

enter

Ratgeber digitale Medien

Herbst 2011

«Sicherheit»

Cybermobbing und soziale Netzwerke

Fallen im Netz

Sichere Einstellungen

Alles, was Recht ist

Gesprächsleitfäden für Eltern



Vorwort

des Herausgebers



Liebe Leserin, lieber Leser

Sicherheit ist ein Grundbedürfnis. Wir wollen geschützt sein, wollen wissen, wo Gefahren drohen und wie man ihnen begegnet. Dieses Sicherheitsbedürfnis entwickelt sich mit dem Älterwerden. Kinder und Jugendliche gehen mit Gefahren naturgemäss oft noch fahrlässig um. Niemals würden wir unsere Kinder allein eine Strasse überqueren lassen, ohne ihnen vorher zu erklären, wie sie sicher auf die andere Seite kommen.

«Luege – lose – loufe» – die altbewährte Regel gilt im virtuellen Raum genauso wie im Strassenverkehr. Im Ratgeber *enter* zum Thema Sicherheit zeigen wir Ihnen, welche Risiken Kinder eingehen, wenn sie diese Regel nicht auch im Internet beachten. Jugendliche berichten über eigene Erfahrungen, und Experten geben wertvolle Tipps für Ihren Alltag als Vater, Mutter oder Lehrperson.

Unser Ziel ist es, dass Sie um die Relevanz von Sicherheit im digitalen Leben wissen und Ihr Wissen an unsere Jugend weitergeben. So fördern Sie die kritische und selbstverantwortliche Nutzung der digitalen Medien. Und darin unterstützen wir Sie gerne.

Auf swisscom.ch/enter finden Sie ergänzende Informationen: Video-Interviews, Checklisten, Gesprächshilfen und Links. Sie können auf diese Inhalte auch direkt von Ihrem Smartphone aus zugreifen, wenn Sie die Seiten dieses Ratgebers fotografieren.

Herzlich
Swisscom AG

Michael In Albon,
Jugendmedienschutz-Beauftragter

Inhalt

> Hintergrund

- 04 Die Welt von heute
- 07 Halten wir Schritt?
- 14 Eltern müssen sich einmischen
- 26 Smarte Nutzer für smarte Phones

> Gesprächsleitfaden

- 15 Cybermobbing, Franz Eidenbenz
- 20 Soziale Netzwerke, Dr. med. Myriam Caranzano-Maitre
- 25 Fallen im Netz, Chantal Billaud
- 29 Handy und Sicherheit, Nicolas Martignoni

> Interview

- 12 Theatereinblick: Goethes «Zauberlehrling» im Web
- 16 Meinungen: Sozial vernetzt? Sicher!
- 21 Wortwechsel: Fallen im Netz
- 30 Servicemail: Schützen Sie Ihre Geräte

> Ratgeber

- 33 Früh übt sich



swisscom.ch/enter

Die Lupe signalisiert, dass ein Thema im Internet vertieft wird. Die Filmklappe weist auf Video-Interviews mit Experten hin.



Smartphonebesitzer?

Im App Store oder Android Market nach «kooaba Paperboy» suchen, das App installieren und die Seiten mit Lupe oder Filmklappe fotografieren. So gelangen Sie auf Ihrem Handy direkt zum Zusatzinhalt.

Die Welt von heute

Internet, Smartphone und Co. verändern bei Jugendlichen zwischen 12 und 19 Jahren das Gefühl für Raum und Zeit. Der Wunsch nach echten Begegnungen aber bleibt.

Aufmerksamkeitsspanne: **die nächsten 5 Minuten**



Quelle: JAMES-Studie 2010
swisscom.ch/james

haben in sozialen Netzwerken Privatsphärenoptionen aktiviert

57%

Stunden pro Tag unter der Woche im Netz

2

92% nutzen das Handy mehrmals pro Woche

89%

nutzen das Internet mehrmals pro Woche



51% surfen auf dem Computer gerne einfach drauflos

82% treffen sich mehrmals pro Woche mit Freunden

3

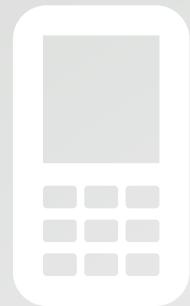
20% unternehmen mehrmals pro Woche etwas mit ihrer Familie

ist die Anzahl sehr guter Freunde



Privatsphäre: **ist eine Option auf Facebook**

Kommunikationsmittel: **SMS, Social Media, Instant Messengers**



80% chatten in sozialen Netzwerken

67%

nutzen Web 2.0 (Facebook) als Informationsquelle

25%

der Jugendlichen spielen allein Online-Games

Arbeitszeiten: **immer online**



So tickt die Generation Internet

Alles ist neu? Nicht alles, aber einige wichtige Veränderungen sollten Erwachsene kennen.

- > **Generationenwechsel**
Jugendliche nutzen das Internet ganz anders als Erwachsene. Sie posten oft voreilig Informationen, die Erwachsene nicht ins Internet stellen würden.
- > **Es braucht keine Fachkenntnisse mehr**
Jeder kann mitmachen; und die meisten Jugendlichen tun das auch. Zudem surfen sie nicht nur mit dem PC im Internet, sondern auch mit dem Handy.
- > **Wahrheit ist relativ**
Das Internet kennt keine Zensur. Jeder kann Informationen ins Netz stellen, wie es ihm gefällt. Deshalb gilt: Inhalte kritisch würdigen und hinterfragen. Was ist wahr, was nicht? Was glaube ich, was nicht?
- > **Privatheit neu definieren**
Unter Jugendlichen herrscht heute ein digitaler Exhibitionismus. Deshalb ist es wichtig, dass Eltern mit ihren Kindern die Fragen diskutieren: Was von mir ist öffentlich, was privat?
- > **Das Internet vergisst nie**
Was einmal online war, kann man kaum mehr löschen. Es gilt also, gut zu überlegen: Was stelle ich online und was nicht? Von Anfang an.
- > **Freundschaftsbegriff hat sich verändert**
Als Freunde bezeichnen Jugendliche sowohl virtuelle Bekanntschaften wie auch reale Bezugspersonen. Sie verwenden also für unterschiedliche Qualitäten denselben Begriff.



Einblicke ins Pilotprojekt «iPod touch im Unterricht»

Thierry Maire vom Gymnase intercantonal de la Broye.



Halten wir *Schritt?*

So beeinflussen digitale Medien unsere Kommunikation, die Schule, die Arbeit und die Rolle von Eltern und Pädagogen.

Roc, drei Jahre alt, liebt das Klavier. Und am liebsten malträtiert er möglichst viele Tasten auf einmal – mit dem Unterarm oder mit den Fäusten gar. So richtig laut. Dann lauscht er, lacht und sagt: «Klavier macht Lärm!»

Erstaunlich viele Menschen bewegen sich auf einer ähnlichen Erkenntnis-ebene, wenn es um die sozialen Auswirkungen von Technik geht: Das Klavier macht den Krach, das Motorrad den Unfall und der Computer das Problem. Dabei verursacht in Wirklichkeit ja nicht das Klavier den Lärm, sondern der kleine Roc, ohne den das Instrument einfach still bliebe.

Besonders wenn sich eine Technologie gerade erst verbreitet, überwältigt sie Zeitgenossen oft so sehr, dass sie ihr gewaltige Wirkungen zutrauen. Digitale Medien wie Facebook, Netlog, MySpace oder Twitter bildeten da keine Ausnahme. Internet-Netzwerke sollten angeblich ihre Nutzer in bildungsfeindliche und kritikunfähige Konsumenten verwandeln, deren

Aufmerksamkeitsspanne sich nur noch in Millisekunden angeben lässt. Allein, so einfach ist es nicht. Wie beim Klavier kommt es darauf an, wer die Netzwerke benutzt und zu welchem Zweck. Denn nicht das Internet ist das Problem, sondern der Umgang damit.

Stunde um Stunde

Junge Menschen verbringen viel Zeit im Netz: Schweizer Mädchen und Jungen zwischen 12 und 19 Jahren surfen an Wochentagen durchschnittlich zwei Stunden durchs Internet, an Wochenendtagen gar drei Stunden. So lautet das Ergebnis der JAMES-Studie, die von Forschern der Zürcher Hochschule für Angewandte Wissenschaften, der Uni Genf und der Uni der italienischen Schweiz durchgeführt wurde. Die Studie zeigt noch weitere Details: 66 Prozent der Heranwachsenden nutzen ihren Computer zuhause täglich oder mehrmals pro Woche, um Arbeiten für Schule und Lehrstelle zu erledigen. 89 Prozent nutzen Internetdienste

«Computer, Internet und Handy prägen unseren Alltag: Wir sind überall zuhause, tragen die Welt in der Tasche, sind rund um die Uhr vernetzt. Dies verändert unser Leben, die Art und Weise, wie wir lieben und Freundschaften pflegen; wie wir kommunizieren, arbeiten und unsere Gesellschaft organisieren.»

Detlef Vögeli, Stapferhaus Lenzburg

täglich oder mehrmals pro Woche, aber nur 75 Prozent den Fernseher. Und was tun sie im Internet? Nach eigenen Aussagen lernen sie mit ihm und suchen mit Google, Facebook und Wikipedia nach Informationen; sie lesen Blogs und Nachrichtenportale. Sie informieren sich über Events und hören Podcasts. Und sie orientieren sich mit den digitalen Medien – 61 Prozent hören täglich oder mehrmals pro Woche Musik im Internet, 41 Prozent sehen sich Videos an, 55 Prozent stöbern in sozialen Netzwerken und 51 Prozent surfen einfach mal drauflos.

Kinder unserer Zeit

Viele Eltern stehen dem arglosen Austausch im Internet eher kritisch gegenüber. Sie empfinden es als aufwendig, mit der neuen Technologie Schritt zu halten. Denn die neue Zeit bringt neue Herausforderungen: Immer und überall verfügbare Informationen wollen auch sinnvoll, effektiv und produktiv verarbeitet werden. Bereits heute arbeiten in der Schweiz 38 Prozent der Büroangestellten von unterwegs – während über der Hälfte ihrer Arbeitszeit; 79 Prozent der arbeitenden Schweizer sind Büroangestellte. Das wird uns die nächsten Jahre weiter fordern – einzelne Menschen, aber auch Unternehmen, die ihre Mitarbeitenden nicht in einem Zustand der Jederzeit-Erreichbarkeit halten können.

«Der Schlüssel zu einem sinnvollen Umgang mit den vielen Informationen und Reizen ist die Fähigkeit einer selbstkontrollierten Nutzung. Wer sich selbst kontrollieren kann, sich nicht treiben lässt von zufälligen Reizen, der wird profitieren von den digitalen Medien.»

Prof. Lutz Jäncke, Leiter Lehrstuhl für Neuropsychologie, Universität Zürich

Medienerziehung ist kein Kinderspiel

Der Laptop war die erste Revolution weg von den Fesseln des festen Arbeitsplatzes, aber erst die nachwachsende Generation wird in den vollen Genuss des ungebundenen Arbeitens kommen: Sie werden Diskussionen mit Vorgesetzten über SMS abwickeln, Kollegen und Konkurrenten am Laptop wie in einem Videospiel im Auge behalten und Projektdetails auf einem Tablet im Café abrufen. Das kennen sie aus dem Effeff, aus ihrem Schulalltag. Und rüsten sich so schon heute für die Zukunft.



Zusammenhänge zwischen Gehirn und Einsatz digitaler Medien

Lutz Jäncke

Kinder wachsen ganz selbstverständlich mit einem breiten Medien-Ensemble auf. Deshalb sind sie ihren Eltern in der Bedienung der Medien oft ein Stück voraus. Was ihnen aber fehlt, ist die mediengerechte soziale Kompetenz. Sie wissen zwar bestens, wie Facebook funktioniert – können aber nicht einschätzen, welche Informationen man besser nicht veröffentlicht. Das wissen Erwachsene. Und darum ist es wichtig, dass Eltern die relevanten Aspekte der digitalen Medien kennen und ihre Kinder im Netz begleiten. Eltern sind gefordert: Sie sind nicht mehr die Wissenden, die vermitteln; im Zentrum steht neu der Lernprozess an sich. Damit kommt Eltern und Lehrern gleichzeitig die Aufgabe zu, Kinder und Jugendliche auf das Leben in einer durch und durch von Medien geprägten Gesellschaft vorzubereiten.

Medienerziehung ist nicht konfliktfrei. Aber unterschiedliche Meinungen und Wünsche sind Chancen für offene Gespräche über Medien in der Familie und darüber hinaus. Wenn Eltern und Kinder diese Chancen kreativ nutzen, erfüllen die Medien ihren eigentlichen Zweck: Mittel für die Kommunikation zu sein.

«Eltern und Lehrpersonen fungieren weniger als Wissensvermittler und vermehrt als Coach und Lernbegleiter. Die traditionelle Hierarchie zwischen den Lehrpersonen als Wissenden und den Lernenden als Unwissenden zeigt Auflösungserscheinungen. Beide sind Suchende und Konstruierende.»

Prof. Dominik Petko, Leiter Institut für Medien und Schule, PH Zentralschweiz, Schwyz



Warenkorb von Cyberkriminellen

Hunderttausende Computernutzer werden täglich angegriffen – Trojaner, Würmer oder Phishing-Mails versuchen, in die Anwendernetze einzufallen. Letztes Jahr überstiegen die Umsätze der Online-Kriminalität erstmals diejenigen der Drogenkriminalität. Denn Daten sind bares Geld wert, wie die Preise auf dem Schwarzmarkt eindrücklich zeigen.

Daten	Preis
Zugang zu E-Mail-Konto	18 \$
E-Mail-Adresse	bis 1 \$
Volle Identität	3–20 \$
Gültige Kreditkarte mit Sicherheitscode (CVV)	bis 100 \$
Hacker-Software	5–20 \$ pro Monat
Botnetz mieten	100 \$ pro Tag
Schädliche Software	2–5 \$
Spam-Mailserver	1–5 \$

Die Realität

Die nationalen Koordinationsstelle zur Bekämpfung der Internet-Kriminalität (KOBik) ist die Anlaufstelle für Personen, die verdächtige Internetinhalte melden möchten. Jedes Jahr gehen 6000 bis 7000 Anzeigen ein, die sich für das Jahr 2010 wie folgt aufteilen lassen:

- > **Austausch von illegalem Material**
Am häufigsten wurde harte Pornografie gemeldet, darunter auch Kinderpornographie, die 26,3 Prozent aller Anzeigen ausmachte. Hinzu kamen Anzeigen zu Extremismus, Rassismus und Gewaltdarstellungen.
- > **Betrugsfälle, Spam und Cybercrime**
6,2 Prozent aller Anzeigen drehten sich um Betrug. Wirtschaftsdelikte machten 5,6 Prozent der Anzeigen aus, dazu gehörten etwa Phishing und Spam. Und Cybercrime im engeren Sinn betrafen 1,4 Prozent der gemeldeten Fälle. Darunter: Datenbeschädigung, unbefugtes Eindringen in Computersysteme und betrügerische Nutzung eines Rechners.
- > **Cybermobbing**
Die Anzeigen zu Cybermobbing machten 1,1 Prozent aller Fälle aus, sie teilten sich auf in «Ehrverletzung und Verleumdung» und «Drohung, Nötigung, Erpressung».

Im Theaterstück «Cyberlehrling» denunzieren zwei Mädchen einen Kollegen im Internet und können die Lawine, die sie lostreten, nicht mehr stoppen. «enter» spricht mit zwei Darstellerinnen sowie dem Lehrer und Autor.

Goethes «Zauberlehrling» im Web

Von links nach rechts: Achim Lück, Vivien, Laura



Der «Cyberlehrling»

Dieses moderne Theaterstück beschäftigt sich mit Cybermobbing, angelehnt an Goethes «Zauberlehrling».

Wie seid ihr auf die Idee gekommen, aus Goethes «Zauberlehrling» einen «Cyberlehrling» zu gestalten?

Laura: Weil Cybermobbing ein sehr aktuelles Thema ist. Man hört's immer und überall.

Vivien: Ich weiss von einer guten Kollegin, dass sie ab und zu gemobbt wird. Es werden einfach dumme Sprüche über sie gemacht im Internet. Sie beachtet das nicht gross. Sie löscht die Kommentare einfach gleich wieder. Und sie spricht mit ihrer Mutter darüber. Auch mir erzählt sie es immer wieder.

Sprechen wir über das Stück: Welche Rolle hattest du da?

Vivien: Ich hatte die Rolle der Steffi, die Rolle einer Bösen, die Daniel mobbte. Das tat ich, weil er mir eigentlich gefiel und ich es nicht mochte, dass er mit Chiara flirtete.

Und du warst eine, die mitmacht?

Laura: Ja, Steffi und ihre beste Kollegin haben angefangen. Wenn man sieht und merkt, der andere ist ein Loser, ein Aussenseiter, dann macht man mit. Es haben auch immer mehr mitgemacht. Das ist so bei Cybermobbing. Wenn einer beginnt, machen viele mit. Denn wenn man da nicht dabei ist, wird man selber zum Loser.

Haben Sie Cybermobbing an Ihrer Schule schon erlebt, Herr Lück?

Lück: Ja, ich hatte schon Schüler, die gemobbt wurden. Nicht offensichtlich in der Klasse, sondern hintenherum via Facebook.

Wie kam es ans Licht?

Lück: Die Eltern kamen auf mich zu. Da musste ich als Klassenlehrer eingreifen und es thematisieren. Das Opfer erhielt dann die Gelegenheit, der Klasse zu erzählen, wie es sich fühlte, und daraus entstand eine Diskussion. Erst da realisierten die Täter, was sie angerichtet hatten. Denn die meisten fanden es einfach lustig. Die Kommentare fanden sie «easy». Fanden: Das kann man ja einfach wieder löschen, ist doch nicht so schlimm.

Wie sieht der Prozess in der Schule eigentlich aus, wenn so etwas passiert?

Lück: Der korrekte Weg ist: vom Klassenlehrer zum Schulsozialarbeiter zur Schulleitung. Die Vertrauensperson sollte die Schulsozialarbeiterin sein. Denn sie untersteht der Schweigepflicht, deshalb kommt bei ihr meist mehr zutage. Ein Lehrer ist befangen, weil er die Schüler benotet.

Wann sollen Eltern das Thema mit ihren Kindern aufgreifen?

Laura: Von Anfang an, wenn man noch leichtgläubig ist. Damit man weiss, was man darf und was nicht. Man soll mit den Kindern auch diskutieren, wie sie auf Kommentare reagieren sollen wie: «Du bist fett. Du bist megahässlich.» Eltern sollen ihren Kindern vermitteln: Melde es dem Lehrer. Und: Du kannst immer mit uns sprechen.

Wollen das Jugendliche denn hören?

Laura: Eltern sollten sich einmischen. Auch wenn wir das sicher nicht cool finden.

Eltern müssen sich einmischen

Was geht in Jugendlichen vor, wenn sie im Internet gemobbt werden? Welche Hilfe brauchen sie?

Ein Opfer fühlt sich überrumpelt, überrascht und weiss nicht, wie es so weit kommen konnte. Wieso plötzlich alle gegen es sind – sogar seine Freunde. Täter und Mitläufer begreifen es meist ebenso wenig. Mobbingopfer fühlen sich verraten, haben Angst, schämen sich. Im Internet bleiben die Beleidigungen zudem oft haften.

«Die Schmähungen sind wie ein Tattoo.»

Urs Gasser, Berkman Center for Internet & Society

Aus eigener Kraft können sich Mobbingopfer meist nicht befreien. Cybermobbing unter Jugendlichen verlangt deshalb nach Erwachsenen mit Mut. Menschen, die sich einmischen und alle Beteiligten unterstützen: Opfer, Täter und auch Mitläufer. Jugendliche müssen erleben, dass sich Erwachsene erfolgreich bemühen, die zerstörten Beziehungen zu flicken. Dabei geht es nicht allein darum, die Täter zu verfolgen, sondern vor allem darum, Verhaltens-

muster aufzudecken und zu begreifen sowie Bewältigungsstrategien zu entwickeln.

In seiner Entwicklung erlebt jeder Mensch unterschiedliche Konflikte. Erfahrungen darin, wie man Konflikte löst, festigen im Gehirn das Verständnis für konstruktives Handeln. Konstruktiv gelöste Konflikte dienen in Zukunft also als Lösungsmuster. Überall dort, wo Erwachsene gemeinsam mit betroffenen Jugendlichen die vernichtenden Vorgänge bearbeiten, festigen sich durch die gemeinsamen Lösungsversuche neue Verstehens- und Handlungsmuster. Diese tragen letztendlich zu einer langfristigen und nachhaltigen Lösung bei.



Cybermobbing in Stufen

Cybermobbing bezeichnet unterschiedliche Ausprägungen von Mobbing mithilfe digitaler Medien. Mehr dazu online.



Erkenntnisse zu Cybermobbing

Eveline Hipeli Müller, wissenschaftliche Mitarbeiterin am Schweizerischen Institut für Kinder- und Jugendmedien und an der Zürcher Hochschule für angewandte Wissenschaften.

Franz Eidenbenz
Psychologe und Experte für Fragen zu digitalen Medien



Sprechen Sie mit Ihrem Kind über Cybermobbing

Beugen Sie vor

Schauen Sie mit Ihrem Kind zum Beispiel den Kurzfilm «Let's Fight it Together» an (direkter Link unter swisscom.ch/enter) und sprechen Sie darüber: «Was sind deine Eindrücke? Wie fühlen sich die Akteure der Geschichte? Wie würdest du dich in den verschiedenen Rollen fühlen?»

Oder: Setzen Sie sich mit Ihrem Kind vor den Computer und recherchieren Sie zusammen zum Thema Cybermobbing. Interessieren Sie sich für die Meinung Ihres Kindes zu den verschiedenen Hilfsangeboten für Jugendliche und Eltern: «Was denkst du, würde dir in einer solchen Situation helfen?» Und: «Was würdest du dir von mir als Mutter, als Vater wünschen?»

Seien Sie aufmerksam

Cybermobbing läuft oft verdeckt ab; dennoch gibt es Merkmale, die darauf hinweisen, dass Ihr Kind Opfer sein könnte: Wirkt es bedrückt, zurückgezogen, verletzt, wütend? Fühlt es sich ausgeschlossen? Hat es Angst, zur Schule zu gehen? Vermeidet es Ausflüge, Schulreisen, Lager? Melden sich kaum mehr Schulkameraden?

Hören Sie zu

Schaffen Sie eine ungestörte Atmosphäre und suchen Sie das Gespräch. Die Frage «Kennst du jemanden, der Cybermobbing erlebt hat?» kann ein guter Einstieg sein.

Sprechen Sie das veränderte Verhalten an und äussern Sie Ihre Besorgnis: «Ich erlebe dich als zurückgezogen und in dich gekehrt. Mir ist aufgefallen, dass du kaum mehr Freunde triffst. Das bereitet mir Sorgen. Was bedrückt dich?»

Sozial vernetzt? *Sicher!*

84 Prozent aller Jugendlichen haben ein eigenes Profil in einem sozialen Netzwerk – so auch Silvia und Sherin. Sie haben sich zuerst ungeschützt darin bewegt, dann geschützt. Die zwei Schwestern erzählen ihre Erfahrungen.



Sherin (links) und Silvia

Sherin (17)

Ich verwende heute vor allem Facebook. Da habe ich zwei Profile – eines mit meinem Namen und eines mit meinem Spitznamen. Beim ersten Profil hatte ich viel zu viele Freunde. Denn am Anfang habe ich einfach alle Freundschaftsanfragen angenommen. Das wurde mir dann zu viel und ich habe ein neues Profil eröffnet und es stärker personalisiert.

Meine Eltern interessieren sich nicht so fürs Internet. Ausser einmal: Ich hatte Mist gebaut auf MSN. Eine Kollegin und ich hatten so richtig Streit und uns schriftlich heftig beschimpft. Das hat sie alles gespeichert. Was man einmal ins Netz stellt, können andere verwerthen, darüber hat man keine Kontrolle. Das musste ich schmerzlich lernen. Schliesslich ging dann die Mutter meiner Kollegin mit den ausgedruckten Beschimpfungen zu meiner Mutter. Und ich musste mich rechtfertigen.

Wenn ich selber Kinder hätte, würde ich ihnen zeigen, welches die positiven und die negativen Seiten von sozialen Netzwerken sind. Aufpassen muss man vor allem bei den Bildern. Die sind nämlich öffentlich. Das heisst: Jemand kann sie anschauen und speichern. Oder gar verändern, wieder speichern und selber irgendwo veröffentlichen. Da hat man null Kontrolle.

Und dann ist da auch die Zeit, die man online verbringt. Ich habe eine Schulkollegin, die mit dem Handy nonstop online ist. In der Pause ist sie dann an zwei Orten gleichzeitig – auf Facebook mit dem Handy und bei uns am Plaudern. Ihr Profil ist quasi ihr treuer Begleiter. Meine beiden besten Kolleginnen haben beispielsweise kein Facebook-Profil. Wir treffen uns regelmässig, das finde ich cool.

Überhaupt: Der Begriff «Freunde» ist mir auf Facebook zu persönlich. Teil-

weise bin ich mit Leuten «befreundet», die ich gar nicht richtig kenne. Manchmal kommt es vor, dass ich solchen «Freunden» auf der Strasse begegne – und die grüssen dann gar nicht. Also meine Kollegen sind mir näher.

Silvia (21)

Ich habe ein Facebook-Konto. Aber ich habe mein Profil so eingestellt, dass man mich mit «Suchen» nicht findet. Einzig Freunde meiner Freunde finden mich und sonst entscheide ich, wen ich einlade. Das kam so: Ich war im Ausland und habe viele Bilder auf mein Profil geladen. Und da wollte ich nicht mehr, dass jeder alles sieht. Ich wollte mehr Privatsphäre. Deshalb habe ich zuerst mein Profil ausgemistet und dann die Sicherheitseinstellungen angepasst. Ich habe unterschiedliche Gruppen gebildet und entscheide so, wer meine Bilder ansehen darf.

Ich miste regelmässig aus. Etwa jedes halbe Jahr. Und alle, mit denen ich ein Jahr lang keinen Kontakt mehr hatte, lösche ich dann. Das bringt's ja nicht, die zu sammeln. Zudem habe ich schon mindestens zweimal mein Profil deaktiviert. Das erste Mal, als ich mich beworben habe. Denn ich wollte nicht, dass irgendjemand etwas über mich findet. Aber irgendwo schlummern deine Daten noch und das war mir dann noch unheimlicher. Da habe ich das Profil wieder aktiviert.

Ja und dann sind da noch all die Pendingen, die dich angefragt haben, ob du mit ihnen befreundet sein willst.

Und du denkst: Soll ich die jetzt akzeptieren? Wenn ich wahllos Leute akzeptiere, wird das total unübersichtlich. Das will ich nicht. Aber ich lehne sie auch nicht ab.

Ich schaue gern Ferienfotos meiner Kolleginnen an oder interessiere mich für die Empfehlungen meiner Kollegen, also ihre Links. Ich habe auch Freunde, die sind politisch sehr engagiert. Und von denen erfahre ich wichtige Hinweise meistens, bevor ich sie in der Zeitung lese. Der Informationsfluss ist schon hoch. Und wenn du nicht dabei wärst, würdest du verpassen, worüber alle gesprochen haben.



Sicheres Surfen in sozialen Netzwerken

- > In den Privatsphäre-Einstellungen festlegen, wer Profil und Fotos sehen darf – das sollten nur «Freunde» dürfen.
- > Daten, die nicht auf Facebook gehören: Postadresse, Telefonnummer und Schule.
- > Kontrollieren, welche Inhalte Suchmaschinen anzeigen: Google, Yasní oder 123people. Eigene Einstellungen wenn nötig einschränken.
- > Sich angemessen verhalten – Beleidigungen, allzu private Offenbarungen und verbale Ausfälle vermeiden: Das Web vergisst nichts!
- > Auch bei Links von Freunden achtsam bleiben und nur die anklicken, denen man absolut vertraut.



Daten schützen – aber wie?

Unsere Leitfäden zeigen, welche Einstellungen in den sozialen Netzwerken die persönlichen Daten schützen.



Herausforderungen in sozialen Netzwerken.

Myriam Caranzano-Maitre

Dr. med.
Myriam Caranzano-Maitre
Direktorin Kinderschutz-
Stiftung (ASPI)

Sprechen Sie mit Ihrem Kind über **soziale Netzwerke**

Beugen Sie vor

Würden Sie Ihr Kind allein eine Stadt entdecken lassen? Ohne Karte? Ohne es vor möglichen Gefahren zu warnen? Wohl kaum. Das Gleiche gilt fürs Internet.

Erklären Sie Ihrem Kind: Ich bin vielleicht technisch weniger versiert als du, dafür hilft mir meine Lebenserfahrung, Risiken besser zu erkennen. Etwa, ob eine Person in einem Chatroom wirklich die ist, welche sie vorgibt, zu sein.

Seien Sie vorsichtig

Auch wenn Ihr Kind beteuert, es brauche dies nicht, sprechen Sie mit ihm über Prävention und Schutz: «Würdest du dem erstbesten Fremden, der dich in einer fremden Stadt darum bittet, deine Handynummer geben und ein Bild von dir im Badeanzug? Tu das auch nicht im Internet. Bedenke: Alles, was du hier postest, ist offen zugänglich und kaum zu entfernen!»

Erinnern Sie sich an Ihre Jugend zurück. Daran, wie stark der Wunsch von Jugendlichen ist, einer Gruppe anzugehören und mit Gleichaltrigen zu kommunizieren. Das Bedürfnis ist geblieben, nicht aber die Art und Weise, es zu befriedigen: Junge Menschen chatten, nutzen das Internet und soziale Netzwerke. Diese Mittel gehören zu ihrer Zeit. Damit kommunizieren sie, finden neue Freunde.

Damit Ihr Kind diese Erfahrungen bewusst und sicher machen kann, ist es unerlässlich, dass Ihr Kind auch ausserhalb des Netzes Beziehungen und Freundschaften erlebt und dass die Familie ein Vorbild für respektvolle Kommunikation im Alltag ist. Die Bildung im Umgang mit den Medien beginnt also lange bevor Kinder sie nutzen.



Wortwechsel **Fallen im Netz**

Wie gehen Jugendliche zwischen 10 und 16 Jahren mit Fallen im Netz um? Was beschäftigt Eltern und was sagt das Recht? Natacha Robert aus Ardon, Stefan Ingold aus Bern und Rechtsanwalt Dr. Rolf Auf der Maur aus Zürich diskutieren mit «enter».



Natacha Robert hat eine Tochter (10) und einen Sohn (15), Stefan Ingold ist Vater eines Sohns (15)

Sie haben mit Ihren Kindern über Abofallen diskutiert. Das sind vermeintliche Gratisangebote, die zum Beispiel wie ein harmloses Gewinnspiel aussehen, später aber eine Rechnung von mehreren hundert Franken nach sich ziehen.

Stefan Ingold: Mein Sohn hatte bereits mit zehn ein Handy, da er einen weiten Schulweg hatte. Dafür habe ich verbindliche Regeln aufgestellt: Du darfst nie deinen Namen angeben, nie deine Handy-Nummer nennen und sicher auch nie die Kreditkartennummer deines Vaters. Daran hat er sich gehalten.

Natacha Robert: Im Netz habe ich über meinen älteren Sohn keine Kontrolle mehr. Trotzdem: Er ist sich sehr wohl bewusst, was heikel ist. Er bespricht solche Themen vor allem mit seinen Kollegen, darunter sind auch ältere, die mehr wissen. Das ist hilfreich, denn auf ihre Kollegen hören Jugendliche.

Wie sieht es rechtlich aus? Muss ein Jugendlicher, der in eine Abofalle tappt, dafür bezahlen?

Rolf Auf der Maur: Ist das Kind noch minderjährig, dann ist ein solches Geschäft durch den Erziehungsberechtigten genehmigungspflichtig. Eltern können sich also weigern, die Rechnung zu bezahlen. Mit einer Einschränkung: Auch ein Minderjähriger kann sich im Umfang seines Einkommens verpflichten – seines Lehrlingslohns oder Sackgelds also.

Wie sollen Eltern konkret reagieren, wenn sie eine Rechnung erhalten für eine offensichtliche Abofalle?

Rolf Auf der Maur: Sie müssen nicht bezahlen. Oft drohen Anbieter zwar aggressiv mit Betreibung. Davon darf man sich aber nicht beeindrucken lassen. Denn für eine Betreibung benötigt man einen sogenannten Rechtsöffnungstitel, beispielsweise eine schriftliche Schuldanererkennung.

Der Aufwand für eine Klageerhebung ist also meistens viel teurer als der geschuldete Betrag und der Kläger wäre erst noch in einer schlechten Position.

Was ist für Ihre Kinder digitaler Alltag, wovon Sie keine Ahnung haben?

Natacha Robert: Ich weiss zum Beispiel nicht, was Streaming ist. Und auch nicht, wo man Musik und Filme downloaden kann. Und ob man das darf!

Rolf Auf der Maur: Hat Ihr Sohn denn schon online Musik gekauft? Wüsste er überhaupt, wo?

Natacha Robert: Das weiss er und wir haben bis heute auch noch nie eine Rechnung erhalten. Denn er sucht die Gratisangebote, auf Youtube etwa. Für unsere jüngere Tochter richten wir Eltern jetzt Musik auf ihrem iPod ein, und die kaufen wir auf iTunes.

Stefan Ingold: Ich kenne Kids, die sagen: Wofür soll ich denn bezahlen? Das ist ja im Netz und da ist es frei. Ich erinnere mich an Limewire, diese Tauschbörse. Die funktionierte nach dem Prinzip «ich geb dir meins und hole deins». Da machten alle mit.

Rolf Auf der Maur: Herunterladen ist auch kein Problem, nur hochladen ist strafbar – nach Schweizer Recht.

Stefan Ingold: Das wäre dann aber ein Freipass, dass die Kids alles, was sie wollen, herunterladen können?

Rolf Auf der Maur: Das Schweizer Recht ist diesbezüglich grosszügig. Als Privatperson darf ich für den eigenen Gebrauch herunterladen – egal ob Musik, Film oder Bild.



Rolf Auf der Maur, spezialisiert auf rechtliche Aspekte des Internets

Natacha Robert: Das heisst also: Ich darf sehr wohl Musik runterladen und hören, solange ich das für mich allein tue?

Rolf Auf der Maur: Richtig, man darf die Musik nicht zur Verfügung stellen. Genau so funktionieren aber Sharing-Plattformen: Die Computer aller Nutzer sind verbunden und irgendwo steht ein Link-Server. Ich suche dann etwa «Bad Romance» von Lady Gaga. Die Applikation findet das auf dem Computer eines Nutzers und holt es da für mich ab. Dafür holt sich jemand anderes bei mir vielleicht ein Stück von Shakira ab – und dieser sogenannte Upload, dieses Verbreiten, das ist illegal.

Genau das wollen aber Jugendliche – Musik teilen.

Rolf Auf der Maur: CDs und MP3-Dateien darf man auch innerhalb der Familie und im engeren Freundeskreis grundsätzlich weitergeben und auch kopieren. Fürs Teilen im weiteren Freundeskreis gibt es mittlerweile Angebote, die es ermöglichen, Musik online legal und auch relativ günstig zu beziehen.

Zudem: Legale Plattformen garantieren, dass man ein authentisches File erstelt, eine echte Datei also. Ganz anders auf Filesharing-Plattformen – da kommt es häufig vor, dass Dateien mit einem Virus verseucht sind, den man dann auf sein Gerät lädt. Ein weiteres Problem ist, dass nicht immer drinsteckt, was draufsteht. Also etwa: Man will ein Stück von Lady Gaga herunterladen und stattdessen erhält man ein Pornofile.

Stefan Ingold: Es ist also wichtig, dass Jugendliche wissen, wo sie sicher und legal Musik erhalten.

Rolf Auf der Maur: Unbedingt. Eine neue Variante ist Streaming, das kommt gerade immer mehr auf. Streaming ist eine Möglichkeit, übers Web Inhalte zu konsumieren, ohne sie vollständig herunterzuladen. Dabei kann man sich Filme, Serien und Musik im Browser ansehen, muss diese Daten jedoch nicht speichern und auch nicht wie beim Filesharing anderen Nutzern zur Verfügung stellen. Das ist sicher und legal.

Natacha Robert: Wie funktioniert das denn genau?

Rolf Auf der Maur: Simfy etwa ist ein Musikcatalog mit rund elf Millionen

Songs, auf den die Nutzer des Dienstes unbegrenzt zugreifen können. Es ist auch möglich, Playlists anzulegen und untereinander zu teilen. Die Songs werden über eine einmal installierte Software im Streaming-Verfahren abgespielt. Man kann den Service kostenlos nutzen, muss dafür aber Einschränkungen in Kauf nehmen, wie Werbeeinblendungen oder maximale Hördauer. Mit einem Abo für circa zwölf Franken kann man alle Lieder ohne Einschränkungen abspielen.

Sind diese Angebote bekannt?

Stefan Ingold: Also bei Jugendlichen nicht; Streaming heisst für sie einfach Youtube. Da die Musikindustrie nicht offen kommuniziert, weiss man nicht, welche Optionen es gibt.

Rolf Auf der Maur: In der Schweiz werden solche Angebote noch wenig genutzt. Aber als Eltern sollte man seine Kinder eigentlich darauf hinweisen. Denn im Gegenzug kann man so seinen Kindern eher illegale Plattformen verbieten.



Stream me up

Erfahren Sie, welche legalen Angebote es im Internet gibt – für Musik, Filme und Bücher.

Alles, was Recht ist

Weitere Informationen zum Urheberrecht finden Sie online.

Chantal Billaud

Stv. Geschäftsleiterin,
Schweizerische Kriminalprävention (SKPPSC)



Sprechen Sie mit Ihrem Kind über

Fallen im Netz

Beugen Sie vor

Schauen Sie etwa mit Ihrem Kind den Film «Internet-Fallen – lassen Sie sich nicht abzocken» an (direkter Link unter swisscom.ch/enter). Besprechen Sie anschliessend die genannten Fallen: «Was hast du dazu schon gehört? Gelesen? Gesehen?»

Wo gratis draufsteht, ist nicht gratis drin

Auch im Internet ist selten etwas kostenlos. Weisen Sie Ihr Kind darauf hin, bei «Gratis»-Angeboten stets missverständlich zu sein; ganz besonders, wenn es sich mit persönlichen Angaben registrieren muss. Also etwa mit Namen, Vornamen, Adresse, Telefonnummer. Wenn Sie das nächste Mal über ein verfängliches Pop-up stolpern, speichern Sie es als Bild ab und besprechen Sie es mit Ihrem Kind. «Würdest du auf einen solchen Hinweis im Internet reagieren? Wie? Warum? Was fällt dir auf?»

Bitten Sie Ihr Kind auch, das «Kleingedruckte» zu lesen, und lassen Sie sich erklären, was da genau steht. Entstehen Kosten? Wie viele? Kann man aussteigen?

Musik in den Ohren

Bitten Sie Ihr Kind, Ihnen zu zeigen, welche Musiktitel es im Internet entdeckt hat. Lassen Sie sich die Website erklären. Hören Sie aufmerksam zu, ohne zu werten. Suchen Sie nun zusammen die allgemeinen Geschäftsbedingungen (AGB). Lesen Sie diese zusammen genau durch. Und diskutieren Sie, was hier steht.

Fragen Sie Ihr Kind: «Hast du auch schon Musik heruntergeladen? Was hast du dafür bezahlt? Hast du auch schon Musik hochgeladen?» Informieren Sie sich gemeinsam mit Ihrem Kind über Urheberrechte und legale Angebote im Netz.

Smarte Nutzer für smarte Phones

Für ihr Leben in den digitalen Medien nutzen Jugendliche zunehmend Smartphones. Diese kleinen Computer können immer mehr – je mehr sie aber können, desto verwundbarer werden sie. Wer sich und seine Kinder schützen will, sollte ein gesundes Misstrauen entwickeln.

Auf Smartphones und Tablets lassen sich genau wie auf einem PC oder einem Notebook unterschiedliche Programme installieren. Anders als PCs sind diese mobilen Geräte oft permanent mit dem Internet verbunden und werden dadurch auch für Hacker immer interessanter. Wer sich nicht vorsieht, installiert möglicherweise ein betrügerisches App. So gibt es Programme, die sich als Spiele ausgeben, tatsächlich aber im Hintergrund unbemerkt SMS-Kurznachrichten an eine Premiumnummer versenden – für teures Geld. Noch sind solche Betrugs-Apps die Ausnahme. Aber früh stellt sich darauf ein, wer gewappnet sein will.

Bei Apps ist grundsätzlich gesundes Misstrauen angebracht. Denn oft fordern sie dazu auf, Zugriffsrechte zu akzeptieren. In diesen Zugriffsrechten kann stehen, dass ein App auf persönliche Daten wie Adress- und Telefonbuch, E-Mail-Konto etc. zugreifen oder gar den aktuellen Standort orten darf. Wofür diese Daten verwendet werden, ist oft nicht zu erkennen. Vielleicht werden sie an Dritte verkauft oder für personalisierte Werbung genutzt. Deshalb gilt es, vor dem Zustimmung genau zu prüfen, welche Rechte für die Nutzung eines Apps wirklich erforderlich sind. Und fragwürdige Zugriffsrechte abzulehnen und auf die Nutzung dieser Apps zu verzichten.

Mobile Bedrohung

Immer online, den gesamten E-Mail-Verkehr in der Hosentasche, Adressdaten oder Musikstücke austauschen –

einfach und unabhängig mit Bluetooth oder WLAN. Das erleichtert die Kommunikation. Einerseits. Andererseits eröffnen sich Angreifern eine Vielzahl von Wegen. Smartphone-Viren, die beispielsweise Bluetooth nutzen, können andere Geräte im Umkreis von zehn bis dreissig Metern infizieren, wenn sie bei ihnen einen offenen Kanal entdecken. Deshalb: Bluetooth nach Gebrauch ausschalten. Und auch die WLAN-Verbindung nicht immer eingeschaltet lassen.

In fremden Händen

Die weitaus häufigste und grösste Gefahr droht jedoch bei Verlust oder Diebstahl, denn mehr als die Hälfte der Nutzer von mobilen Geräten vergessen, diese ausreichend mit Passwörtern (Display- oder Geräteschutz) vor Zugriff durch Fremde zu schützen. War es früher damit getan, die SIM-Karte zu sperren, genügt dies bei Smartphones längst nicht mehr. Hier sind alle Zugangsdaten für E-Mail, soziale Netzwerke und Apps hinterlegt, die sich bei Aufruf in der Regel direkt nutzen lassen. Ein Dieb hält damit einen Passepartout zu allen Daten in der Hand; konfigurierte WLANs öffnen einem Angreifer zudem den Zugang ins heimische Netz. Um das zu vermeiden, sollte das Gerät grundsätzlich durch den vorinstallierten Zugriffsschutz gesichert werden. Einen zusätzlichen Schutz bietet die Notbremse aus der Ferne: Über ein anderes mobiles Gerät oder ein Webportal lassen sich neue Modelle bereits fernsperren oder löschen auf Befehl gar alle Daten.



Ihr Rechner ist Ihr Tresor, behandeln Sie ihn auch so

- > **Passwörter:** Verwenden Sie unterschiedliche Passwörter – für jede Anwendung. Und wechseln Sie diese regelmässig. So begrenzen Sie im Ernstfall den Schaden.
- > **E-Mail-Adressen:** Arbeiten Sie mit mehreren E-Mail-Adressen: einer Hauptadresse für wichtige E-Mails, einer Zweitadresse für Anmeldungen bei Facebook etc.
- > **Skeptisch bleiben:** Im Internet ist Zurückhaltung angebracht. Wenn Sie Ihre Daten gar nicht erst mitteilen, bieten Sie potenziellen Angreifern weniger Missbrauchsmöglichkeiten. Daten wie Adresse oder Telefonnummer sollten Ihre Kinder nur nach Rücksprache mit Ihnen eingeben.
- > **Up to date:** Halten Sie Ihre Software – vor allem den Webbrowser (Firefox, Internet Explorer, Opera, Safari etc.) und das Betriebssystem – immer auf dem neusten Stand. Laden Sie insbesondere angebotene Sicherheits-Updates regelmässig herunter. So schliessen Sie Sicherheitslücken.

Sind Ihre Passwörter sicher?

Wir wissen es: Ein sicheres Passwort besteht nicht aus gewöhnlichen Wörtern; es ist zehn- und mehrstellig, auch wenn nach einem sechsstelligen Passwort gefragt wird; und es besteht aus einem Mix aus Buchstaben, Ziffern und Sonderzeichen. Trotzdem handeln wir oft nicht nach diesen Vorgaben. Dabei sollten wir. Denn es gibt heute spezialisierte Programme, die Passwörter knacken. Ihre Rechenkapazität ist gewaltig: Ein schneller Computer prüft heute pro Sekunde mehr als eine Million Passwortvarianten; Wörterbücher in Dutzenden von Sprachen sind dafür hinterlegt. Die meisten einfacheren Passwörter sind so in null Komma nichts entlarvt.



Passwortcheck

Frischen Sie Ihre Kenntnisse über sichere Passwörter auf und finden Sie pfiffige Passworthilfen.

Nicolas Martignoni

Pädagogische Hochschule
Freiburg, Leiter Fachstelle
fri-tic



Sprechen Sie mit Ihrem Kind über Handy und Sicherheit

Ihr Kind muss Ihnen vertrauen. Nur so können Sie möglichen Sicherheitsproblemen vorbeugen, wenn es sein Handy benutzt.

Vertraut Ihnen Ihr Kind, wendet es sich auch an Sie, wenn etwas Ungewöhnliches geschieht. Sonst traut sich Ihr Kind vielleicht nicht, Ihnen von einer problematischen Situation zu erzählen, und Sie können nicht einschreiten.

Wie aber halten Sie das Gespräch mit Ihrem Kind aufrecht? Zeigen Sie ihm, dass Sie sich dafür interessieren, was es mit seinem Gerät macht. Aber Achtung: Seien Sie nicht aufdringlich, vermeiden Sie den Eindruck, Sie möchten in die Privatsphäre Ihres Kindes eindringen. Kinder brauchen auch ihre Geheimnisse. Respektieren Sie diese Privatsphäre, wird Ihnen Vertrauen geschenkt.

Profitieren Sie von den hervorragenden Kenntnissen Ihres Kindes in Sachen Handy: Fragen Sie es um Rat, lassen Sie es einmal Ihr Lehrer sein. Spielen Sie mit ihm auf dem Gerät sein Lieblingsspiel: Ihr Kind wird Sie schlagen und stolz darauf sein. Bei dieser Gelegenheit zeigen Sie ihm auch gleich, dass auch Sie Ihr Telefon gelegentlich zur Unterhaltung nutzen.

Natürlich bedeutet das nicht, dass Ihr Kind mit seinem Gerät alles machen darf: Sie legen die Nutzungsregeln fest und diese werden auch eingehalten. Machen Sie doch einfach selbst den Anfang und dienen Sie als Vorbild: Benutzen Sie Ihr Handy nicht bei Tisch oder während eines Gesprächs.

Wenn Sie mit Ihrem Kind im Gespräch bleiben, können Sie ihm dabei helfen, mit den modernen Technologien aufzuwachsen, und es gleichzeitig auf die Sicherheitsprobleme aufmerksam machen.

Schützen Sie Ihre Geräte

Die Kombination von Medienkompetenz und technischen Hilfsmitteln ist die beste Basis für einen verantwortungsvollen Medienkonsum. Dieter Mosimann fasst zusammen, was man unbedingt haben muss. Bei Swisscom gestaltet er Kundenerlebnisse rund um Sicherheitslösungen.



Liebe Leserinnen und Leser von *enter*
Hier sind meine Tipps an Sie:

Schutz vor Cyberkriminellen

Cyberkriminelle versuchen oft, sich in das Betriebssystem eines Computers einzunisten. Mittels sogenannter Rootkits übernehmen sie dann die zentrale Steuerung des Computers. Um zu verhindern, dass Rootkits auf den PC gelangen, gilt es, Massnahmen wie gegen andere Schadprogramme (Viren, Würmer etc.) anzuwenden. Dazu gehören eine Firewall, ein Browser-Schutz, ein Antivirenprogramm und eine Analyse der ablaufenden Prozesse im Computer. Eine umfassende Schutzsoftware enthält alle diese Komponenten.

Technische Sicherheitsvorkehrungen für PC und Handy

Für mobile Geräte sowie Netbooks und Desktop-Computer gilt eine dreistufige Formel für den Schutz gegen Cyberkriminelle:

- > den Zugang von Schadprogrammen auf das Gerät verhindern;
- > Schadprogramme erkennen und entfernen, wenn sie aufs Gerät gelangen;
- > Schaden begrenzen, wenn die Programme trotzdem auf dem Gerät ausgeführt werden.

PC schützen

Umfassende Schutzprogramme berücksichtigen alle drei Stufen. Kostenlose Schutzprogramme, etwa reine Antivirenprogramme, enthalten in der Regel nur eine dieser drei Schutzstufen. Installiert der Nutzer für alle drei Stufen Produkte von unterschiedlichen Herstellern, fehlt die Kommunikation unter den einzelnen Schutzprogrammen, um einen optimalen Schutz des Gerätes sicherzustellen.

Umfassende Schutzprogramme bieten zudem oft auch eine Elternkontrolle (Parental Control) für das Surfen der Kinder im Internet. Diese Elternkontrolle erlaubt es Eltern, die Surfzeiten ihres Kindes zu definieren und die Zugriffe auf bestimmte Inhalte im Internet zu beschränken.

Unerlässlich ist auch ein Back-up der wichtigsten Daten. Das bedeutet: Sichern Sie Ihre Daten regelmässig auch auf einem externen Datenträger, einem verbundenen PC oder in einer Cloud (Datenserver im Internet) eines Herstellers. Denn einerseits können gespeicherte



Daten auf Ihrem PC verloren gehen, gelöscht oder unlesbar gemacht werden. Andererseits könnten Cyberkriminelle Sie mit einem Schadprogramm erpressen, indem sie Ihre Daten auf dem PC verschlüsseln. Für die Freigabe der Daten verlangen sie dann Geld.

Mobile Geräte schützen

Schutzfunktionen für mobile Geräte befinden sich teilweise schon in den verschiedenen Betriebssystemen selbst. Die wichtigste Schutzfunktion ist der Geräteschutz durch ein Passwort, einen PIN oder bei einigen Modellen durch einen Mustercode (grafischer Sperrcode). Wichtig ist, dass der Nutzer entgegen der Bequemlichkeit ein möglichst starkes Passwort verwendet und die Zeiteinstellung für das Einsetzen der Gerätesperre bei Inaktivität kurz genug wählt. Weitere Funktionen, die teilweise bereits schon mit dem Betriebssystem mitgeliefert werden, sind etwa Back-up-Funktionen.

Schutzprogramme gegen Diebstahl, Phishing, verseuchte Webseiten, Webseiten mit Inhalten, welche nicht für Jugendliche geeignet sind, Antiviren-/Antispyware und Schutz gegen Hacker mittels Firewall werden von den bekannten Schutzprogrammerstellern wie etwa F-Secure angeboten.

Ihr Dieter Mosimann



Sicher ist sicher

Swisscom bietet umfassende Schutzprogramme für Computer und mobile Geräte, basierend auf den preisgekrönten Programmen von F-Secure. Eine Übersicht der gängigen Sicherheitsprogramme auf dem Markt finden Sie online.



Früh übt sich

Fachleute betonen immer wieder, wie wichtig es ist, vor allem mit Kindern, die kurz vor der Pubertät sind, ins Gespräch zu kommen – bevor digitale Medien eine immer wichtigere Rolle in ihrem Leben spielen. Eine Angebotsübersicht für alle Altersstufen.

4 bis 7 Jahre: spielend entdecken

Die Kinder werden neugierig. Sie finden Spiele und kurze Filme interessant. Besuchen Sie die Seiten zusammen mit Ihrem Kind. Hat es bereits mehrfach Ausflüge auf diese Websites mit Ihnen unternommen, kann es die Navigation allein bedienen. Legen Sie einen speziellen Lesezeichenordner an und speichern Sie hier beliebte Seiten.

lilibiggs.ch
jamadu.ch
wdrmaus.de/spielen
kindernetz.de/kribbeltz
netla.ch

8 bis 11 Jahre: spannende Inhalte

Die Vielfalt wird nun zunehmend interessant. Kinder erkunden spannende Inhalte, etwa über ihre Hobbys. Spielen bleibt beliebt; zusätzlich wird Kommunizieren mit Gleichaltrigen langsam ein Thema. Nun sind Sie als Eltern besonders gefragt. Suchen Sie zusammen geeignete Seiten und speichern Sie diese als Favoriten. Lassen Sie Ihr Kind am Anfang nicht allein. Denn: Die richtige Suche im Internet kennt es noch nicht. Helfen Sie ihm beim Auswählen von Suchbegriffen. Weisen Sie es auf Fallen hin, auf Gefahren. So lernt es den Umgang mit dem Medium. Richten Sie geeignete Filterprogramme ein. Wenn Ihr Kind kompetenter und verantwortungsbewusster wird, können Sie es auch mal eine kurze Zeit allein reisen lassen.

Onlinespiele zum sicheren Umgang mit dem Internet

internauten.de
netla.ch
labbe.de/mellvil

Suchmaschinen

blinde-kuh.de
fragfinn.de

Wissen

helles-koepfchen.de
kindernetz.de

Kreativität

minibooks.ch

Ab 12 Jahren: die weite Welt

Ihr Kind nutzt nun immer häufiger das gesamte Spektrum der digitalen Medien. Es schliesst virtuelle Kontakte, lädt Musik herunter, kopiert Filme. Die Zeit, die es online verbringt, nimmt zu. Technisch ist Ihnen Ihr Kind vielleicht schon überlegen. Bleiben Sie souverän – weder Angst noch Laisser-faire helfen Ihrem Kind. Vor allem: Bleiben Sie neugierig. Und nehmen Sie weiterhin an der Welt Ihres Kindes teil.

Videosammlung für mehr Sicherheit im Netz

klicksafe.de/spots

Datenschutz

netla.ch

Impressum

Herausgeberin	Swisscom AG
Redaktion	Swisscom AG, Bern, und Textkantine, Zürich
Copyright	© 2011 by Swisscom AG, Group Communications, Bern
Ausgabe	enter «Sicherheit», Herbst 2011
Druck	Stämpfli Publikationen AG, Bern
	Klimaneutral gedruckt auf 100% Recyclingpapier
Auflage	400 000 (d/f/i)

Alle Rechte vorbehalten. Ohne Genehmigung von Swisscom dürfen das Werk oder Teile davon weder reproduziert noch unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Bei der Zusammenstellung der Texte und Abbildungen wurde mit grösster Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Websites ändern sich ständig. Swisscom kann deshalb nicht für die Übereinstimmung der Zitate und Abbildungen mit den aktuellen Websites garantieren. Auch für fehlerhafte Angaben und deren Folgen kann keine Verantwortung oder Haftung übernommen werden.

Sprachliche Gleichstellung
 Personenbezeichnungen in der maskulinen Form schliessen auch die weibliche Form ein.

In eigener Sache: Jugendschutzkurse

Im Swisscom-Jugendschutzkurs lernen Eltern und Pädagogen die wichtigsten Anwendungen auf Handy und Internet live kennen und erfahren, wie sie Gefahren begegnen. Weiter im Angebot: ein Schülerkurs für die Oberstufe.

swisscom.ch/jugendschutzkurse



swisscom

 **Hallo Zukunft**

Unser Engagement
für Umwelt und Gesellschaft
www.swisscom.ch/hallozukunft

