Datensicherheit

Von allen wichtigen Daten (Texte, Digitalfotos, Musik, Mailadressen, etc.) sollten regelmäßig Sicherungen (Backups) angelegt werden, am besten auf ein externes Festplattenlaufwerk oder Datenträger wie CDs oder DVDs, wobei die Lebensdauer selbstgebrannter Scheiben weit geringer ist als ursprünglich behauptet, und sich unter ungünstigen Bedingungen (Hitze, Feuchtigkeit, direkte Sonneneinstrahlung) sogar auf wenige Monate reduzieren kann. Auch USB-Sticks sind für dauerhafte Sicherungen nicht geeignet. Virenbefall oder Festplattenversagen hat schon viele wichtige Daten urplötzlich und unwiederbringlich ins Nirwana befördert.

Sicherheit von WLAN-Netzen

Drahtlose Netzwerkverbindungen müssen unbedingt per Verschlüsselung gesichert werden, bevorzugt mit WPA oder WPA2. Der Verschlüsselungsmodus WEP ist veraltet und nicht mehr sicher. V.a. ältere WLAN-Geräte sind jedoch zum Teil so konfiguriert, dass sie bei Inbetriebnahme sofort eine Verbindung herstellen, ohne dass der Benutzer zum Einstellen der Verschlüsselung aufgefordert wird. Solche offenen Netze können von jedermann genutzt werden, etwa von Nachbarn zum illegalen Tausch von Musik oder Filmen. Steht dann die Polizei vor der Tür, ist nicht nachweisbar, dass ein Fremder das eigene Netz missbraucht hat. Rechtlich ist der Besitzer eines WLAN-Netzes für alle Aktivitäten in diesem Netz verantwortlich und muss Fremdnutzung gegebenenfalls beweisen („Störerhaftung“). Bei Inbetriebnahme muss als erstes das Administratorpasswort (für den Zugang zum Router) geändert werden, anschließend schaltet man die Verschlüsselung ein und vergibt ein Passwort dafür (NICHT gleich dem Admin-Passwort!)

Die Sicherheit eines WLAN-Netzes lässt sich durch weitere Maßnahmen erhöhen:

1. Abschaltung der Übertragung (Broadcast) des Netzwerknamens (SSID) in der Administrationsoberfläche des WLAN-Geräts. So können nur Personen, denen der Name des WLANs bekannt ist, einen Zugang dazu herstellen.
2. Aktivierung des Mac-Filters. Jede WLAN-Karte hat eine weltweit eindeutige so genannte Mac-Adresse. Diese ist auf der Karte aufgedruckt und im Routermenü sichtbar. Aktiviert man den Mac-Filter im WLAN-Router und trägt dort die Mac-Adressen der Rechner im Haushalt ein, können nur diese Geräte sich mit dem WLAN verbinden.

Online-Banking

Folgen Sie niemals einem Link in einer Email oder auf einer Website, um die Internetseite Ihrer Bank zu öffnen, um dem sogenannten "Phishing" zu entgehen, bei dem Hacker arglose Bankkunden auf täuschend echt nachgebildete Bankseiten locken. Tippen Sie die Adresse immer direkt im Browser ein. Ihre Bank wird Sie niemals per Email nach Kontodaten, Passwörtern oder TAN-Nummern fragen.

Dieser kompakte Ratgeber kann nur einen sehr groben Überblick über das Thema geben. Ausführliche Hilfen und Infos finden sich unter www.medien-sicher.de

GBS Ratgeber „Ins Netz – aber sicher!“

Stand: Januar 2011

THEMEN:
- ✓ Medienerziehung und Jugendmedienschutz
- ✓ Übermäßige Nutzung / Computersucht
- ✓ Privatsphäre und Datenschutz
- ✓ Viren und andere Schädlinge
- ✓ Downloads und Urheberrecht
- ✓ Trickbetrüger im Internet
- ✓ Sichere Passwörter
- ✓ Datensicherheit
- ✓ Sicherheit von WLAN-Netzen
- ✓ Online-Banking

Medienerziehung, Jugendmedienschutz, Aufsichtspflicht

Keine technische Neuerung hat die Lebenswelt Heranwachsender so einschneidend verändert wie die elektronischen Medien. Insbesondere das Internet ist faszinierend und bietet unendliche positive und produktive Möglichkeiten. Doch auf der Datenautobahn lauern auch zahlreiche Gefahren, die sich zudem ständig verändern. Grundsätzlich sind die Eltern Minderjähriger für alles verantwortlich, was diese mit ihren Computern und Handys anstellen. Das betrifft Verstöße gegen das Urheberrecht, Mobbing, Pornografie und Gewalt verherrlichende Inhalte ebenso wie altersbeschränkte Computerspiele. Da sich das WWW als weltweites Datennetz weitgehend dem deutschen Jugendschutzgesetz entzieht, finden sich kritische Inhalte dort an allen Ecken und Enden.

Wer Kindern einen Rechner mit Onlinezugang zur Verfügung stellt, muss daher einerseits Medienerziehung leisten und über Regeln, Risken und Gefahren aufklären, andererseits aber auch ein Mindestmaß an Kontrolle über die Computeraktivitäten des Nachwuchses behalten. Die Benutzerkonten der Kinder sollten nicht mit Administratorrechten ausgestattet werden, damit diese nicht unkontrolliert problematische Programme installieren können. Die Passwörter der Eltern dürfen den Kindern nicht bekannt sein, auch wenn es manchem lästig sein mag, bei jeder Installation helfen zu müssen. Auch über die von den Kindern besuchten Internetseiten sollte man informiert sein. Es gibt eine ganze Reihe guter Jugendschutzprogramme (gratis: www.fragfinn.de, www.jugendschutzprogramm.de kommerziell: www.surf-sitter.de, www.salfeld.de) auf dem Markt, die sowohl Inhalte als auch den zeitlichen Umfang der Computeraktivitäten beschränken, und zum Teil auch die Möglichkeit bieten, Surfberichte per Email an Eltern zu verschicken - darüber sollte man die Kinder allerdings unbedingt informieren! Als Hardwarelösung bieten etwa die Fritz!Box Telefonanlagen und Router der Firma AVM die Möglichkeit Internet-Zeitkontingente für bestimmte Rechner oder Benutzer einzurichten, allerdings fehlt hier ein Inhaltsfilter. Ein komplettes Paket bieten die Router von www.surf-sitter.de. Perfekt bzw. als Elterner-

© Günter Steppich, Gutenbergschule, Mosbacherstr. 1, 65187 Wiesbaden, www.gutenberg-gym.de

satz tauglich ist allerdings keiner dieser Filter, sie entbinden nicht von der Notwendigkeit, sich mit der Mediennutzung des Nachwuchses zu beschäftigen. Ein Übermaß an Überwachung beschädigt zum einen das Vertrauensverhältnis und fördert zum anderen Umgehungsstrategien. Heimlich hinterher spionieren sollte man seinen Kindern auf keinen Fall!

Wichtiger als Kontrollen und Verbote sind Aufklärung und Erziehung zu vernünftigem und vorsichtigem Umgang mit dem Medium. Wenn Kinder negative Erfahrungen mit dem Netz machen, müssen die Eltern als vertrauensvolle Ansprechpartner zur Verfügung stehen. Viele Kinder wenden sich aber aus Angst vor Verboten oder weil es ihnen peinlich ist nicht an ihre Eltern und müssen so mit teils übelsten Erlebnissen alleine klarkommen.

Das Internet verändert sich täglich, bekannte Risiken verschwinden (z.B. durch Sicherheitsupdates der Hersteller oder Gesetzesänderungen), neue Gefahren entstehen. Nur mit einer guten Portion grundsätzlicher Skepsis und unter Beachtung des Mottos "Denk nach bevor du klickst!" lässt sich das Medium auf Dauer ausreichend sicher beherrschen.

Übermäßige Nutzung / Computersucht

Exzessive Mediennutzung kann zur Sucht werden und dazu führen, dass die Betroffenen kaum noch am realen Leben teilnehmen. Nach einer aktuellen Studie des KFN sind 8% der 15-jährigen deutschen Jungen computerspielsüchtig! Mehr als 5 Stunden PC-Nutzung mit steigender Tendenz, ständiger PC-Streit mit den Eltern, nachlassende schulische Leistungen, Desinteresse an anderen Aktivitäten, Überwiegen von Onlinekontakten gegenüber realen sowie nervöses, gereiztes oder depressives Verhalten bei längerer PC-Abstinenz sind deutliche Anzeichen für eine solche Verhaltenssucht. Wenn Jugendliche ihre Mahlzeiten am PC einnehmen wollen, sollten die Alarmglocken schrillen. Negative Auswirkungen auf den Schulerfolg und die Persönlichkeitsentwicklung kann ungeregelter Bildschirmkonsum aber auch hervorrufen, wenn keine Suchtproblematik vorliegt. Studien belegen, dass die Schulleistungen vieler Jungen seit Beginn der 90er in alarmierendem Ausmaß nachgelassen haben, weil sie kaum noch lesen und sich stattdessen lieber mit Videospielen beschäftigen.

Privatsphäre und Datenschutz – Einmal im Netz, immer im Netz!

Gerade Kinder und Jugendliche kommunizieren zunehmend über das Internet und sind sich häufig nicht der Risiken bewusst, denen sie sich dabei aussetzen können. So werden in Messenger Programmen wie ICQ, MSN und in Onlinenetzwerken wie SchülerVZ (www.schuelervz.de), Facebook (www.facebook.com) oder Wer-Kennt-Wen (www.wer-kennt-wen.de) freigiebig persönliche Angaben wie Name, Adresse, Telefonnummer, Geburtsdatum, Kontakte und private Fotos veröffentlicht, die dann weltweit für jedermann einsehbar sind. Auch in Foren oder auf anderen Internetseiten veröffentlichte persönliche Angaben und Fotos sind selbst nach deren Löschung noch Monate lang im WWW zu finden, bis die Suchroboter ihre Verzeichnisse aktualisiert haben. Da Personalchefs heute gerne die Namen von Bewerbern erst einmal "googeln", mit Personensuchmaschinen (z.B. www.yasni.de) und in Onlinenetzwerken recherchieren, können unüberlegt veröffentliche Dinge sehr negative Auswirkungen auf die Karriere haben, und sei es nur für die Bewerbung auf einen Praktikumsplatz.

Trickbetrüger im Internet, die "kostenlos"-Masche: Abofallen

Viele Schüler, aber auch Erwachsene, haben Probleme mit Online-Abos, die sie aufgrund angeblich kostenloser Lockangebote irrtümlich oder unvorsichtig abgeschlossen haben. Grundsätzlich muss man immer, wenn Dinge im Internet als kostenlos angepriesen werden, damit rechnen ein im Kleingedruckten verstecktes Abo untergeschoben zu bekommen.

Hilfe dazu findet sich unter http://www.medien-sicher.de/?p=89. **Grundsatz: Auf keinen Fall zahlen!** Auf den Internetseiten der Verbraucherzentralen finden sich Musterbriefe, mit deren Hilfe man die lästigen Abmahner los wird. Grundsatz: Nicht von juristischen Pseudo-Argumenten verunsichern lassen und auf keinen Fall zahlen!

Die wichtigsten Punkte zu minderjährigen Opfern: Minderjährige gehen oft aufgrund ihrer Unerfahrenheit in die Vertragsfalle. Treffen nun Mahnschreiben ein, gehen die Eltern oft fälschlicherweise davon aus, für ihre Kinder haften zu müssen. Minderjährige können jedoch nur mit der Einwilligung der Eltern Verträge abschließen. Liegt diese nicht vor, so ist der Vertrag schlicht unwirksam. Der Taschengeldparagraf 110 BGB greift hier nicht.

Nicht jede Lüge ist ein Betrug im Sinne des Strafrechts, es sei denn, man hätte sich auf der Seite mit falschen Daten angemeldet hat, um den Betreiber zu schädigen. Genau das ist nicht der Fall, wenn man die Kosten übersehen hat und wenn Kinder ein falsches Alter angegeben haben, um sich bei der Website anmelden zu können. Das gerne benutzte Argument des Seitenbetreibers, man hätte richtig hinsehen müssen, genügt nicht, denn einen fahrlässigen Betrug gibt es im Strafgesetzbuch nicht. Kinder unter 14 Jahren sind schon deswegen aus dem Schneider, weil sie noch nicht einmal strafmündig sind.

Die Minderjährigkeit wird den Seitenbetreibern per Musterbrief mitgeteilt. Forderungen, die Minderjährigkeit durch eine Kopie der Geburtsurkunde nachzuweisen, muss man nicht nachkommen.

Widerrufsrecht: Verbrauchern steht beim Abschluss von Verträgen über das Internet grundsätzlich das Recht zu, den Vertrag innerhalb von 14 Tagen zu widerrufen. Diese Frist beginnt aber erst, wenn man mit der Vertragsbestätigung, mindestens per E-Mail, eine schriftliche Widerrufsbelehrung erhalten hat.

Sichere Passwörter

Ein sicheres Passwort besteht aus mindestens 6 Zeichen in einer Kombination aus Klein- und Großbuchstaben und Zahlen (z.B. SichA32). Auf keinen Fall sollten reale Begriffe, Namen von Haustieren oder Verwandten verwendet werden. Trotzdem muss ein Passwort natürlich leicht zu merken sein, da man es möglichst nicht aufschreiben sollte. Man kann etwa den Namen des Haustiers mit Zahlen mischen, wie z.B. G1arfiel2D

Ein Passwort ist nur sicher, wenn es privat bleibt. Auch besten Freunden oder Geschwistern sollte man es nicht verraten, denn Freundschaften können sich ändern und Geschwister können sich streiten - wer weiß was sie dann damit anstellen. Wenn ein anderer sich Zugang zu einer passwortgeschützten Seite verschafft und dort Unsinn anstellt, ist es kaum nachweisbar, dass das Benutzerkonto missbraucht wurde.

© Günter Steppich, Gutenbergschule, Mosbacherstr. 1, 65187 Wiesbaden, www.gutenberg-gym.de

mit falscher Erweiterung darstellen zu lassen. Die Datei *coolesbild.jpg.exe* wird dann z.B. in Emails nur als harmlose *coolesbild.jpg* angezeigt.

Sicherer als Microsoft-Produkte sind **alternative Betriebssysteme** wie Linux (kostenlos!) oder das MacIntosh OS (nur für Apple Computer), sowie das **kostenlose Officepaket "Open Office"** (http://de.openoffice.org), das den gleichen Funktionsumfang bietet wie MS Office und sehr ähnlich aufgebaut ist. Als Emailprogramm empfiehlt sich z.B. Mozilla Thunderbird, das wesentlich sicherer und auch seltener Ziel von Virenattacken ist. Das gleiche gilt für den Browser **Mozilla Firefox**, der zudem schneller und komfortabler ist als der Internet Explorer und zahllose Erweiterungen (Add-ons) bietet, z.B. „NoScript", das Hackerattacken abfängt. Beide Programme finden sich unter http://www.mozilla.com

Zusätzlich empfiehlt sich ein Spamfilter (z.B. www.spamihilator.com), der unerwünschte Werbemails aussortiert und es ermöglicht, dass Emails nur von bekannten Absendern angenommen werden, gerade bei Kindern eine sehr nützliche Funktion, um Sexmails zu blockieren. Auch die meisten Freemailanbieter (web.de, gmx.de, yahoo.de, etc) gut funktionierende Spamfilter.

Ein **Virenscanner** mit täglich aktuellen Virensignaturen ist Pflicht, eine gute kostenlose Software ist AntiVir Personal (http://www.free-av.de). Ein **Anti-Spyware Programm** wie Ad-Aware (www.lavasoft.de) befreit den PC von weiteren Schädlingen, die sich unbemerkt eingenistet haben, eine **Firewall** (ab Windows XP enthalten) kontrolliert den Datenverkehr mit dem Internet und blockiert unerwünschte Zugriffe. Zusätzliche Firewall-Software ist nicht notwendig.

Unter Windows sollte grundsätzlich mit **eingeschränkten Benutzerkonten** gearbeitet werden, da viele Viren Administratorrechte benötigen, um sich im System einnisten zu können. Zur Installation von Programmen sollte ein extra dafür verwendetes Administratorkonto eingerichtet werden, das nur zu diesem Zweck verwendet wird, keinesfalls zum Surfen und Mailen, auch wenn Windows Vista und Windows 7 in dieser Hinsicht besser geschützt sind als ihre Vorgänger. Kinder sollten grundsätzlich keine Administratorrechte besitzen, damit die Eltern die Übersicht und Kontrolle über installierte Programme behalten. Mehr dazu im folgenden Abschnitt.

Downloads und Urheberrecht

Sogenannte File-Sharing Programme wie Emule, Kazaa, BitTorrent, BearShare etc. dienen zum Download von kopiergeschützter Musik, Filmen, Computerspielen und Programmen. Dies ist zum einen illegal und zum anderen gefährlich, weil sich die Nutzer über die IP-Adresse des Computers, die beim Tauschvorgang übertragen wird, leicht ermitteln lassen und über solche Tauschbörsen auch häufig Viren in Umlauf gebracht werden. Insbesondere das Bereitstellen von kopiergeschütztem Material wird von der Industrie und den Behörden hartnäckig verfolgt und kann empfindliche Strafen nach sich ziehen. Eltern sollten ihre Kinder darüber aufklären und auch kontrollieren, dass sich keine solchen Programme auf deren Rechnern befinden. Wer ganz sicher gehen will, sperrt im DSL-Router die Ports, die solche Programme benötigen. Nach einer Gesetzesänderung ist seit dem 1.1.2008 ausdrücklich nicht mehr nur das zur Verfügung stellen, sondern auch das Herunterladen offensichtlich illegal bereit gestellter Angebote strafbar! Übliche Schadensersatzforderung pro mp3: 1000€!

Um keine unliebsamen Überraschungen zu erleben, sollte man also genau abwägen, wie viel man von sich preisgibt, und ob man wirklich möchte, dass JEDER, der bei einer Website angemeldet ist, das eigene Profil einsehen, die Freundesliste und die Fotoalben betrachten darf, etc. Auch in den Profilen von Messenger- und Chat-Programmen (ICQ, MSN, AIM) sowie Foren und Chatrooms haben Namensangaben, Geburtsdaten, Adressen und Telefonnummern grundsätzlich nichts verloren. Insbesondere Mädchen spielen sich damit in die Hände von Pädophilen und Stalkern, die sich ihre Opfer wie im Warenhauskatalog in aller Ruhe aussuchen können.

Im **SchuelerVZ** ist trotz der für die Anmeldung notwendigen „Einladung" absolut nicht gewährleistet, dass nur Schüler dort Mitglied werden können. Nach Google-Statistiken sind 40% der Besucher der SVZ-Seite über 25 Jahre alt, und es gibt sicherlich auch unter den 5 Millionen angemeldeter Schüler einen ordentlichen Anteil merkwürdiger Gestalten, die man nicht über seine Interessen, Hobbys, Freunde, etc informieren möchte. Nach gravierenden Sicherheitsproblemen im ersten Jahr haben die Betreiber inzwischen auf die massive Kritik reagiert und die Privatsphäre-Einstellungen umfassend überarbeitet. So sind z.B. die Profile aller Neuanmeldungen unter 16 Jahren standardmäßig privat eingestellt, d.h. nur für die Freundesliste sichtbar.

Viele Schüler breiten ihr Privatleben aber so ausführlich aus, dass man ohne großen Aufwand herausfinden kann, wo sie sich wann, warum und mit wem aufhalten. Der Menüpunkt „Privatsphäre" spielt daher in allen Onlinenetzwerken die entscheidende Rolle zur Sicherung persönlicher Daten und damit zur Vermeidung unangenehmer Nebenwirkungen. Grundsätzlich sollten sämtliche dort aufgeführten Punkte immer auf die höchste Sicherheitsstufe eingestellt werden; diese heißt in der Regel „Nur meine Freunde". Wobei man sich immer bewusst sein muss, dass es hier nur um teils sehr flüchtige Kontakte und Bekanntschaften geht. Von „Freunden" kann man bei durchschnittlich 150 Kontakten definitiv nicht sprechen. Dabei besteht auch immer die Gefahr, dass jemand versucht, sich mit einem gefälschten Profil Zugang zu den Inhalten anderer Nutzer zu verschaffen, denn in allen Netzwerken ist es problemlos möglich, die Identität eines anderen zu stehlen, indem man dessen Angaben in ein neues Profil kopiert und damit Freundschaftsanfragen stellt!

Auch für jedes Fotoalbum müssen die Zugriffsbeschränkungen separat eingestellt werden und immer wieder einmal kontrolliert werden! Vor allem Facebook ändert häufig Privatsphäreeinstellungen, ohne seine Nutzer darüber zu informieren, und so sind dann plötzlich Bilder für Fremde sichtbar, die man nur für Freunde frei gegeben hatte. Bei Facebook werden Neuerungen wie die Ortungsfunktion oder demnächst Gesichtserkennung grundsätzlich für alle User aktiviert und müssen erst gezielt und teils sogar an mehreren Stellen in den Privatsphäreeinstellungen abgeschaltet werden.

Die wenigen Klicks für ein deutliches Plus an Sicherheit und Privatsphäre sollte man also unbedingt machen, es sei denn man möchte wirklich, dass jeder x-beliebige sich

private Fotos anschauen, diese kopieren und alles lesen kann, was man ihm nie erzählen würde! Grundsätzlich sollte man sehr sorgfältig abwägen, was man ins Netz stellt, denn alle Inhalte können - auch von „Freunden“ - kopiert und an anderer Stelle veröffentlicht werden. Die Löschung aller Kopien ist in der Regel unmöglich. Im Zweifelsfall: Einfach einmal mit den Eltern darüber sprechen! Doch laut Umfragen wird in jeder zweiten Familie nicht über diese Gefahren gesprochen, d.h. viele Kinder und Jugendliche werden bedenkenlos, unaufgeklärt und unkontrolliert auf das Internet losgelassen. Medienerziehung ist heutzutage eine extrem wichtige Aufgabe der Eltern Erziehung, die Schule kann hier zwar unterstützen, aber nur sehr begrenzt nach Hause wirken.

Ein weiterer Aspekt solcher Community-Seiten: StudiVZ und SchülerVZ wurden nach Presseberichten in 2007 für 85 Millionen € von einem großen Berliner Verlag gekauft, Wer-Kennt-Wen ging für 10 Millionen an RTL. Das offensichtliche Motiv: 2 Millionen Studenten und 12 Millionen Schüler sind eine riesige Werbezielgruppe mit einer Kaufkraft im Milliardenbereich. Schon allein deshalb muss man sich genau überlegen, welche Daten man von sich preisgibt. Grundsätzlich sind US-Anbieter wie Facebook oder MySpace in Bezug auf den Datenschutz noch deutlich problematischer als deutsche Betreiber. Facebook sichert sich z.B. in seinen AGB eine „*übertragbare, unterlizensierbare, unentgeltliche, weltweite Lizenz für die Nutzung jeglicher Inhalte*“!

Zudem verschafft sich der Marktführer Zugang zu den Daten Dritter, die gar nicht bei dem Netzwerk angemeldet sind, indem er über die Funktion „Freundefinder“ die kompletten Daten aus den Emailadressbüchern der User ausliest, die diesen vermeintlichen „Service“ nutzen. Facebook verschickt dann im Namen des Nutzers Einladungen an sämtliche Adressen aus dessen Adressbuch, denen dann praktischer Weise Kontakte vorgeschlagen werden, die sie eventuell kennen könnten. Dieses Verfahren erklärt auch, warum neuen Facebooknutzern unmittelbar nach der Anmeldung ihnen tatsächlich bekannte Personen als potentielle „Freunde“ vorgeschlagen werden. Nach deutschem Datenschutzrecht ist dieses Verfahren schlicht illegal!

Cyber-Bullying/Mobbing: Ca. jeder dritte Jugendliche hat schon unangenehme Erfahrungen mit Belästigungen, Beleidigungen, Hänseleien u.ä. über elektronische Medien (Handy, Email, Chatseiten, Foren) machen müssen, sogar jeder zweite war schon als Täter aktiv. Durch die elektronische Distanz werden hier sehr leicht natürliche Hemmschwellen („Beißhemmungen“) überschritten. Durch die dabei hergestellte Öffentlichkeit ist die Wirkung von Cyber-Mobbing extrem heftig, zudem verfolgt es die Opfer bis an den heimischen PC. Im schlimmsten Fall kann Cybermobbing sogar zum Selbstmord oder Amoklauf führen.

Die Grundregeln für korrektes Online-Verhalten: 1. Was du jemandem nicht ins Gesicht sagen würdest, solltest du auch nicht tippen. 2. Was du jemandem nur unter vier Augen sagen würdest, gehört nicht öffentlich sichtbar ins Internet. 3. Denke, bevor du klickst.

Sexuelle Belästigung: Pädophile tummeln sich mit Vorliebe auf Chatseiten für Kinder, wo sie bevorzugt Mädchen ansprechen, um Ihnen pornographische Fotos schicken, sie zu Telefonkontakten zu animieren oder zu persönlichen Treffen zu überreden. Auf beliebten Seiten wie www.knuddels.de dauert es nur wenige Minuten, bis ein solcher Kontakt zustande kommt. Wirklich sicher sind nur geschlossene Chaträume,

in die sich nur persönlich bekannte Chatpartner einloggen können.

Recht am eigenen Bild: Nicht zuletzt wegen der flächendeckenden Verbreitung von Fotohandys ist es Mode geworden, bei jeder Gelegenheit Fotos zu schießen. Häufig werden diese dann – nicht nur von Jugendlichen – ins Internet gestellt, ohne dass die abgebildeten Personen davon Kenntnis haben, geschweige denn um Erlaubnis gefragt wurden. Nach § 22 des Kunsturheberrechtsgesetzes handelt gesetzeswidrig, wer Bilder anderer ohne deren Zustimmung veröffentlich, insbesondere wenn die Namen dieser Personen in Bildunterschriften oder per Verlinkung genannt werden. Dies gilt auch für Zeichnungen, Karikaturen, Fotomontagen u.ä. In den meisten Onlinenetzwerken besteht die Möglichkeit, Personen auf Fotos zu verlinken, d.h. der Name wird in das Foto eingeblendet und ein Klick darauf führt zu dessen Profil. So sind viele User auf Fotos zu identifizieren, obwohl sie ihre Profile abgesichert und keine Bilder von sich veröffentlicht haben!

Umgang mit Email: Häufig bestehen Emailadressen von Schülern aus Vorname und Nachname, manchmal auch kombiniert mit einer Altersangabe. Auf keinen Fall sollte man Adressen wie *lieschen_mueller92@xyz.de,* die Name und Alter verraten, in Chatrooms, Foren und Gästebüchern verwenden, denn auch damit gibt man ein großes Stück Privatsphäre preis. Häufig ist es so Personen, die man vermeintlich anonym online kennen gelernt hat, möglich, durch simples "googeln" die wahre Identität heraus zu bekommen. Für die Verwendung im Internet sollte daher eine zweite Adresse angelegt werden, die keine persönlichen Angaben preisgibt, wie z.B. *ichbinsocool@xyz.de*.

Auf Spam-Emails und unerwünschte Newsletter darf man niemals antworten, weil dadurch die Emailadresse von den Spammern als gültig erkannt wird, wodurch sich der Marktwert der Adresse erhöht, d.h. sie kann besser weiterverkauft werden. Folge: Die Spamflut nimmt zu.

Sensible Daten wie Passwörter, Kreditkartennummern, etc. sollten auf keinen Fall per Email versandt werden, es sei denn, man nutzt ein Verschlüsselungsprogramm wie PGP (Pretty Good Privacy).

Um die Verbreitung von Viren und Spam einzudämmen, sollte man keine Mails an offen sichtbare Verteilerlisten schicken, sondern dafür das BCC-Feld (Blind Carbon Copy) des Email-Programms benutzen, wodurch jeder Empfänger nur seine eigene Adresse sehen kann. Es lässt sich in der Regel über das Menü "Ansicht" einblenden.

Viren, Trojaner, Spyware und Co.

Die wichtigste Waffe gegen Computerschädlinge ist der **gesunde Menschenverstand**. Wer arglos Emailanhänge öffnet, im Internet dubiose Seiten aufruft und bereitwillig kostenlose Programme, Spiele und Raubkopien herunter lädt, darf sich nicht wundern, wenn der Rechner mit Viren verseucht wird. Zusätzlich gibt es unumgängliche technische Maßnahmen, um die Sicherheit zu erhöhen: Das Betriebssystem sollte immer aktuell gehalten werden, indem **Updates und Sicherheitspatches** über die Windows-Updatefunktion geladen werden.

Weiterhin sollte unbedingt im Windows Explorer unter *Extras – Ordneroptionen - Ansicht* die Option "**Erweiterungen bei bekannten Dateitypen ausblenden" deaktiviert** werden, da es sonst mit einem simplen Trick möglich ist, ein Schadprogramm

© Günter Steppich, Gutenbergschule, Mosbacherstr. 1, 65187 Wiesbaden, www.gutenberg-gym.de