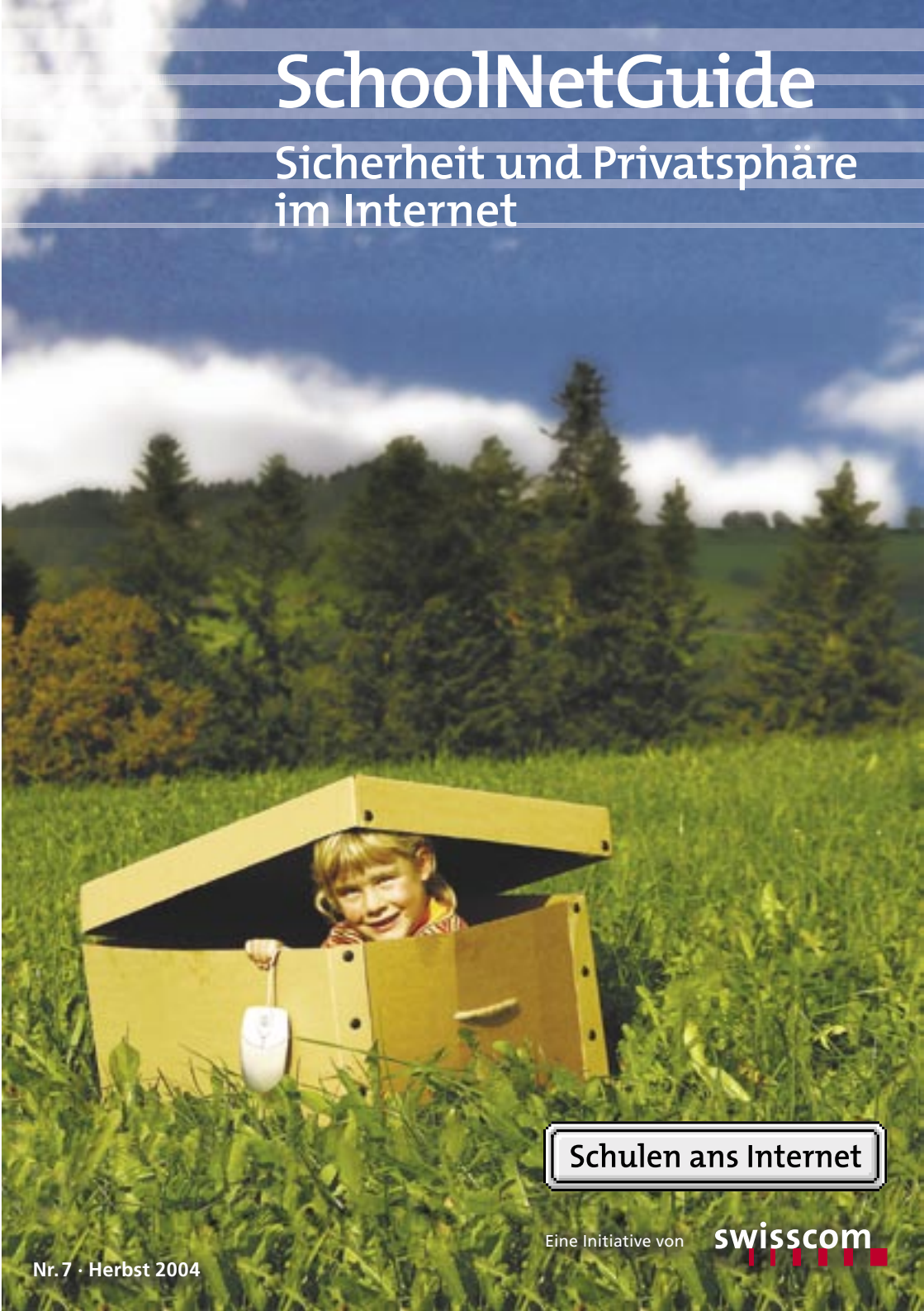
# SchoolNetGuide

## Sicherheit und Privatsphäre im Internet



Schulen ans Internet

Eine Initiative von swisscom

Nr. 7 · Herbst 2004

# Grusswort des Herausgebers


Liebe Internet-Nutzer

Mit den letzten Ausgaben des SchoolNetGuide richteten wir uns teils an Lehrpersonen, teils an die Eltern von Schulkindern. Das Thema dieser siebten Ausgabe – Sicherheit – betrifft uns alle: in der Schule, im Familienkreis oder im Berufsleben.

Fragen zur Sicherheit stellen sich nicht erst seit dem Erfolg des Internets, sondern begleiten uns im Alltag von jeher; wir haben uns an sie gewöhnt, können Gefahren einschätzen und damit umgehen. Wir wissen, dass Sicherheitsschlösser an der Haustür nicht prinzipiell unüberwindbar sind, fühlen uns aber sicher genug, um nachts ruhig schlafen zu können. Angesichts des Hinweisschilds «Achtung Diebe» beim Check-in am Flughafen geraten wir nicht in Panik oder entscheiden uns gar, in Zukunft lieber ganz auf das Fliegen zu verzichten. Und im vollen Tram achten wir automatisch besser auf das Portemonnaie als beim Spaziergang im Grünen.

Diese Prinzipien – Gefahren kennen, sich davor schützen, angemessen handeln im Einzelfall – gelten auch für Sicherheit und Privatsphäre im Internet. Auf den folgenden Seiten erfahren Sie, woher welche Gefahr drohen kann, welche Sicherheitsvorkehrungen es gibt und wie Sie im Bedrohungsfall reagieren sollten.

Mit dem diesmal etwas umfangreicheren SchoolNetGuide tragen wir zur Ausstellung «Cybernetguard» im Verkehrshaus der Schweiz in Luzern bei, die wir gerne unterstützt haben.

Sicheres und unbeschwertes Surfen wünscht Ihnen

Swisscom AG

M. Pfister

Marc Pfister
Leiter Schulen ans Internet

# Inhalt

**1. Gefahren und Ärgernisse**
Wieso gibt es Sicherheitsprobleme? 4
Von wo kommt die Gefahr? 5
Vorsicht beim Mailen! 6
Ärgernisse im Posteingang 8
Betrügerische E-Mails 9
Vorsicht beim Surfen 10
Vorsicht mit sensiblen Daten 12
Wehret den Spionen 14
Übersicht Bedrohungen 15

**2. Sicher daheim**
Gefahren trotz neuem PC 16
Gefahren beim Internet-Zugang 17
Das 3x3 der Sicherheit zu Hause 18
Firewall und Antiviren-Software 19
Einrichten von Schutz-Software 20
Komplettlösung von Norton 21
Die Frage der sicheren Einstellung 22
Aktualisierungen (Updates) 24
Sicherheitskopien (Backups) 25
Sicherheitslücke Passwort 26
Regeln fürs Mailen 27
Regeln fürs Surfen 29
Richtiges Verhalten im Notfall 30
Linktipps zur Selbsthilfe 32

**3. Sicherheit im Zahlungsverkehr**
Der richtige Kunde – die echte Firma 33
Sicheres Bezahlen 34
Beispiel Direct Net 35

**4. Drahtlose Kommunikation**
Kabellose Netzwerke sichern 36

Checkliste 38
«Verkehrserziehung» für die Datenautobahn! 39
Index 40
Bestelltalon 41
Weiterführende Links 43
Impressum 43

## PaperLink

Alle in dieser Broschüre verzeichneten Links können Sie schnell und einfach mit «PaperLink» aufrufen: **700 www.swisscom.com/sai**

1. Rufen Sie die Seite **www.schoolnet.ch/guide** auf.
2. Tippen Sie die Zahl neben dem Link, zum Beispiel 700, in das PaperLink-Eingabefeld ein.
3. Sie werden automatisch weitergeleitet.

# Wieso gibt es Sicherheitsprobleme?

Um mögliche Sicherheitsrisiken zu verstehen, kann es helfen, die Motive des möglichen «Feindes» zu verstehen. Zu unterscheiden sind **technische Bedrohungen**, die zerstörerisch sein können, auch wenn das dem Verursacher gar nichts nützt, **Ärgernisse**, die keinen Schaden an Ihren Daten anrichten können, aber Sie Zeit und Nerven kosten können, und **betrügerische Aktivitäten**, d. h. «jemand will an Ihr Geld». Im Folgenden treffen wir eine kurze Unterscheidung dieser drei Arten von Sicherheitsproblemen, die Ihnen in diesem Guide immer wieder begegnen werden und die entsprechend gekennzeichnet sind.

### ▲ Technische Gefahren

Programme sind die Software, die Dateien öffnen, Bilder oder Texte anzeigen und Musik abspielen kann. Die meisten Programme auf Ihrem Computer sind gutartig, aber jemand, der Ihnen schaden will, kann ein schlechtes Programm einschleusen. Dazu später mehr. Viren, Würmer, Trojaner oder Spyware werden gemeinsam auch «Malware» genannt (engl. Abkürzung für «malicious Software» = bösartige Software). Der Programmierer dieser schlechten Software hat dabei nichts von dem Schaden, der bei Ihnen entsteht. Er legt es nur auf ein Kräftemessen mit den Herstellern von «Gegenmassnahmen» aller Art an und will sich im zweifelhaften Glanz sonnen, zumindest für kurze Zeit schlauer gewesen zu sein als diese.

### ■ Ärgernisse

Man könnte darüber diskutieren, ob überhaupt als Sicherheitsproblem gilt, was keinen Schaden anrichtet. Ärgerlich ist aber die verschwendete Zeit. Werbung im Posteingang, falsche Warnungen vor nicht existierenden Gefahren oder plötzlich auf dem Bildschirm erscheinende Meldungen stellen keine echte Bedrohung dar, aber der Empfänger würde oft trotzdem gern auf sie verzichten. Die Urheber sind entweder unseriöse Werbetreibende wie im Fall von unverlangten kommerziellen Mails («Spam») oder Spassvögel, die es nicht wirklich böse meinen. Spam bewegt sich dabei in einer Grauzone: Werbe-Mails können sowohl eine wenig seriöse Methode sein, an sich «anständige» Produkte zu verkaufen (ironischerweise z. B. Spamfilter), als auch einen Betrugsversuch darstellen.

### ● Betrügerische Aktivitäten

Mit dem Internet haben Trickbetrüger einen neuen Kanal gefunden, auf dem sie versuchen, Ihnen direkt Geld abzunehmen oder an vertrauliche Informationen zu gelangen. Die verwendeten Tricks kennen wir teilweise längst aus dem Alltag – doch im Internet fehlt uns noch die Erfahrung und das Gespür, um den Betrugsversuch sofort zu erkennen. Dieses Gespür kann man jedoch schulen, indem man einfach die Parallelen aufzeigt. Eine wichtige Rolle spielt z. B. das «Stehlen von Identitäten», ähnlich wie beim Diebstahl von Kreditkarte und Ausweis.

### ● Spione

Zu den Sonderfällen Hacker, Spyware und Wardriving vergleichen Sie Seite 14.



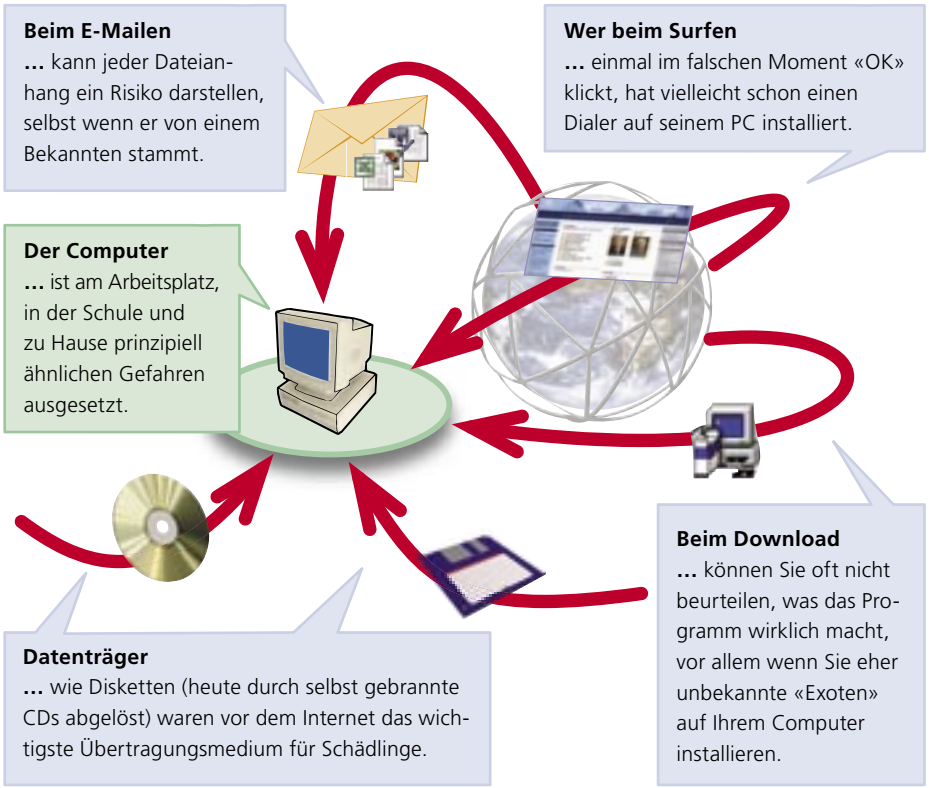


# Von wo kommt die Gefahr?

**Verschiedene Einfallstore**

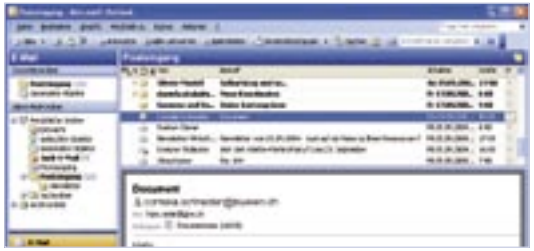
Die Gefahr lauert an verschiedenen Orten. Wichtig ist, dass Sie sich bewusst sind, bei welcher Tätigkeit Sie jeweils worauf achten müssen.

- Wichtigstes Einfallstor für Viren, Würmer und andere Schädlinge sind **E-Mails**. E-Mail-Anhänge von Unbekannten sollten daher Ihre Alarmglocken am lautesten läuten lassen. Aber auch reine Texte können «bösartig» sein, wenn Sie sie mit falschen Angaben auf unseriöse Websites locken wollen.
- Ebenso können Sie sich beim **Surfen** Schädlinge einfangen – früher vor allem auf Websites mit «zweifelhaften» Inhalten wie Erotikangeboten, heute gibt es «Dialer» auch auf Seiten mit Kochrezepten.
- Vorsicht ist auch immer geboten, wenn Sie **Software herunterladen**. Vor allem Gratisprogramme tun nicht immer genau das, was sie vorgeben.
- Schädlinge können auch von **Wechseldatenträgern** wie Disketten oder CDs auf Ihren Computer gelangen. Diese Art der Verbreitung wird jedoch zunehmend seltener – via Internet ist es einfach viel praktischer, auch für die Bösen.



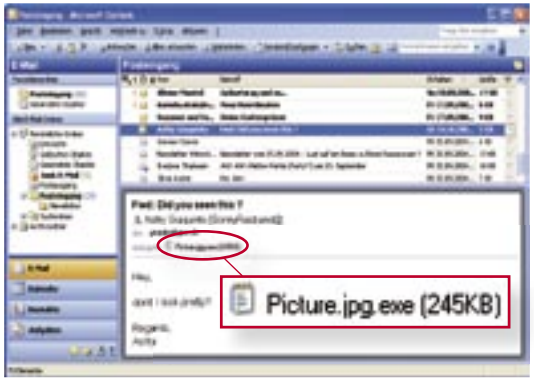
# Vorsicht beim Mailen!

**Technische Gefahren**
Ist weniger gefährdet, wer nur mailt und wenig surft? Nein. Die meisten Schädlinge verbreiten sich als Dateianhang. Wenn Sie diesen öffnen, kann das Programm starten, Ihr Betriebssystem angreifen und versuchen, sich über Ihren PC weiterzuverbreiten.



▲ **Einfacher Virus** L250
Auch wenn Sie den Absender kennen, besteht die Möglichkeit, dass im Anhang ein Virus steckt. Infiziert ein Virus Ihren PC, kann er wiederum Dateien infizieren, die Sie an andere versenden.

| Gefährdung durch … | Vorsicht bei Dateiendungen mit … |
|---|---|
| … Zugriff auf das Betriebssystem | .bat, .com, .exe, .htm, .html, .inf, .js, .jse, .vbe, .vbs |
| … Starten von Programmen | .chm, .lnk, .pif, .rm, .rt, .scr |
| … Ausführen ungewollter Aktivitäten (versteckt im normalen Dokument) | .mdb, .pps, .wsh, .doc, .xls |




▲ **Getarnter Virus**
Virenprogrammierer tarnen ausführbare Programme, indem Sie sie mit doppelten Dateiendungen versehen. Im Windows-Explorer und in Mailprogrammen werden Dateiendungen standardmässig nicht angezeigt, sodass die Datei **Picture.jpg.exe** wie ein «harmloses» Bild **Picture.jpg** aussieht. Wenn Sie dieses «Bild» anschauen wollen, installieren Sie in Wirklichkeit den Virus auf Ihrem Computer.

Viren hängen sich bevorzugt an Installationsdateien, rufen andere Programme auf oder nisten sich auf Disketten oder CD-ROMs ein. Auch Word- oder Excel-Dokumente können Viren enthalten (= **Makroviren** L414).

Die gute Nachricht: Viren müssen in der Regel aktiviert werden, d. h. solange Sie einen verdächtigen Mail-Anhang nicht öffnen, kann das Virus Ihrem Computer auch nicht schaden. Ausserdem erkennen laufend aktualisierte Virenscanner fast alle Viren.





Anders ist dies bei **Würmern** L415: Sie haben zwar letztlich ähnliche Auswirkungen wie Viren, funktionieren aber etwas anders: Ein Virus braucht wie in der Natur einen «Wirt» und muss zum Ausführen vom User angeklickt werden. Er versucht, Dateien auf einem Computersystem zu infizieren. Der Wurm dagegen ist ein eigenständiges Programm, das sich sozusagen selbst ausführt (möglich z. B. durch zu laxe Sicherheitseinstellungen im **Browser** L210 oder im Mail-Programm) und dann versucht, sich auf verschiedene Computer in einem Netzwerk auszubreiten.


Aufgrund dieser Eigenschaften verbreiten sich Würmer meist deutlich schneller als Viren und sind daher in den letzten Jahren auch in den Medien zu Berühmtheit gelangt: Nach dem ersten grossen Aufruhr um den Wurm «ILOVEYOU» im Jahr 2000 folgten Schädlinge wie «Lovsan», «Sobig» und «MyDoom». Oft nutzten diese Lücken in Microsoft-Betriebssystemen oder -Programmen, gegen die es schon «Gegenmittel» gab, sodass die Verbreitung deutlich langsamer vonstatten ginge, wenn alle User ihre Computer aktualisieren würden.

▲ **Mail-Wurm**
E-Mail-Würmer sind eine Kombination aus Viren und Würmern. Sie versuchen, sich selbst als E-Mail-Anhang an Adressen zu versenden, die sie z. B. im Adressbuch des Mail-Programms finden. Auch als (angebliche) Absenderadresse wird oft eine fremde E-Mail-Adresse verwendet. Der Besitzer des Adressbuchs und der richtige Eigentümer der Adresse bekommen davon nichts mit.

**Gegenmassnahmen bei technischen Gefahren im Mail-Verkehr**
Gegen einen Viren- oder Wurmbefall per Mail können Sie sich einfach schützen.

1. Installieren Sie eine Antiviren-Software (vgl. S. 19–20).
2. Überprüfen Sie die Sicherheitseinstellungen Ihres Mail-Programms (vgl. S. 23).
3. Wägen Sie ab, bevor Sie E-Mails oder Dateianhänge von Unbekannten öffnen (vgl. S. 28).

Die meisten Viren und Würmer werden mit der Absicht programmiert, Schaden anzurichten, obwohl der Verursacher davon keinen direkten eigenen Nutzen hat. Allerdings gibt es auch Würmer ohne spezielle «Schadensroutine». Doch selbst diese können erheblichen wirtschaftlichen Schaden anrichten, indem sie nur durch ihre Weiterverbreitung z. B. ein Firmennetzwerk so belasten, dass es vorübergehend für jede normale Arbeit unbrauchbar wird.

# Ärgernisse im Posteingang

### Spam oder Junk-Mail L267

Unerwünschte Werbe-Mails (= Spam) werden an viele Empfänger gleichzeitig versandt und werben für alles Mögliche, vom Diätprodukt bis zum PC-Zubehör. Die dahinter stehenden Absichten reichen vom Verkauf seriöser Produkte bis hin zur illegalen Abzocke, z. B. indem versucht wird, User mit verlockenden Gewinnversprechungen zu Investitionen in dubiose Anlagen zu bewegen.

Sie erkennen Spam z. B. an der ungewöhnlichen Absenderadresse oder prägnanten Betreffzeilen («Erste Mahnung», «Kennst Du mich noch?»). Wenn Sie vor allem auf Deutsch mailen, sind englische Spam-Mails immerhin leicht zu erkennen. Spam ist eigentlich ungefährlich, kann aber im Anhang Viren mitführen oder auf eine Website mit einem Dialer verweisen (vgl. S. 11). Spam-Mails sollten Sie weder öffnen noch beantworten, auch nicht, um sie abzubestellen (Link auf «unsubscribe»), denn jede dieser Handlungen kann dazu führen, dass der Absender erst sicher weiss, dass es Ihre Adresse wirklich gibt.

### Hoaxes L253

(engl. hoax = Jux, Schabernack)
Hoaxes sind Falschmeldungen, z. B. über eine angeblich neue Gefahr («Virus-Warnung !!!»). Sie erkennen Hoaxes an der Aufforderung, sie an alle Ihre Bekannten weiterzuleiten, an der drastischen Beschreibung des Schadens («löscht die gesamte Festplatte») und den Bezug auf scheinbare Autoritäten wie Microsoft, AOL oder die Polizei. Nehmen Sie aufgrund solcher Mails keine Änderungen am PC vor.

**Verhaltensregeln gegen unerwünschte Mails**

1. Spam sollten Sie möglichst nicht öffnen oder gar beantworten (vgl. S. 28).
2. Installieren Sie einen Spamfilter (vgl. S. 17).
3. Leiten Sie Warnmeldungen über angebliche Bedrohungen nicht ungeprüft weiter (vgl. S. 27).





# Betrügerische E-Mails

### «Phishing» L407

(von engl. «Password Fishing», d. h. Fischen nach dem Passwort) Hier können Sie ernsthaft geschädigt werden: Die Täter versenden E-Mails, die als Absender Ihre Bank oder einen Shop (z. B. eBay oder Amazon) vortäuschen. Im Phishing-Mail werden Sie unter einem Vorwand aufgefordert, sich auf der Website des Anbieters mit Kunden- bzw. Kontonummer und Passwort anzumelden.Der Link führt jedoch zu einer gefälschten Site, die dem Original täuschend ähnlich sieht. Wenn Sie tatsächlich Ihre Daten eingeben, können die Täter schlimmstenfalls auf Ihr Bankkonto zugreifen oder in Ihrem Namen einkaufen.


Phishing-Mails erkennen Sie an:


- einer unpersönlichen Anrede wie «Lieber Kunde» (der Betrüger kennt, im Gegensatz zum echten Anbieter, Ihren Namen nicht)
- der dringenden Aufforderung, sich sofort einzuloggen, oft verbunden mit der Drohung, dass sonst Ihr Konto gelöscht wird
- einem direkten Link im Text zur Login-Maske, um zu vermeiden, dass Sie die Adresse der echten Homepage eintippen
- manchmal an der falschen Sprache. Wenn Sie bei eBay Schweiz angemeldet sind, erhalten Sie von eBay keine englischen Mails.

**Verhaltensregeln gegen betrügerische E-Mails**

1. Seien Sie misstrauisch, wenn ein Mail Sie zu sofortigem Handeln auffordert.
2. Klicken Sie nicht auf Links in verdächtigen Mails, sondern tippen Sie die Ihnen bekannte Adresse des Anbieters ein.
3. Informieren Sie sich auf der Website des Anbieters über die verwendeten Sicherheitsmerkmale (bei einer Bank z. B. richtiges digitales Zertifikat, siehe S. 33–35).
4. Informieren Sie den Anbieter umgehend über den Vorfall.

# Vorsicht beim Surfen

## Technische Gefahren

Einige Schädlinge gelangen beim Surfen oder Herunterladen von Programmen aus dem Internet auf Ihren Computer.

### ▲ Würmer L415

Würmer – schon erwähnt im Abschnitt E-Mail – können zur Verbreitung auch Ihre Internet-Verbindung benutzen. Einer der berüchtigsten Würmer heisst «Blaster», auch «Lovsan» genannt. Würmer nutzen oft Sicherheitslücken im Betriebssystem, um den PC zu infizieren. Der Blaster-Wurm kann auf Ihren Computer gelangen, ohne dass Sie etwas herunterladen oder einen Mail-Anhang öffnen. Häufiges Aktualisieren des Betriebssystems und der Schutzsoftware stoppt die Ausbreitung der meisten Würmer, so auch die des Blaster.

### ▲ Trojaner L251

Trojaner haben ihren Namen vom berühmten trojanischen Pferd. Sie geben vor, etwas anderes zu sein, als sie in Wahrheit sind: Ein vermeintlich nützliches Programm, z. B. zum schnelleren Herunterladen von Musik oder zur Vernichtung eines Schädlings, enthält in Wirklichkeit ein «schlechtes» Programm.

### ■ IP-Popups/Windows-Nachrichtendienst

IP-Popups (**IP** = Internet-Protokoll L107, engl. pop up = auftauchen) sind plötzlich erscheinende Windows-Meldungen mit Hinweisen auf Websites. Ursprünglich waren sie für kurze Meldungen in Firmennetzwerken gedacht, doch da der «Nachrichtendienst» bei jedem Windows-PC zuerst aktiv ist, können sie von jedem nicht durch eine Firewall geschützten PC empfangen werden. Die Meldungen sind nervig, aber ungefährlich, solange Sie die erwähnte Website (die meist einen Dialer enthält) nicht besuchen. Eine direkte Schädigung des PC ist nicht möglich; die Popups kennen ausser dem OK-Button keine Funktion.

### Verhaltensregeln gegen technische Gefahren beim Surfen

1. Aktualisieren Sie regelmässig Ihr Betriebssystem (vgl. S. 24).
2. Installieren Sie eine Firewall (vgl. S. 20–21).
3. Installieren Sie eine Antiviren-Software (vgl. S. 20–21).
4. Schalten Sie den Windows-Nachrichtendienst ab (vgl. S. 23).





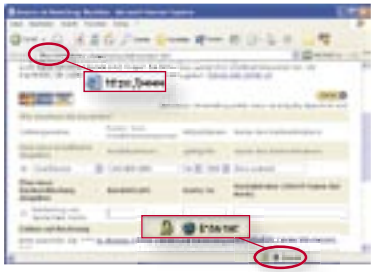
## Betrügerische Aktivitäten

Auch beim Surfen oder Online-Einkaufen gilt es, wie im wirklichen Leben die Anzeichen für Betrugsversuche zu erkennen und ein gesundes, aber nicht übertriebenes Misstrauen zu entwickeln.

### ● Dialer L371


bieten die Möglichkeit, kostenpflichtige Inhalte übers Internet zu beziehen und der Telefonrechnung zu belasten. Unlauter ist ihr Einsatz, wenn der Verbindungspreis nicht oder versteckt angegeben ist oder der Dialer unbemerkt die Standard-Verbindung ersetzt. Dies ist nur möglich bei einer Einwahlverbindung («DFÜ», Datenfernübertragung), beim Zugang über ADSL können Dialer keinen Schaden anrichten. Das Beispiel rechts zeigt einen offensichtlichen Dialer: Bestätigen Sie hier mit der Eingabe **OK**, würden Sie der Installation des Dialers auf Ihrem PC zustimmen. In der Schweiz ist die Verwendung von 0900er-Nummern durch Dialer verboten. Dialer können aber immer noch eine Internet-Verbindung über kostenpflichtige internationale Nummern aufbauen.

### ● Kreditkarteneinsatz



Geben Sie Kreditkarteninformationen (wie auch Kontoangaben) grundsätzlich nur auf sicheren Seiten an. Nicht sichere Verbindungen könnten «abgehört» werden und Ihre Zahlungsinformationen in falsche Hände geraten. Sichere Seiten erkennen Sie am kleinen Vorhängeschlosssymbol in der Statusleiste Ihres Browsers oder am Kürzel http**s** in der Adresszeile. (vgl. S. 29)

### ● Betrug durch Nichtlieferung/-zahlung

Bei Online-Auktionen (z. B. bei eBay oder ricardo.ch) ist Ihr Handelspartner meist eine Privatperson oder ein Kleinunternehmer. Darunter können sich schwarze Schafe befinden. Beachten Sie vor Abgabe eines Gebots oder Angebots die Informationen über den Partner und den Käufer- oder Verkäuferschutz des jeweiligen Marktplatzes.

### Verhaltensregeln gegen betrügerische Aktivitäten beim Surfen

1. Klicken Sie «Nein», wenn Sie gefragt werden, ob etwas installiert werden soll, das Sie nicht selbst zum Herunterladen ausgesucht haben.
2. Achten Sie bei Bezahlungen im Internet auf die Verschlüsselung (vgl. S. 33).
3. Überprüfen Sie vor Käufen und Verkäufen online, ob Ihnen der jeweilige Anbieter vertrauenswürdig erscheint.

# Vorsicht mit sensiblen Daten

Wenn Sie sich im Internet bewegen, hinterlassen Sie Spuren. Einige davon entstehen automatisch, andere Spuren können Sie selbst «legen» oder auch zurückhalten. Grundsätzlich gilt (solange Sie nichts Illegales tun): Sie sind als Person im Internet so lange anonym unterwegs, bis Sie selbst sich auf einer Website identifizieren, z. B. um einzukaufen oder sich für einen Dienst anzumelden.

**Spuren im Netz**

Die **IP-Adresse** L107 ist die eindeutige Adresse jedes Rechners im Internet. Wenn Sie Ihren Computer mit dem Internet verbinden, weist Ihr Internet-Anbieter Ihrem PC automatisch eine IP-Adresse zu. Als Privatperson haben Sie in der Regel keine feste IP-Adresse, sondern erhalten bei jedem Internet-Besuch eine andere gerade freie Adresse.

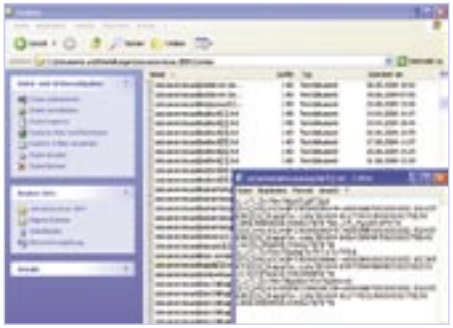
| Website | IP Adresse |
|---|---|
| www.swisscom.ch | 130.190.1.60 |
| www.creditsuisse.ch | 198.240.212.225 |
| www.microsoft.ch | 207.46.250.119 |

Wenn Sie eine Website aufrufen oder einen Beitrag in einem **Forum** L408 schreiben, wird die aktuelle IP-Adresse Ihres Computers automatisch auf dem **Server** L116 des Betreibers aufgezeichnet. Nur Ihr **Provider** L103, z. B. Bluewin, könnte nachvollziehen, wer wann mit welcher IP-Adresse unterwegs war. Gegenüber dem Betreiber der Website bleiben Sie also anonym, bis Sie sich freiwillig zu erkennen geben. Der Provider muss die Information, wer wann welche IP-Adresse benutzt hat, sechs Monate lang aufbewahren, und sie – bei Verdacht auf kriminelle Handlungen – auf Anordnung den Ermittlungsbehörden herausgeben. Dies ist jedoch klar die Ausnahme von der Regel.

**Cookies** L254

Cookies sind kleine Textdateien, die auf Ihrem PC abgelegt werden, damit der **Webserver** L177 Sie wiedererkennt. Es existieren viele Halbwahrheiten über Cookies. In Wahrheit gibt es zwei Sorten:

**Session-Cookies** (engl. Session = Sitzung) werden bei jedem Besuch neu angelegt. Sie ermöglichen z. B., dass Sie in einem Online-Shop über mehrere Seiten Ihren Warenkorb füllen können. Sobald Sie die Website verlassen, wird das Cookie gelöscht. **Dauerhafte Cookies** dagegen bleiben auf Ihrem Computer gespeichert. In beiden Fällen gilt: Der Server erkennt jeweils lediglich Ihren Computer wieder – er weiss nicht, wer Sie persönlich sind, bis Sie sich selbst identifizieren.







**Beispiel für dauerhafte Cookies**


Wenn Sie bei Amazon etwas einkaufen, melden Sie sich an. Ihre persönlichen Daten (Name, z. B. «Erika Leuthold», Adresse, Zahlungsinformationen usw.) werden in der Kundendatenbank gespeichert – und auf Ihrem Computer ein Cookie hinterlegt, das z. B. nur die Zahl 1234567890 enthält. Diese Nummer wird auch in der Kundendatenbank gespeichert. Wenn Sie nun das nächste Mal Amazon besuchen, kann der Server die Zahl im Cookie – und nur diese! – auslesen. Über die Kundendatenbank wird die Verbindung zwischen Ihrem Computer und Ihnen hergestellt; Sie werden persönlich begrüsst: «Hallo Erika Leuthold» und Bereiche wie «Ihre persönlichen Empfehlungen» werden angezeigt.

Amazon gibt dem Benutzer jedoch sehr einfach die Möglichkeit, das Cookie zu löschen – wenn Sie diesmal nicht erkannt werden wollen oder wenn Sie es gar nicht selbst sind, weil etwa eine andere Person denselben Computer benutzt. Dafür gibt es die Funktion: «Wenn Sie nicht Erika Leuthold sind oder sich abmelden wollen, klicken Sie hier.» So wird das Cookie wieder gelöscht – bis sich wieder jemand anmeldet.

Wo diese Funktion nicht vorhanden ist, kann man Cookies im Browser auch von Hand löschen sowie die Annahme teilweise oder vollständig einschränken. (Internet-Explorer: **Menü Extras > Internetoptionen > Datenschutz > Button Erweitert**). Dann muss man aber auch auf die beschriebenen Annehmlichkeiten verzichten.

**Surfen mit verschiedenen Identitäten**

Wie anonym Sie im Internet bleiben, hängt davon ab, wie viel über sich selbst Sie auf verschiedenen Websites preisgeben. Ein Set an Informationen nennt man auch «elektronische **Identität**» L409. Je mehr Angaben Sie machen, umso unverwechselbarer ist das Bild Ihrer Person. Es ist sinnvoll zu differenzieren, wie viel Informationen Sie angeben. Während Sie in einem Shop zwingend Angaben, z. B. Ihre Adresse, machen müssen, können Sie in einem Chat anonym bleiben. Sicherer ist es allemal, bisweilen zurückhaltend mit persönlichen Informationen zu sein. Sensible Angaben, die Sie im Shop machen, sind i. d. R. vor unbefugten Zugriffen geschützt.

**Beispiele für mehrere Identitäten einer einzigen Person:**

- Im Online-Shop: Erika Leuthold, Laubenweg 2, Bern, Kreditkarte: 1243 …
- In einem Online-Gästebuch: Erika L., erika.leuthold@bluewin.ch
- In einem Chat: Supererika29

# Wehret den Spionen

Die Verursacher von «Lausch»-Angriffen können sehr unterschiedlicher Art sein.

### ● Hacker L310

Hacker sind Programmierer, die als Hobby in fremde Computersysteme eindringen. Sie interessieren sich kaum für Ihre (privaten) Daten, könnten aber Ihren PC missbrauchen, um andere Computer, z. B. die grosser Firmen, anzugreifen.

### ● Spyware L410

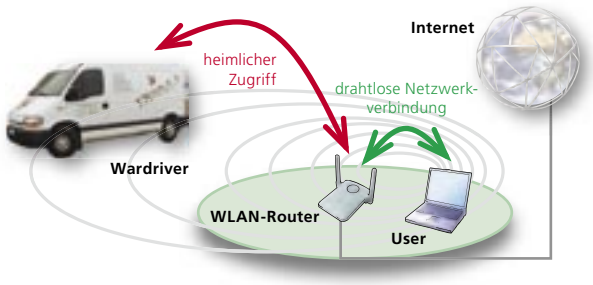
(engl. «spyware», dt. etwa Spionageprogramm) ist Software, die ohne Ihr Wissen auf Ihren Computer gelangt. Sie sammelt Informationen auf Ihrem PC und nutzt Ihre Internet-Verbindung, um diese unbemerkt zu versenden.

| Verursacher | Auswirkung |
|---|---|
| **Adware** | Zeichnet besuchte Websites auf und initialisiert entsprechende Werbe-Popups. |
| **Keylogger** | Zeichnet Tastatureingaben auf (engl. «key» = Taste). Dadurch können sensible Daten wie z. B. Passwörter entwendet werden. |
| **Hijacker** | Verändern die Einstellungen des Internet-Programms. Meist sind die Startseite oder die Favoritenliste betroffen. |
| **Trojaner** | Schleusen Viren ein oder ermöglichen die Fernsteuerung eines PCs und somit den Zugriff auf gespeicherte Daten. |

### ● Wardriving L411

(engl. Wireless Access Revolution Driving) erinnert an die Spionageabwehr in Kriegsjahren, als mit antennenbewehrten Autos nach verbotenem Funkverkehr gesucht wurde. Wardriver versuchen mit der gleichen Methode, ungeschützte Funknetzwerke zu entdecken, und finden diese insbesondere in privaten drahtlosen Netzen (WLAN).

Der Wardriver fängt dann den Datenverkehr zwischen den angeschlossenen Computern ab oder nutzt Ihre Internet-Verbindung, z. B. um Spam-Mails zu verschicken.




**Verhaltensregeln gegen Spionageversuche**

1. Installieren bzw. aktivieren Sie eine Firewall (= Schutzmauer gegen Horcher) und aktualisieren Sie diese regelmässig (vgl. S. 19–21).
2. Installieren Sie bei Verdacht Schutz-Software gegen Spyware von einer vertrauenswürdigen Website (vgl. S. 31).
3. Schränken Sie den Zugriff auf Ihr drahtloses Netzwerk (WLAN) ein und verwenden Sie nur verschlüsselte Funkverbindungen (vgl. S. 36–37).





# Übersicht Bedrohungen

| Gefahren | Beschreibung | Schaden |
|---|---|---|
| ▲ **Viren** | kleine schädliche Programme oder Programmstücke, die sich an Dateien anhängen oder die Programme Ihres PCs nutzen, um sich zu vermehren und Schaden anzurichten | • Löschen/Überschreiben von Daten<br>• Systeminstabilität<br>• Übertragung von Viren |
| ▲ **Würmer** | Haben ähnliche Auswirkungen wie Viren, können sich jedoch selbstständig verbreiten. | |
| ▲ **Trojaner** | kleine Programme, die vorgeben, nützlich zu sein, tatsächlich aber schädigenden Code enthalten | |
| ● **Spyware** | Software, die ohne Ihr Wissen auf Ihrem Computer installiert ist. Sie sammelt Informationen auf Ihrem PC und nutzt Ihre Internet-Verbindung, um diese unbemerkt zu versenden. | • Verlust der Datenvertraulichkeit<br>• Datenmissbrauch<br>• Missbrauch des PCs zum Angriff auf andere Systeme |
| ● **Hacker** | Programmierer, die in fremde Computersysteme eindringen | • Datenklau (meist bei Unternehmen)<br>• Datenmissbrauch<br>• Missbrauch des PCs zum Angriff auf andere Systeme |
| ● **Wardriving** | Systematisches Suchen nach ungeschützten Wireless LANs mit Hilfe eines Autos. Bei Erfolg hat der Wardriver weit reichenden Zugriff auf das interne Netz des WLAN-Betreibers. | |
| **Cookies** | kleine Textdateien, die entweder nur während des Surfens oder für längere Zeit auf PCs abgelegt werden | • Mitbenutzer Ihres PCs könnten Informationen über Ihr Surf-Verhalten erlangen |
| ● **Dialer** | Einwählprogramm, das die Möglichkeit bietet, kostenpflichtige Inhalte übers Internet zu beziehen und der Telefonrechnung zu belasten. Können zu betrügerischen Aktivitäten missbraucht werden. | • finanzielle Schäden durch überhöhte Telefongebühren (falls Internet-Zugang analog oder per ISDN erfolgt) |
| ● **Nichtlieferung** | Nichtlieferung von Bestellungen nach Internet-Einkäufen bei unseriösen Anbietern | • finanzieller Schaden |
| ● **Kreditkarteneinsatz** | Eine ungesicherte Internet-Verbindung kann angezapft werden, um Kreditkarteninformationen abzuhören. | |
| ● **Phishing** | Phishing, d. h. Trickdiebstahl per E-Mail: vermeintlich echte Nachricht von Firmen, die Sie zur Bekanntgabe Ihrer Passwörter z. B. für Ihr Online-Banking bringen soll | |
| ■ **Hoax** | Falschmeldungen, z. B gefälschte Warnungen vor Gefahren wie Viren | • Verursachung Spam<br>• evtl. Systemschädigung |
| ■ **IP-Popup** | Nachrichten, die als Warnhinweise auf Ihrem Bildschirm angezeigt werden | • Verunsicherung, da die Meldungen als Warnhinweise getarnt sind |
| ■ **Spam** | unerwünschte Werbe-E-Mails | • übervolles E-Mail-Konto<br>• Gefahr von verseuchten E-Mail-Anhängen<br>• Gefahr falscher Gewinnversprechungen |

# Gefahren trotz neuem PC

Wenn Sie einen neuen PC haben oder ein neues Betriebssystem installieren, sieht zwar alles brandneu aus, ist aber oft bereits nicht mehr aktuell, da die CD mit der Software vielleicht schon einige Monate alt ist – in vielen Fällen eine kleine Ewigkeit.

**Sicherheitslücken in der Standard-Software**
Microsoft Windows und alle anderen Microsoft-Produkte sind besonders häufig Ziel von Viren- oder Hackerattacken, doch auch Apple-Systeme werden zunehmend angegriffen. Die Herstellerfirmen liefern sich laufend ein Wettrennen mit den Virenprogrammierern, wer Lücken in den Systemen zuerst findet und wie schnell sie wieder gestopft werden können.

Wenn Sie einen neuen PC einrichten, sollten Sie deshalb als Erstes einige Sicherheitsvorkehrungen treffen.

**Absicherung des Administrators**
Wenn Sie Windows XP, Windows 2000 oder Windows NT verwenden, können Sie die Benutzerkonten mit einem Passwort schützen. Wichtig ist dies vor allem für das Administrator-Konto – also den «Verwaltungs-Modus» Ihres PCs, das mehr Rechte hat als das «normale» User-Konto. Deshalb sind die Administrator-Rechte für Eindringlinge auf Ihrem PC besonders interessant.

Selbst wenn Sie Ihren PC allein benutzen, sollten Sie sich nicht immer als Administrator anmelden, sondern für den täglichen Einsatz ein Benutzerkonto mit eingeschränkten Rechten verwenden. Eine Anleitung dafür finden Sie unter:
701 **www.microsoft.com/switzerland/de/security/windows**

Um ein Passwort für das Administrator-Konto unter Windows XP Home einzurichten, wählen Sie **Start > Systemsteuerung > Benutzerkonten**. Unter Windows XP Professional melden Sie sich mit dem Benutzernamen «Administrator» an und bestätigen mit «Enter» (wenn Sie bei der Ersteinrichtung kein Passwort festgelegt haben, bleibt das Feld hier leer). Halten Sie die Tasten **Ctrl** und **Alt** fest und drücken Sie **Del**. Klicken Sie «Passwort ändern» und geben in der Maske Ihr neues Passwort ein (zu guten Passwörtern vgl. S. 26, Regeln zur Passwortsicherheit).

**Verhaltensregeln bei Inbetriebnahme eines neuen PCs**

1. Installieren Sie eine Firewall, bevor Sie den neuen Computer das erste Mal mit dem Internet verbinden (vgl. S. 19–21).
2. Aktualisieren Sie danach sofort Ihr neues Betriebssystem (vgl. S. 24).
3. Installieren Sie eine Antiviren-Software (vgl. S. 19–21).
4. Sichern Sie Ihr Administratorkonto mit einem «guten» Passwort (vgl. S. 26).



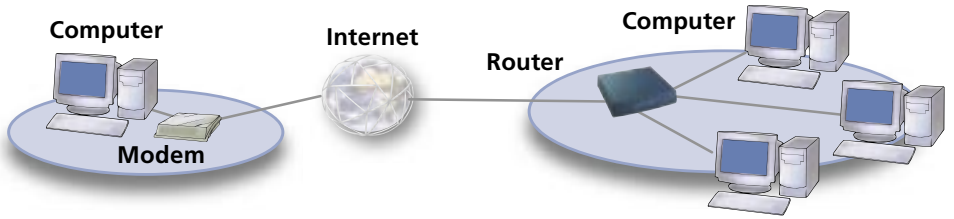


# Gefahren beim Internet-Zugang

Wenn Sie mit dem neuen PC auch einen Internet-Anschluss anschaffen, sollten Sie bei der Wahl Ihres Internet-Anbieters («Provider») folgende Punkte berücksichtigen.

**1. Anschlussart**
Bei der Entscheidung für den Anbieter (z. B. Bluewin) und die Verbindungsart (analog, ISDN oder ADSL) spielen mehrere Faktoren eine Rolle. Ein schneller Breitbandzugang erhöht nicht nur den Komfort, sondern schützt Sie auch vor Dialern, da die Nutzung nicht mehr im Minutentakt abgerechnet wird. Dafür steigt dadurch, dass Sie ständig online sein können, das Risiko eines direkten Angriffs, z. B. durch einen Wurm.

**2. Kauf der Hardware**
Für einen Breitbandzugang benötigen Sie ein **ADSL Modem** L412 (wenn Sie nur einen PC haben) oder einen **ADSL Router** L413 (wenn Sie mit mehreren PCs ins Internet wollen; engl. router = Vermittlungsknoten, eine Art «Datensortierstelle»). Die Funktion des ADSL Modem ist bei einem ADSL Router bereits integriert.




Es gibt Geräte mit eingebauter Firewall (= «Brandschutzmauer»). Solche «Hardware-Firewalls» schützen in der Regel besser als eine Firewall-Software – allerdings sind die Unterschiede eher gering; wichtig ist, dass man überhaupt irgendeinen Schutz hat.

**Tipp**: Ändern Sie bei der Installation der Firewall sofort das (Standard-)Passwort, damit sie nicht von Eindringlingen manipuliert werden kann.

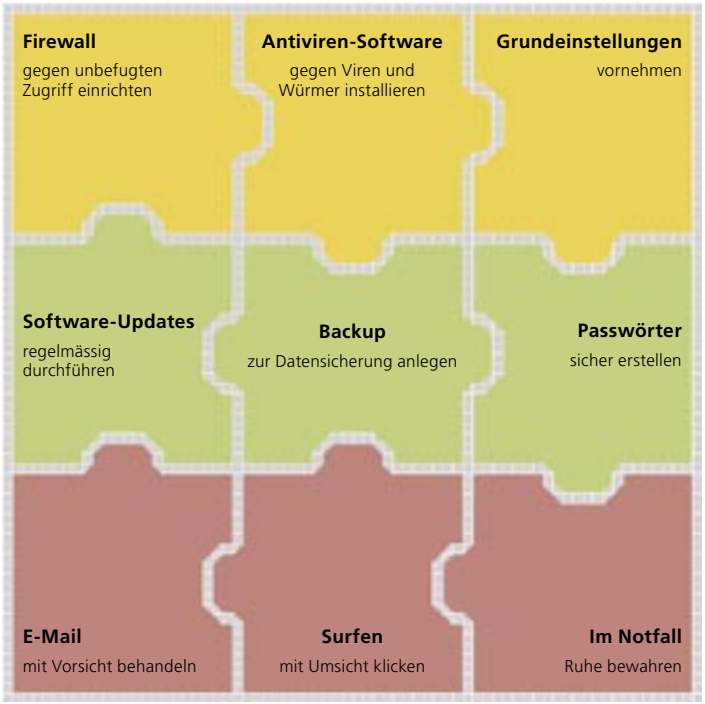
**3. Zusatzdienste des Anbieters**
Einige Internet-Anbieter bieten Zusatzdienste an, mit denen Sie die Sicherheit Ihres PCs ohne grossen Aufwand erhöhen können. Bluewin bietet z. B. einen je nach Abo kostenlosen Spam- und Virenschutz und eine Firewall, die Sie nur noch aktivieren müssen. Vorteil dieser Dienste ist, dass Sie sich bei der Auswahl, was wie gefährlich ist, auf die Einschätzung des Anbieters verlassen können.

702 **de.bluewin.ch/services/sicherheit**

# Das 3x3 der Sicherheit zu Hause

Durch das Befolgen einiger Verhaltensrichtlinien und durch wenige technische Massnahmen können Sie Ihren Computer und Ihre Privatsphäre wirkungsvoll schützen. Sie müssen kein/e Computerexperte/in sein, um die wichtigsten Schutzmassnahmen erfolgreich umzusetzen.

**Sich rundum schützen mit 3x3 Verhaltensregeln**
Auf den folgenden Seiten stellen wir die Bausteine vor, mit denen Sie Ihren Computer und Ihre Privatsphäre wirkungsvoll schützen können. Jedes Puzzleteil erhöht Ihre Sicherheit.



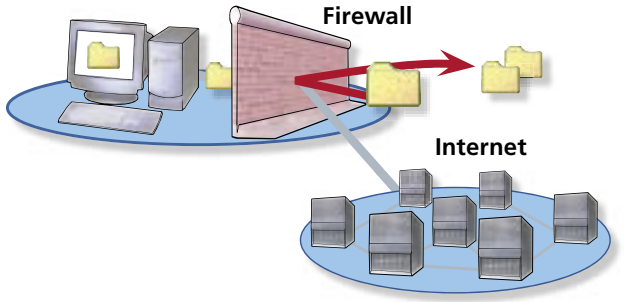

Am Ende des Hefts finden Sie eine Checkliste, die Sie bei der Absicherung Ihres PCs unterstützen kann (vgl. S. 38).





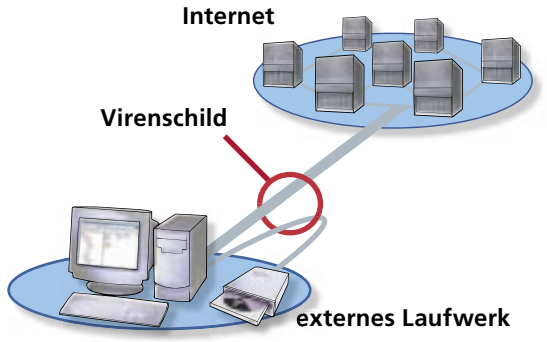
# Firewall und Antiviren-Software

**Was macht eine Firewall?**
Eine **Firewall** L112 ist eine Art Türsteher, der alle Daten, die zwischen dem Internet und Ihrem PC hin- und hergeschickt werden, einzeln kontrolliert. Dadurch wird Ihr PC vor Missbrauch durch Eindringlinge geschützt.




**Was macht eine Antiviren-Software?**
Unter Antiviren-Software versteht man Programme, die «Eindringlinge» wie Viren und Würmer aufspüren, entfernen und abhalten können. Sie besteht aus:

- einer **Virenbibliothek**, die Merkmale von Tausenden von Viren enthält, die der Virenscanner und der Virenschild erkennen,
- einem **Virenscanner**, dem Hauptprogramm, das in regelmässigen Abständen Ihren PC nach Viren, Würmern und Trojanern durchsucht sowie diese allenfalls entfernt, und
- einem **Virenschild**, der ständig aktiv ist und alle Daten, die über die Internet-Verbindung (oder auch von Diskette oder CD-ROM) auf den PC kommen, daraufhin untersucht, ob sie Viren, Würmer oder Trojaner enthalten.




**Firewall und Antiviren-Software – warum Sie beides haben müssen**
Hauptaufgabe der Firewall ist es zu kontrollieren, wer Daten ins Internet verschicken und aus dem Internet empfangen darf. Beispielsweise darf Ihr E-Mail-Programm Nachrichten versenden und empfangen; ein Spyware-Programm, das auf Ihren PC geraten ist, darf dies nicht. Von einem Webserver, bei dem der Internet Explorer Inhalte angefordert hat, wollen Sie Datenpakete empfangen; von einem Hacker, der über einen fremden Server Daten an Ihren PC schickt, dagegen nicht. In der Regel erteilt die Firewall diese Erlaubnis einem Programm – Ihre E-Mail-Software steht dabei auf der «weissen» Liste. Doch *welcher Art* die durchgelassenen Daten sind; ob sie dennoch Viren, Würmer oder Trojaner enthalten, weiss die Firewall nicht. Dies überlässt sie der Antiviren-Software.

# Einrichten von Schutz-Software

Neue Computer werden oft mit Testversionen von Firewall und Virenschutz geliefert. Bei Windows XP ist bereits eine Firewall enthalten, die Sie aber zuerst aktivieren müssen. Firewalls und Antiviren-Software können Sie im Handel kaufen oder kostenlos (teils befristet) aus dem Internet laden. Beachten Sie beim Herunterladen, dass

- sich hinter vermeintlichen Gratisschutzprogrammen auch Trojaner verbergen können, die selbst Viren oder Spyware auf Ihrem PC installieren.
- das Herunterladen lange dauert, wenn Sie sich über eine «normale» Telefonleitung (analog) oder per ISDN ins Internet einwählen. In diesem Fall sollten Sie sich grössere Software-Pakete auf CD besorgen.

Die **Bluewin-Firewall** läuft statt bei Ihnen zu Hause «an Bluewins Ende» der ADSL-Leitung, etwa wie die Combox Ihres Handys auch kein Gerät ist, sondern ein Dienst. Sie brauchen Sie weder zu installieren noch zu aktualisieren, sondern müssen sie nur abonnieren. Wenn Sie aber einen Laptop haben und damit auch unterwegs ins Internet gehen, nützt Ihnen diese Lösung dort nichts.

Bevor Sie Virenschutz-Software installieren: Prüfen Sie, ob sich bereits eine Antiviren-Software auf Ihrem PC befindet. Diese **muss unbedingt entfernt werden**, bevor Sie ein neues Schutzprogramm installieren, da es sonst zu Konflikten kommen kann. (Entfernung über **Start > Systemsteuerung > Software**; suchen Sie dort nach einem Eintrag mit «Antivirus», etwa von McAfee, Norton oder Symantec (alles bekannte Hersteller von Schutz-Software). Klicken Sie zum Löschen ungenutzter Einträge auf Ändern/Entfernen.

**Antivir** ist eine bewährte Antiviren-Software, die Privatanwender kostenlos nutzen können.
Überlegen Sie sich vor dem Herunterladen einzelner Schutzprogramme, ob Sie nicht gleich eine Komplettlösung anschaffen möchten, bei der Sie z.B. auch Anspruch auf telefonische Hilfestellung haben (siehe Folgeseite).


703 **www.free-av.de**

704 **free.grisoft.com/freeweb.php/doc/2** – «AVG Anti-Virus» ist eine englischsprachige kostenlose Antiviren-Software mit besonders kleinen Aktualisierungsdateien. Deshalb eignet sie sich speziell, wenn Sie sich über Telefon (analog, ISDN) ins Internet einwählen.





# Komplettlösung von Norton

Kombinierte Software-Pakete lohnen sich, sobald Sie zwei Bestandteile daraus sowieso anschaffen würden. Norton Internet Security ist eine solche kombinierte Sicherheitslösung, die Virenschutz, Firewall, Spam-Filter, einen Schutz für vertrauliche Daten (Privacy Control) und Kinderschutz-Software (Parental Control) in einem Paket enthält.

**30 Tage Testversion**
Unter 705 **www.schoolnet.ch/norton** steht Ihnen eine kostenlose Testversion dieses Software-Pakets zum Herunterladen zur Verfügung. Nach Ablauf der Testphase von 30 Tagen können Sie entscheiden, ob Sie diese Software kaufen wollen oder wieder deinstallieren möchten.

**Installation der Testversion**
Vergessen Sie nicht, allfällige andere Antiviren-Software vorab von Ihrem PC zu entfernen. Melden Sie sich dazu als Administrator an. Laden Sie die Datei herunter und starten Sie die Installation. Folgen Sie dafür den Empfehlungen in den Installationsfenstern. Alle Sicherheitspakete werden auf einmal installiert.

**Kontrolle der Aktivität**
Unten rechts neben der Uhr im «System Tray» (wörtl. «Systemablage») informiert Sie ein Symbol über den Status von Norton ( = aktiv; = deaktiviert). Kontrollieren Sie gelegentlich, ob die Software auch aktiv ist. Falls das einmal nicht der Fall sein sollte, klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie **Norton Internet Security aktivieren**.


**Warnmeldung bei Bedrohung**
Im selben Bereich wird Ihnen auch angezeigt, wenn die Sicherheit Ihres PCs angegriffen wird. Virusmeldungen des Programms informieren Sie meist darüber, dass ein Sicherheitsproblem auftrat, aber schon unter Kontrolle ist. Mehr zum richtigen Verhalten bei Befall finden Sie ab Seite 30.

# Die Frage der sicheren Einstellung

Alle Programme, die am Datenverkehr mit dem Internet beteiligt sind, können so eingestellt werden, dass sie weniger anfällig gegen Angriffe sind:

- Betriebssystem (= «Verwaltungseinheit» des Computers)
- Browser (= Internet-Abfrageprogramm, z. B. Internet Explorer)
- E-Mail-Programm (z. B. Outlook, Outlook Express, Eudora, Thunderbird)
- Anwendungsprogramme wie Word und Excel

Wie auch in der realen Welt gilt jedoch oft: Komfort geht auf Kosten der Sicherheit, und umgekehrt. Zudem ist das Verändern dieser Einstellungen eher eine sicherheitstechnische Feineinstellung – es kann die Installation von Firewall und Antiviren-Software sowie die regelmässigen Aktualisierungen des Betriebssystems keinesfalls ersetzen.

1. **Enttarnen Sie versteckte Viren**
   Wie auf S. 6 erwähnt tarnen sich Virenprogramme durch eine falsche doppelte Endung («Picture.jpg.exe») als harmlose Dateien. Unter **Arbeitsplatz** > **Extras** > **Ordneroptionen** > **Ansicht** sollten Sie die «gefährliche» Option «**Erweiterung bei bekannten Dateitypen ausblenden**» deaktivieren, sodass die Endung immer angezeigt wird.

2. **Passen Sie die Sicherheitsstufen des Internet Explorer an**
   Im Internet Explorer können Sie im Menü **Extras** > **Internetoptionen** die Sicherheitseinstellungen des Programms verändern. Klicken Sie dazu auf die Registerkarte **Sicherheit, dort auf Stufe anpassen** und wählen Sie die gewünschte Stufe. Mit Klick auf **OK** ändern Sie die Sicherheitsstufe. Die maximale Stufe («hoch») macht das Surfen jedoch mühsam, da ganze Webseiten nicht mehr angezeigt werden, auch wenn sie nicht sehr «unsicher» sind. Alles zuzulassen (Stufen «niedrig»/«sehr niedrig») macht Sie dagegen angreifbarer. Sie können hier auch gezielt einzelne Einstellungen auswählen.





3. **Kontrollieren Sie das Speichern von Passwörtern im Internet Explorer**
   Das Speichern von Passwörtern z. B. für Webmail- oder Kundenkonten ist zwar praktisch, hebelt aber den Sicherungseffekt aus. Ob Sie dies zulassen möchten, entscheiden Sie selbst. Ausschalten können Sie die Option unter **Extras** > **Internetoptionen** > **Inhalte** > **AutoVervollständigen**.

4. **Schalten Sie den Nachrichtendienst ab.**
   Melden Sie sich auf Ihrem PC als «Administrator» an. Klicken Sie dann (bei Windows XP) im Menü **Start** > **Systemsteuerung > Verwaltung > Dienste** oder bei Windows 2000 im Menü **Start > Einstellungen > Systemsteuerung > Verwaltung > Dienste**.
   Klicken Sie dann mit der rechten Maustaste auf **Nachrichtendienst** und wählen Sie **Beenden**. Klicken Sie noch einmal mit der rechten Maustaste auf **Nachrichtendienst** und wählen Sie **Eigenschaften**. Setzen Sie dort im Registerreiter **Allgemein** den «Starttyp» auf **Deaktiviert**.

5. **Sichern Sie Ihr E-Mail-Programm**
   Bestimmte Virentypen werden bereits bei Ansicht im Vorschaufenster aktiv, wenn Sie das betreffende Mail im Posteingang anwählen. Schalten Sie also die automatische Vorschau besser ab. In Outlook Express wählen Sie dazu im Menü **Ansicht > Layout** und deaktivieren Sie die Checkbox «Vorschaufenster anzeigen». Bestätigen Sie die Änderung mit **Übernehmen** und dann mit **OK**. Seit Version 6 von Outlook Express können Sie verhindern, dass das Programm potenziell gefährliche E-Mail-Anhänge öffnet, indem Sie im Menü **Extras > Optionen** auf der Registerkarte **Sicherheit** die Option «Speichern oder Öffnen von Anlagen, die möglicherweise ein Virus enthalten könnten, nicht zulassen» aktivieren.

Weitere Sicherheitseinstellungen für die gängigsten Programme finden Sie unter
**706 www.microsoft.com/switzerland/de/security/settings.**

# Aktualisierungen (Updates)

Da ständig neue Viren- und Wurmvarianten auftauchen, müssen Firewall, Virenschutz und Betriebssystem immer wieder aktualisiert werden, d. h. so genannte Updates (engl. update = Aktualisierung) vorgenommen werden. Falls Sie Ihre Aktualisierungen manuell durchführen (und nicht automatisch von der Software ausführen lassen), hier ein paar Richtwerte für die Zeitabstände:

| | |
|---|---|
| **Virenschutz-Software** | Mindestens wöchentlich, wenn Sie Ihren Computer seltener verwenden, empfehlen wir, dies bei jedem Start zuerst zu tun. |
| **Betriebssystem** | Aktualisierung mindestens monatlich, besser öfter, je nach Verfügbarkeit neuer Updates |
| **Firewall** | Aktualisierung mindestens alle drei Monate, besser öfter |

Das Laden und Installieren dauert nur wenige Minuten und kann auch im Hintergrund laufen, während Sie weiterarbeiten.
**Tipp**: Nutzen Sie Erinnerungsdienste! Die meisten Programme haben Funktionen, die Sie automatisch benachrichtigen, wenn ein neues Update vorhanden ist.

**Hinweis**: Updates werden niemals per E-Mail versandt. Haben Sie ein solches Mail im Posteingang, löschen Sie es, da sich vermutlich ein Virus im Anhang befindet.

Für die Betriebssysteme Windows 2000, ME oder XP gibt es «Automatische Updates», die auch den Internet Explorer und die XP-Firewall aktualisieren. Je nach Version können Sie zwischen verschiedenen Automatisierungsgraden wählen. Es ist egal, welchen Sie nehmen, solange Sie generell aktualisieren. Eine Anleitung gibt es unter 707 **www.microsoft.com/switzerland/de/windowsupdates**

Aktualisierungen für Mac OS können Sie unter **Apfelmenü > Über diesen Mac > Software aktualisieren** ausführen.

**Aktualisierungen der Schutz-Software**
Schutzprogramme erhalten i. d. R. eine automatische Aktualisierungsfunktion, die Ihnen hilft, sie auf dem neusten Stand zu halten. Bei Norton können Sie überprüfen, ob diese Funktion eingeschaltet ist, indem Sie auf Ihrem Desktop das Symbol der Software anklicken und unter **Optionen** kontrollieren, ob das Kästchen «Autom. LiveUpdate aktivieren» einen Haken hat. Falls nein, empfehlen wir, diese Option zu aktivieren.

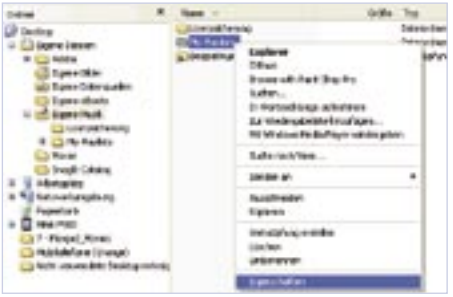




# Sicherheitskopien (Backups)

Egal, welche weiteren Sicherheitsmassnahmen Sie treffen: Wir empfehlen Ihnen, regelmässig Sicherheitskopien (= Backups) der wichtigsten Daten anzulegen. Sollte Ihr Computer doch einmal befallen sein, können Sie so den Schaden begrenzen. Je nach Menge der Daten, die Sie sichern, benötigen Sie unterschiedliche Speichermedien.

Um abzuschätzen, wie viele Megabyte die Datenordner umfassen, die Sie speichern wollen, klicken Sie mit der rechten Maustaste auf einen Ordner und dann auf **Eigenschaften**.



Rechnen Sie zusammen und wählen Sie das geeignete Speichermedium. Für die Datensicherung privater Anwender eignen sich folgende Datenträger:

| Datenträger | Datenmenge | Beschreibung | Kosten |
|---|---|---|---|
| **USB Memory Sticks oder Speicherkarten**  | 128 bis ca. 512 MB (z.B. für grössere Berichte, Fotos) | • können eingesteckt und wie ein Laufwerk genutzt werden<br>• beliebig oft beschreibbar<br>• eher zum Transport und zur kurzfristigen Sicherung | • grosse Preisunterschiede je nach Kapazität<br>• 256 MB ab ca. CHF 75.- |
| **CD-ROM, DVD**  | • CD: 700 MB (für private Anwender meist ausreichend)<br>• DVD: ca. 4 bis 5 GB | • Aufnahme mit CD-/DVD-Brennern<br>• Brenner kann auch für Musik-CDs genutzt werden<br>• CD-R sind nur einmal beschreibbar, CD-RW mehrfach | • CD-/DVD-Brenner sind in neueren PCs eingebaut, sonst ab CHF 150 erhältlich<br>• CHF 0.50–1.00 pro CD-Rohling<br>• CHF 1.00–5.00 pro DVD-Rohling |
| **externe Festplatte**  | ab 20 GB (viel Platz für Musik, Filme, digitale Fotos) | • handliche Grösse<br>• teilweise mit mehr Speicherplatz als die PC-Festplatte<br>• kann bei Bedarf auch an andere Computer angeschlossen werden | • ab CHF 200.– |

Für komplette Verzeichnisse und grössere Datenmengen gibt es …

- **Backup-Programme**, die Ihnen bei der Datensicherung helfen, z. B. «Backup-Maker»: 708 **www.ascomp.net/backupmaker.php** oder
- **Image-Programme**, die Sie dabei unterstützen, eine komplette Kopie der Festplatte anzulegen, z. B. «Norton Ghost»: 709 **www.symantec.com/region/de/product/ghost/pe_index.html**

# Sicherheitslücke Passwort

Benutzername und Passwort begleiten uns auf allen Einkäufen, Mail-Konten und vielen anderen Diensten im Web. Hier einige Tipps, mit denen Sie Unbefugten den Zugriff auf Ihre Daten bzw. Ihre Passwörter schwer machen können:


| Gut | Schlecht |
|---|---|
| **Einfaches Passwort:** Sie sollten sich Ihr Passwort gut merken können – zugleich sollte es für andere schwer zu erraten sein. Beispiel: Das Kinderlied «Mein Hut, der hat 3 Ecken» als Passwort: **MHdh3E** | **Nicht aus dem Lexikon:** Benutzen Sie keine Wörter, die in einem Lexikon stehen. Vertauschen Sie besser einzelne Buchstaben (z. B. **bachstuben**, **nexikol**). |
| **Kombinieren Sie Buchstaben und Zahlen:** z.B. **t0b1as** (statt Tobias). | **Nichts Offensichtliches:** Verwenden Sie keinesfalls den Namen Ihres Partners, Haustiers oder Wohnorts unverändert. |
| **Verschiedene Konten, verschiedene Passwörter:** Wenn ein Angreifer z.B. an das Passwort für Ihr E-Mail-Konto kommt, sollte er damit nicht auch das Passwort für Ihr eBay-Konto haben. | **Kein Post-it-Kleber am Monitor:** Wenn Sie Ihre Passwörter partout aufschreiben wollen, auf keinen Fall direkt am Monitor oder in der obersten Schublade aufbewahren. |
| **Wechseln Sie Ihre Passwörter:** Empfohlen wird oft monatliches Ändern. Wie realistisch das für Sie ist, entscheiden Sie. Hin und wieder wechseln ist besser als nie. | **Passwort geheim halten:** Geben Sie keine Passwörter an Dritte weiter, auch nicht auf Anfrage. Kein seriöser Anbieter wird jemals per E-Mail oder telefonisch nach Ihrem Passwort fragen. |
| **Vorsicht mit Sonderzeichen:** Nicht überall sind diese auf denselben Tasten. Wenn Sie im Internet-Café irgendwo auf der Welt das Zeichen # nicht finden, haben Sie sich ausgesperrt. | **Keine Wiederholungen, keine nahe liegenden Zeichenkombinationen:** wie z.B. **lalala**, **abcdefg** oder **qwertz** (Anordnung auf der Tastatur) |
| **Variieren Sie Ihr Hauptpasswort**: Wenn Sie mehrere Passwörter verwalten müssen, verwenden Sie Variationen Ihres Hauptpassworts: z. B. mat0b1as (Mail), bat0b1as (Banking), sht0b1as (shopping). Das System sollte jedoch nicht auf den ersten Blick erkennbar sein. | **Nicht auf Ihrem Computer speichern:** etwa im Dokument «passwoerter.doc» |





# Regeln fürs Mailen

Nichts ersetzt in Sicherheitsfragen den gesunden Menschenverstand – deswegen hier noch mal alle Verhaltenstipps auf einen Blick. Damit halten Sie sich auch Angreifer und Nervensägen vom Leib, die an den technischen Vorkehrungen vorbeischlüpfen.

1. Öffnen Sie keine Mail-Anhänge von Unbekannten, insbesondere nicht, wenn diese Dateiendungen wie .exe, .vbs oder .bat oder doppelte Dateiendungen (z. B. .doc.exe) haben.

2. Kein Software-Anbieter, insbesondere weder Microsoft noch Apple, versendet Aktualisierungen per E-Mail. Dies sind Fälschungen mit gefährlichen Inhalten.

3. Ein seriöser Anbieter wird Sie niemals auffordern, sich umgehend auf einer Seite mit einer merkwürdigen Adresse einzuloggen oder Passwörter oder Kontoinformationen per E-Mail bekannt zu geben.

4. Reagieren Sie kritisch auf Virenwarnungen per Mail, auch von Bekannten.

   a. Löschen Sie keine Dateien voreilig, wenn dies in der Warnung empfohlen wird.

   b. Schauen Sie nach, ob die Meldung bereits als schlechter Scherz bekannt ist: beim Software-Hersteller oder z. B. unter 710 **www.hoax-info.de**).

   c. Leiten Sie das Mail nicht an Ihre Bekannten weiter, insbesondere nicht, wenn Sie dazu aufgefordert werden.

   d. Informieren Sie den Versender von falschen Warnungen, sofern Sie ihn oder sie persönlich kennen.

5. Verwenden Sie mehrere E-Mail-Adressen, davon eine als «persönliche» Adresse. Teilen Sie diese nur Freunden und Bekannten mit.

6. Richten Sie mindestens eine weitere Adresse ein, z. B. zum Abonnieren von Newslettern, zur Registration oder für Beiträge in öffentlichen Foren. Sollten Sie dort zu viel Spam erhalten, wechseln Sie die Adresse.

7. Meiden Sie Adressverzeichnisse. Gratis-E-Mail-Dienste bieten bei Anmeldung den Eintrag in «Telefonbücher» an; die Adressen sind dort jedoch leicht «abzuholen».

8. Öffnen Sie möglichst Mails mit Spam-Inhalt erst gar nicht, da diese den Absender teils über die erfolgreiche Übermittlung informieren können.

9. Antworten Sie nicht auf Spam und benutzen Sie etwaige Abmeldefunktionen («unsubscribe») im Text nicht. Dadurch bestätigen Sie nur, dass Ihre E-Mail-Adresse benutzt wird.


10. Wenn Sie ganz sicher gehen wollen, nutzen Sie Verschlüsselungsverfahren für Ihre E-Mails (dies ist allerdings etwas für Fortgeschrittene).



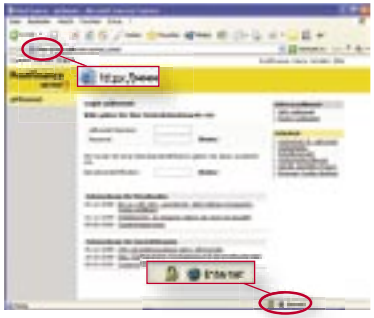


# Regeln fürs Surfen

1. Aktualisieren Sie regelmässig den Internet Explorer. Bei Aktualisierung des Betriebssystems (vgl. S. 24) werden auch Sicherheitslöcher im Internet Explorer behoben, die sonst z. B. von Würmern ausgenützt werden könnten. Dies gilt speziell, wenn Sie – etwa nach den Ferien – Ihren Computer längere Zeit nicht mehr benutzt haben.

2. Meiden Sie «unseriöse» Websites. Hinweise auf die Seriosität bieten z. B.

- ein gut auffindbares Impressum mit Postadresse und Telefonnummer des Anbieters
- klare Angabe von eventuellen Kosten (z. B. für Informationen/Artikel, für Software), Liefer- und Zahlungsbedingungen
- Übermittlung von sensiblen Informationen über SSL-Verschlüsselung (erkennbar am Kürzel http**s** in der Adresszeile und am Vorhängeschloss in der Statusleiste des Browser-Fensters).



Wenn Sie auf eine verdächtige Website gelangen, schliessen Sie umgehend das Fenster. Verwenden Sie dazu das Kreuz rechts oben im Fenster oder die Tastenkombination **Alt-F4**, keinesfalls Buttons innerhalb der dubiosen Website (die allenfalls etwas anderes machen, als sie vorgeben).

3. Seien Sie misstrauisch gegenüber Downloads, die Ihnen von einer Website «aufgedrängt» werden. Drücken Sie nicht **OK** oder **Abbrechen** in einem Web-Fenster (das Klicken auf Abbrechen kann zur Installation führen), sondern schliessen Sie das Fenster.

4. Bedenken Sie, wer ausser Ihnen Zugang zu Ihrem PC hat: Lassen Sie z. B. im Internet-Café keine Passwörter auf dem Bildschirm stehen, auch nicht maskiert durch ****. Vermeiden Sie es, Online-Shops mit dauerhaften Cookies an öffentlichen PCs zu nutzen (d. h. Websites, die Sie z. B. immer persönlich begrüssen oder Kundendaten von Ihnen automatisch anzeigen). Dies gilt insbesondere für die Kombination von Cookies mit gespeicherten Passwörtern.

5. Geben Sie Konto- und Zahlungsdaten bei Bestellungen über das Internet nur auf verschlüsselten Übertragungswegen an.

# Richtiges Verhalten im Notfall

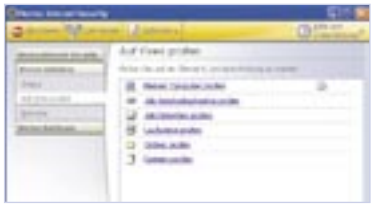
Manchmal «gewinnt» ein Virus, Trojaner oder Dialer kurzfristig den Wettlauf mit den Sicherheitsexperten der Software-Firmen und kann sich trotz aller Vorsichtsmassnahmen auf Ihrem Computer einnisten. **Symptome** eines Virenbefalls sind z. B., dass

- der PC ungewöhnlich schwerfällig läuft
- Probleme beim Starten auftreten
- unverständliche Meldungen auf dem Bildschirm angezeigt werden
- Daten verschwinden, die Sie mit Sicherheit nicht gelöscht haben.

**Keinesfalls in Panik geraten.**
Bleiben Sie ruhig. Oft entstehen grössere Schäden durch unkontrolliertes Löschen vermeintlich gefährlicher Dateien oder gar Löschen der gesamten Daten auf der Festplatte. Kompletter Datenverlust ist sehr selten. Da Viren und Würmer Software sind, können Sie Ihren Computer zwar temporär lahm legen, aber nicht permanent physisch beschädigen.

**Entfernung bei Symptomen**

1. **Speichern** Sie offene Dateien und wichtige Daten auf Diskette oder einer CD-ROM (lieber befallene Daten, die man später «reinigen» kann, als keine Daten).
2. **Informieren** Sie sich über aktuelle Viren und die Möglichkeiten, die Schäden zu beheben. Nutzen Sie dazu die Website der Hersteller Ihrer Antiviren-Software oder spezialisierte Informationsportale (vgl. S. 32).
3. **Aktualisieren** Sie Ihre Antiviren-Software. Bei neueren Viren steht wenige Stunden nach Auftauchen ein entsprechendes Update der Schutzsoftware bereit.
4. **Starten** Sie danach Ihre Antiviren-Software. Erschrecken Sie nicht, wenn sich dann ein Virus meldet – ein identifizierter Schädling kann mit grosser Wahrscheinlichkeit auch sofort gelöscht oder unter Quarantäne gestellt werden.
   Im letzteren Fall finden Sie Entfernungshilfen auf den Websites der Hersteller.



**Nach erfolgreicher Bekämpfung:**

1. Prüfen Sie Dateien, die Sie in letzter Zeit auf Disketten oder auf CD gespeichert haben, um ein «Verschleppen» des Virus zu verhindern.
2. Informieren Sie Bekannte, denen Sie in jüngster Zeit Dateien geschickt haben.

**Bei Misserfolg:**
Je nach Dringlichkeit können Sie

- sich an eine Fachperson wenden
- überprüfen, ob Spyware die Ursache ist, und entsprechende Software einsetzen
- warten, bis ein entsprechendes Update vorliegt (einige Stunden, max. 2 Tage).





**Befall durch Spyware bzw. Trojaner**
Spyware auf dem eigenen PC bleibt oft lange unentdeckt. Meist kommt sie als unsichtbares Anhängsel von Gratisprogrammen auf Ihren PC. Mögliche **Symptome** sind:

- Verschlechterung der Systemleistung (d. h. längere Wartezeiten als sonst)
- sich häufig öffnende Werbefenster oder
- veränderte Einstellungen des Internet-Programms (z. B. andere Startseite).

**Entfernung:**

1. Wenn Ihr Virenscanner den Trojaner findet, kann er ihn ziemlich sicher auch entfernen.
2. Ist dies erfolglos, installieren Sie ein Anti-Trojaner-Programm. Informationen dazu finden Sie unter: 711 **www.trojaner-info.de**. Gegen Spyware-Befall hilft die Software von Spybot Search & Destroy (gratis Download unter 734 **www.spybot.safer-networking.de**).
3. Falls auch dies erfolglos ist, wenden Sie sich an eine Fachperson.

**Befall durch unseriöse Dialer**
Wenn sich ein Dialer auf Ihrem PC befindet und Sie vermuten (von Ihrer Telefonrechnung, ständig abrufbar via «Festnetzrechnung online»), dass er bereits finanziellen Schaden angerichtet hat, ist es wichtig, dass Sie «Beweise sichern», bevor Sie den Dialer löschen. So haben Sie im Falle einer Anfechtung etwas in der Hand.
Bei Dialerschäden: 712 **www.konsum.ch/pdf/09xx-Nummern.pdf**
Verbindungsnachweis online: 713 **www.swisscom-fixnet.ch/rechnungonline**

**Sichtbare Dialer entfernen** (Dialer hat offensichtlich neue DFÜ-Verbindung installiert)
Windows XP: Wählen Sie im Menü **Start** > **Systemsteuerung** > **Netzwerkverbindungen** (ältere Systeme: **Start** > **Systemsteuerung** > **DFÜ-Einstellungen**).

1. Falls es neben den Einträgen Ihres Internet-Dienstleisters, z. B. Bluewin oder anderen, fremde Einträge gibt, löschen Sie diese (Rechte Maustaste > **Löschen**).
2. Prüfen Sie die Einwahlnummer Ihres Providers (rechte Maustaste > **Eigenschaften**, Reiter «Allgemein»).
   Mehr unter: 714 **www.microsoft.com/switzerland/de/security/dialer**

**Getarnte Dialer entfernen** (Dialer ist nicht sofort auffindbar)
Einige Dialer «tarnen» sich regelrecht. Neue Antiviren-Software enthält bereits spezielle Funktionen zum Auffinden und Entfernen solcher Dialer.

1. Aktualisieren Sie Ihre Antiviren-Software und verwenden Sie die entsprechende Funktion.
2. Falls erfolglos, installieren Sie ein Antidialer-Programm, z. B. den «Dialerwarner»: 715 **www.swisscom-fixnet.ch/fx/privatkunden/dienste/dialerschutz**
3. Sollte auch das Antidialer-Programm keine Wirkung zeigen, wenden Sie sich an eine Fachperson.

# Linktipps zur Selbsthilfe

So zahlreich Virenprogrammierer auch sein mögen – letztlich sind sie eine kleine Minderheit. Es gibt im Internet zahlreiche Adressen, die Sie unterstützen. Eine Auswahl.

**Virenmeldungen der Unternehmen**
Die Websites von Microsoft und Apple sowie die Schutz-Software-Hersteller enthalten immer auch aktuelle Virenmeldungen, z. B.

716 **de.mcafee.com/virusinfo**
717 **www.antivir.de/de/vireninfos**

**Fachpresse online**
Die Websites der Computer-Fachpresse enthalten alle Virenmeldungen bzw. Spezialseiten zur Sicherheit, z. B.

718 **www.pctipp.ch/helpdesk/virenticker**
719 **www.heise.de/security**
720 **de.bluewin.ch/services/sicherheit/index.php/sicherheitslage_de**

**Hoaxinfo**
Verschiedene Plattformen sammeln Meldungen der User insbesondere über Spam und Hoaxes (falsche Virenwarnungen). Hier können Sie nachschlagen, aber auch neue Übeltäter melden: 710 **www.hoaxinfo.de**

**Gemeinsam stark gegen Spam: SpamNet**
Menschen sind besser beim Erkennen von Spam als Software: Wenn viele Benutzer der Software SpamNet ein eingehendes Mail als Spam markieren, wird es einer zentralen Datenbank gemeldet und diese blockiert es für alle weiteren Nutzer. Gratistestversion unter: 721 **www.cloudmark.com/products/spamnet**

**Sicherheits-Checks online**
Testen Sie online kostenlos Ihre Konfiguration, wenn Sie unsicher sind, ob Sie ausreichend geschützt sind.


722 **www.heise.de/security/dienste/emailcheck**
723 **www.kaspersky.com/remoteviruschk.html**
724 **www.symantec.com/region/de/avcenter**



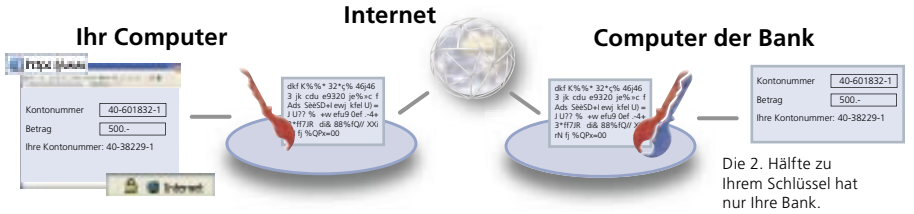


# Der richtige Kunde – die echte Firma

Wenn es im Internet ums Einkaufen, genauer ums Bezahlen, geht, wollen Sender *und* Empfänger sicher sein, dass die andere Person wirklich die ist, für die sie sich ausgibt.

**Einfache Authentifikation**
Im Alltag würde man sich den Ausweis des Gegenübers zeigen lassen; im Internet wird dies über eine elektronische Identitätsprüfung (= Authentifikation) durchgeführt. Der Kunde legt vor dem ersten Kauf ein Benutzerkonto auf der Website des Verkäufers an und gibt sich bei jedem Besuch mit Benutzernamen und Passwort zu erkennen (= Login). Der Benutzername ist eindeutig und identifiziert so die Person. Das Passwort ist eine Zahlen-/Buchstabenkombination, die nur ihm selbst bekannt ist. Der Benutzername ist offen lesbar, das Passwort wird bei der Eingabe maskiert als **** angezeigt.

**SSL-Verschlüsselung zur Geheimhaltung**
Die Geheimhaltung von Zahlungsangaben wird durch die SSL-Verschlüsselung L217 (steht für «Secure Sockets Layer», ein von der Firma Netscape entwickeltes Übertragungsprotokoll) der Verbindung erreicht. SSL ist das Standard-Verfahren für die Verschlüsselung von Datenübertragungen im Internet, die so für Dritte unleserlich werden. Erkennbar sind SSL-Verbindungen am Vorhängeschlosssymbol in der Statusleiste des Browsers sowie am Kürzel http**s** (s wie «secure», dt. sicher) in der Adresszeile.

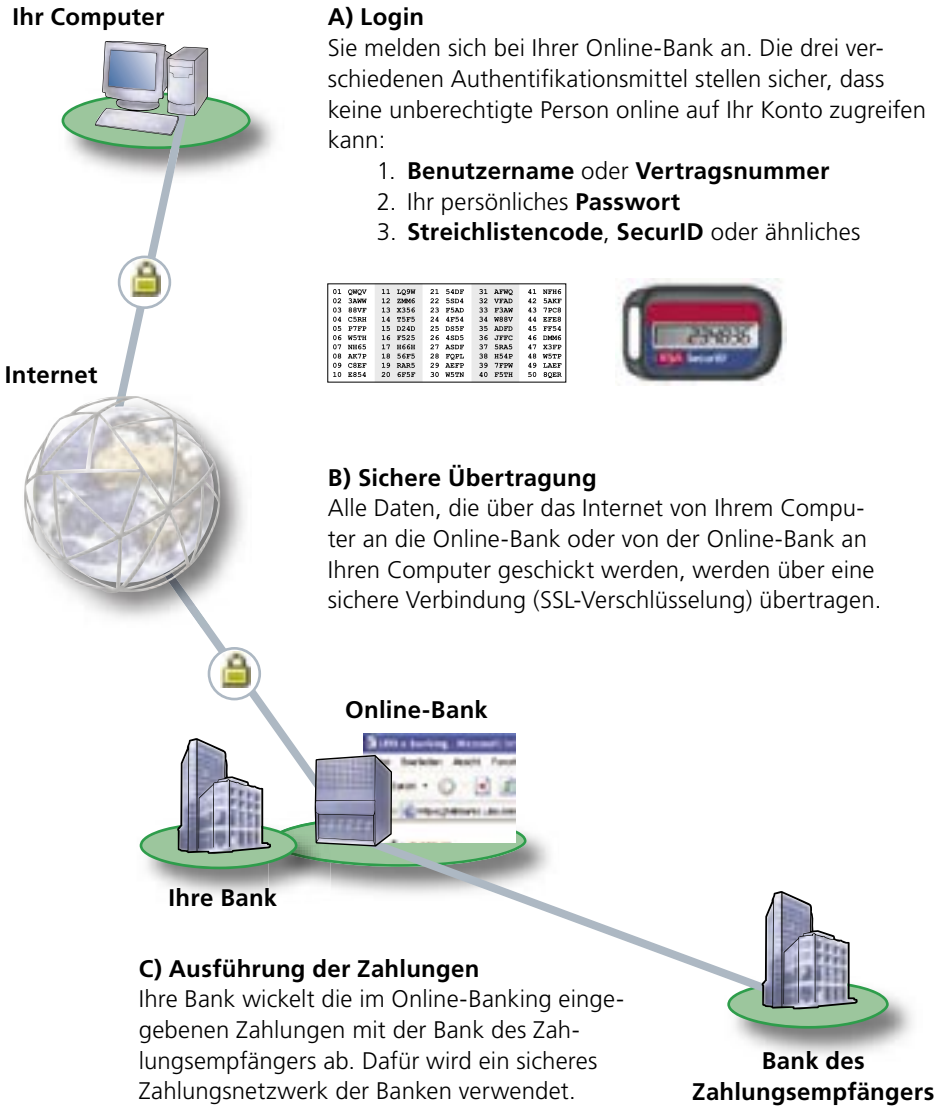



**Digitale Zertifikate**
Durch Doppelklick auf das Vorhängeschlosssymbol in der Fusszeile können Sie das digitale Zertifikat jeder verschlüsselten Webseite ansehen. Dabei handelt es sich um eine elektronische Bescheinigung der Identität einer Organisation. Im Zweifelsfall können Sie so überprüfen, ob Sie Ihre Angaben wirklich auf der richtigen Website machen.

**Hinweis:** Wenn Ihr Browserfenster die Statuszeile nicht anzeigt, können Sie diese im Menü **Ansicht** unter **Statusleiste** einblenden.

# Sicheres Bezahlen

**Dreifache Authentifikation beim Online-Banking**
Die Sicherheitsvorkehrungen der Banken für Online-Banking gehen über die von anderen Online-Anbietern noch hinaus. Zusätzlich zu Benutzername und Passwort wird ein drittes Authentifikationsmittel verwendet. Kunden können so über das Internet jederzeit und überall gesichert auf das eigene Konto zugreifen.




**A) Login**
Sie melden sich bei Ihrer Online-Bank an. Die drei verschiedenen Authentifikationsmittel stellen sicher, dass keine unberechtigte Person online auf Ihr Konto zugreifen kann:

1. **Benutzername** oder **Vertragsnummer**
2. Ihr persönliches **Passwort**
3. **Streichlistencode**, **SecurID** oder ähnliches

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 01 | QWQV | 11 | LQ9W | 21 | 54DF | 31 | AFWQ | 41 | NFH6 |
| 02 | 3AWW | 12 | ZMM6 | 22 | 5SD4 | 32 | VFAD | 42 | 5AKF |
| 03 | 86VF | 13 | X356 | 23 | F5AD | 33 | F3AW | 43 | 7PC8 |
| 04 | C5NH | 14 | T5F5 | 24 | 4F54 | 34 | W88V | 44 | EFE8 |
| 05 | P7FP | 15 | D24D | 25 | DS5F | 35 | ADFD | 45 | FF54 |
| 06 | W5TH | 16 | F525 | 26 | 4SD5 | 36 | JFFC | 46 | DMM6 |
| 07 | NH65 | 17 | H66H | 27 | ASDF | 37 | 5RA5 | 47 | X3FP |
| 08 | AK7P | 18 | 56F5 | 28 | FQPL | 38 | H54P | 48 | W5TP |
| 09 | CBEF | 19 | RAR5 | 29 | AEFP | 39 | 7FPW | 49 | LAEF |
| 10 | E854 | 20 | 6F5F | 30 | W5TN | 40 | F5TH | 50 | 8QER |



**B) Sichere Übertragung**
Alle Daten, die über das Internet von Ihrem Computer an die Online-Bank oder von der Online-Bank an Ihren Computer geschickt werden, werden über eine sichere Verbindung (SSL-Verschlüsselung) übertragen.

**C) Ausführung der Zahlungen**
Ihre Bank wickelt die im Online-Banking eingegebenen Zahlungen mit der Bank des Zahlungsempfängers ab. Dafür wird ein sicheres Zahlungsnetzwerk der Banken verwendet.





# Beispiel Direct Net


Wenn Sie sich für Direct Net der Credit Suisse anmelden, erhalten Sie eine Vertragsnummer (entspricht dem Benutzernamen bzw. der Benutzeridentifikation) und ein automatisch generiertes Initialpasswort, das Sie bei der ersten Anmeldung ändern müssen. (Beachten Sie dabei die Empfehlungen für sichere Passwörter auf Seite 26.) Als zusätzliches Sicherheitsmerkmal für den Zugriff auf Ihr Konto benötigen Sie ein weiteres «Passwort», das bei jeder Anmeldung wechselt:


Die **SecurID** ist eine Karte mit einer Zahlenanzeige; sie zeigt minütlich eine andere sechsstellige Ziffernfolge an. Wenn Sie sich anmelden, bildet die aktuelle Reihe Ihr zweites Sicherheitsmerkmal. Da diese Ziffernfolge ständig wechselt, kann niemand die Zahlen kopieren und später verwenden.

Die **Streichliste** ist eine Liste mit 100 Zahlen-/Buchstabenkombinationen. Bei jeder Anmeldung identifizieren Sie sich mit dem nächsten Code. Diese Listen werden von vielen Banken als drittes Sicherheitsmerkmal eingesetzt; auch in der Variante, dass man nicht mehr abstreicht, sondern die Stelle vorgegeben wird.

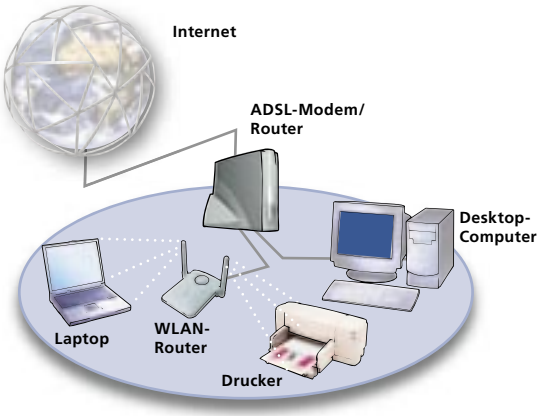
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 01 | QWQV | 11 | LQ9W | 21 | 54DF | 31 | AFWQ | 41 | NFH6 |
| 02 | 3AWW | 12 | ZMM6 | 22 | 5SD4 | 32 | VFAD | 42 | 5AKF |
| 03 | 86VF | 13 | X356 | 23 | F5AD | 33 | F3AW | 43 | 7PC8 |
| 04 | C5NH | 14 | T5F5 | 24 | 4F54 | 34 | W88V | 44 | EFE8 |
| 05 | P7FP | 15 | D24D | 25 | DS5F | 35 | ADFD | 45 | FF54 |
| 06 | W5TH | 16 | F525 | 26 | 4SD5 | 36 | JFFC | 46 | DMM6 |
| 07 | NH65 | 17 | H66H | 27 | ASDF | 37 | 5RA5 | 47 | X3FP |
| 08 | AK7P | 18 | 56F5 | 28 | FQPL | 38 | H54P | 48 | W5TP |
| 09 | CBEF | 19 | RAR5 | 29 | AEFP | 39 | 7FPW | 49 | LAEF |
| 10 | E854 | 20 | 6F5F | 30 | W5TN | 40 | F5TH | 50 | 8QER |

Sie können dazu beitragen, dass die Sicherheitsvorkehrungen optimal funktionieren:

- Verwenden Sie zur Anmeldung immer die offizielle Adresse Ihrer Bank, hier **www.credit-suisse.com** oder **www.directnet.com**.
- Öffnen Sie während der Nutzung des Online-Bankings keine weiteren Internet-Seiten.
- Beachten Sie Sicherheitshinweise auf Ihrem Bildschirm wie Informationen zu Ihrer letzten Nutzung des Online-Banking.
- Achten Sie darauf, sich nach jeder Nutzung abzumelden (Button: **Beenden**).
- Leeren Sie die temporären Internet-Dateien Ihres Programms nach der Sitzung (**Extras > Internetoptionen >Allgemein > Dateien löschen**).
- Verwenden Sie stets die aktuelle und durch Ihre Bank empfohlene Browser-Version.

Weiterführende Hinweise zur Sicherheit von Direct Net und detaillierte Angaben zum Zertifikat unter: 725 **www.directnet.com/de/media/pdf/dn_de_sicherheit_10_04.pdf**
Inzwischen haben fast alle Banken und Postfinance solche Informationsseiten zur Sicherheit ihres Online-Banking zusammengestellt.

# Kabellose Netzwerke sichern




Wenn Sie zu Hause ein WLAN (Abkürzung für engl. Wireless Local Area Network = kabelloses Netzwerk) installiert haben, müssen Sie dieses speziell schützen. Andernfalls kann jeder, der sich innerhalb der Reichweite befindet, darauf zugreifen.

Wir zeigen am Beispiel des von Bluewin vertriebenen WLAN-Routers (engl. Router = Vermittlungsknoten) von Netopia die nötigen Einstellungen. Wenn Sie ein anderes Gerät einsetzen, führen Sie die Schritte analog anhand der Bedienungsanleitung durch.

**Schritt 1: Passwort ändern**

Eindringlinge kennen die werkseitig eingestellten Passwörter der Router und könnten so auf Ihr Gerät zugreifen. Setzen Sie daher ein eigenes sicheres Passwort (vgl. S. 26, «Sicherheitslücke Passwort»).

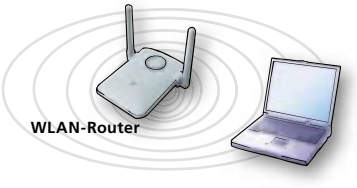
1. Tippen Sie **http://192.168.1.1** in das Adressfeld Ihres Browsers ein, um auf die Einstellungen des Netopia Router zuzugreifen. (Anmerkung: Diese Zugangsadresse funktioniert für viele gängige Router.)
2. Melden Sie sich mit dem Benutzernamen (z. B. «Admin») und dem werkseitig vorgegebenen Passwort an. Beides finden Sie in der Bedienungsanleitung.
3. Ändern Sie dieses Passwort im Menü **Experten Modus** > **Konfigurieren** > **Router Kennwort**.

**Hinweis**: Die Geräte verfügen in der Regel über eine Fernwartungsfunktion, die Service-Technikern Zugang zu Ihrem Router über das Internet geben soll. Diese können sich auch Angreifer zunutze machen. Bei Netopia Routers ist diese Funktion (engl. «Remote Management») sicherheitshalber bereits standardmässig deaktiviert, sodass Sie sie zuerst aktiv einschalten müssen, wenn Ihnen jemand via Fernwartung helfen soll.





**Schritt 2: Netzwerk «abschliessen»**




Wer in ein drahtloses Netzwerk eindringen will, muss dessen «Namen», die «SSID» (Service Set ID, manchmal auch «ESSID» für «Extended …») kennen. Verhindern Sie daher, dass Ihr Router seine SSID allen drahtlosen Geräten in seiner Reichweite mitteilt.

Beim Netopia Router findet sich diese Einstellung unter **Experten Modus** > **Konfigurieren** > **Wireless** > **Erweitert**. Aktivieren Sie dort die Option «Erlaube geschlossenen System Modus».

**Schritt 3: Funkverkehr verschlüsseln**

1. Schalten Sie unter **Experten Modus** > **Konfigurieren** > **Wireless** > **Erweitert** die «WEP Verschlüsselung» auf «Ein – automatisch».
2. Denken Sie sich einen Satz mit mindestens 26 Zeichen aus (z. B. «Fischers Fritz fischt frische Fische»). Diesen Satz verwendet das System dann zum Verschlüsseln der Daten.
3. Stellen Sie die Grösse des Verschlüsselungscodes auf 128 bit (eine noch höhere Codierung würde Ihren PC verlangsamen).
4. Speichern Sie Ihre Änderungen.

**Wichtig**: Nehmen Sie die folgenden Einstellungen analog auf jedem Computer vor, der das drahtlose Netzwerk mit benutzen soll:

1. Melden Sie sich als Administrator an den Computern an und klicken Sie auf **Start > Netzwerkverbindungen.** Klicken Sie dort mit der rechten Maustaste auf **Drahtlose Netzwerkverbindung** und wählen Sie im Kontextmenü **Eigenschaften**. Klicken Sie dann bei den bevorzugten Netzwerken den Button **Hinzufügen**.
2. Tragen Sie dort Ihre SSID im vorgesehenen Feld ein und deaktivieren Sie das Kästchen «Schlüssel wird automatisch bereitgestellt».
3. Tragen Sie auch hier den gleichen Verschlüsselungssatz («Fischers Fritz … ») ein.
4. Klicken Sie **OK**, um Ihre Änderungen zu speichern.

Weitere Informationen zu WLAN:

726 **de.bluewin.ch/internetzugang/index.php/wlan_traveller**
727 **www.windows-netzwerke.de/wlansicherheit.htm**

# Checkliste

| Zu erledigen | erledigt | Bemerkungen | Seite |
|---|---|---|---|
| **Betriebssystem: Typ und Version festgestellt?**<br>z. B. unter Windows: Start > Programme > Ausführen «winver» eingeben, OK. | ☐ | Typ: | |
| **1. Aktualisierungen für das Betriebssystem herunterladen**<br>Achtung: als Administrator anmelden | ☐ | | 24 |
| **2. Testversion für Komplettlösung für Schutzsoftware herunterladen** oder | ☐ | *Norton Internet Security 2005* | 21 |
| **Firewall beschaffen**<br>bei XP: Firewall aktiviert?<br>andere Betriebssysteme: Firewall gekauft/heruntergeladen | ☐ | *Microsoft XP Firewall* | 19/20 |
| **Antiviren-Software beschaffen** | ☐ | | 19/20 |
| **3. Automatische Aktualisierung des Betriebssystems und für Schutz-Software gesetzt** | ☐ | | 24 |
| **4. Eigene Passwörter sicher erstellt?** | ☐ | nicht notieren! | 26 |
| **5. Administrator-Konto mit Passwort geschützt?** | ☐ | nicht notieren! | 16 |
| **6. Sicherheitseinstellungen überprüft?**<br>• bekannte Dateiendungen einblenden<br>• Sicherheitsstufen des Internet Explorer anpassen<br>• Autovervollständigen bei Passwörtern aus<br>• Windows Nachrichtendienst aus<br>• Mail-Programm (z. B. Outlook Express) gesichert | ☐ | | 22/23 |
| **7. Sicherheitskopien angelegt**<br>• Speicherplatzbedarf ermittelt<br>• Speichermedium ausgewählt und gekauft<br>• Kalendereinträge für nächstes Backup gemacht | ☐ | Neue Kopien alle ___Wochen | 25 |
| **8. Erinnerungsdienste aktiviert**<br>(oder eigene Erinnerungen im Kalender notiert) | ☐ | | 24 |
| **Nur bei kabellosem Netzwerk**<br>1. Passwort geändert<br>2. Netzwerk «abgeschlossen» (SSID deaktiviert)<br>3. Funkverkehr verschlüsselt | ☐ | | 36/37 |

**728 www.schoolnet.ch/checkliste.pdf**



# «Verkehrserziehung» für die Datenautobahn

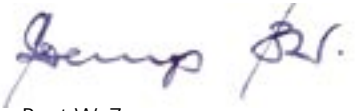
Liebe Lehrerinnen und Lehrer

Die Sicherheitsfragen, die in diesem SchoolNetGuide beschrieben werden, gehen uns alle an und sind natürlich auch Thema für die Schule: Wir erinnern uns noch an die schulische Verkehrserziehung, die uns das sichere Verhalten im Strassenverkehr gelehrt hat. Nun folgt die «Verkehrserziehung» für die modernen Datenautobahnen: der sichere Umgang mit dem Internet.

Auch hier ist es hilfreich, die nötigen Schritte nicht nur nachzulesen, sondern so weit wie möglich auch «anfassen» und ausprobieren zu können. Es freut mich deshalb, dass die Ausstellung «Cybernetguard» im Verkehrshaus der Schweiz in Luzern diese Gelegenheit bietet. Ich möchte Ihnen somit einen Besuch der Ausstellung mit Ihrer Klasse empfehlen. Diese ist keineswegs nur aus der Perspektive des Fachs Informatik interessant; vielmehr zeigt sie Risiken und Grundregeln für den Umgang mit Informations- und Kommunikationstechnologien auf, die für uns alle im Alltag wichtig sind.

Nutzen Sie also auch die Möglichkeit, wirtschaftliche, soziale und ethische Aspekte der Internet-Verbreitung aufzugreifen, z. B. mit Diskussionen zur Vorbereitung des Ausstellungsbesuchs zu Themen wie der Balance zwischen Sicherheit und Privatsphäre oder der Motivation von Virenprogrammierern, deren zerstörerische Schaffenskraft ihnen keinen direkten Nutzen bringt. Nutzen Sie es, wenn Sie Internet-Begeisterte in der Klasse haben: Der modulartige Aufbau der Ausstellung erleichtert es, diese Inhalte vor Ort von Schülerinnen und Schülern erklären zu lassen.
Weitere Informationen und Unterrichtstipps finden Sie auf der Website zur Ausstellung: www.cybernetguard.ch.

Ich wünsche Ihnen viel Vergnügen und Erfolg bei dieser Exkursion.



Beat W. Zemp

Zentralpräsident Lehrerinnen
und Lehrer Schweiz (LCH)

# Index


Administrator 16, 21, 23, 38
ADSL 11, 17, 20, 36
Adware **14**
Aktualisierung (Update) 17, 18, 22, **24**, 27, 29, 30
Analoger Internet-Zugang 17, 20
Antivir 20
Antiviren-Software 7, 10, 16–18, **19**, 20–22, 24, 30–31, 38, 43
Authentifikation **33**, 34

Backup 18, **25**, 38,
Benutzername 26, 33, 36,
Betriebssystem 6, 10, **16**, 18, 22, 24, 29, 38
Blaster 10
Browser 11, 18, 22, 33, 35

CD-ROM 5, 6, 16, 19, 20, 25, 30
Chat 13,
Cookies **12–13**, 15, 29,
Cybernetguard 2, 39, 43

Dateiendungen 6, 27
DFÜ (Einwahlverbindung) 11, 31
Dialer 5, 8, 10, **11**, 15, 17, 30, **31**
Digitales Zertifikat 33, **35**
Direct Net (Credit Suisse) 35
Diskette 5, 6, 19, 30
Download 5, 10, 20–21, 29

E-Mail 5, **6–7**, 9, 18–19, 23, 26–28
Erinnerungsdienst 24, 38
externe Festplatte 25

Fernwartung (Remote) 36,
Firewall 10, 14, 16–18, **19**, 20–22, 24, 38, 43
Forum 12, 28

Gratisprogramme 5, 20, 31
Grundeinstellungen 7, 18, **22–23**, 38

Hacker **14**, 15–16, 19
Hijacker **14**
Hoax **8**, 15, 27, 32

Identität 4, **13**, 33
Image-Programm 25
Internet Explorer 19, 22, 24, 29, 38
IP-Adresse 10, **12**
IP-Popup **10**, 15
ISDN 15, 17, 20

Keylogger **14**
Kinderschutz 21
Kreditkarte **11**, 15

Laptop 20, 36
Login 9, 33–35
Lovsan 10

Makroviren 6
Malware 4
Megabyte 25
Memorystick 25
Modem 17
Netopia 35
Norton **21**, 24
Notfall 18, 21, **30**, **31**

Outlook Express 21–22, **23**

Passwort 9, 14–18, 23, **26**, 27, 29, 33, 35, 36
Phishing 9, 15
Privatsphäre (Privacy) 2, 18, 21
Programme **4**, 6, 10, 15, 19, 20, 22, 23, 35
Provider 12, **17**, 31

Router **17**, 36, 37

Sicherheitseinstellungen 7, 18, **22–23** 38
Software 4, 16, 17, 21, 24, 29, 30, 32, 36
Spam 4, **8**, 14, 15, 17, 21, 28, 32
Speicherkarte 25
Spyware 4, **14**, 15, 19, 20, 30–31
SSID 37
Streichliste 35

temporäre Internet-Dateien 35
Trojaner 4, 10, **14**, 15, 19, 20, 30– 31

Update 17, 18, 22, **24**, 27, 29, 30

Verschlüsselung 11, 14, 28, 29, **33**, 37
Virus 4–5, **6**, 7–8, 14–16, 19–24, 27, 30, 32, 43
Virenbibliothek **19**
Virenscanner 7, **19**, 31
Virenschild **19**

Wardriving **14**, 15
Webserver 12, **19**
Windows-Nachrichtendienst 10, **23**
WLAN 14–15, **36**, 37
Wurm **4**, **5**, **7**, **10**, 15, 17–19, 24, 29–30

# Weiterführende Links

729 **www.cybernetguard.ch** – Website zur Ausstellung über Computersicherheit und Privatsphäre im Internet im Verkehrshaus der Schweiz in Luzern. Lehrpersonen können das Verkehrshaus zur Vorbereitung von Klassenbesuchen kostenlos besuchen. Die Halle COM 1 kann für den Unterricht vor Ort reserviert werden.

730 **www.microsoftsecurity.ch** – Sicherheitsportal von Microsoft Schweiz mit aktuellen Vireninformationen und Schritt-für-Schritt-Anleitungen für alle Sicherheitseinstellungen.

731 **www.bsi-fuer-buerger.de** – Das ausführliche Sicherheitsportal des deutschen Bundesamts für Sicherheit und Informationstechnik ist verständlich geschrieben und aktuell.

732 **www.rokop-security.de** – Hier finden Sie Beschreibungen und Software-Tests für verschiedene Sicherheitsprogramme: Firewalls, Antiviren-Software usw.

733 **www.sicherheit-online.net** – Private Website zu den Themen Sicherheit und Privatsphäre.


**Impressum**

**Herausgeberin** Swisscom AG, Schulen ans Internet

**Redaktion und Gestaltung** Zeix AG, Zürich





**Ausgabe** SchoolNetGuide Nr. 7 · Herbst 2004

**Auflage** 400'000 (d/f/i)

**Druck** Zollikofer AG, St. Gallen




**Die Ausgabe Nr. 8 des SchoolNetGuide ist für Frühjahr 2005 vorgesehen.**



**Bitte in einem frankierten Kuvert schicken**


**Swisscom AG**
Schulen ans Internet
Alte Tiefenaustrasse 6
Postfach
3050 Bern


Für die Schweizer Schulen
wird die Welt etwas kleiner!
Swisscom hat mit ihrem Engagement «Schulen ans Internet» in den letzten drei Jahren über 3000 Schulen kostenlos ans Internet angeschlossen. Und es werden immer mehr. Schulen, die von diesem Engagement von Swisscom profitieren wollen, erfahren alles Nötige unter www.swisscom.com/sai.
www.swisscom.com/sai
Schulen ans Internet
swisscom