



Mailen und Surfen – mehr müssen Sie nicht tun, um im Internet Spuren zu hinterlassen, die missbraucht werden können. Doch Sie können sich schützen.

■ von Bruno Habegger

Das Heer der neugierigen oder sogar gefährlichen Datenschnüffler ist fast unüberschaubar: Kriminelle ziehen unbedarften Anwendern mit allerlei Tricks das Geld aus der Tasche, Cracker versuchen in Ihren PC einzubrechen und Kreditkartendaten zu stehlen, Viren und Würmer attackieren ungeschützte PCs, Staat und Industrie versuchen die totale Kontrolle über die Online-Nutzer zu erlangen, Online-Belästiger, die so genannten Cyberstalker, kommunizieren ungefragt mit fremden Menschen, nerven und verängstigen sie. Darum muss Ihr Grundsatz im Internet sein: so viel Offenheit wie nötig, so viel Privatsphäre wie möglich.

Wir zeigen Ihnen Bereiche, wo Sie – wissentlich oder unwissentlich – persönliche Daten hinterlassen, und geben allgemeine Hinweise, wie Schnüffler arbeiten und wie Sie sich schützen. Erst wenn Sie wissen, wo Ihre privaten Daten zu

finden sind, können Sie leichter Vorkehrungen gegen den Missbrauch treffen und behalten die Kontrolle darüber, wer was von Ihnen weiss. Die vorgestellten Quellen können Sie aber durchaus auch positiv nutzen, etwa zum Wiederauffinden alter Klassenkameraden.

Wer sich schon heute umsichtig verhält, ist gerüstet für die immer ausgefeilteren Technologien, Menschen via Internet zu durchleuchten.

Verräterische E-Mail-Adressen

Hier finden Schnüffler Ihre Daten: Eine E-Mail-Adresse ist meist der Ausgangspunkt für eine Personenrecherche. Die elektronische Adresse wird oft einfach durch Erraten gefunden, nach dem Muster «vorname.nachname@provider.ch».

Nutzer von Gratismaildiensten verstecken sich oft hinter Fantasiebezeichnungen. Eine Adresse wie hobbit@provider.ch verrät zwar nicht den Namen, gibt aber Aufschluss über Hobby und Vorlieben einer Person.

Zentrale Register, in denen sämtliche Adressen aufliegen, gibts aus Gründen der Spam-Vermeidung nicht. Der MetaEmailSearchAgent (MESA, <http://mesa.rzn.uni-hannover.de>) ist aber eine recht ergiebige Adressquelle. Geben Sie hier einen Namen ein – vielleicht spuckt die Suchmaschine eine passende E-Mail-Adresse aus. Da viele Leute sich mittlerweile scheuen, ihre E-Mail-Adressen einem solchen Verzeichnis bekannt zu geben, ist die Chance grösser, alte Adressen zu finden, die unter Umständen noch aktiv sind.

Wissen Schnüffler, wo jemand arbeitet, ist die Person vermutlich unter vorname.name@firma.ch oder vname@firma.ch erreichbar. Auf der Firmen-Website recherchieren Schnüffler persönliche Details: Manche Firmen oder Institutionen bieten Telefonlisten oder umfangreiche Organigramme öffentlich an.

Gegenmassnahmen:

■ Lassen Sie keine E-Mail-Adressen in Telefonbuch- oder E-Mail-Directories registrieren.

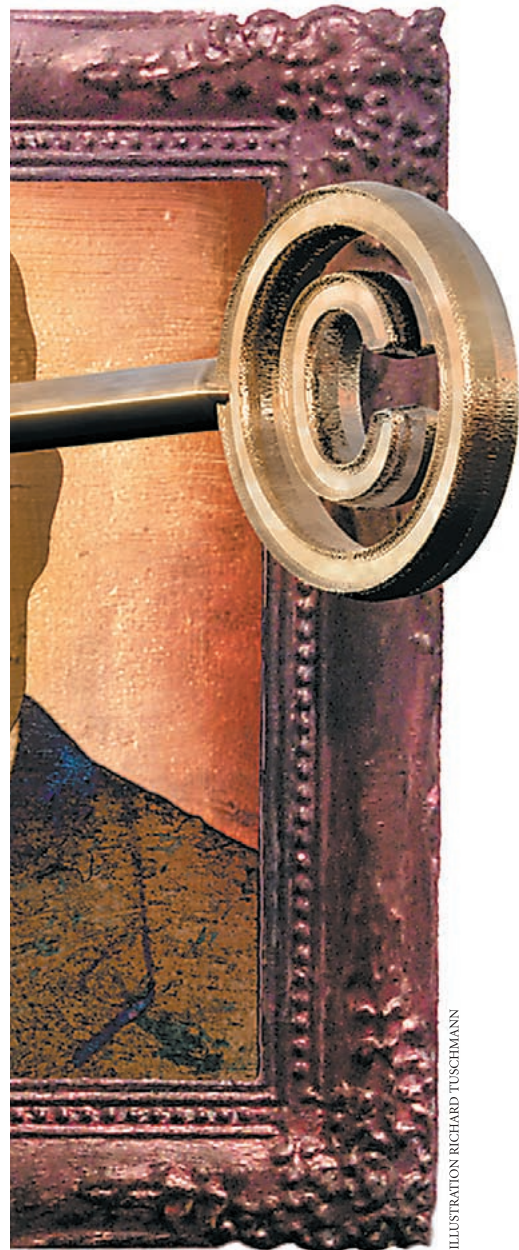
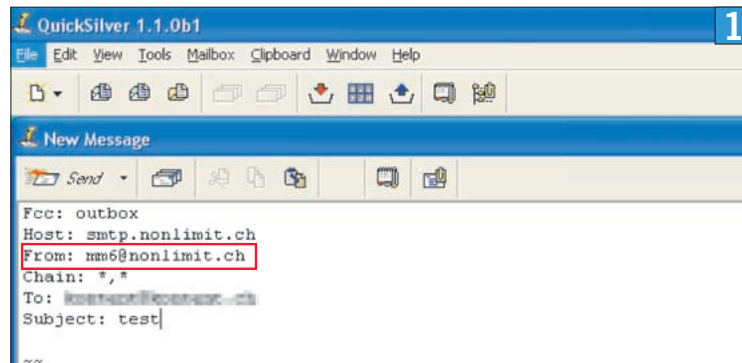
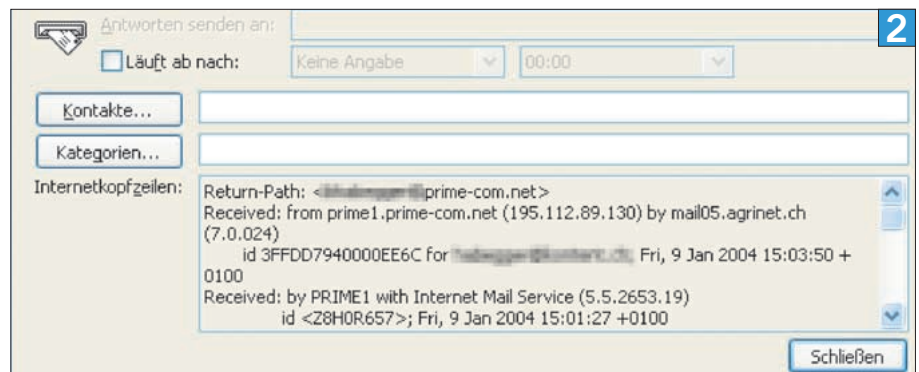


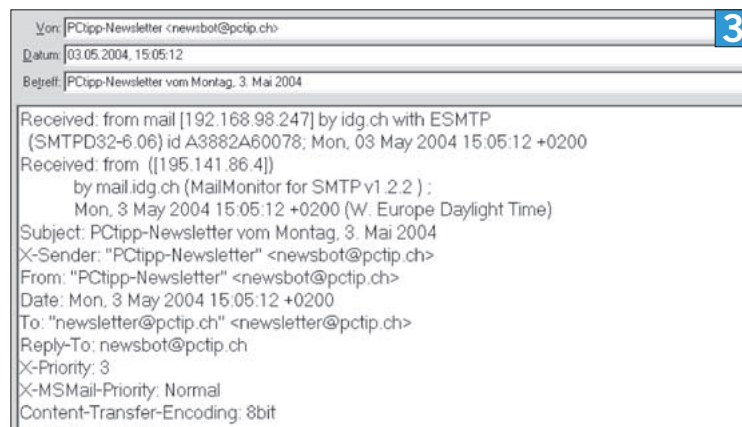
ILLUSTRATION RICHARD TUSCHMANN



1 Mit QuickSilver verbergen Sie Ihre E-Mail-Adresse



Den Header finden Sie in einer geöffneten Outlook-2003-Nachricht über ANSICHT/OPTIONEN



3 Im Header erfahren Sie einiges über den Absender, hier die Mail des PCtipp-Newsletters

■ Verwenden Sie für öffentliche Bereiche und im Kontakt mit Unbekannten immer Gratisadressen (z. B. von Freesurf, Bluemail oder Hotmail), die Sie im Notfall wieder aufgeben können. Wählen Sie eine Adresse (Zeichenfolge vor dem @, die nichts mit Ihrer Person zu tun hat).

■ Geben Sie Ihre ganz persönliche E-Mail-Adresse nur ausgewählten Personen.

■ Verwenden Sie anonyme E-Mail-Dienste. Diese verschleiern den Weg Ihrer Nachricht. Anleitung samt Linkliste unter www.anon.gildemax.de.

Ein praktischer Dienst, um Ihre E-Mail-Adresse zu verbergen, ist QuickSilver. Laden Sie das Gratis-Programm herunter (<http://quicksilver.skuz.net>). Ein – leider englischer – Assistent führt Sie durch die Einrichtung des Programms. Eine genaue Anleitung finden Sie hier: <http://kai.iks-jena.de/quick/index.html>. Danach können Sie mit dem Programm bequem anonyme E-Mails versenden – Ihre eigene Adresse taucht nirgends auf, **Screen 1**.

Gar nicht nett: E-Mail-Kopfzeilen

Hier finden Schnüffler Ihre Daten: Antworten Sie einem Unbekannten auf seine E-Mail, laufen Sie Gefahr, in eine Schnüfflerfalle zu tappen: Die Kopfzeilen (der so genannte Header) Ihrer E-Mail-Antwort legt viele Details über Sie offen.

Überprüfen Sie es selbst: Öffnen Sie eine beliebige Nachricht in Ihrer Mailbox. Wie Sie in der geöffneten E-Mail zur Header-Ansicht gelangen, unterscheidet sich von Mailprogramm zu Mailprogramm. In Outlook Express klicken Sie in der Ordneransicht mit der rechten Maustaste auf eine Mail und wählen EIGENSCHAFTEN/DETAILS/QUELLETEXT. Maximieren Sie das folgende Fenster, um einen besseren Überblick zu bekommen. In Outlook XP wählen Sie ANSICHT/OPTIONEN, **Screen 2**.

Sie sehen jetzt z. B. schon, welches E-Mail-Programm der Absender verwendet. Das ist eine wichtige Information, wenn Ihnen jemand ein Spionage-Programm unterjubeln will. Die An-

gabe finden Sie in der Zeile «X-Mailer» oder «User Agent». Fehlt die Zeile, stammt die Nachricht wohl von einem Webmail-Service.

Wichtig sind auch die «Received»-Zeilen. Es handelt sich um die eigentlichen, von den transportierenden Mailservern hinzugefügten Zustellvermerke. Sie geben unter anderem Auskunft über den Provider des Absenders. Die letzte Zeile ist im Prinzip die erste, stammt also vom eigenen Mailserver, **Screen 3**.

Wollen Sie selbst mit Hilfe des Headers einem üblen Zeitgenossen auf die Spur kommen, der Sie beispielsweise mit Spam eindeckt oder gar mit Viren, sollten Sie nicht allzu viel auf die Header-Informationen geben: Viele Angaben in der Kopfzeile lassen sich fälschen. Im Prinzip müssen Sie mit Hilfe von Tools wie der IP-Adressensuche unter www.network-tools.com überprüfen, ob die IP-Adressen mit den angegebenen Servernamen übereinstimmen. Die IP-Adresse ist eine vom Provider zugeteilte Nummer. Suchen Sie ►

erst mit der vorhandenen IP-Adresse nach einem Domain-Namen und dann mit diesem Domain-Namen wiederum nach der passenden IP-Adresse. Details zur Analyse von Kopfzeilen lesen Sie auf www.th-h.de/faq/headerfaq.html. Wie man Mails seziert, lesen Sie im PCtipp-Online-Archiv unter www.pctipp.ch mit **WEBCODE pdf020740**.

Gegenmassnahmen:

■ Verwenden Sie für heikle Nachrichten eine Webmail-Oberfläche. Die meisten Provider bieten eine solche an: Green bereits auf der Homepage www.green.ch, Bluewin auf www.blue-mail.ch. Meist melden Sie sich mit demselben Benutzernamen/Passwort an, die Sie auch für die Abfrage mit dem E-Mail-Programm erhalten haben. Wählen Sie wenn vorhanden die Option «Sicheres E-Mail» – dann wird die Kommunikation mit dem Mailserver verschlüsselt.

■ Anonyme Postfächer schützen Ihre Privatsphäre (siehe vorangegangener Tipp).

Auskunftsfreudige Domain-Registrierstellen

Hier finden Schnüffler Ihre Daten: Homepage-Besitzer mit eigenem Domain-Namen sind leicht aufzuspüren. Die Schweizer Registrierstelle Switch (www.switch.ch) führt eine öffentlich zugängliche Datenbank mit Post- und E-Mail-Adressen der Domain-Halter. So gehört z.B. die Adresse www.pctipp.ch der Firma IDG. Schnüffler können der Suchmaschine einen Familiennamen an-

AUF EINEN BLICK

Ihre Spuren im Internet

■ Die **E-Mail-Adresse** verrät Arbeitgeber und Provider.

■ Die **persönliche Website** liefert Details zum Privatleben.

■ **Domain-Registrierstellen** verraten Postadressen und Telefonnummern.

■ Die **Arbeitgeber-Website** verrät berufliche Details wie Kollegen, Arbeitsumfeld und Abteilungen.

■ **Newsgroups** und **Chatrooms** erlauben Rückschlüsse auf private oder sogar intime Details.

■ **Tauschbörsen** offenbaren die IP-Adresse eines Anwenders. Unvorsichtige Nutzer stellen heikle Dokumente oder illegale Dateien in den freigegebenen Ordner.

■ **Einträge in Gästebüchern** verraten persönliche Kontakte.

■ **Server** halten Verbindungsdaten (z.B. IP-Adressen) und Aktivitäten in Logdateien fest.

■ Die Inhalte von **Webformularen**, **Kreditkartendaten** und **Kundenprofilen** dienen dem Firmemarketing und werden oft an andere Anbieter verkauft.

■ **Amtsstellen** bieten Adressdaten immer häufiger per Internet an.

geben oder einen möglichen Domain-Namen. Besitzt eine Person mehrere Domain-Namen, gibt die Trefferliste möglicherweise Aufschluss über Hobbys oder Leidenschaften. Internationale Domain-Namen-Halter finden sich z.B. auf http://uwhois.com. Die Suchmaschine ist für Schnüffler allerdings weniger interessant, weil sie keine Personennamen schluckt.

Gegenmassnahmen:

■ Wollen Sie nicht lokalisiert werden, nutzen Sie eine Gratis-Homepage ohne eigenen Domain-Namen, also z.B. www.mypage.bluewin.ch/meineseite anstatt www.meineseite.ch. Die meisten Provider bieten für solche Zwecke genügend Platz

an. Die Webseite ist dann über eine lange Adresse des Providers zu erreichen. Vorsicht: Manche Anbieter wie Bluewin bieten eine Suchmaschine für private Sites an.

■ Network Solutions (www.networksolutions.com) bietet für 5 Dollar pro Jahr an, die persönlichen Daten des Domain-Halters vor neugierigen Blicken zu verbergen. Allerdings können Sie dann keine .ch-Domain-Namen registrieren.

Tratschtanten Google & Co.

Hier finden Schnüffler Ihre Daten: Suchmaschinen sind ergiebige Quellen für private Informationen. Tippen Sie mal «cv.doc» ein, der geläufige Datei-

name für Lebenslauf (Curriculum Vitae), und staunen Sie: Mehr als 18000 Menschen stellten ihren detaillierten Lebenslauf online. Oder kombinieren Sie einen Firmennamen mit dem Wort «Lebenslauf»: Jeder Mensch nennt in seinem Lebenslauf mehrere Firmennamen, und auch Firmen veröffentlichen auf ihrer Homepage häufig private Mitarbeiterdaten.

Suchmaschinen helfen Schnüfflern auch beim Aufspüren von privaten Websites. Sie können es selbst bei einem beliebigen Provider ausprobieren. Einige, wie zum Beispiel Bluewin auf <http://mypage.bluewin.ch>, bieten eine Suchmaschine oder einen Katalog der gespeicherten privaten Homepages an.

Mit ein Grund für mehr Vorsicht: Schon allein mit Ihren Online-Adressdaten können Unbekannte zum Beispiel bei Versandhäusern massenhaft Waren bestellen.

Gegenmassnahmen:

- Stellen Sie Ihren Lebenslauf nicht online, oder, wenns denn unbedingt sein muss, nur stark gekürzt und allgemein formuliert.
- Lassen Sie generell Vorsicht walten beim Publizieren persönlicher Angaben auf Homepages (zum Beispiel privaten Seiten oder Weblogs).
- Nie veröffentlichen: Telefonnummer und private Adresse.
- Ebenfalls heikel sind Namen von Kindern, vom Partner, Details über die eigene Firma und den Arbeitsalltag.

Geschwätzige Diskussionsforen

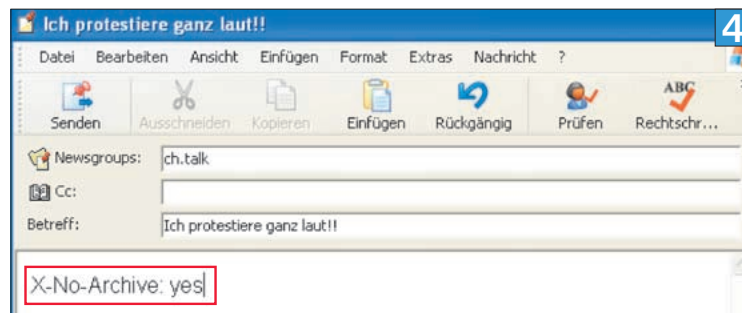
Hier finden Schnüffler Ihre Daten: Google weist eine besondere Suchfunktion aus, die Schnüffler und neugierige Anwender geradezu herausfordert: Google Groups (<http://groups.google.ch>). Hier sind sämtliche Beiträge des Usenets seit 1981 gespeichert. Damit googelt man in der Vergangenheit. Das Usenet ist ein besonderer Teil des Internets, der ausschliesslich Diskussionsforen («schwarze Bretter») enthält.

Wer irgendwann mal einen Beitrag zu einer Diskussion geleistet hat, ist unter Umständen geliefert. Etwa der anfänglich seriös wirkende Buchhalter, der früher mal in einer dubiosen Diskussionsgruppe für ein noch dubiores Schneeballsystem warb. Oder die Hobby-Marathonläuferin, die in einer Newsgroup ein ihr peinliches Leiden offenbarte, weil sie dachte, unter Gleichgesinnten zu sein. «Ich war geschockt», sagt sie, «als mir jemand mailte, mein Beitrag sei nun für immer von jedermann abrufbar.»

DATENSAMMLER

Was Ihr Browser verrät

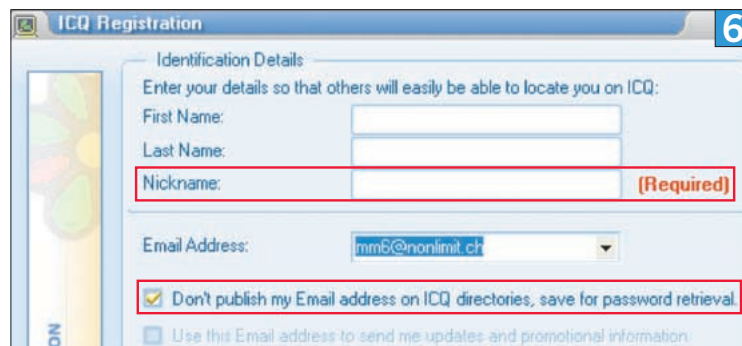
Wenn Sie eine Website besuchen, hinterlassen Sie auf dem Logfile (einem Protokoll aller Besuche) des Webserverns Spuren. Sie bemerken es nicht – aber der Server sammelt einige Daten über Ihren PC und dessen Konfiguration. Auf <http://check.lfd.niedersachsen.de> können Sie dies nachprüfen. Die Daten werden in den meisten Fällen technisch verwertet, etwa um den Besucher auf eine bestimmte Sprachseite umzuleiten oder gewisse Funktionen aufzurufen. Sie geben Schnüfflern auch gewisse Anhaltspunkte.



Wenn Sie Ihren Newsgroup-Beitrag so beginnen, wird er nicht archiviert



Hier können Sie versuchen, jemanden zu finden, der leichtsinnig genug war, seinen Namen einzufügen



Der Nickname reicht für dieses ICQ-Formular. Das Veröffentlichen der E-Mail-Adresse verhindern Sie durch ein Häkchen

Gegenmassnahmen:

- Seien Sie generell vorsichtig beim Publizieren persönlicher Angaben.
- Eröffnen Sie eine anonyme E-Mail-Adresse, die Sie nur für die Teilnahme in Newsgroups verwenden.
- Es widerspricht zwar der Etikette in Newsgroups, aber trotzdem: Für einzelne heikle Anfragen können Sie ein Pseudonym verwenden. Wenn Sie erklären, weshalb Sie dies tun, dürften die anderen Mitglieder Verständnis für diese Massnahme aufbringen.
- Verwenden Sie die Header-Zeile «X-No-Archive: yes». Das geht am einfachsten, indem Sie diese Zeile in die erste Zeile Ihres Nachrichtentextes einfügen. Dann wird Ihr Posting nicht archiviert, **Screen 4**.

I see you: Instant Messaging

Hier finden Schnüffler Ihre Daten: Das umfangreiche Mitgliederverzeichnis der beliebtesten Chat-Software ICQ erreichen Sie unter <http://web.icq.com/whitepages>.

Zwar müssen neue Mitglieder bei der Registrierung (siehe «Gegenmassnahmen», unten) keine persönlichen Daten angeben, viele tun es aber trotzdem – freiwillig. Suchen Sie jemanden, tippen Sie in die Felder des englischsprachigen Formulars zunächst nur den Vornamen (First Name) und den Nachnamen (Last Name) ein, **Screen 5**. Die Option «Only Online Users» zeigt alle Mitglieder an, die zurzeit online sind. Sie sehen, eine gewisse Vorsicht beim Ausfüllen des Anmeldeformulars ist angebracht.

Beim Konkurrenten MSN finden Sie das Mitgliederverzeichnis unter <http://members.msn.com>. Bei diesen Member-Verzeichnissen von Instant-Messaging-Anbietern ist grösste Vorsicht geboten: Viele der Profile sind gefälscht und führen zu Porno-Seiten.

Gegenmassnahmen:

- Blockieren Sie bei der Installation, dass Ihre E-Mail-Adresse im ICQ-Verzeichnis gespeichert wird. Sie müssen hier auch nur Ihren «Nickname» (Fantasiennamen) eingeben, **Screen 6**.

ANONYMIZER

Tarnkappen-Surfer

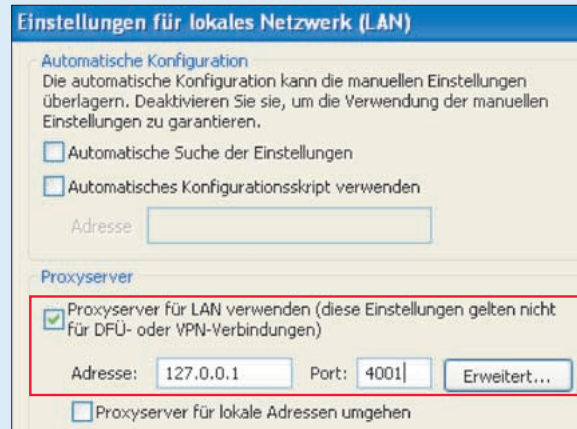
Um sich vor Schnüffeleien zu schützen, verwenden Sie einen so genannten Proxyserver, über den Sie künftig beim Surfen einen Umweg machen und so Ihre Spuren verwischen.

Als effektivster Dienst gilt JAP (Java Anonymous Proxy)

<http://anon.inf.tu-dresden.de>, ein Projekt der Uni Dresden. Dazu müssen Sie sich die Java-Software von der Webseite herunterladen und gemäss Anleitung installieren. Falls noch kein Java installiert ist, laden Sie sich das vollständige Setup-Programm herunter. Im Webbrowser muss dann nur noch der JAP-Proxyserver eingetragen werden. Dazu gehen Sie im Internet Explorer zu EXTRAS/INTERNETOPTIONEN/VERBINDUNGEN/LAN-EINSTELLUNGEN/EINSTELLUNGEN. Hier setzen Sie bei Punkt «Proxyserver für LAN verwenden» ein

Häkchen und tragen als Adresse 127.0.0.1 und als Port 4001 ein, [Screen](#). Wollen Sie anonym surfen, starten Sie die JAP-Software und wählen die Option «Anonymen Webzugriff aktivieren». Dann öffnen Sie den Internet Explorer.

Die Surfgeschwindigkeit verlangsamt sich leider etwas. Möchten Sie wieder ungeschützt ins Netz, müssen Sie im Internet Explorer die Proxy-Einstellungen wieder deaktivieren, indem Sie das zuvor gesetzte Häkchen entfernen.



Die Proxyserver-Einstellungen für JAP

Den folgenden Fragebogen überspringen Sie besser. Im nächsten Fenster, [Screen 7](#), wählen Sie im Kästchen «Privacy & Security Settings» den Punkt «My authorization is required...» aus. So müssen Fremde immer zuerst Ihr Einverständnis einholen, bevor Sie in deren Kontaktliste aufgenommen werden.

■ Unterdrücken Sie die Kontaktaufnahme durch Unbekannte im MSN Messenger. Die Einstellungen finden sich in EXTRAS/OPTIONEN/PRIVATSPHÄRE, [Screen 8](#). Hier legen Sie fest, wer bei Ihnen anklopfen darf (links) und wer abgeblockt werden soll (rechts).

■ Sämtliche sicherheitsrelevanten Einstellungen lassen sich in MAIN/PREFERENCES AND SECURITY jederzeit verfeinern, [Screen 9](#).

Auskunftsreudige Telefonbücher

Hier finden Schnüffler Ihre Daten: In der Schweiz ist der Eintrag ins Telefonbuch schon seit Jahren keine Pflicht mehr. Trotzdem sind die elektronischen Telefonbücher im Internet oder auf CD-ROM noch immer eine wertvolle Informationsquelle. Weisseseiten (www.weisseseiten.ch) bietet den vollen Swisscom-Bestand, der sich sogar über die Eingabe einer Telefonnummer durchsuchen lässt.

Auf www.telefonbuch.com finden sich beinahe alle Links zu internationalen Online-Telefonbüchern.

Gegenmassnahme:

■ Alle Festnetztelefonkunden können sich nachträglich aus den Verzeichnissen entfernen lassen. Kontakt: 0848 86 80 86 (8 Rp./Min.). Dabei haben Sie die Wahl zwischen einer totalen Sperre für Telefonbuch- und Online-Abfrage (liste noire), einer Sperre nur fürs Telefonbuch (liste verte) sowie einer totalen Sperre der Telefonnummer, nicht aber der Adresse (liste rouge).

Wegweisende IP-Adressen

Hier finden Schnüffler Ihre Daten: IP-Adressen braucht es immer, wenn zwei Computer mittels des TCP/IP-Protokolls Daten austauschen. Es handelt sich dabei um die «Hausnummer» eines online erreichbaren PCs. Ohne diese Nummer kein Datenaustausch. In Tauschbörsen etwa verraten sich so Nutzer. Die Musikindustrie zwingt mit Klagen die Provider, die zur IP-Nummer gehörenden Nutzerdaten herauszurücken. Nur der Provider weiss nämlich, welcher seiner Kunden zu welcher Zeit auf welcher bestimmten Seite verweilte oder einen bestimmten Service nutzte.

Für Schnüffeleien und zum Eingrenzen des Suchgebietes reichen auch Online-Tools wie beispielsweise VisualRoute (<http://visualroute.visualware.com>). Nach Eingabe einer IP-Adresse zeigt der Service auf einer Karte den Einwahlpunkt des Surfers an. Zur Nutzung des Tools muss Java im Browser installiert sein (www.java.com).

Gegenmassnahmen:

■ Surfen Sie mit Tarnkappe und verwenden Sie anonyme Proxyserver. Das Prinzip: Sie holen sich die Daten nicht direkt von den entsprechenden Webservern ab, sondern über den Umweg via einen Proxyserver. Mehr darüber lesen Sie im Kasten «Tarnkappen-Surfer», links.

■ Seien Sie sich mit jedem Klick bewusst, dass Sie ohne besondere Schutzmassnahmen nie anonym unterwegs sind. Sogar mit Proxyserver-Tarnkappe nicht. Mindestens der Betreiber dieses Servers weiss mit Sicherheit, wo Sie im Internet unterwegs waren.

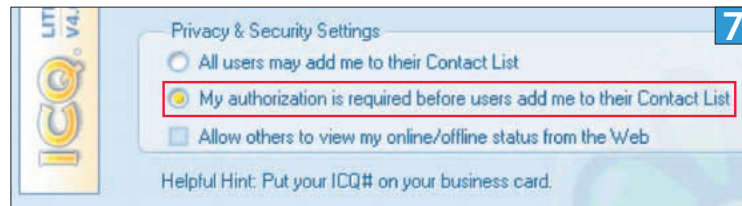
■ Alle anonymen Surfdienste auf einer Seite: <http://anonbrowse0.cjb.net>. Geben Sie einfach die Adresse ein, die Sie aufsuchen wollen, und schon gelangen Sie anonym ans Ziel.

Amtsstellen

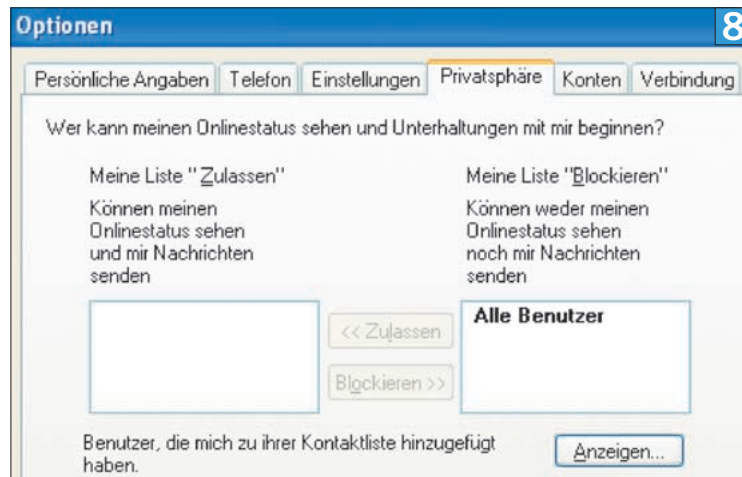
Hier finden Schnüffler Ihre Daten: Adressdaten sind bei der Einwohnerkontrolle jeder Gemeinde registriert. Je mehr Geschäfte am Online-Schalter abgewickelt werden, desto einfacher wird es für Schnüffler, an die Daten zu kommen. Die Stadt Zürich etwa bietet ein Webformular und verschickt für eine Gebühr von 10 Franken Name, Adresse und Datum von Zu- und Wegzug. Wer einen Interessennachweis erbringt, zum Beispiel eine Betreuungskunde, erfährt sogar, wohin die gesuchte Person umgezogen ist.

Gegenmassnahmen:

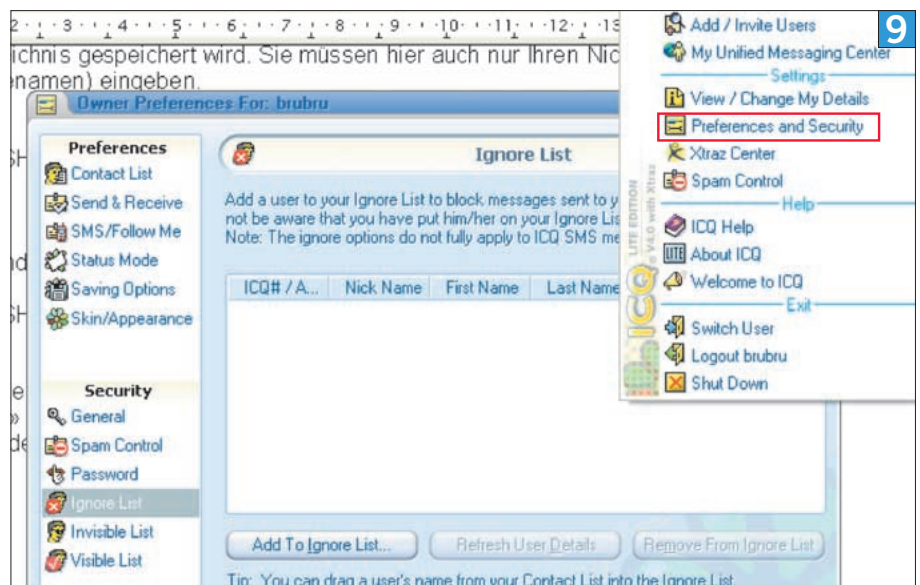
■ Nehmen Sie Einsicht in die gespeicherten Daten und lassen Sie diese wenn möglich sperren. Allerdings: In bestimmten Fällen – etwa bei Anfragen von Polizei und anderen Amtsstellen – dürfen Adressen trotz Sperre bekannt gegeben werden. Aber das muss Sie nicht weiter bekümmern: Schliesslich sind Sie in dieser Geschichte nicht der «Bad Guy».



7 Lassen Sie sich nur mit ausdrücklicher Erlaubnis in eine ICQ-Kontaktliste aufnehmen



8 MSN Messenger: unerwünschte Kommunikation blockieren



Unter MAIN/PREFERENCES AND SECURITY finden Sie in ICQ viele wichtige Einstellungen

AUF EINEN BLICK**Spionageabwehr**

■ Gehen Sie mit Ihren Daten überlegt um. Nicht jeder Dienst muss Ihren Namen und die Adresse kennen. Oft steht in Eingabefeldern, dieses oder jenes Feld sei zwingend. Meistens können Sie beliebige Zeichen eingeben – und die Eingabe wird akzeptiert.

■ Geben Sie niemals per Mail oder am Telefon Auskunft über Passwörter oder die von Ihnen genutzte IT-Infrastruktur (PC, Betriebssystem, Netzwerk).

■ Halten Sie Ihren PC auf dem neusten Stand. Das heisst: Regelmässig Windows Update (<http://windowsupdate.microsoft.com>) besuchen, Firewall- und Antiviren-Software verwenden.

■ Verwenden Sie Anti-Spionage-Tools wie Ad-aware (www.javasoft.de) oder Spybot Search & Destroy (<http://security-kolla.de>). Weitere Programme finden Sie im Download-Bereich von www.pctipp.ch.

■ Falls Sie doch persönliche Daten wie Adresse und Telefonnummer veröffentlichen, schützen Sie sich gegen das automatisierte Auslesen. Machen Sie einen Screenshot von Ihren persönlichen Angaben und fügen Sie diese als Bild auf Ihrer Webseite ein, so lassen sie sich nicht automatisch auslesen.

■ Eröffnen Sie eine nur für die Öffentlichkeit bestimmte anonyme E-Mail-Adresse.