

Sicheres Surfen im Internet

Der folgende Text informiert Sie über die Sicherheitsrisiken bei der Nutzung des Internets. Sie erhalten Tipps, wie Sie die Sicherheit Ihres Systems optimieren können. Im beigefügten **Anhang** finden Sie eine Aufstellung mit kostenloser Software (Share- bzw. Freeware) für Ihre Systemsicherheit. Gerade für Privatanwender und Einsteiger bieten diese Programme durch die einfache Steuerung und Funktion ausreichenden Schutz.

Sicher durchs weltweite Datennetz

Wie im realen Leben gibt es auch bei der Nutzung des Internets Risiken. Genau so wie Sie nicht die Wohnung verlassen, ohne die Tür zu verschließen oder einer unbekannt Person Ihre Kreditkarte überlassen, sollten Sie sich auch vor dem Surfen im World Wide Web mit den Sicherheitsfragen des Internet auseinandersetzen. Nur so wird Online-Surfen für Sie zu einem Erlebnis ohne unerwünschte Nebenwirkung. Mit der rasant wachsenden Zahl der Internet-Nutzer sowie der steigenden wirtschaftlichen Bedeutung dieses Netzwerks nehmen auch die Gefahren zu. Lassen Sie sich aber hierdurch nicht abschrecken. Denn es gibt für den normalen Nutzer weitaus weniger Bedrohung, als gemeinhin angenommen wird. Zumindest nicht mehr, als im realen Leben auch. Welche Gefahren lauern genau im Internet?

Typische Gefahrenquellen im Internet:

1. Mitlesen und Verändern von Daten aufgrund einer offenen Übertragung (Unverschlüsseltes WLAN, Nicht SSL-geschützte Verbindungen)
2. **Viren&Würmer:** Kleine Programme, die sich selbständig "vermehren" und weiterverbreiten (z.B. durch das Versenden verseuchter Mails) und Schaden an Ihrem Computersystem anrichten können, z.B. die Festplatte formatieren oder die Leistung bremsen.
3. **Trojanische Pferde/Keylogger:** Programme, die andere Funktionen ausführen, als dem Nutzer bewusst sind, z.B. die Passwortdatei an einen Angreifer übertragen oder die Tastatureingaben mitlesen und übersenden.
4. **Backdoor:** Der „Hintereingang“ in ein Computerprogramm, welcher vom Programmierer oder andern Personen unter Umgehung der Sicherheitsbarrieren des Computers genutzt werden kann.
5. **Denial of Service - DoS/Flooding:** Überlastung eines Servers bzw. Rechners durch zahlreiche, gleichzeitige Attacken.
6. **Phishing/Pharming/Spoofing:** Diese Techniken wurden besonders im Zusammenhang mit dem veralteten PIN/TAN-Online-Bankings mit den TAN-Listen bekannt. Hier wird versucht auf gefälschte Websites umzuleiten bzw. TAN-Nummern abzufragen. Hier ist es auch denkbar, dass die Absenderadressen manipuliert und dadurch falsche Angaben vorgetäuscht werden.

Unsere neuen Online-Banking-Verfahren mobileTAN und Sm@rtTAN plus unterstützen die neuesten Sicherheitsstandards: Trennung der Übertragungswege - die Überweisungserfassung und Übermittlung der TAN erfolgen auf unterschiedlichen Wegen - und TAN-Bindung - die erzeugte TAN ist an den jeweiligen erfassten Zahlungsauftrag gebunden.

Sicheres Surfen im Internet

Sie müssen kein Internet-Profi oder Programmierer sein, um sich gefahrlos durch die Online-Welt zu bewegen. Schon wenn Sie die folgenden **zehn Grundregeln** beachten, können Sie Ihre Sicherheit im „www“ um ein Vielfaches steigern.

1. Machen Sie einen persönlichen **Sicherheits-Check**
2. Überlegen Sie genau, **wer Ihr Vertrauen verdient**.
3. Speichern Sie **sensible Daten** (Passwörter, Kreditkartennummern usw.) nicht auf Ihrer Festplatte ab.
4. Betrachten Sie **Programme aus dem Internet** erst einmal als unzuverlässig.
5. Nutzen Sie nur die **aktuelle Version** Ihrer Internet-Zugangssoftware
6. Aktivieren Sie die **Sicherheitsoptionen** Ihres Internet-Browsers
7. Setzen Sie **zusätzliche Sicherheitssoftware** ein (Virens Scanner, Firewalls)
8. Übermitteln Sie sensible Daten über offene Leitungen **nicht unverschlüsselt**
9. Machen Sie regelmäßige **Sicherheitskopien** von Ihren Datenbeständen
10. Für Power-Surfer: Konfigurieren Sie sich einen **eigenen Internet-PC**

Regel Nr.1: Machen Sie einen persönlichen Sicherheits-Check

Nehmen Sie sich Zeit, bevor Sie Ihren neuen Internet-Anschluss aktivieren. Machen Sie einen persönlichen und realistischen Sicherheits-Check. Nutzen Sie die Sicherheitseigenschaften des Betriebssystems und installieren Sie keine überflüssige Software, durch die der Rechner erst von außen erreichbar wird. Vor allem: Welchen Schaden verkraften Sie, wenn trotz aller Vorsicht etwas schief geht? Hier gilt z.B.: Ein PC, der größere Mengen sensibler Daten speichert (z.B. die Korrespondenz eines Rechtsanwalts), sollte nicht als Internet-PC eingesetzt werden. Außerdem: ein Online-Shopper wird sich vor allem um die Sicherheit bei der Übermittlung seiner Kreditkartennummer sorgen. Diejenigen, die gerne in den Internet-Programmsammlungen stöbern, sollten sich vorwiegend mit der Wirksamkeit von Antiviren-Programmen auseinandersetzen. In jedem Fall heißt es: Bleiben Sie realistisch. Nicht überall im Internet lauern Piraten, die es nur darauf absehen, Ihre privaten e-Mail zu lesen. Nicht jeder "Chat-Partner" will Sie schädigen.

Regel Nr. 2: Überlegen Sie genau, wer Ihr Vertrauen verdient

Nicht jeder ist im Internet der, der er zu sein vorgibt. Für Experten ist es vergleichsweise einfach, eine e-Mail-Adresse zu fälschen oder eine ganze Website vorzugaukeln. Vorsicht ist ebenso angebracht bei manchem günstigen Angebot im Web. Die Seriosität des Anbieters kann schwer zu überprüfen sein. Vergleichen Sie also regelmäßig die Adressen, die Sie in der sog. URL-Leiste angeben (oder des Links, den Sie anklicken), mit den Angaben, die Sie in der Status-Leiste sehen. Diese Angaben sind schwieriger zu fälschen. Und darüber hinaus: Geben Sie Informationen nur preis, wenn Sie verlässlich wissen, wer diese Daten erhält und was mit diesen geschehen soll. "Social Engineering", d.h. Erschleichung von Auskünften bei potenziellen Opfern, ist bei Hackern beliebt ("Entschuldigen Sie, ich heiße Meier, bin Sicherheitschef bei X-Online und brauche Ihr Passwort, um Sicherheitstests durchführen zu können."). **Tipp:** e-Mails unbekannter Empfänger ignorieren und löschen! Keinesfalls sensible Daten ungesichert über das Netz oder sogar per e-Mail versenden!

Sicheres Surfen im Internet

Regel Nr. 3: Speichern Sie sensible Daten (Passwörter, Kreditkartennummern usw.) nicht auf der Festplatte ab

Der Zugriff auf die Festplatte steht nicht nur dem PC-Eigentümer offen; solange Sie online sind, können sich unter Umständen auch Außenstehende Dritte ein Bild von Ihrem Datenspeicher machen. Dies erfordert zwar überdurchschnittliches Expertenwissen, doch Ihr Computer hat im Netz eine eigene Adresse und ist damit zugänglich auch für "Kontaktangebote" der unerwünschten Art. Am besten trennen Sie die Leitung nach Abschluss Ihrer Online-Sitzung auch "physikalisch", d.h. lösen Sie das DSL-Modem- bzw. ISDN-Kabel zwischen PC und Telefonanschluss.

Regel Nr. 4: Betrachten Sie Programme aus dem Internet zunächst grundsätzlich als unzuverlässig.

Sie können kaum sicher beurteilen, ob die Quelle seriös ist. Mit Programmen, die aus dem Internet auf die eigene Festplatte geladen werden, können Viren oder Trojanische Pferde übertragen werden. Dies kann auch durch das Öffnen eines Anhangs einer elektronischen Mail geschehen. Deshalb öffnen Sie solche Anhänge nicht, während Sie gerade online sind. Speichern Sie den Inhalt zuerst ab, prüfen Sie ihn mit entsprechenden Programmen oder durch Kontrolle des Quellcodes (z.B. bei einem JavaScript-Programm) und öffnen Sie **erst dann** die fragliche Datei. Testen Sie unbekannte Programme, falls möglich, auf einem Zweitrechner. Beobachten Sie aufmerksam, ob es dabei zu "Überraschungen" kommt, wie z.B. Warnmeldungen Ihres PCs oder nicht von Ihnen veranlasste Einwahlversuche.

empfohlenes Programm aus der Anlage: Avira AntiVir (Windows),
ClamXAV (Mac OSX)

Regel Nr. 5: Nutzen Sie nur die aktuelle Version Ihrer bevorzugten Internet-Zugangssoftware

Nur die jeweils aktuellen Versionen der gängigen Internet-Software können gewährleisten, dass die bis dahin bekannt gewordenen Sicherheitslücken in diesen Programmen geschlossen sind. Fast täglich werden neue Sicherheitsprobleme entdeckt, zu schnell um jeweils mit neuen Versionen des ganzen Programms darauf zu antworten. Nicht zuletzt deshalb arbeiten die Programmierer der großen Hersteller stets mit Hochdruck daran, sog. "Bug-Fixes" bzw. Patches zu entwickeln. Dies sind kleine Programme bzw. Updates, mit denen sich konkrete Probleme beheben lassen. Nutzen Sie keine BETA-Software! Informieren Sie sich regelmäßig über die neueste Entwicklung: die meisten Hersteller unterhalten entsprechende Informationsdienste. Überlegen Sie sich genau, ob Sie Zusatzprogramme für Ihren Web-Browser einbinden wollen. Denn auch solche Zusatzprogramme, sog. Plug-Ins, können zusätzliche, unkontrollierbare Sicherheitslücken öffnen.

empfohlenes Programm: Browser Mozilla Firefox (Windows & Mac OSX)

Sicheres Surfen im Internet

Regel Nr. 6: Aktivieren Sie die Sicherheitsoption Ihres Internet-Browsers

Ihre Sicherheit im Internet lässt sich beträchtlich steigern, wenn Sie die Sicherheitsoptionen Ihres Internet-Browsers intelligent einsetzen. Wichtig ist hier vor allem, dass Sie die Zulassung von ActiveX-Controls ausschließen und die Ausführung von Java-Applets nur nach Rückfragen gestatten. Bei diesen sog. "aktiven Inhalten" handelt es sich um kleine eigenständige Programme, die auf Ihrem PC ausgeführt werden und dort u.U. ein unkontrollierbares Eigenleben entwickeln können (z.B. Ihre Passwortdaten per e-Mail versenden).

Cookies (zu Deutsch: "Kekse"), die einige Webseiten auf Ihrem Rechner anlegen, dienen häufig dazu, Inhalte von Warenkörben beim Online-Shopping oder Daten über die besuchten Seiten zwischenspeichern, so dass Sie bei einem erneuten Besuch "wiedererkannt" werden. Diese Daten können natürlich auch durch die Firma der Website dazu genutzt werden, um ein Benutzerprofil anzulegen. In ihrem Browser können Sie die Akzeptanz von Cookies genau steuern und ungewollte Seiten ausschließen.

Für das **InternetBanking** der Pax-Bank müssen Sie die Verwendung von Cookies erlauben. Dies dient hier Ihrer eigenen Sicherheit, da so sichergestellt wird, dass Sie und **nur Sie** während der gesamten Sitzung im InternetBanking der Pax-Bank arbeiten. Das Cookie unseres Online-Bankings beinhaltet keine persönlichen Daten, sondern lediglich eine Zufallszahl und wird beim Verlassen der Seite wieder entfernt. Die im Zusammenhang mit dem InternetBanking notwendigen Einstellungen für den Browser können Sie in unserer Internet-Banking Anwendung unter dem Punkt FAQ nachlesen.

Für einige Browser (z.B. Firefox) gibt es auch spezielle Sicherheits-Plugins, die die Sicherheitseigenschaften des Browsers noch verbessern und auf sicherheitskritische Aktivitäten hinweisen.

empfohlenes Programm: Browser Mozilla Firefox mit dem Plugin NoScript (Windows & Mac OSX)

Regel Nr. 7: Setzen Sie zusätzliche Sicherheitssoftware ein

Manche Sicherheitsprobleme lassen sich nicht allein "mit Bordmitteln", wie z.B. der Windows-Firewall lösen. Wichtigstes Zusatzwerkzeug: ein leistungsfähiger Virensch scanner, der in der Lage ist, auch neue Viren zu erkennen. Fast täglich werden neue Viren entdeckt und es ist durchaus möglich, dass Sie sich bei einem Ausflug in die Online-Welt "infizieren". Bei weiterer Sicherheitssoftware sollten Sie ernsthaft prüfen, vor welchen konkreten Gefahren Sie sich dadurch schützen wollen und vor allem, ob das Kosten/Nutzenverhältnis stimmt. Auch hier gilt: Absolute Sicherheit kann es auch im Internet nicht geben - selbst wenn manche Hersteller das versprechen.

empfohlenes Programm aus der Anlage: Avira AntiVir (Windows),
ClamXAV (Mac),
Firewall Zone Alarm (Windows)

Sicheres Surfen im Internet

Regel Nr. 8: Übermitteln Sie sensible Daten über offene Leitungen niemals unverschlüsselt

Jede Datenübertragung im Internet kann von potentiellen Angreifern grundsätzlich abgefangen und ausgespäht werden. Schützen Sie daher Ihre private und geschäftliche Korrespondenz durch den Einsatz sicherer Verschlüsselungsverfahren. Die Qualität hängt dabei nicht nur von der Schlüssellänge und dem verwendeten Algorithmus ab. Auch Verfahren mit 40 Bit Schlüssellänge, wie sie heute teilweise im Einsatz sind, bieten einen gewissen Schutz. Die Verwendung von längeren Schlüsseln ist aber in jedem Fall empfehlenswert. Ein Angreifer mit einer "normalen" Ausstattung müsste dann erhebliche Mühe aufwenden, um aus dem Kryptogramm den Klartext zu gewinnen - meist mit mehr Mühe als es die verschlüsselten Daten wert sind.

Bei unserer SSL-gesicherten Internet-Banking-Anwendung wird ein sicherer "Datentunnel" von Ihrem Rechner zu uns aufgebaut. Wir bedienen uns dabei einer 256-Bit-Verschlüsselung, die Ihnen einen hohen Sicherheitsstandard gewährt. Die Internet-Banking-Anwendung läuft auf speziell gesicherten Rechnern unseres Rechenzentrums, die sich in einem Hochsicherheits-Bereich befinden. Mehrfache, durch unabhängige Prüfungsgesellschaften zertifizierte Sicherungssysteme sorgen zusätzlich für Ihre und unsere Sicherheit.

Wenn eine Website Ihnen eine Verschlüsselung anzeigt, sollten Sie diese bei der Übertragung wichtiger und kritischer Daten vorher überprüfen. Durch einen Klick auf das Schloss (in der Regel wird dieses Symbol verwendet) wird das Zertifikat angezeigt. Überzeugen Sie sich davon, dass der Anbieter der Seite und der Inhaber des Zertifikats gleich sind!

Regel Nr. 9: Machen Sie regelmäßige Sicherheitskopien (Backups) von Ihren Datenbeständen

Dies ist eine der **wichtigsten** Regeln überhaupt, denn hinterher ist meist zu spät (und wenn, dann sehr teuer), die gespeicherten Informationen zu retten. Zum bequemen Datensichern können Sie z.B. einen USB-Stick, eine Wechselfestplatte oder einen DVD/CD-Brenner einsetzen. Wichtig ist jedoch, dass Sie regelmäßig (z.B. wöchentlich) eine Sicherung der geänderten sowie der neu dazugekommenen Daten vornehmen. Bewahren Sie Ihre Backups unbedingt **getrennt** vom PC auf. Die hier beschriebene Sicherungsart ist lediglich für Privatanwender ausreichend. In Unternehmen werden regelmäßige Sicherungen durchgeführt. Die Sicherungsmodalitäten und der personelle Zugriff auf die Datenträger sind dort genau festzulegen.

empfohlenes Programm aus der Anlage: Personal Backup (Windows)
TimeMachine (MacOSX)

Sicheres Surfen im Internet

Regel Nr. 10: Konfigurieren Sie sich einen eigenen Internet-PC (für Power-Surfer)

Ganz Sicherheitsbewusste sollten mit einem separaten PC in das Internet starten. Ausstattung: Betriebssystem und Internetzugangsoftware, sowie die Programme aus dem Anhang. Dann sind Sie sicher vor den meisten Bedrohungen, die derzeit vom weltweiten Datennetz bekannt sind. Internettaugliche PCs sind heute bereits kostengünstig zu haben: Mindestausstattung: 133MHz, 32MB RAM, 500MB Festplatte. Halten Sie sich dennoch zusätzlich an unsere Sicherheitstipps. So kann kaum noch etwas schief gehen bei Ihren Ausflügen in die Online-Welt.

Weiterführende Informationen

Weitere Ausführungen zum Thema Informationssicherheit bietet Ihnen das Bundesamt für Sicherheit in der Informationstechnik (www.bsi.de) und die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen (www.lfd.nrw.de).

Aktuelle Informationen und Meldungen zum Datenschutz und zur Sicherheit finden Sie unter www.heise.de .

Sicheres Surfen im Internet

Kostenlose Programme für die Sicherheit Ihres PCs (Stand: 09.09.2009)

Hinweis: Zum Zeitpunkt unserer Recherchen standen die u.a. Programme bei den Herstellern kostenlos zum Download zur Verfügung. Dies kann sich jedoch jederzeit ändern. Des gleichen können wir keinerlei Haftung für die Funktionstüchtigkeit oder die Sicherheit der genannten Programme übernehmen. **Der Support** für das jeweilige Programm kann **nur durch den Hersteller** geschehen. Bei Fragen wenden Sie sich daher bitte direkt an den Hersteller. Bitte beziehen Sie die **Updates** der Programme direkt **von der Seite des Herstellers** und **nicht über e-mail!**

Virens Scanner:

- **Avira AntiVir Personal Edition:** www.free-av.de (für Windows)
Dieses für **Privatanwender** kostenlose Antivirenprogramm erkennt über 50.000 Viren und kann kostenlos aktualisiert werden.
- **Bitdefender:** www.bitdefender.de (für Windows)
Auf der Website von Bitdefender kann sowohl eine kostenlose Version bezogen, als auch ein Onlinescan des Systems vorgenommen werden.
- **ClamXAV:** www.clamxav.com (für MacOSX)
Obwohl aufgrund der Systemarchitektur und des Fehlen von echten Viren für MacOSX im Moment (2009) weniger Gefahren für das Apple-Betriebssystem vorhanden sind, kann der kostenlose Scanner sicherlich nicht schaden.

Firewalls:

- **Windows Firewall (im Betriebssystem vorhanden)**
- **Mac OSX Firewall (im Betriebssystem vorhanden)**
- **Zone Alarm:** www.zonealarm.com (für Windows)
Dieses Programm der Firma Zone Labs ist ein Firewallsystem, welches für **Privatanwender** kostenlos ist. Jedes Programm, welches einen Zugriff für das Internet benötigt, wird von Zone Alarm verwaltet und kontrolliert. Alle anderen Verbindungen **von** und **nach** außen werden unterbunden. Zugriffsversuche von außen werden protokolliert. Eine regelmäßige Updatekontrolle kann durch den Benutzer ausgewählt werden.

Backupsoftware:

- **Windows Backup (im Betriebssystem vorhanden):** Das Windows-Backup hat den entscheidenden Nachteil, dass die Backup-Dateien in einer Gesamtdatei gespeichert und nicht 1:1 ausgelagert werden.
- **Personal Backup:** <http://personal-backup.rathlev-home.de/> (Windows)
Komfortable Software zur Erstellung von 1:1 Kopien der Daten. Besser als das Windows-Backup
- **TimeMachine (MacOSX, im Betriebssystem vorhanden):** Komfortable Software zur automatisierten Sicherung des gesamten Systems inklusive der Daten.

Sonstige Software:

- **Mozilla Firefox:** www.mozilla.org – alternativer, kostenloser Browser
- **Spybot Search&Destroy:** www.safer-networking.org - Schützt Ihren PC vor Spyware
- **Spamihilator:** www.spamihilator.com - Schützt Ihr Mail-Programm vor SPAM