orell füssli

Norbert Pohlmann / Markus Linnemann

Sicher im Internet

Tipps und Tricks für das digitale Leben

Sicher im Internet
Norbert Pohlmann
Markus Linnemann
orell füssli

Ein Projekt vom Institut für Internet-Sicherheit:

securityNews: Kostenlose App für mehr Sicherheit im Netz

- Kostenlose App vom Institut für Internet-Sicherheit
- Aktuelle Sicherheitshinweise für Smartphone, Tablet, PC und Mac
- Warnung vor Sicherheitslücken in Standardsoftware, dank BSI-Schwachstellenampel
- Konkrete Anweisungen für Privatanwender und Unternehmen

» www.it-sicherheit.de

Available on the App Store

ANDROID APP ON Google play

Mit freundlicher Unterstützung

Bundesamt für Sicherheit in der Informationstechnik

Norbert Pohlmann/Markus Linnemann

Sicher im Internet
Tipps und Tricks
für das digitale Leben

Teil 5: Sicher bewegen im Internet –
Internettelefonie & Chatten,
Kindersicherung fürs Internet

orell füssli Verlag AG

Internettelefonie & Chatten – Kommunikation total

«Ich ruf dich aus Amerika an, sobald ich eine Telefonzelle gefunden habe, denn Handytelefonate und SMS aus dem Ausland sind ganz schön teuer. Allerdings fürchte ich, dass wir dann nicht oft voneinander hören werden …» Kennen Sie Sätze wie diese noch? In Zeiten des Internets gehören sie endgültig der Vergangenheit an, denn das Internet ist ein Kommunikationswunder – global und nicht standortgebunden. Urlauber können E-Mails anstelle von teuren und langsamen Briefen schreiben oder, wenn sie sich gleichzeitig mit ihrem Gesprächspartner im Internet befinden, einander Nachrichten schicken und direkt darauf antworten. Selbst um die Stimme eines anderen zu hören wird das herkömmliche Telefon nicht mehr unbedingt benötigt. Nutzer können heute mithilfe des Internets über alle Grenzen hinweg telefonieren und kommunizieren. Aber um ganz ehrlich zu sein: Eine E-Mail ist einfach nicht das Gleiche wie eine von Hand geschriebene Postkarte, die um den halben Erdball gereist ist. Nichtsdestotrotz soll in diesem Kapitel dargestellt werden, wie Sie das Internet für Telefonie und zum Chatten nutzen können und an welchen Stellen die Sicherheit eine Rolle spielt.

Internettelefonie – Wie funktioniert das?

Grundsätzlich bedeutet Internettelefonie nur, dass die Sprachdaten nicht mehr über das herkömmliche Telefonnetz übermittelt werden, sondern als Datenpakete über die Internetinfrastruktur. Daher wird die Internettelefonie als Voice over IP, kurz VoIP, bezeichnet, wobei IP (Internetprotokoll) einfach ausgedrückt das Protokoll ist, mit dem die Daten im Internet übertragen werden.

Einige Telefonanbieter nutzen VoIP bereits seit Jahren im Hintergrund, um die Sprachdaten an ihr Ziel zu befördern. Aber auch viele Nutzer telefonieren heute – manche sogar, ohne es zu wissen – mit VoIP. Denn zahlreiche DSL-Anbieter stellen den Telefondienst über das Internet zur Verfügung. In diesem Fall ist bei der ausgelieferten Hardware ein Modem dabei, an das die Telefonanlage oder das herkömmliche Telefon angeschlossen wird. Darüber hinaus gibt es natürlich auch «echte» VoIP-Telefone, die direkt an den Internetanschluss (beziehungsweise Netzwerkanschluss) angeschlossen werden. Dann müssen nur noch die Zugangsdaten des jeweiligen VoIP-Anbieters eingegeben werden, und schon kann der Nutzer telefonieren. Dabei handelt es sich entweder um reine VoIP-Anbieter, wie zum Beispiel sipgate, oder um den Provider des Internetanschlusses.

Für VoIP wird jedoch nicht zwingend ein Telefon benötigt. Die Telefonie kann genauso direkt über den Computer ablaufen. Dazu benötigt der Nutzer eine Mikrofon/-Lautsprecher-Kombination (Headset) sowie ein Softphone. Ein Softphone (siehe Abbildung 28) ist ein Computerprogramm, das ein Telefon simuliert. Sie können es kostenlos im Internet herunterladen (Softlink 371). Auch hier müssen nur

die Zugangsdaten des VoIP-Anbieters eingegeben werden, und schon kann telefoniert werden. Für Gespräche innerhalb des Internets fallen dabei normalerweise keine Kosten an.

Abbildung 28: Ein typisches Softphone

VoIP-Anbieter ermöglichen über entsprechende Gateways zudem Anrufe ins Fest- oder Mobilfunknetz. Hierfür werden zwar Gebühren berechnet, aber diese sind meist wesentlich geringer als die eines herkömmlichen Telefonanbieters.

VoIP ist technisch inzwischen sehr ausgereift und bietet in der Regel eine gute Sprachqualität sowie einige Komfortfunktionen, die beim herkömmlichen Telefonieren nicht möglich sind. Voraussetzung ist allerdings ein schneller DSL-Anschluss (mit Flatrate), der die zügige Übertragung großer Datenmengen zulässt, da beim Telefonieren die Leitung nicht

nur für den Austausch der Sprachdaten, sondern auch für die Übermittlung aller anderen Daten genutzt wird – schnelles UMTS (siehe Seite 160 f.) funktioniert natürlich ebenso. Das ist auch der Grund, warum die Sprachqualität bei einem sehr hohen Datenaufkommen leidet.

In der Standardanwendung ist VoIP nicht verschlüsselt. Das bedeutet, dass ohne zusätzliche Vorkehrungen alle Sprachdaten von Dritten, die auf irgendeine Weise an die Leitung angeschlossen sind, wie zum Beispiel andere Computer im Netzwerk, «mitgeschnitten» werden können. Es ist daher sinnvoll, einen Anbieter zu wählen, der eine Verschlüsselung zur Verfügung stellt. Geht das aus der Beschreibung nicht hervor, sollten Sie nachfragen, ob und wie der VoIP-Anbieter verschlüsselt und welche Einstellungen Sie dafür eventuell vornehmen müssen.

TIPP: Internettelefonie

- Die Qualität eines VoIP-Gesprächs hängt stark von der Leistungsfähigkeit (Bandbreite) des Internetanschlusses ab. Aktuelle DSL-Anschlüsse sind die Mindestanforderung.
- VoIP ist in der Standardanwendung nicht verschlüsselt. Informieren Sie sich deshalb bei Ihrem Anbieter, ob Ihre Telefonate verschlüsselt werden und welche Einstellungen Sie dafür gegebenenfalls vornehmen müssen.
- VoIP-Telefonie ist nur bei einer Flatrate sehr kostengünstig, da viele Daten übertragen werden.

Chatten – die moderne Echtzeitkommunikation

Chatten bedeutet so viel wie plaudern und bezeichnet die Kommunikation per Texteingabe in Echtzeit. Das ist die offi-

zielle Definition, aber es gibt mittlerweile sehr unterschiedliche Ausprägungen.

Webchat

Webchats, die in Webseiten eingebettet sind, sind die Chats der ersten Stunde. Der Nutzer meldet sich an und kann in einem Chatroom mit anderen Nutzern Textnachrichten austauschen. In den Webchats sind meist mehrere Personen gleichzeitig anwesend, aber es gibt auch die Möglichkeit, mit einzelnen Anwesenden ein «Privatgespräch» zu beginnen.

Der Erfolg der Chatrooms lässt sich auch darauf zurückführen, dass die Gesprächspartner anonym bleiben. Ein Chatter meldet sich mit einem fiktiven Namen an, und niemand weiß, wer sich dahinter verbirgt – ob Mann, ob Frau, ob jung, ob alt. Diese Anonymität hat sowohl positive als auch negative Auswirkungen.

Von Vorteil ist diese Art der Kommunikation zum Beispiel für Beratungsstellen. Die Hemmschwelle der Betroffenen, über ihre Probleme zu reden, ist dabei deutlich geringer. Auch für Serviceaufgaben lassen sich Chats gut verwenden, zum Beispiel für Supportanfragen zu Produkten oder bei Reklamationen. Auf der anderen Seite bringt die Möglichkeit, genau die Identität anzunehmen, die man gerade haben möchte, Gefahren mit sich, welche die Chats ziemlich in Verruf gebracht haben. Denn im realen Leben würde man sich intuitiv von zwielichtigen, nicht vertrauenswürdig wirkenden Menschen fernhalten und es gar nicht erst zu einer Kontaktaufnahme kommen lassen. Anonyme Chatrooms machen aber genau das nahezu unmöglich. So können auch Menschen mit kriminellen Absichten durch längere Gespräche Vertrauen bei ihrem Gegenüber aufbauen. Sollte es dann zu einem realen

Treffen kommen, kann es gefährlich werden. Deshalb ist es wichtig, dass jedem Chatter die Anonymität des Chats und ihre Folgen bewusst sind. Lassen Sie sich also nicht auf seltsame Gespräche oder spätere Treffen ein, wenn Ihr Gegenüber sich vorher nicht glaubwürdig zu erkennen gegeben hat. Außerdem sollten Sie in einem Chat nicht leichtfertig persönliche Daten preisgeben. Der gewählte Benutzername, auch Nickname genannt, den sich jeder Chatter geben muss, sollte keine Rückschlüsse auf Ihre reale Identität zulassen. Eventuell ist Ihr Gesprächspartner ein potenzieller Einbrecher und versucht über geschickte Fragen herauszufinden, wo Sie wohnen und wann Sie nicht zu Hause sind.

Eine ganz andere Gefahrenquelle stellen die Links dar, die in Chats verteilt werden. Für sie gilt dasselbe wie für Links in E-Mails und auf Webseiten (siehe Seite 73 ff.): Niemals unbedacht anklicken!

TIPP: Das sollten Sie im Webchat beachten

- Denken Sie immer daran, dass Sie in einem anonymen Chat nie sicher wissen können, wer sich hinter dem Namen des Gegenübers verbirgt.
- Geben Sie nicht leichtfertig Informationen über sich preis.
- Wählen Sie als Nickname immer einen Fantasienamen, der keine Rückschlüsse auf Sie zulässt.

Instant Messaging

Deutlich stärker verbreitet und auch in Firmen im Einsatz ist mittlerweile das Instant Messaging. Für diese Art des Chattens wird ein Programm auf dem Computer benötigt, das mit einem entsprechenden Dienst im Internet verbunden wird. Bekannte Anbieter von Messaging-Diensten sind ICQ, MSN

und GoogleTalk. Jeder dieser Anbieter stellt meist ein eigenes Programm (Messenger) für das Instant Messaging zur Verfügung. Es gibt jedoch auch freie – meist kostenlose – Messenger wie Pidgin oder Trillian, welche die Möglichkeit bieten, mehrere Konten von verschiedenen Anbietern gleichzeitig zu verwalten (siehe Abbildung 29).

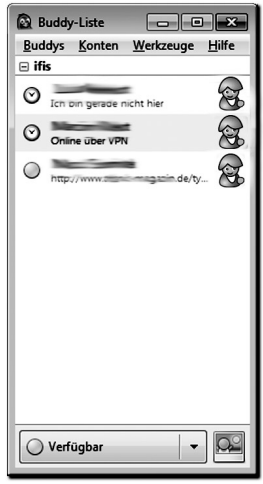

Abbildung 29: Typischer Messenger mit zwei aktiven Konten

Beim Instant Messaging führt der Nutzer eine Liste von Gesprächspartnern, mit denen er spontan Kontakt aufnehmen kann. Er kann sehen, wann die Teilnehmer online sind und in separaten Chatfenstern mit ihnen kommunizieren. Anonym ist der Gesprächspartner in diesem Fall normalerweise nicht.

Instant Messaging ist zu einer gängigen Art der Kommunikation geworden, um mit Freunden und Kollegen in Echtzeit kurze Informationen auszutauschen. Zusätzliche Komfortfunktionen, wie zum Beispiel die Übertragung von Dateien, sind bei den Messengern inzwischen Standard.

Allerdings bilden Messenger auch eine Spielwiese für Angreifer. Es gilt daher auch hier wieder das Gebot, keine unbekannten Links anzuklicken und möglichst wenige Informationen über sich preiszugeben. Schauen Sie sich dazu die angebotenen Einstellungen zur Privatsphäre genau an. Auch sollten Sie Anfragen von Fremden, die in Ihre persönliche Kontaktliste aufgenommen werden möchten, grundsätzlich ablehnen, da es sich dabei um Angriffe oder um Spam, also unerwünschte Werbeangebote, handeln kann.

Genau wie bei der Internettelefonie (siehe Seite 126 ff.) sind die Nachrichten beim Instant Messaging zunächst einmal nicht verschlüsselt. Dementsprechend sollten keine sicherheitskritischen Daten übermittelt werden. Für manche Messenger gibt es allerdings entsprechende Plug-ins, also Zusatzprogramme, die eine sogenannte Ende-zu-Ende-Verschlüsselung zwischen den Gesprächspartnern zulassen. Ein solches Plug-in ist OTR (Off-the-Record), was so viel wie «vertraulich» bedeutet. Neben der Verschlüsselung der Nachrichten kann bei OTR auch nicht mehr nachvollzogen werden, wer die Nachrichten geschrieben hat. Im Fachjargon spricht man bei dieser Funktion von Abstreitbarkeit. Das Einrichten von OTR ist einfach und basiert darauf, dass die beiden kommunizierenden Personen ein Geheimnis austauschen, beispielsweise ein Passwort (OTR-Workshop, siehe Softlink 372).

TIPP: Wichtig beim Instant Messaging

- Schauen Sie sich die Einstellungen des Messengers zur Privatsphäre an und geben Sie so wenig persönliche Informationen wie möglich preis.
- Nehmen Sie nur Ihnen bekannte Personen in Ihre Kontaktliste

auf und weisen Sie Anfragen von Unbekannten grundsätzlich zurück.
- Klicken Sie nicht unbedarft auf Links in Nachrichten, die Sie nicht zuordnen können.
- Geben Sie keine sicherheitsrelevanten Daten über einen Messenger weiter, außer Sie nutzen eine Verschlüsselung wie OTR.

Exkurs: Skype – ein prominenter Vertreter für VoIP und Messaging

Skype ist der wohl bekannteste Internettelefondienst und soll deshalb hier kurz aufgeführt werden. Er vereint Internettelefonie und Messaging, womit Skype allerdings nicht allein ist. Auch andere Dienste bieten bereits beides in Kombination an. Telefonate innerhalb des Skype-Netzes, also zwischen zwei Skype-Nutzern, sind kostenlos.

Der Nutzer hat aber darüber hinaus die Möglichkeit, Geld auf sein Skype-Konto zu laden und so auch ins Fest- oder Handynetz zu telefonieren, SMS zu schreiben oder Faxe zu verschicken. Skype-Telefonate sind verschlüsselt, allerdings gibt Skype nicht preis, auf welche Art. Im Fachjargon wird dies «Security by Obscurity» genannt, aber aktuell scheint die Verschlüsselung sicher zu sein. Hinzu kommen noch einige weitere Komfortfunktionen.

TIPP: Skype
- Skype-Telefonate sind von vornherein verschlüsselt.
- Bei der Benutzung von Skype sind alle Tipps zu beachten, die auch schon bei den Punkten «Internettelefonie» und «Messaging» genannt wurden.

Kindersicherung fürs Internet – keine Sorge um den Nachwuchs

Kinder sind «Digital Natives», das bedeutet, dass sie in eine Welt mit Computern, Internet und Handys geboren wurden. Die aktive Nutzung des Internets ist deshalb ein natürlicher Teil ihres Lebens. Es ist neben der Familie, dem Freundeskreis, der Schule und Freizeitgruppen auch erheblich an der Erziehung der Kinder beteiligt und prägt ihre Wertvorstellungen und Verhaltensweisen.

Daher muss es das Ziel sein, Kinder frühzeitig mit diesem Medium vertraut zu machen, damit sie den eigenverantwortlichen und kompetenten Umgang mit dem Computer und dem Internet lernen. Sie müssen wissen, welche Gefahren im Internet lauern, welche Regeln es einzuhalten gilt und wie man sich generell im Internet verhält. Das können Eltern, Lehrer und andere Erziehungsverantwortliche aber nur dann vermitteln, wenn sie selbst über die entsprechende Internetkompetenz verfügen!

TIPP: Entwicklung von Internetkompetenz

- Eignen Sie sich als Erziehungsverantwortlicher selbst die nötige Internetkompetenz an, damit Sie in der Lage sind, diese weiterzuvermitteln.
- Seien Sie Vorbild im Umgang mit dem Internet. Wenn Sie von Ihren Kindern erwarten, dass sie keine Musik illegal herunterladen, dann sollten Sie das ebenfalls nicht tun.
- Erkunden Sie gemeinsam mit Ihren Kindern die Nutzungsmöglichkeiten des Internets und seien Sie bereit, von Ihren Kindern zu lernen.

Welche Inhalte für Kinder geeignet sind und worauf Sie achten müssen

Kinder sind leichter zu beeinflussen, zu beeindrucken und auch zu verunsichern als Erwachsene. Deshalb sollten sie nicht auf Webseiten geraten können – absichtlich oder zufällig –, die schädlich für sie sind, wie zum Beispiel solche mit Gewalt verherrlichenden, pornographischen und rassistischen Inhalten. Aber auch soziale Netzwerke können für Kinder eine Gefahr darstellen: Pädophile versuchen, Kinder im Chat zu persönlichen Treffen zu überreden, Dealer nutzen die Internetplattform, um Drogen zu verkaufen, und Selbstmordforen gefährden Kinder, die sich in einer labilen Stimmungslage befinden.

Um Ihre Kinder davor zu schützen, sollten Sie mit ihnen regelmäßig über mögliche Gefahren reden und ihnen entsprechende Regeln und Handlungsempfehlungen an die Hand geben (siehe Tipp).

TIPP: Allgemeine Verhaltensregeln für Kinder

- Glaube nicht alles, was du im Internet liest.
- Gib niemals im Internet deinen Namen, deine Adresse und deine Telefonnummer bekannt.
- Pass auf, wenn du aus dem Internet Dateien herunterlädst.
- Sprich mit deinen Eltern oder anderen Vertrauenspersonen, bevor du dich mit Bekanntschaften aus dem Internet triffst.
- Das Internet ist kein rechtsfreier Raum.
- Das Umgehen von Schutzmaßnahmen ist verboten.
- Denke dir in Chaträumen einen Fantasienamen aus und erfinde eine Adresse (das ist keine Lüge, sondern ein Schutz).
- Vertraue deine Passwörter niemandem an.

Kinder unter zehn Jahren

Kinder unter zehn Jahren sollten bei der Nutzung des Internets sehr intensiv betreut werden und nicht unbeaufsichtigt im Internet «unterwegs» sein. Zwar reicht der Basisschutz aus, um schädliche Software abzuwehren, aber Kinder haben den gesunden Menschenverstand für das Surfen noch nicht entwickelt. Sie sind noch nicht in der Lage, sich gegen Gewaltdarstellungen, Pornographie usw. selbst zu schützen.

Für Kinder im Vorschul- und Grundschulalter gibt es im Internet ein breit gefächertes Angebot an speziellen Kinderwebseiten und Suchmaschinen, deren Inhalte dem Alter angemessen sind. Beispiele dafür sind:

- http://www.fragfinn.de
- http://www.blinde-kuh.de
- http://www.internauten.de
- http://www.internet-abc.de

Eine ausführlichere Auflistung von kindgerechten Webseiten finden Sie unter http://www.seitenstark.de. Da sich das Angebot jedoch ständig verändert, sollten Sie sich gemeinsam mit den Kindern ein Bild darüber machen, welche Webseiten tatsächlich für das jeweilige Alter angemessen sind.

Die Webseite http://schau-hin.info rät, bei der Suche nach guten Kinderwebseiten besonders auf folgende Kriterien zu achten:

- *Gut gemacht*: Die Themen der Webseite sind attraktiv, aktuell, spielerisch, kind- und altersgerecht sowie interaktiv aufbereitet. Kinder finden sich leicht auf der Webseite zurecht.
- *Sicherheit*: Damit Kinder sicher chatten können, gibt es bestimmte Mindeststandards. Dazu gehört, dass erwachsene

Moderatoren bei den Chats anwesend sind, Kinder über einen Notruf jederzeit mit der Redaktion sprechen können und Datenaustausch sowie Webcam-Übertragungen tabu sind.

- *Persönliche Daten*: Gute Kinderwebseiten sollten nur die nötigsten Angaben abfragen. Persönliche Daten wie Adresse, Telefonnummer und Hobbys bleiben geheim.
- *Keine Werbung*: Kinder können Werbung von redaktionellen Informationen nur schwer trennen. Deshalb enthalten geeignete Kinderwebseiten möglichst keine Werbung. Wenn doch, ist die Werbung klar als solche gekennzeichnet und stört nicht beim Surfen.
- *Klarer Absender*: Die Kinderwebseite beinhaltet eine kurze Selbstdarstellung. Darin wird beantwortet, worum es bei dem Onlineangebot geht, wer dahinter steckt und wie derjenige zu erreichen ist.

Kinder über zehn Jahren

Kinder, die älter als zehn Jahre sind, lassen sich in der Regel nicht mehr gern «über die Schulter» schauen. Und sie neigen dazu, alles am Computer und im Internet auszuprobieren. Die Vorteile dieses unbefangenen Umgangs mit dem Internet liegen auf der Hand: Die Kinder können mit Freunden chatten, neue Freundschaften knüpfen, spielen, Musik hören und vieles mehr.

Allerdings ist es notwendig, dass Sie als Eltern im kontinuierlichen Gespräch mit den Kindern bleiben und darüber informiert sind, was diese im Internet tun. Auch sollten Sie entsprechende Nutzungsvereinbarungen mit Ihren Kindern treffen (wie oft und wie lange).

TIPP: Vereinbarungen mit Kindern

- Stellen Sie für Ihre Kinder Regeln bezüglich der Nutzung des Internets auf (zeitlich und inhaltlich) und achten Sie auf deren Einhaltung.
- Verabreden Sie mit Ihren Kindern, dass sie Ihnen Dinge im Internet zeigen, die ihnen seltsam vorkommen oder Angst machen.

Kinderschutzprogramme

Es gibt auch Software, die dabei hilft, das Risiko für Kinder im Internet zu minimieren. Beispiele für kostenlose Jugendschutzprogramme sind www.parents-friend.de und www.jugendschutzprogramm.de.
Das Leistungsspektrum solcher Programme ist umfangreich. In der Regel bieten sie folgende Sicherheitsmaßnahmen:

- Sperrung bestimmter Webseiten
- Beschränkung der Zeiten, innerhalb derer das Internet oder der Computer durch die Kinder genutzt werden kann.
- Beschränkung der Laufzeiten bestimmter Programme, wie zum Beispiel von Computerspielen.
- Absicherung von Systemeinstellungen, die Kinder versehentlich oder bewusst verändern möchten.
- Einschränkungen von Verzeichnissen, Laufwerken und Programmen

Neben Jugend- und Kinderschutzprogrammen für den gesamten Computer gibt es auch entsprechende Add-ons für den Browser. Ein Beispiel hierfür ist das Add-On Glubble für den Firefox (Softlink 381), das wie auf Seite 45 beschrieben installiert wird. Damit lässt sich eine Familienseite anlegen,

und es können Rechte für die einzelnen Familienmitglieder vergeben werden. Wird der Browser in den Kindermodus geschaltet, bekommt er ein kindgerechtes Aussehen und zeigt nur noch bestimmte Seiten an. Möchte das Kind einen Inhalt sehen, der noch nicht freigeschaltet ist, kann es automatisiert eine Anfrage an die Eltern senden. Achtung: Ist ein zweiter Browser ohne Kinderschutz installiert, kann das Kind natürlich auch diesen nutzen und ungeschützt im Internet surfen. Das sollte entsprechend vermieden werden. Glubble sollte jedoch immer nur ein unterstützender technischer Zusatz sein und das gemeinsame Entdecken des Internets nicht ersetzen.

TIPP: Verbotene Inhalte

Wenn Sie oder Ihre Kinder fragwürdige oder verbotene Webseiten und Angebote im Internet entdecken, dann melden Sie dies dem Verband zur Freiwilligen Selbstkontrolle unter www.internet-beschwerdestelle.de. Diese Einrichtung kann gegebenenfalls geeignete Schritte gegen den Webseitenbetreiber einleiten. Weitere und aktualisierte Informationen zum Kinderschutz im Internet finden Sie unter Softlink 382.

Freuen Sie sich auf Teil 6:
Antennen ausfahren – Zugang zum Internet

Ab 11.02.2013 zum kostenlosen Download auf
www.internet-sicherheit.de