Kinder / Jugendliche im Internet

US 2012

Wussten Sie, dass…

- *Nur 57% der Jugendlichen, die soziale Netzwerke wie Facebook benutzen, auch Massnahmen getroffen haben, ihre Privatsphäre zu schützen?*
- *29% der 12-19 Jährigen schon erlebt haben, dass Fotos oder Videos von ihnen ohne ihre Zustimmung ins Netz gestellt wurden?*
- *8% der Jugendlichen angeben, dass über sie schon Beleidigendes im Internet verbreitet wurde?*

Kinderschutz gegen Pornografie und Gewalt im Internet

Überall im Internet können Kinder und Jugendliche auf Inhalte stossen, die nicht für sie geeignet sind. Da blinken unverhofft nackte Frauen im Bildschirmfenster auf und leiten auf pornografische Seiten. Auf anderen Portalen sind Gewaltszenen in Videos festgehalten. Wie Sie Ihr Kind vor Pornografie und Gewalt im Internet schützen können, erfahren Sie hier.

Gegen Pornografie, Rechtsextremismus, Gewaltdarstellungen und Pädosexualität im Internet können Sie Ihre Kinder schützen. Zum einen sollten Sie Aufklärungsarbeit leisten. Konkret heisst das: Sprechen Sie mit Ihren Sprösslingen über gefährliche Inhalte, surfen Sie gemeinsam und erklären Sie, warum etwas unanständig oder illegal ist. Zum anderen kann Ihnen eine Kinderschutzsoftware helfen. Es gibt Filterprogramme, die Ihre Kinder von bestimmten Webseiten fernhält.

Aufklärungsarbeit leisten

Kinder und Jugendliche sollten mit gefährlichen Webseiten zu nicht alleine gelassen werden. Ist Ihr Kind auf diese Inhalte gestossen, so lassen Sie dies nicht unkommentiert stehen. Suchen Sie das Gespräch und bieten Sie an, Fragen zu beantworten. Oder geben Sie Ihrem Kind, falls das Miteinander-Sprechen schwer fällt, Links und Adressen von Beratungsstellen an.

Während Jugendliche untereinander oft sehr locker über Sex und ihre Erfahrungen reden können, haben sie Hemmungen, sich mit Fragen an Eltern zu wenden. In der Familie über Sex, Pornografie und Gewalt zu sprechen, ist wichtig, auch wenn es nicht leicht fallen mag. Wie man das am besten macht, erfahren Sie zum Beispiel in der Broschüre «Sexualerziehung bei Kleinkindern und Prävention von sexueller Gewalt». Die Stiftung Kinderschutz Schweiz hat sie für Eltern und Erziehende von Kindern zwischen 0 und 6 Jahren herausgegeben. Sie ist bei den Mütter- und Väterberatungen Ihrer Region, aber auch bei der Stiftung Kinderschutz Schweiz erhältlich.

Leben in digitalen Welten

Soziale Netzwerke und Netzgemeinschaften als Teil der sozialen Medien stehen hoch im Kurs. Auch Kinder und Jugendliche haben Spass daran, sich mit Freunden zu vernetzten, neue Freunde kennenzulernen und sich der Welt mitzuteilen. Der Einstieg in die virtuellen Welten beginnt häufig mit dem Anlegen eines persönlichen Profils – einer digitalen Identität.

In individuellen Profilen stellen sich Kinder und Jugendliche in sozialen Netzwerken in möglichst authentischer Weise – so wie man sich sieht oder von anderen gesehen werden will – dar, geben Auskunft in Bild und Wort über Alter, Geschlecht, Schule und Interessen und verknüpfen sich nach Lust und Laune mit anderen Internetnutzern in der ganzen Welt. Dabei üben sie die Auseinandersetzung mit sich selbst und mit anderen und eignen sich Kompetenzen in computerbasierter Kommunikation an – sie erstellen und leben ein Stück ihre digitale Identität.

Diese Aktivitäten leben davon, dass sie die Wirklichkeit widerspiegeln und damit die reale Vernetzung vieler Menschen ermöglichen. Die Kunst beim Anlegen eines persönlichen Profils besteht in der Gratwanderung zwischen der identifizierbaren Gestaltung der eigenen Identität und der Beachtung von Regeln zum Schutz der Privatsphäre. Dies ist eine grosse Herausforderung, wenn man davon ausgeht, dass diese Form der Selbstdarstellung ein wichtiger Bestandteil der Identitätsfindung von Heranwachsenden ist.

Risiken sozialer Netzwerke

Neben vielen Annehmlichkeiten birgt die neue Netzweltkultur auch Risiken. Im Fokus steht dabei die Frage nach dem Schutz der Persönlichkeit und der Privatsphäre. Wer viel in sozialen Netzwerken kommuniziert, wird sichtbar – und das schnell für die ganze Welt. Häufig geben Kinder und Jugendliche viele persönliche Informationen preis, da sie sich in sicherer Umgebung wähnen. Es werden Freundeslisten erstellt, zu denen scheinbar nur die Zugang haben, die man selbst als Freunde ausgewählt hat. Es werden Bilder, Videos und Texte ins Netz gestellt, ohne darüber nachzudenken, welche Folgen dies haben könnte.

Ausgestattet mit handfesten Regeln sollten Kinder und Jugendliche ausreichendes Wissen an die Hand bekommen, damit sie zu kompetenten und verantwortungsvollen Netzwerknutzern heranwachsen. Erst wenn sie sich der Gefährdungen bewusst werden, sind sie in der Lage, ihr eigenes Verhalten zu reflektieren.

Persönliche Daten und Fotografien

Weiter ist es sehr wichtig, dass die Profile in Sozialen Netzwerken und Communities geschützt werden und nicht öffentlich von jedem Internetnutzer einsehbar sind. Wie man sein Profil in einigen der beliebten Communities schützt, erfahren Sie hier.

Auch Fotos im Internet zu veröffentlichen, ist schnell und bequem. Die Verbreitung, Änderung oder Verwendung in anderen Kontexten ist jedoch ebenso leicht und kaum

zu verhindern. Kopien des Fotos können leicht an mehrere Orte wandern und vielleicht nie mehr gelöscht werden. Überlegen Sie es sich genau, bevor Sie persönliche Daten in Verbindung mit einem Foto bereitstellen.

Besonders unangenehm kann es für Jugendliche werden, welche auf Lehrstellensuche sind. Die meisten Arbeitgeber schicken den Namen des Kandidaten durch eine Suchmaschine im Internet. Werden dann Fotos von wilden Partys oder andere unangenehme Bilder gefunden, welche viele Jugendliche über Soziale Netzwerke ins Internet stellen, wirft das bestimmt kein gutes Licht auf den Kandidaten. Dasselbe gilt für Filme auf YouTube oder MyVideo.

Ebenso, wie es Ihr Kind zu schützen gilt, sollte Ihr Kind aber auch die Privatsphäre anderer respektieren und weder Fotos von anderen ohne Genehmigung ins Netz stellen, noch Verunglimpfungen veröffentlichen.

Finden Sie heraus, welche Informationen über Sie oder Ihre Kinder bereits im Internet verfügbar sind: Geben Sie Ihren Namen in eine Suchmaschine ein (z.B. Bing) und entscheiden Sie selbst, ob Sie mit dem Resultat einverstanden sind. Es ist zwar schwierig, bereits veröffentlichte Daten wieder zu löschen, aber nicht unmöglich. Kontaktieren Sie dazu die Urheber der Information, oder nötigenfalls die Systemadministratoren und Betreiber der betreffenden Homepage.

Die Eingabe von Profildaten

Um überhaupt ein Profil, beispielsweise bei Facebook, anlegen zu können, werden Sie gebeten, sich mit Ihrem richtigen Namen und Ihrer privaten E-Mailadresse zu registrieren. Auch viele anderen Websites fordern zu einer Registrierung auf oder zur Eingabe persönlicher Daten, wenn Sie Vergünstigungen erhalten möchten wie zum Beispiel Zugang zu einem Dienst, zur Teilnahme an einem Gewinnspiel, zu Gratisprodukten oder zur Teilnahme an einer Diskussion. Gewerbetreibende können die Kontaktdaten von Kindern und Jugendlichen für Marketingzwecke erfassen.

Nicht alle Betreiber einer Website wahren die Vertraulichkeit persönlicher Daten – auch wenn sie vom Datenschutzgesetz dazu verpflichtet wären. Legen Sie Ihren Kindern ans Herz, vorsichtig zu sein bei der Angabe persönlicher Daten.

Tipps zur Eingabe von Profildaten

- Treffen Sie Abmachungen mit Ihrem Kind
  Es ist hilfreich, Grundsätze für die Weitergabe von Daten im Internet und in sozialen Netzwerken zu vereinbaren. Wenn Sie Ihrem Kind erlauben, Informationen weiterzugeben, sollten Sie von der Vertrauenswürdigkeit der betreffenden Seite überzeugt sein.
- Überprüfen Sie die Datenschutzrichtlinien
  Prüfen Sie, ob die Site Datenschutzrichtlinien enthält. Darin sollten die Verwendung der persönlichen Daten, der Zeitraum und der Zweck ihrer Verwendung erläutert werden.

- Geben Sie nur obligatorische Informationen an
  Normalerweise müssen nur wenige Daten zwingend angegeben werden. Wenn Sie gefragt werden, ob Sie Direktmarketing zulassen, können Sie die Frage mit Nein beantworten. Wenn Sie aus Versehen eine Genehmigung erteilt haben, können Sie diese widerrufen, indem Sie sich an den Webmaster wenden.
- Richten Sie eine Familien-Mailadresse ein
  Verwenden Sie die Familien-Mailadresse für Profile, Einkäufe im Internet und Ähnliches. So schützen Sie Ihre eigene, persönliche Mailadresse und beugen auch Spam darauf vor.

Sicherer PC

- Der Computer und das Internet bieten Eltern wie Kindern phantastische Möglichkeiten. Damit die Computernutzung aber langfristig Spass macht, muss der PC gegen verschiedene Gefahren geschützt werden. Besonders wichtig ist der Schutz Ihrer persönlichen Daten, Ihrer Fotos und Unterlagen. Um das zu gewährleisten brauchen Sie einerseits gewisse Programme und Einstellungen, die Ihren Computer schützen, andererseits können Sie sich und Ihre Geräte auch durch gewisse Verhaltensweisen schützen.

Was sind die Gefahren?

- Um sich optimal schützen zu können, gilt es Schwachstellen in Ihrem Computer und den Programmen aufzudecken, um Eindringlingen keine Chance zu geben.
- Zu diesem Thema informiert Sie unser Partner Norton:
  "Schwachstellen sind Fehler in einer Computersoftware, durch die Lücken in der allgemeinen Sicherheitsstruktur des Computers bzw. Netzwerks entstehen. Schwachstellen können auch als Folge unsachgemäßer Computer- oder Sicherheitskonfigurationen auftreten. Bedrohungen nutzen die durch Schwachstellen hervorgerufenen Sicherheitsanfälligkeiten aus, so dass es zu Schäden am Computer oder an den persönlichen Daten kommen kann."

Spionageprogramme

- Spionageprogramme (Spyware) können über Webseiten, E-Mail-Nachrichten, Instant Messaging-Nachrichten und über Direktverbindungen zur Dateifreigabe heruntergeladen werden. Darüber hinaus können Benutzer unwissentlich Spionageprogramme erhalten, wenn sie die Endbenutzerlizenzvereinbarung eines Softwareprogramms akzeptieren.

SPAM

- Spam-E-Mails sind Werbesendungen in elektronischer Form. In Spam-E-Mails wird die gleiche Nachricht – oft unerwünschte Werbung – an eine große Zahl von Empfängern gesendet. Spam-E-Mails sind ein ernstzunehmendes Sicherheitsproblem, da sie Trojanische Pferde, Viren, Würmer, Spionageprogramme und gezielte Phishing-Versuche enthalten können.

Phishing

- Phishing ist Bauernfängerei online und Phisher sind nichts anderes als technisch versierte Schwindler und Datendiebe. Sie nutzen Spam-E-Mails, gefälschte Webseiten oder E-Mail- bzw. Instant Messaging-Nachrichten, um andere zur Herausgabe vertraulicher Informationen zu verleiten, beispielsweise Einzelheiten zu Bank- und Kreditkartenkonten.

Malware

- Als "Malware" bzw. Schadprogramme wird eine Kategorie bösartigen Codes bezeichnet, die Viren, Würmer und Trojanische Pferde umfasst. Malware bedient sich gängiger Kommunikationsprogramme zu ihrer Verbreitung. Dazu gehören per E-Mail und Instant Messaging verschickte Würmer, über Webseiten abgelegte Trojanische Pferde und virusinfizierte Dateien, die aus Peer-to-Peer-Verbindungen heruntergeladen werden. Malware versucht darüber hinaus, etwaige Schwachstellen in Systemen heimlich für einen ungehinderten Zugriff auszunutzen.

Schritte zur Computersicherheit

Schritt 1: Datensicherung

- Damit im Fall eines unbeabsichtigten Datenverlustes – z. B. durch Viren, Spannungsschwankungen oder Wasserrohrbrüche – Ihre persönlichen Daten nicht unwiederbringlich verloren sind, sollten Sie diese unbedingt regelmässig sichern und die Sicherungskopie separat vom Computer aufbewahren. Eine Sicherungskopie Ihrer Daten (Fotos, Bankauszüge, Adressbücher, E-Mail-Verkehr etc.) können Sie beispielsweise auf eine CD oder DVD brennen, auf eine externe Festplatte kopieren oder auf eine Onlineplattform (z.B. auf Ihren persönlichen SkyDrive) laden.

Schritt 2: Antivren-Programme

- Computerviren, Würmer und Trojaner sind heimtückische Programme, die Ihren Computer und darauf gespeicherte Daten manipulieren, ausspähen oder auch löschen können. Schützen Sie sich mit einer Antiviren-Software, welche verhindert, dass schädliche Programme auf Ihrem Computer Unheil anrichten können. Achten Sie ausserdem darauf, dass Sie regelmässig Updates herunterladen. Am besten ändern Sie die Einstellungen so, dass das Programm die neusten Definitionen selbst vom Internet herunterladen darf. Nur ein aktuelles Antivirenprogramm bietet Schutz!
- Es gibt eine grosse Anzahl von Anbietern von Antiviren-Software, beispielsweise Norton. Ein kostenloses Antivirenprogramm finden Sie hier: Microsoft Security Essentials

Schritt 3: Firewall

- Um sich vor Bedrohungen durch Hacker aus dem Internet zu schützen, hilft u. a. eine so genannte Firewall. Sie ist der digitale «Türsteher» für Ihren Computer und lässt nur die Daten durch die Netzwerkverbindung, die Sie auch wirklich angefordert haben. Sie entscheidet, was rein kommt und was draussen bleibt. Die Firewall ist normalerweise in das Betriebssystem integriert.
  Weitere Informationen zur Firewall auf Windows7, Windows Vista, Windows XP.

Schritt 4: Softwareupdates

- Entdecken Hersteller eine Schwachstelle in ihrer Software, wird ein Update (auch Patch genannt) veröffentlicht, damit Hacker die Schwachstelle nicht ausnutzen können. Die regelmässige Installation von Updates gehört zur Routinewartung Ihres Computers.

Schritt 5: Aufpassen

- Dies ist das wichtigste Sicherheitselement. Die obigen vier technischen Schritte sind wichtig, aber nutzen Sie auch Ihren gesunden Menschenverstand: Ein Grundmass an Misstrauen ist im Internet angebracht. Seien Sie vorsichtig im Umgang mit Ihren persönlichen Daten. Falls Sie eine drahtlose Internetverbindung (Wireless) nutzen, muss diese unbedingt passwortgeschützt sein. Falls Ihre Kinder denselben Computer nutzen wie Sie, richten Sie ihnen eigene Profile ein und schützen Sie alle Profile mit Passwörtern. So können die Kinder auch nicht versehentlich Ihre privaten Daten online stellen oder löschen.
- Kinder- und Jugendschutzeinstellungen
- Es gibt unterschiedliche kostenlose und kostenpflichtige Angebote, die auf dem Computer installiert werden können, um den Internet- und Computerkonsum der Kinder einzuschränken oder zu überwachen. Wichtig

dabei ist: Kinderschutzeinstellungen und –Software sind immer nur Begleitmassnahmen. Sprechen Sie aber unbedingt mit Ihrem Kind über die getroffenen Massnahmen. Ihre Begleitung und Anteilnahme nützen mehr als Kontrolle und Verbote!

- Windows 7 und Windows Vista bieten weitreichende Funktionen im Bereich Kinder- und Jugendschutz. Mithilfe des Jugendschutzes legen Eltern fest, welche Spiele ihre Kinder spielen, welche Programme sie verwenden und welche Websites sie sich ansehen dürfen - und wann. Eltern können die Computernutzung auf bestimmte Zeiten beschränken und darauf vertrauen, dass diese Beschränkungen von Windows 7/Windows Vista eingehalten werden, auch wenn sie nicht zu Hause sind.

Kinderschutzsoftware einrichten

Ihr Kind surft sicherer, wenn Sie auf dem Computer eine Kinderschutzsoftware installieren. Gleichzeitig ist das aber auch ein Hinweis darauf, dass Sie Ihrem Sohn oder Ihrer Tochter nicht vertrauen. Installieren Sie solche Programme erst, wenn Ermahnungen nicht geholfen haben oder Ihnen keine persönliche Kontrolle möglich ist. Bei einem neuen Mac oder PC können Eltern im Betriebssystem die Kindersicherung einrichten. Für ältere Computer gibt es spezielle Programme, die man aus dem Internet herunterladen kann.

Bevor besorgte Väter und Mütter Geld für Kinderschutz-Software ausgeben, sollten sie erst die Bordmittel des Rechners aktivieren. Mac-Nutzern bleibt gar nichts anderes übrig: Laut Walter Mehl von der Zeitschrift «Macwelt» gibt es keine Kinderschutz-Programme, die man für den Mac kaufen könnte. Dafür bringt das Betriebssystem selbst das Programm «Kindersicherung» mit: Mit einfachen Konfigurationsschritten können Eltern Regeln für ihre Kinder festlegen.

Mit dem Mac-eigenen Kinderschutz-Programm lässt sich bestimmen, zu welchen Zeiten und wie lange der Nachwuchs insgesamt den Rechner nutzen darf. Zudem lässt sich festlegen, welche Internetseiten aufgerufen werden dürfen. **Dies funktioniere jedoch nur mit Safari**, dem Browser von Apple. Wer vermeiden will, dass die Kids mit einem anderen Browser an den Vorgaben vorbei auf unerwünschte Seiten surfen, muss dies durch eine Definition der Programme tun, die Kinder nutzen dürfen.

Arbeitsintensiv. Dass es Arbeit macht, den Rechner kindersicher zu machen, liegt in der Natur der Sache: Wer seinen Kindern die Nutzung des Rechners und den Zugang nicht pauschal verbieten will, muss eben differenziert einschränken. So können Eltern beim Mac eine Liste mit E-Mail-Adressen oder Chat-Partnern anlegen, mit denen die Kinder kommunizieren dürfen. Das erfordert Geduld. So kann es ein paar Wochen dauern, bis die Einstellungen stimmen.

Soll der Nachwuchs iTunes nutzen dürfen, sind auch hier Einstellungen sinnvoll. Nach dem Motto «Bushido ist gesperrt» lässt sich die Wiedergabe von Filmen abhängig von der offiziellen Altersfreigabe unterdrücken. Mit der Musik ist es nicht so einfach.

Um den Nachwuchs vor unappetitlichen Songtexten zu schützen, ist das Anlegen einer Mediathek notwendig. Möglich ist es auch, iTunes so zu konfigurieren, dass die Kinder nicht im Store einkaufen können. Und nach dem Motto «Vertrauen ist gut, Kontrolle besser» lässt sich die Option «Protokolle» unter «Kinderschutz» verwenden.

Versuchen Sie dennoch immer, mit Ihrem Kind über gefährliche Inhalte zu reden, denn

- Durch Filterprogramme und Verbote ist das Kind zwar vor gewissen Gefahren geschützt. Doch es lernt nicht, sich angesichts der Gefahren selbständig und verantwortungsvoll zu verhalten. (Schweizerische Kriminalprävention auf www.stopp-kinderpornografie.ch)

Im Folgenden finden Sie einen Überblick über Kinderschutzsoftware.

Die verschiedenen Kinderschutz-Programme, die derzeit auf dem Markt sind, funktionieren ganz unterschiedlich. Einige wenden das **«Keyword-Blocking»** an. Internetseiten, welche verbotene Wörter enthalten, werden nicht angezeigt. Der Nachteil an dieser Software ist, dass Bilder oder Videos, die keinen beschreibenden Text enthalten, nicht herausgefiltert werden. Zudem schaut das Programm nicht auf die inhaltliche Bedeutung von Texten. Damit werden Seiten zur Sexualaufklärung oder Gesundheitsberatung geblockt, Wörter wie Staatsexamen, welches das Wort Sex enthält, werden ebenso gefiltert.

Filtersoftware, die auf dem Prinzip des **«Site-Blocking»** funktioniert, enthält Negativ-Listen mit den Internetadressen unerwünschter Seiten. Die Herstellerfirmen aktualisieren die Listen. Deshalb muss der Kunde für das Programm regelmässig Updates herunterladen. Diese Software ist oft sehr teuer. Ausserdem kommen die Hersteller nicht hinterher, weil täglich mehr neue Seiten online gehen, als in die Liste aufgenommen werden können.

Andere Systeme arbeiten mit den **Inhalt-Einstellungen des Browsers**, also Ihres Internet-Explorers oder des Firefox. Anbieter kennzeichnen ihre Webseiten nach vorgegebenen Kriterien (Gewalt, Sex, Nacktheit, rohe Sprache) mit einem Label, das vom Browser erkannt wird. Da die Deklaration freiwillig ist, nehmen nur wenige daran teil. Das macht dieses System recht unwirksam.

Software: www.kindersicherung.de Kindersicherung von Salfeld 30.00 Euro
www.tss-productions.de Wintimer von Tss 23.00 Euro
www.kindersicherung-internet.de von Haug Leuschner GRATIS
www.parents-friend.de von TH Ware 5- 10 Euro
Schau genau Verlinkung von Anleitungen Mac und PC

Internetlinks zum Thema Kinder / Jugendliche und Internet

- www.security4kids.ch sehr Aktuelle Seite von Microsoft und Swisscom und weiteren Partnern
- Kinderschützer Seite von Microsoft Seite von Marion & Markus Bachmann Kinderschützer bei Microsoft
- www.kinderonline.ch Linksammlung Spiele, Sicherheit, Infos
- www.netcity.org Spielerisch das Internet und seine guten und schlechten Seiten kennen lernen.
- iPhone sicher machen
- Windows 7 sicher machen
- Gratis Virenschutz von Microsoft für den ganzen Computer inkl Outlook
- Bluewin Chat abgestellt hier ein Chatersatz oder www.facebook.com