ist. Besprechen Sie mit Ihrem Kind, wie einfach es im Internet ist, sich als eine andere Person auszugeben, und dass es sich lohnt, bei Online-Bekanntschaften misstrauisch zu sein.
- Unterstützen Sie Ihr Kind dabei, NEIN sagen zu können. Kinder und Jugendliche, die sich gegen Annäherungsversuche von Beginn an wehren, sind für Sex-Täter/innen schnell uninteressant. Sie suchen sich lieber leichtere Beute. „Nein-Sagen" muss trainiert werden, damit es im Anlassfall klappt.
- Stärken Sie Ihr Kind von klein auf darin, auf das eigene Bauchgefühl zu hören. Wird dieses immer wieder verwirrt und gestört, verlernen Kinder, auf ihre Intuition zu achten.
- Webcams können bei sexueller Belästigung im Internet eine wichtige Rolle spielen. Oft ist nicht klar, wann eine Webcam ein- bzw. ausgeschalten ist. Beschäftigen Sie sich gemeinsam mit den Funktionen der Webcam und klären Sie, wie man diese ausschalten kann. Anfragen von Unbekannten sollten abgelehnt werden.
- Vereinbaren Sie mit Ihrem Kind, dass es eine Bekanntschaft aus dem Netz niemals treffen soll.

Gewalt- und Pornovideos

Gewalt- und Porno-Videos haben für Kinder und Jugendliche einen besonderen Reiz– seien es mit dem Handy selbst gefilmte Gewaltszenen (Happy Slapping), Downloads aus dem Internet oder von Freunden geschicktes Material. Für die Nutzung dieser Inhalte gibt es vor allem zwei entscheidende Motive:

- **Unterhaltungsmotiv und Grenzerfahrung**
  Der emotionale Kick und das Überschreiten von Grenzen stehen hier im Mittelpunkt. Der Wunsch nach Ablenkung, Protest und Abgrenzung spielt eine zentrale Rolle.
- **Soziale und sozialintegrative Motive**
  Das gemeinsame Bestehen von extremen Situationen ist die zentrale Komponente – das Anschauen der

Videos wird zum Gemeinschaftserlebnis. Besonders extreme Inhalte geben auch ein gutes Gesprächsthema in der Gruppe ab oder werden zur Anerkennung genutzt. Dazu zählt auch, schockierende Videos an jüngere Mitschüler als eine Art Mutprobe weiterzuschicken.

Auch wenn wir uns das wünschen würden: Eine 100%ige Garantie für sicheres Surfenkann und wird es nie geben. Deswegen auf Handy und Internet zu verzichten oder die Nutzung radikal einzuschränken, kann keine Lösung sein. Unter Anleitung können die Risiken sehr gut eingeschränkt werden.Behalten Sie vor allem dann einen kühlen Kopf, wenn Ihr Kind mit einem ungeeigneten Inhalt in Berührung gekommen ist. Drohen Sie nicht mit Strafen oder Verboten, sonst verlieren Sie Ihre Rolle als Vertrauensperson. Seien Sie Vorbild und leben Sie Ihrem Kind den Umgang mit Medien vor, den Sie sich von ihm wünschen.

Empfehlungen für Eltern:

- Sprechen Sie Ihr Kind seinem Alter entsprechend gezielt auf das Thema an. Sagen Sie ihm, dass Sie sich aufgrund der Meldungen in der Presse Sorgen machen.
- Fragen Sie immer wieder einmal nach, ob es derartiges Video- oder Bildmaterial bereits gesehen hat und was Ihr Kind dabei empfand. Sprechen Sie auch mit den Eltern der Freunde Ihres Kindes und/oder den Lehrern über das Thema.
- Machen Sie sich mit den Funktionen moderner Handygeräte vertraut – speziell mit der Datenübertragung per Bluetooth- oder Infrarot-Schnittstelle.
- Prüfen Sie, welches Handy für Ihr Kind geeignet ist und welche Funktionen wirklich sinnvoll sind.
- Treffen Sie mit Ihrem Kind klare Abmachungen über erlaubte und nicht erlaubte Funktionen des Handys.
- Sprechen Sie mit Ihrem Kind über die sinnvolle Nutzung und thematisieren Sie mögliche Gefahren. Dies bedeutet unter anderem, dass Bluetooth grundsätzlich abgeschaltet und nur bei Bedarf aktiviert werden sollte.
- Erfahrungsgemäß ist das Unrechtsbewusstsein junger Menschen beim Verbreiten gewaltverherrlichender Inhalte gering. Machen Sie Ihrem Kind klar, dass die Weitergabe von Videos mit Gewaltdarstellungen strafrechtliche Konsequenzen nach sich ziehen kann. Dies bedeutet unter anderem das Einleiten von Ermittlungen sowie die Sicherstellung/Beschlagnahmung des Handys durch die Polizei.

Manuela Kastl
Marion Thöni


Werbemitteilung
Mit ROL Secure ist die ganze Familie rundum geschützt! Da bin ich mir sicher.
ROL Secure
▪ schützt Kinder beim Surfen und vor Identitätsdiebstahl in Social Networks
▪ schützt bis zu 5 Geräte gleichzeitig, egal ob PC, Mac, Tablet oder Smartphone
▪ schützt beim Online-Banking und Online-Shopping
▪ schützt vor Viren, Hackern und Malware
Infos & Bestellung:
▪ 800 031 031, info@raiffeisen.net
▪ www.raiffeisen.net
(Haushalte / Alles fürs Heimnetz / Antivirus Lösungen)
RaiffeisenOnline

Soziale Netzwerke **vernünftig** nutzen

Was ist ein soziales Netzwerk?

Am leichtesten lässt sich diese Art von Webseite mit einer Party im Internet vergleichen, die 24 Stunden am Tag und 365 Tage im Jahr läuft. Nutzer teilen Videos oder Artikel, die sie im Internet gefunden haben. Wem etwas besonders gefällt, reicht es mit dem „Teilen"-Knopf an seine „Freunde" weiter oder verfasst einen Kommentar dazu.

Wer selbst etwas ins Netz lädt, erstellt einen sogenannten „Post". Unter Jugendlichen besonders beliebt sind Fotos von Ausflügen, Festen oder Freunden.

Um einem sozialen Netzwerk beizutreten, ist eine Registrierung notwendig. Facebook sieht ein Mindestalter von dreizehn Jahren vor. Viele Jugendliche umgehen diese Hürde durch die Angabe eines falschen Geburtsdatums. Pädagogen warnen: Kinder unter zwölf Jahren sollten nicht in diesen Medien aktiv sein.

Worauf ist zu achten?

Eltern sollten ihre Kinder beim Einstieg in diese faszinierende Welt begleiten. Jüngere Benutzer sollten sich nicht mit ihren realen Daten registrieren, sondern Fantasienamen verwenden und keine Fotos von sich in ihr Profil laden. Anonymität bietet Kindern einen gewissen Schutz. Viele Erwachsene stellen sich die Frage, ob sie zur Kontrolle selbst Mitglied bei Facebook werden sollten.

Dies ist möglicherweise der einzige vernünftige Grund, dem Netzwerk selbst beizutreten. Allerdings werden die Jugendlichen mit fortschreitendem Alter über die Profileinstellungen zusehends einschränken, was ihre Eltern von ihnen zu sehen bekommen – wie im echten Leben!

Der Beitritt zu Facebook ist ein idealer Moment, um in der Erziehung den Freundesbegriff kritisch zu hinterfragen und die Unterschiede zwischen Bekanntschaft und Freundschaft herauszuarbeiten. „Freunde sammeln" ist ein beliebter Sport auf Facebook. Im Idealfall fügen Jugendliche

nur Personen, die sie auch kennen, zu ihren „Facebook-Freunden“ hinzu.

Ist wirklich alles öffentlich?

Mit dem Erfolg von Facebook und mit jedem veröffentlichten Foto verzichten wir auf ein Stückchen Privatsphäre. Wer auf Facebook aktiv ist, sollte sich daher genau überlegen, was er für wen sichtbar macht. Dazu bietet Facebook mittlerweile detaillierte Einstellungsmöglichkeiten. Wie’s geht, sehen Sie in der Linksammlung auf S. 22. Nur wirkliche Freunde sollten unsere Daten sehen. Grundsätzlich gilt: Im Internet sollte man nur Dinge veröffentlichen, die man auch am Sonntag auf dem Kirchplatz im Beisein von anderen Personen öffentlich sagen oder zeigen würde.

Das Internet vergisst nichts!

Meist reicht ein einfacher Klick, um Dinge ins Internet hochzuladen. Fotos oder Videos aus dem Internet wieder rauszukriegen, ist ungleich aufwändiger und manches Mal sogar unmöglich. Hat jemand unseren „Post“ mit anderen geteilt, haben wir die Kontrolle darüber längst verloren. Selbst Jahre später taucht das entsprechende Foto dann bei einer Suche nach dem Namen wieder auf (siehe Textbox „Alles kein Problem“).

Warum nicht einfach verbieten?

Der einfachste Weg um diesen Gefahren auszuweichen, ist sicherlich ein Verbot. Für Jugendliche sind die sozialen Netzwerke allerdings eine Kommunikationsform wie das Telefonieren, das Chatten oder das Mailen. Ein Verbot würde sie daher z.T. von ihrem Freundeskreis isolieren, und es ist eine Frage der Zeit, bis sie sich über ein solches Verbot hinwegsetzen. Mehr als 90% der Jugendlichen über 14 Jahren nutzen soziale Medien mittlerweile regelmäßig. Zudem sind sich Pädagogen einig, dass sie eine wichtige Entwicklungsmöglichkeit in unserer Zeit darstellen und dass der kompetente Umgang mit diesen Medien für die Jugendlichen wichtig ist. Eine Begleitung durch Schule und Eltern ist daher zielführender als ein Verbot.

Alexander Wallnöfer

TIPP!

- Die bekanntesten Netzwerke in Südtirol sind Facebook, Netlog, Instagram und Pinterest: 9 von 10 Jugendlichen sind bei einem dieser Netzwerke mit dabei.
- Wohin ein sorgloser Umgang mit Facebook führen kann, zeigt dieses unterhaltsame Video von explainity: **https://www.youtube.com/watch?v=8VVIqRlo7ig**

Kinder unterwegs im Internet

Die Schmuddelecke

Im Internet gibt es Inhalte, die nicht für Kinderaugen bestimmt sind: Pornografie, gewaltverherrlichende Videos, Drogenangebote und vieles mehr (S. 16). Ein Browser, der von Kindern verwendet wird, sollte mit einer kindgerechten Seite, etwa einer für Kinder konzipierten Suchmaschine, geöffnet werden. Gehört Ihr Kind zur Altersklasse 6-13, dann empfiehlt sich zusätzlich eine Kinderschutzsoftware. Damit lassen sich die Surfzeit einschränken, „gute" Seiten freischalten und „gefährliche" Seiten sperren. Je größer das Kind wird, umso mehr Seiten können Sie zugänglich machen. Solche technischen Hilfsmittel funktionieren gut, sie bieten aber keinen 100%-igen Schutz. Irgendwann wird das Kind die Filter umgehen. Sie können Ihr Kind also auch im Internet nicht vor allen negativen Erfahrungen bewahren. Was Sie in jedem Fall tun können: Mit Ihrem Kind über Inhalte im Internet reden, die es nicht alleine verarbeiten kann.

Sicheres Passwort

Zu kurz kommt oft die Sorge um das Passwort - egal ob für den E-Mail-Account, den PC oder für Facebook. Ein sicheres Passwort besteht aus mindestens **acht Zeichen, enthält Groß- und Kleinbuchstaben, Ziffern und Satzzeichen** und es wird alle paar Monate geändert. Allerdings ist es nicht leicht, sich komplizierte Passwörter zu merken. **TIPP:** Aus dem Satz: „**W**enn **i**ch **i**m **I**nternet **u**nterwegs **b**in**, a**chte **i**ch **a**uf **m**ein **P**asswort **u**nd **ä**ndere **e**s **a**lle **6 M**onate!", ergibt sich folgendes Passwort: **Wiilub,aiamPuäea6M**!
Ein Passwort-Verwaltungsprogramm, hilft, die Übersicht zu bewahren: **www.keepass.info** (nur englisch)

Eine Frage des Vertrauens

Die wichtigste Maßnahme: Begleiten Sie Ihr Kind im Internet. Verbringen Sie gemeinsame Zeit vor dem PC. Dadurch wächst die Internetkompetenz des Kindes und Sie lernen Interessantes dazu.
Zeigen Sie Interesse und hören Sie zu. Schaffen Sie eine Vertrauensbasis, damit Ihr Kind rechtzeitig zu Ihnen kommt, falls es negative Erfahrungen im Netz machen sollte. Vereinbaren Sie mit Ihrem Kind Spielregeln (z.B. Nutzungszeiten). Engagieren Sie sich in der Schule, damit das Thema auch von Lehrern und Pädagogen altersgerecht in den Unterricht eingebunden wird.

Alexander Wallnöfer

TIPP!

Richten Sie Ihrem Kind die Suchmaschine „Frag Finn" **(www.fragfinn.de)** als Startseite ein. Alle Seiten im Suchindex werden auf Ihre Kindertauglichkeit überprüft.

Tipps und Service

- **www.fragfinn.de**
- **www.handysektor.de**
- **www.internet-abc.de**
- **www.jugendschutz.net**
- **www.klick-tipps.net**
- **www.klicksafe.de**
- **www.medien-sicher.de**
- **www.mpfs.de**
- **www.saferinternet.at**
- **www.schau-hin.info**
- **www.seitenstark.de**
- **www.surfen-ohne-risiko.net**

Kinderschutzsoftware

- www.kinderserver-info.de
- www.raiffeisen.net

Online einkaufen

- www.euroconsumatori.org
- Fernabsatzverträge: www.euroconsumatori.org/81913d82684.html
- Gewährleistung: www.euroconsumatori.org/81913d82076.html
- www.ombudsmann.at

Soziale Netzwerke vernünftig nutzen

- Leitfäden zum Datenschutz und empfohlene Einstellungen in Facebook: www.klicksafe.de/themen/kommunizieren/facebook/materialien-zum-schutz-der-privatsphaere-in-sozialen-netzwerken-facebook/

Cybermobbing

- **Cyber-Mobbing unter Jugendlichen: Warum es so gefährlich ist, wer die Opfer sind und was man dagegen tun kann.** Von Claudine Hengstenberg (2009), Verlag: FastbookPublishing.
  Online erhältlich auf www.fastbooks.de.
- **Rache@**. Von Antje Szillat (2009), Edition Zweihorn. Spannungsgeladene Geschichte über den Außenseiter Ben und das Thema „Mobbing”; für Jugendliche ab 12 Jahren

Smartphone und Apps

- www.rataufdraht.at – jugendgerechte Infos über Handy, Internet sowie interessante Quizzes und Tests für Jugendliche, z. B. zum Thema „Kennst du Grooming-Tricks?“
- www.klicksafe.de/themen/kommunizieren/smartphones/apps-datenschutz/
- www.chatten-ohne-risiko.net
- de.gute-apps-fuer-kinder.de/index.php?title=Intro
- www.kinderapps.info

Downloaden und tauschen

- www.irights.info

Onlinespiele

- www.spielbar.de
- www.spieleratgeber-nrw.de/

Problematische Inhalte

- Download www.saferinternet.at: Elternratgeber „Sexualität & Internet“
- Video auf YouTube: Teachtoday: Gefahren beim Chatten (Thema Grooming)

Nützliche Adressen

Europäisches Verbraucherzentrum in Bozen
Brennerstraße 3, 39100 Bozen
T. 0471 980 939
info@euroconsumatori.org
www.euroconsumatori.org

Verbraucherzentrale Südtirol
Zwölfmalgreinerstrasse 2, 39100 Bozen
T. 0471 975 597
info@verbraucherzentrale.it
www.verbraucherzentrale.it

Familienberatung - Verein Ehe– und Erziehungsberatung Südtirol
Sparkassenstraße 13, 39100 Bozen
T. 0471 973 519
Elterntelefon: 800 892 829
kontakt@familienberatung.it
www.familienberatung.it
Büros in Bruneck, Meran, Schlanders, St. Ulrich

Lilith
Marlingerstr. 29,, 39012 Meran
T. 0473 212 545
info@lilithmeran.com
www.lilithmeran.com

P. M. Kolbe
Mendelstr. 19, 39100 Bozen
T. 0471 401 956
kolbebolzano@yahoo.it
www.consultoriokolbe.it
Büros in Brixen, Meran, Leifers

IVDE - AIED
Eisackstraße 6, 39100 Bozen
T. 0471 979 399
info@aiedbz.it
www.aied.it

Centro Studi Mesocops
Dr.-Streiter-Gasse 9, 39100 Bozen
T. 0471 976 664
consultoriomesocops@teletu.it
www.mesocops.it

Young+Direct - Vertrauliche und kostenlose Beratung für junge Menschen
Andreas-Hofer-Straße 36, 39100 Bozen
T. 0471 060 420
online@young-direct.it
www.young-direct.it
Jugendtelefon: 8400 36366
Skype: young.direct
WhatsApp: 345 0817 056

Post- und Kommunikationspolizei Bozen
T. 0471 531 413
Die Beamten können auch per Mail (auf Deutsch) kontaktiert werden an poltel.bz@poliziadistato.it

Auf der Webseite der Autonomen Provinz Bozen sind die verschiedenen Familienberatungsstellen aufgelistet.

Ich vertraue dem, auf den ich mich verlassen kann.

Die Raiffeisenkasse ist grundsolide und fest verwurzelt. Ihre lokale Ausrichtung und die genossenschaftlichen Werte garantieren größtmögliche Sicherheit für mein Geld. Die Bank meines Vertrauens.

www.raiffeisen.it

Raiffeisen Meine Bank