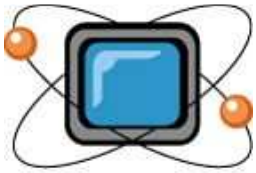
Evangelische Kirchengemeinde Scheib-Furpach, Neunkirchen

Tipps für jugendliche Internet-User

Gefahren durch Internet und neue Medien

Inhalt



Diese Broschüre ist ein Ratgeber für jugendliche Internet-Benutzer. Firmenbezeichnungen und Markennamen werden ohne Berücksichtigung eines Copyrights verwendet.
Die erteilten Auskünfte und Ratschläge wurden nach bestem Wissen zusammengestellt, ohne Gewähr und Haftung. Sie ersetzen keine juristische Beratung, sondern dienen als Hinweise auf die potenziellen Gefahren der Internet-Nutzung. Stand 2006.
Agentur-Fotos S. 1, 2, 6, 7, 8, 11 © www.fotolia.de mit Genehmigung

Zusammenstellung: Oliver Ludwig
Evangelische Kirchengemeinde Scheib-Furpach
Beerwaldweg 9, 66539 Neunkirchen

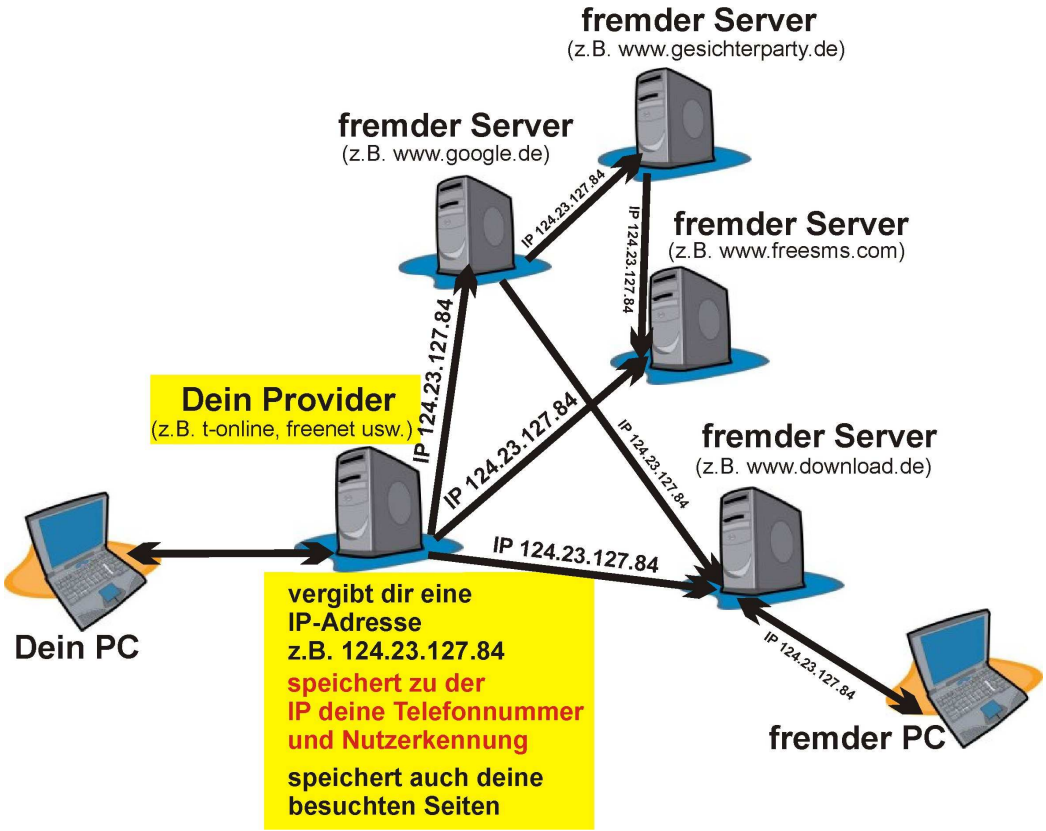
Wie anonym ist das Internet?

Was passiert eigentlich, wenn du dich über ein Modem, ISDN oder DSL ins Netz einwählst?
Dein PC stellt eine Verbindung zu einem **Server-Rechner** deines Internetproviders her (z.B. t-online, freenet, Arcor, Strato usw.). Dort bist du angemeldet, entweder über einen Vertrag oder mittels Call-by-call.
In jedem Fall vergibt dir dieser Server-Rechner eine so genannte **IP-Adresse** (IP = Internet Protokoll). Dies ist eine Kombination aus 4 Zahlen, zum Beispiel 124.23.127.48. Im Web stellt diese deine „Visitenkarte“ dar, denn der Server-Rechner speichert zusammen mit deiner IP auch deine Telefonnummer und deine Einwahldaten (Nutzername, Passwort).

Nutzername und Passwort sind bei Call-by-call-Anbietern wie freenet natürlich anonym und nicht direkt einer Person zuzuordnen. Deine Telefonnummer ist aber eindeutig.

Einwand: „Bei unserem Telefon wird die Rufnummer aber nicht übertragen!“

Irrtum! Jedes Telefon überträgt immer seine Rufnummer. Deshalb können zum Beispiel auch Behörden wie Polizei und Feuerwehr immer ausmachen, wer einen Notruf startet. Du kannst deine Nummer nur für „normale“ Nutzer unsicht-



bar machen. Deren Telefone unterdrücken dann die Darstellung. Bei einem Internet-Provider kommt deine Telefonnummer **immer** an.

Sobald du jetzt also über deinen Browser (Internet Explorer, Netscape, Firefox, Opera usw.) eine Internetseite öffnest, fordert der Server-PC deines Providers diese Seite im Netz an. Dazu überträgt er bei jeder Anfrage an die anderen PCs im Netz deine IP-Adresse.

Das bedeutet: jede Firma, deren Seite du siehst, kennt automatisch deine IP-Adresse. Schließt du jetzt über das Internet einen Vertrag ab, so bist du zurückzuverfolgen.

Beispiel:

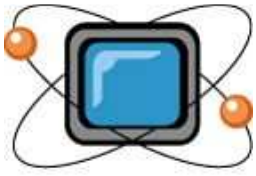
Du meldest dich bei einem Anbieter wie *www.sende-free-sms.de* oder *www.123simsen.com* an, um scheinbar kostenlose SMS verschicken zu können. Nach Angabe deiner Handynummer und Benutzerdaten und Bestätigen der AGB (Allgemeine Geschäftsbedingungen) bist du plötzlich einen Vertrag eingegangen und hast ein wöchentliches Abo begonnen! Du merkst vielleicht zu spät, dass die Dienste gar nicht kostenlos sind und zahlst nicht.
Für diese Firmen kein Problem: sie haben bei deiner Anwahl deine IP-Adresse gespeichert. Damit können sie dich zunächst einmal zu deinem Provider zurückverfolge. Stellen diese Firmen jetzt Strafantrag gegen dich, so muss der Provider deine Kontaktdaten, zumindest deine Telefonnummer herausgeben. Über diese bist du dann durch die Behörden zu identifizieren.

Also:

- Das Internet ist keineswegs anonym, im Gegenteil: durch deine IP-Adresse bist du jederzeit zu identifizieren, egal was du herunterlädst oder welche Internet-Dienste du in Anspruch nimmst.

Willst du wissen, unter welcher IP-Adresse du gerade im Netz angemeldet bist? Geh auf *http://www.ip-adress.com*

Du wirst nicht nur sehen, bei welchem Provider und unter welcher Adresse du eingeloggt bist, sondern sogar, über welchen Einwahlknoten dein PC ins Internet geht.



Wer schenkt dir kostenlose SMS?

Hört sich doch gut an: 100 SMS gratis und noch Handy gewinnen! Und dafür nur die Handynummer und ein paar Daten angeben?

Weit gefehlt: mit dem letzten Mausklick, nachdem du die AGBs (Allgemeinen Geschäftsbedingungen) bestätigt und akzeptiert hast, bist du einen Vertrag eingegangen.
Ab dann hast du ein Abo begonnen, dass dich im Monat richtig Geld kostet.

Wo das steht?
Da:

Kaum zu erkennen: schwarze Schrift auf blauem Grund; die Anbieter der Seite wissen schon, warum sie das so gewählt haben! Was wirklich drinsteht?

„…Mit Anklicken des „Anmelden“-Buttons beauftragen Sie 123simsen.com, für Sie jeden Monat 100 SMS gutzuschreiben, die Sie frei versenden kann. Der Preis von 9,00 Euro monatlich bei einer Laufzeit von 24 Monaten mit einer jährlichen Abrechnung (Gesamtsumme: 99,00 Euro) im Voraus wird Ihnen in Rechnung gestellt…“

Auch wenn zur Zeit Gerichtsverfahren laufen, um endgültig zu klären, ob diese Art des Internethandels nicht gegen die guten Sitten verstößt oder den Benutzer arglistig täuscht, gehe kein Risiko ein!

Bedenke immer:

Warum sollte ein Internet-Anbieter dir irgendetwas schenken?

Scheinbar „kostenlose“ Angebote im Internet haben fast immer einen Hintergedanken: entweder an Daten von dir zu kommen oder dir ein Abo zu verkaufen. Keine Firma hat wirklich etwas zu verschenken. Egal ob es angeblich kostenlose SMS oder ein kostenloser Download oder Gratis-Klingeltöne sind!

Also:

- Schließe keine voreiligen Verträge ab, indem du wild auf irgendetwas klickst und AGBs bestätigst!
- Gib deine persönlichen Daten nicht an, auch nicht deine Handynummer!

Wenn du auf die Idee kommst, unter fremdem Namen ein solches Abo abzuschließen, vergiss es lieber: bedenke, dass du über deine IP-Adresse immer ausfindig zumachen bist. Danach droht dir ein Strafverfahren.

Das Recht am eigenen Bild

Fast jeder jugendliche Internet-User präsentiert sich in Foren. Seiten wie www.gesichterparty.de bieten dazu Galerien, um sich und seine Freunde darzustellen. Seiten wie www.myvideo.de oder www.youtube.com erlauben es, kurze Filme ins Netz zu stellen.

Aber bei all diesen Möglichkeiten, bedenke zunächst einmal folgendes: Du hast kein Recht, Daten eines Fremden auf deinen Seiten, in deinen Galerien oder in deinen Foren darzustellen.
Zu solchen „Daten“ zählen unter anderem Fotos und Videos. Der Gesetzgeber hat dies klar geregelt: ohne Einwilligung ist das Veröffentlichen solchen Bildmaterials strafbar, man spricht salopp vom „Recht am eigenen Bild“ (ausgenommen davon sind in wenigen Fällen nur Personen der „Zeitgeschichte“, die von besonderem öffentlichen Interesse sind, wie z.B. bekannte Politiker).
Das bedeutet für dich: bevor du Videos oder Fotos, auf denen andere Personen zu sehen sind, online stellst, musst du deren Einverständnis einholen. Dieses können sie übrigens jederzeit widerrufen; dann musst du diese Fotos und Videos sofort löschen.
Im Wortlaut der Juristen (nach www.wikipedia.de):

§ 201 a StGB (Strafgesetzbuch)

Am 30. Juli 2004 trat § 201 a („Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen“) Strafgesetzbuch (StGB) in Kraft, der unter bestimmten Umständen schon für das bloße Erstellen von Bildaufnahmen eine Strafe vorsieht. Danach wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer

- (1) von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt.
- (2) Ebenso wird bestraft, wer eine durch eine Tat nach Absatz 1 hergestellte Bildaufnahme gebraucht oder einem Dritten zugänglich macht.
- (3) Wer eine befugt hergestellte Bildaufnahme von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, wissentlich unbefugt einem Dritten zugänglich macht und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Also:

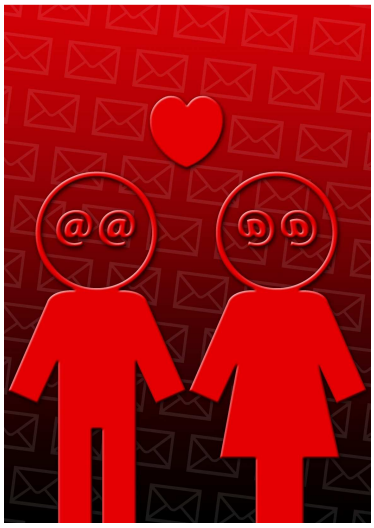
- Frage jeden, von dem du Fotos oder Videos (auch mit dem Handy!) machst, und besonders, wenn du diese ins Netz stellst. Bedenke, dass sich jeder Internet-Benutzer diese Videos und Fotos downloaden kann und damit Unfug anstellen kann.

Fake, Fake, Fake

Nicht alles ist Gold, was glänzt, sagt ein Sprichwort. Und nicht jeder im Internet ist der, für den er sich ausgibt!

Gerade beim Chatten wird gelogen, dass sich die Balken biegen. Sei entsprechend vorsichtig, wenn du Informationen über dich preisgibst. Eigentlich solltest du bei Personen, die du nicht sicher identifizieren kannst, überhaupt keine Auskünfte über dich geben. Du weißt nicht, ob und wie diese missbraucht werden können.

Als Beispiel ein wahres Märchen:



Ein 15 jähriger Jugendlicher aus Hessen hatte beim Chatten ein Mädchen kennen gelernt. Im Laufe der folgenden Tage wurden die Chats immer „heißer“ und das Mädchen schickte ihm einige Fotos von sich. Bei dem Jungen fingen die Hormone an zu brodeln, denn das Mädchen sah absolut super aus. Also schickte er auch ein paar Bilder von sich. Als das Verhältnis immer besser wurde, erhielt er auch zwei Nacktfotos von ihr. Und revanchierte sich, indem er mit dem Handy auch Nacktbilder von sich aufnahm und sie ihr zumailte.
Es kam, wie es kommen musste: ein paar Tage später fand er morgens vor Schulbeginn die Nacktfotos von sich auf DIN A4 groß ausgedruckt an zwei schwarzen Brettern seiner Schule. Noch bevor die Lehrer die Bilder entfernen und vernichten konnten, hatten sie bestimmt ein Drittel der Schule gesehen – peinlicher ging es nicht mehr. Der Hintergrund: das Mädchen war gar kein solches, sondern ein Typ aus seiner Schule, mit dem er Stress hatte. Die Nacktbilder des „Pseudo-Girls“ waren Fakes, die der Typ aus dem Internet gezogen hatte.

Natürlich war das Verhalten des Mitschülers strafbar und wurde auch bestraft. Aufgrund der Schwere des Falles wurde sogar ein Schmerzensgeld fällig. All dies kann aber die Blamage des Jungen nicht aufwiegen.

Also:

- Verschicke keine vertraulichen Daten, auch keine Bilder oder Videos an Personen, die du nicht kennst!

ICQ – I seek you

„Ich suche dich“ ist die wörtliche Übersetzung des lautmalerischen Kürzels für ICQ.
Und über ICQ wird nicht nur munter gechattet, sondern auch Dateien ausgetauscht, Bilder, Videos, Musik und was sonst noch so auf dem Rechner ist.

Aber Vorsicht: gerade bei ICQ ist deine Anonymität überhaupt nicht gewährleistet, und die von dir übertragenen Daten sind nicht geschützt.
Genaueres zeigt ein Blick in die Nutzungsbedingungen von ICQ, die leider fast kein Benutzer kennt:

Ein Ausschnitt daraus frei übersetzt:

„Sie gewähren hiermit ICQ Inc. … das nicht zurücknehmbare, weltweite Recht zur Nutzung, Vervielfältigung, Veränderung, Vermarktung, Speicherung, …, Veröffentlichung, und Verbreitung des Inhaltes (der durch ICQ in seinem Sinne verändert werden darf) durch die ICQ Website.“

Das heißt im Klartext: ICQ darf nicht nur das, was du schreibst, veröffentlichen und nutzen, sondern auch alle Daten, die du überträgst!

Also:

- Übertrage vertrauliche Daten (z.B. persönliche Bilder und Videos) nicht per ICQ, sondern nur per E-Mail.

Wer weiß, wo ich surfe

Woher wissen eigentlich einzelne Internetseiten-Betreiber, was mich interessiert. Warum starten manche Seiten bei einem erneuten Besuch genau an der Stelle, an der ich sie verlassen habe?
Ganz einfach: weil viele Internetseiten, so genannte Cookies („Kekse“) auf deinem PC hinterlassen.

> **Cookies** sind kleine Textblöcke, die der Server an den Browser sendet und später wieder zurück bekommt und benutzen kann. Cookies dienen häufig dazu, den Benutzer zu „markieren“ um ihn später wiedererkennen zu können. Mittlerweile sind Cookies die Standardmethode zur Verfolgung von Seitenbesuchern geworden. Beim ersten Besuch bekommt der Benutzer ein Cookie mit einer eindeutigen Kennnummer aufgedrängt und bei jedem weiteren Seitenaufruf kann der Server den Besucher daran wieder erkennen. Das eigentliche Problem ist, dass nicht nur der Server Cookies setzen kann, der die aufgerufene Webseite liefert. Jede von einem Webserver abgerufene Datei kann mit einem Befehl zum Setzen oder Auslesen eines Cookies kombiniert werden. Da die Werbebanner und Counter-Grafiken auf den meisten Webseiten nicht vom eigenen Server, sondern direkt von den Servern der Werbefirmen eingefügt werden, haben diese Firmen die Möglichkeit, mit Hilfe von Cookies Benutzerbewegungen auf allen angeschlossenen Partner-Webseiten zu verfolgen. (aus www. wikipedia.de)

Cookies erlauben es also nicht nur einem Seitenbetreiber, deine Internetaktivitäten zu beobachten, auch ein unbefugter Benutzer an deinem PC kann schnell herausfinden, wo du eigentlich so rumsurfst.

Trojaner und Backdoor-Programme

www.trojaner-info.de/

Die Kombination dieser beiden Programme macht deinen PC und die Daten, die du darauf hast, „gläsern“. Im schlimmsten Fall können sie beispielsweise Passwörter, die du eingibst, ausspionieren, heimlich in eine Datei schreiben und diese ebenso heimlich per Internet weiterschicken. Auch eine Zugriffskontrolle über deine PC-Dateien ist durchaus möglich.
Meist hängen Trojaner an heruntergeladenen Dateien (Bilder, Videos, Musikfiles) und schleusen Backdoor- („Hintertür“-) Programme auf deinen PC ein. Viele Dateien, die auf unzuverlässigen, wenig vertrauenswürdigen oder illegalen Websites zum Download bereit stehen, sind infiziert. Eine Firewall bietet *keinen* Schutz vor dem Runterladen der Trojaner; sie kann höchstens den Versuch entdecken, dass ein Backdoor-Programm heimlich Daten ins Netz senden will.
Viele Virenkiller entdecken aber zuverlässig Trojaner. Aber: das setzt voraus, dass du eine Originallizenz hast, die regelmäßig geupdatet wird!
Also:

- Original Virenkiller installieren (gibt es bereits für ca. 20 €)
- Downloads nur von vertrauenswürdigen Seiten

Downloads

Illegales Runterladen von Musik, Videos und Spielen ist leider weit verbreitet. Im Gegensatz zum Download über Internetseiten wird meist eine sogenannte „Peer-to-peer“-Verbindung eingerichtet (P2P), das heißt, zwei PCs kommunizieren direkt miteinander und tauschen die Daten aus. Solche Tauschbörsen gibt es viele, KaZaA, eDonkey, eMule, BitTorrent, Shareaza sind nur einige davon.

Vor einigen Jahren war die Musik- und Softwareproduzierende Industrie kaum hinter den „kleinen“ Downloadern her; dies hat sich aber schlagartig geändert.

Stiftung Warentest berichtet:

> „Nun hagelt es Strafanzeigen. Allein in Karlsruhe wurden 40 000 Anzeigen erstattet. Auslöser war unter anderem die Firma Zuxxez, die rund 600 000 illegale Downloads ihres Spiels „Earth 2160“ festgestellt hatte. Legal waren nur 100 000 über den Ladentisch gegangen.
>
> Vor allem die Musikindustrie schießt mit schwerer Munition auf die Nutzer: Ein 21-jähriger Student musste 4 000 Euro zahlen, ein 23-jähriger Azubi 8 400 Euro. Im Durchschnitt, so Ifpi-Sprecher Dr. Hartmut Spiesecke, seien rund 4 000 Euro fällig, im Einzelfall 15 000 Euro. Bundesweit seien 1 300 Strafverfahren eingeleitet, nach den USA weltweit die meisten.“
>
> http://www.stiftung-warentest.de/online/steuern_recht/test/1359649/1359649/1360049.html

„Viele Nutzer von P2P-Börsen glauben, sie blieben beim Download anonym. Doch das stimmt so nicht. Jeder Nutzer erhält beim Surfen eine IP-Adresse aus vier mehrstelligen Zahlen. Sie wird jedes Mal neu vergeben, wenn er ins Internet geht.

Die Schweizer Firma Logistep verfügt nach eigenen Angaben über eine Scan-Software, mit der sie Tauschbörsen überwachen und automatisch die IP-Adressen feststellen kann. Damit ist es möglich, wöchentlich mehrere Tausend Anzeigen zu erstatten. Das Risiko, beim Download entdeckt zu werden, ist also hoch.“

Wurde der illegale Download angezeigt, so passieren zwei Dinge: zunächst wird das Vergehen **strafrechtlich** verfolgt, das heißt, der Gesetzgeber bestraft den

„Täter“ für sein Vergehen. Mit Anwaltskosten können schnell Summen von mehreren 100 Euro zusammenkommen. Dazu kommt aber noch ein **zivilrechtlicher** Schadensersatz. Das bedeutet, die geschädigte Firma verlangt jetzt vom Täter (auch von Jugendlichen!) eine Entschädigung für den Verlust, der ihr entstanden ist. Natürlich wird das Unternehmen immer davon ausgehen, dass der Downloader die Filme, Musikclips und Dateien an andere weitergegeben hat und schätzt den Schaden sehr großzügig: oft auf mehrere 1000 Euro.

Die dänische Anti-Piracy-Group (APG) hat rund 150 Internet-Surfern in Dänemark Rechnungen über insgesamt 133.600 Dollar geschickt. Grund: Sie hatten sich illegal Musiktitel, Videospiele und Filme aus dem Internet heruntergeladen, wie die Computerwoche berichtet. Morten Lindegaard, Anwalt der Anti-Softwarepiraterie-Gruppe sagte, man fordere eine volle Entschädigung für das patentrechtlich geschützte Material.

Lindegaard und seine Gruppe hatten ein Softwareprogramm entwickelt, mit dem sie Surfer bis zu ihrer Internet-Protokoll-Adresse zurückverfolgen konnten.
Auf diese Weise hatten sie dänische User identifiziert, die in den beiden bekannten Peer-to-Peer-Netzen Kazaa und eDonkey unerlaubterweise Dateien auf ihre PCs herunterluden. Das Programm hielt auch fest, welches Material unerlaubterweise auf private Festplatten kopiert wurde und wann der Softwareklau ablief. Nachdem die Identität so halbwegs offenbar wurde, hatte ein dänischer Richter die Internet-Service-Provider (ISP) aufgefordert, die Rechnungsadressen von den mutmaßlichen Softwarepiraten zu offenbaren.
(…)
Die Strafen für die einzelnen Surfer betragen in Einzelfällen bis zu 13360 $. Zu den Beschuldigten gehören Schüler genauso wie Angestellte. Die APG verlangte pro Musiktitel 2,67 $, für einen illegal heruntergeladenen Film 26,70 $ und für ein Videospiel 50 $.

Die Zeiten, in denen Schüler mit Straffreiheit rechnen konnten, sind vorbei.

Also:

- Lade keine Dateien, egal ob Spiele, Videos, Filme oder Musik herunter, die urheberrechtlich geschützt sind. Bedenke, dass praktisch alle kommerziellen Erzeugnisse urheberrechtlich geschützt sind!