

# **☰ Breitbandinternet sicher nutzen**

**TIPPS zur sicheren Nutzung  
des schnellen Internet**



## Impressum

Medieninhaber, Herausgeber und Sitz der Redaktion:  
Saferinternet.at / Österreichisches Institut für angewandte Telekommunikation  
Margaretenstraße 70  
1050 Wien

Website: [www.saferinternet.at](http://www.saferinternet.at)  
E-Mail: [office@saferinternet.at](mailto:office@saferinternet.at)

Die nichtkommerzielle Vervielfältigung und Verbreitung ist ausdrücklich erlaubt unter Angabe der Quelle Saferinternet.at und der Website [www.saferinternet.at](http://www.saferinternet.at).

Alle Angaben erfolgen ohne Gewähr.

Eine Haftung der Autorinnen und Autoren oder von Saferinternet.at/  
Österreichisches Institut für angewandte Telekommunikation ist ausgeschlossen.

Gefördert durch:  
Bundesministerium für Verkehr, Innovation und Technologie  
Europäische Kommission – Safer Internet *plus* Programm

## Vorwort



Das Internet wurde innerhalb weniger Jahre eines der wichtigsten Kommunikationsmittel für Beruf, Schule und Freizeit. Nach aktuellen Daten (Integral/Saferinternet.at) nutzten im September 2007 bereits 68 Prozent der Österreicherinnen und Österreicher ab 14 Jahren das Internet. Rasche Informationssuche, Einkaufen im Internet, E-Mail etc. machen das Leben oft bequemer und einfacher. Immer schnellere Internetverbindungen (auch Breitband genannt) beschleunigen nicht nur bestehende Anwendungen, sondern ermöglichen auch neue Angebote im Internet wie z. B. Internetfernsehen oder (Video)Telefonieren über Internet.

Mit dieser Broschüre wurden für Sie die wichtigsten Informationen und Tipps für eine sichere Internetnutzung zusammengestellt, damit sie die faszinierende Möglichkeiten des Internet voll ausschöpfen können. Keine Sorge: Sie müssen dazu kein/e ComputerexpertIn werden. Mit der Einhaltung von einfachen Regeln können Sie die meisten Risiken mühelos vermeiden. Zum Beispiel: Ein regelmäßig aktualisierter Virenschanner auf dem Computer sollte genau so eine Selbstverständlichkeit sein wie Vorsicht bei der Bekanntgabe persönlicher Daten oder das Interesse der Eltern für die Online-Aktivitäten Ihrer Kinder.

Neben dieser Broschüre finden Sie auch im Internet auf dem Behördenportal [Help.gv.at](http://Help.gv.at) sowie auf [www.saferinternet.at](http://www.saferinternet.at) finden Sie viele wichtige Informationen für ein sorgenfreies Surfen im Internet. Falls es trotzdem Probleme geben sollte, finden Sie hier auch den direkten Kontakt zu Beratungsstellen und zu weiterer Unterstützung von Saferinternet.at.

Viel Spass beim Lesen

Ihr Bundesminister  
Werner Fayman





# Inhalt

Breitband = Schnelles Internet	6
Schutz des Computers	7
Einkaufen im Internet	8
Spam	12
Illegale Inhalte im Internet	14
Schutz der persönlichen Daten	16
Urheberrechte im Internet (Tauschbörsen)	18
Phishing	20
Computer- und Onlinespiele	22
Belästigung im Internet („Cyber-Stalking“)	23
Kinder vor ungeeigneten Inhalten schützen	25
Medienerziehung für Eltern	27



## **≡ Breitband = schnelles Internet**

Internetfernsehen, Musikdownload und Videos aus dem Internet um nur einige Beispiele zu nennen, haben eines gemeinsam: Sie benötigen schnelles Internet. Eine Internetverbindung über die große Datenmengen rasch übertragen werden können wird meist auch Breitband oder Breitbandinternet genannt.

Es gibt verschiedene technische Möglichkeiten des schnellen Internetzuganges, wobei vor allem zwischen leitungsgebundenem und drahtlosem Zugang unterschieden wird. Internetzugang über Kabelfernsehnetze und Telefonleitungen (ADSL) sind leitungsgebunden. Mobile Breitbandzugänge greifen auf die Funknetze der Mobilfunkanbieter zurück.

Ein leistungsfähiger Zugang ist die entscheidende Voraussetzung, um die Vorteile des Internet in allen Lebensbereichen nützen zu können. Deshalb hat das Bundesministerium für Verkehr, Innovation und Technologie in enger Kooperation mit den Bundes-

ländern 2003 die österreichische Breitbandinitiative ins Leben gerufen. Damit konnte die Verfügbarkeit von Breitband nahezu in ganz Österreich erreicht werden.

Neben der technischen Grundausstattung ist für eine erfolgreiche Internetnutzung aber auch wichtig die möglichen Risiken zu verstehen. Auf den folgenden Seiten finden Sie daher die wichtigsten Tipps für sicheres Surfen im Breitbandinternet.



### **TIPP**

Informationen zur Breitbandinitiative des Bundesministeriums für Verkehr, Innovation und Technologie finden Sie im Internet unter [www.bmvit.gv.at/telekommunikation/politik/breitband/](http://www.bmvit.gv.at/telekommunikation/politik/breitband/)

# Schutz des Computers

## Computerviren und andere schädliche Programme.

Kurz gesagt sind Computerviren kleine Programme, die sich in andere Computerprogramme oder Bereiche des Betriebssystems einnisten und dort nicht kontrollierbare, oft schädliche Veränderungen vornehmen. Umgangssprachlich werden auch sogenannte „Würmer“ und „Trojanische Pferde“ (kurz: „Trojaner“) als Viren bezeichnet.

In der Praxis gibt es viele Mischformen der unterschiedlichen Schädlingstypen. Viren verstecken sich am häufigsten in ausführbaren Dateien. Diese sind durch Dateierendungen wie „EXE“ oder „COM“ erkennbar.

Sogenannte „Spyware“ und „Adware“ beeinträchtigen zwar die grundsätzliche Systemfunktionalität nicht, sind jedoch mit anderen Nachteilen verbunden. Spyware sammelt Daten über die Tätigkeit von Computernutzern und -nutzerinnen und leitet diese an Dritte weiter. Adware wird ohne Zustimmung der Nutzer und Nutzerinnen für Werbung oder auch Marktforschung eingesetzt.



### TIPP

Weitere Informationen zu kostenlosen und kostenpflichtigen Schutzprogrammen finden Sie auf den Seiten von <http://saferinternet.at/themen/viren/>



### Wie kann ich meinen Computer schützen?

Beachten Sie folgende Punkte, um Ihren Computer bestmöglich zu schützen:

- 1 Verwenden Sie eine Internetfirewall (ein Schutzprogramm, das unerwünschte Zugriffe von außen auf Ihren Computer abblockt).
- 2 Nutzen Sie aktuelle Software und laden Sie regelmäßig die Aktualisierungen herunter.
- 3 Verwenden Sie aktuelle Anti-Viren-Software und gegebenenfalls Zusatzprogramme zum Schutz vor Spyware oder Adware.
- 4 Öffnen Sie keine E-Mails und E-Mail-Anhänge von verdächtigen oder Ihnen unbekanntem Absendern.
- 5 Legen Sie in Ihrem Betriebssystem Benutzerkonten mit eingeschränkten Berechtigungen für Ihre Kinder an. Damit können Sie die versehentliche Installation von unerwünschten Programmen bei den Entdeckungsreisen Ihrer Kinder durch das Internet verhindern.

# Einkaufen im Internet

## Wie erkenne ich seriöse Onlineshops?

Die Vielfalt der Produkte und Dienstleistungsangebote im Internet bietet den Konsumenten und Konsumentinnen eine breite Auswahl- und Vergleichsmöglichkeit.

Den Angeboten von bekannten Unternehmen können Sie in der Regel auch im Internet vertrauen. Durch den E-Commerce-Boom treten aber auch viele neue und bisher unbekannte Unternehmen als Anbieter im Internet auf. Dabei ist es nicht immer einfach, die Seriosität

dieser Angebote zu beurteilen. In Österreich können sich vertrauenswürdige Onlineshops mit dem E-Commerce-Gütezeichen auszeichnen lassen. Am sichersten ist es außerdem, bei Anbietern oder Anbieterinnen einzukaufen, die zumindest über eine inländische Niederlassung verfügen. Bei Problemen mit Bestellungen im Ausland ist es oft schwer, die eigenen Rechte in Anspruch zu nehmen. Saferinternet.at hat unter [www.saferinternet.at](http://www.saferinternet.at) die wichtigsten Infos zum Einkauf im Ausland zusammengefasst.

Mit den folgenden zehn Tipps können Sie die Seriosität eines Onlineangebots bereits vor dem Kauf überprüfen:





## TIPPS

- 1** Der Anbieter oder die Anbieterin ist eindeutig durch Firmenname, Anschrift, Telefonnummer, E-Mail-Adresse, Nennung einer Kontaktperson und Firmenbuchnummer zu identifizieren.
- 2** Der Anbieter oder die Anbieterin stellt leicht zugängliche und transparente Vertragsbedingungen für das Onlineshopping bereit.
- 3** Die Leistungsmerkmale der angebotenen Produkte und die Garantiebedingungen sind genau und übersichtlich dargestellt.
- 4** Der Produktpreis enthält – einzeln aufgelistet – sämtliche Zusatzkosten für Lieferung, Verpackung, bestimmte Zahlungsformen etc.
- 5** Eine technisch sichere, für den Konsumenten nachvollziehbare Zahlungsmöglichkeit ist gewährleistet.
- 6** Jede Bestellung wird vom Anbieter oder der Anbieterin nochmals per E-Mail bestätigt.
- 7** Ein Rücktritts- und Rückgaberecht wird dem Konsumenten oder der Konsumentin ausdrücklich zugestanden und die Bedingungen dafür werden genau erläutert.
- 8** Die voraussichtliche Lieferzeit ist exakt angegeben.
- 9** Der Anbieter oder die Anbieterin verpflichtet sich, keine Daten des Kunden an Dritte weiterzugeben.
- 10** Angebote, Produktbeschreibungen und Support erfolgen durchgängig in der jeweiligen Landessprache des Anbieters oder der Anbieterin bzw. in der Sprache, in der die Bestellung abgewickelt wird.

In Österreich können sich vertrauenswürdige Onlineshops mit dem E-Commerce-Gütezeichen auszeichnen lassen. Am sichersten ist es außerdem, bei Anbietern oder Anbieterinnen einzukaufen, die zumindest über eine inländische Niederlassung verfügen. Bei Problemen mit Bestellungen im Ausland ist es oft schwer, die eigenen Rechte in Anspruch zu nehmen. Saferinternet.at hat unter <http://saferinternet.at/themen/online-shopping/> die wichtigsten Infos zum Einkaufen im Ausland zusammengefasst.

## Internetbetrug und „Gratis“-Angebote im Internet.

Mit vermeintlich kostenlosen „Gratis“-Angeboten locken heute viele Internetseiten. Von „Gratis“-SMS über Hausübungshilfen bis hin zu Lebenserwartungsprognosen und IQ-Tests ist praktisch alles scheinbar gratis im Internet zu finden. Das System dahinter ist meist gleich: Es reicht eine einfache Registrierung mit Angabe von ein paar persönlichen Daten. Einige Tage nach der Registrierung folgt eine Rechnung oder gar eine Mahnung. Daher ist es wichtig, die Allgemeinen Geschäftsbedingungen (AGB) oder die Nutzungsbedingungen zu lesen, die meist versteckt auf ein kostspieliges Abo hinweisen.

## Zahlungsmöglichkeiten im Internet.

Auch im Internet kommen die herkömmlichen Bezahlungssysteme zur Anwendung: Überweisungen, Lastschriftabbuchungen, Zahlung mit Kreditkarte, mit dem Handy oder per Nachnahme. Vermeiden Sie generell die Bezahlung durch Vorkasse, also Bezahlung der Ware vor dem Erhalt.



### TIPP

Detaillierte Informationen zur sicheren Bezahlung im Internet finden Sie auf den Seiten von <http://saferinternet.at/themen/online-shopping/>

## Rückgaberecht bei Onlinebestellungen.

Beim Onlineshopping können Sie innerhalb von sieben Werktagen vom Vertrag zurücktreten. Die Frist für einen Rücktritt kann sich verlängern, wenn der Händler oder die Händlerin den Informationspflichten nicht nachkommt. Wichtig ist, den Zeitpunkt des Rücktritts zu dokumentieren (z. B. per eingeschriebenem Brief oder Fax).



**Achtung:** Es gibt aber auch Ausnahmen beim Rücktrittsrecht.



### TIPPS

Seien Sie bei „Gratis“-Angeboten und Gewinnspielen stets misstrauisch. Auch im Internet ist selten etwas wirklich „gratis“. Oft handelt es sich um Lockangebote, bei denen später laufende Kosten entstehen.

Lesen Sie die Allgemeinen Geschäftsbedingungen (AGB) des Anbieters immer genau, bevor Sie diese bestätigen! Oft verstecken sich darin Verpflichtungen wie jene, ein kostenpflichtiges Abo zu erwerben. Achten Sie speziell auf die angegebenen Fristen und eventuell entstehende Kosten.

Stornieren Sie Testzugänge sofort wieder, wenn Sie diese nicht brauchen bzw. geben Sie zum unverbindlichen Testen von Onlinediensten niemals Ihre persönlichen Daten an.

Stornieren Sie unerwünscht bzw. versehentlich eingegangene Verträge (bzw. kostenpflichtige Anmeldungen) immer per Post mit einem eingeschriebenen Brief und behalten Sie eine Kopie des Schreibens.

Wenn Sie trotz aller Vorsicht auf ein derartiges Angebot eingegangen sind oder Ihre Kündigung nicht akzeptiert wird, wenden Sie sich sofort an eine Konsumentenschutzorganisation (z. B. Internet Ombudsmann, Arbeiterkammer, Verein für Konsumenteninformation).

Das Bundesministerium für Soziales und Konsumentenschutz [www.bmsk.gv.at](http://www.bmsk.gv.at) bietet Ihnen einen Informationsfolder zum Thema „Internet Abzocke- „Gratis“-Angebote im Internet“.



## Versteigerungen im Internet.

Auktionssysteme wie eBay, OneTwoSold und andere haben sich als beliebte Plattformen zum Ein- und Verkaufen im Internet etabliert. Für eine sichere Teilnahme an Onlineauktionen sollten Sie Folgendes beachten:

- Vorkasse vermeiden: Wenn Ihr Vertragspartner oder Ihre Vertragspartnerin bereits kassiert hat, aber nicht liefert, haben Sie Schwierigkeiten, Ihr Geld zurückzubekommen. Einige Versteigerungsplattformen lösen dieses Problem, indem sie unter bestimmten Bedingungen bis zu einem gewissen Betrag einspringen (Käuferschutzprogramme). Außerdem werden Treuhandsysteme angeboten, die Sie besonders bei größeren Beträgen in Anspruch nehmen sollten.
- Bevor Sie sich zum Mitbieten entscheiden, sollten Sie die Artikelbeschreibung genau durchlesen. Achten Sie besonders auf den Artikelzustand, Versandkosten und Rückgabemöglichkeiten. Gewerbliche Anbieter und Anbieterinnen sind gesetzlich verpflichtet, über das Internet gekaufte Produkte innerhalb von sieben Werktagen zurückzunehmen. Das Rücktrittsrecht ist aber ausgeschlossen, wenn Sie Produkte von Privatpersonen ersteigern.
- Falls Sie bei einem Angebot noch Fragen haben, kontaktieren Sie den Verkäufer oder die Verkäuferin

rechtzeitig vor Ablauf der Auktion. Ein gewissenhafter Verkäufer oder eine gewissenhafte Verkäuferin wird Ihre Fragen gerne beantworten.

- Informieren Sie sich über Ihren zukünftigen Vertragspartner (z.B. mit Hilfe des Bewertungssystems).

**Beratung bei Onlineshopping-Problemen** bieten Ihnen die folgenden Stellen:

- Internet Ombudsmann, [www.ombudsmann.at](http://www.ombudsmann.at), bietet kostenlose Hilfe und Streitschlichtung bei Problemen mit dem Einkaufen im Internet
- Verein für Konsumenteninformation, [www.vki.at](http://www.vki.at)
- Arbeiterkammer, [www.arbeiterkammer.at](http://www.arbeiterkammer.at)



### TIPP

Das Bundesministerium für Soziales und Konsumentenschutz, [www.bmsk.gv.at](http://www.bmsk.gv.at), bietet Ihnen dazu die Informationsbroschüre „Sicher einkaufen im Internet“.

Weitere Informationen zum Thema „Online Shopping“ finden Sie auf den Seiten von <http://saferinternet.at/themen/online-shopping/>

# Spam

## Was ist Spam?

Viele Internetnutzer und Internetnutzerinnen klagen über unerwünscht zugesendete E-Mails, die meist massenhaft verschickt werden und oft Werbung, aber auch Computerviren oder Betrugsabsichten zum Inhalt haben.

In Österreich ist die Zusendung elektronischer Post, einschließlich SMS, verboten, wenn die Zusendung ohne vorherige Einwilligung zu Zwecken der Werbung erfolgt oder an mehr als 50 Empfänger gerichtet ist (auch ohne Werbung).



### TIPP

Auf den Seiten der Rundfunk und Telekom Regulierungs-GmbH, [www.rtr.at](http://www.rtr.at), finden Sie den Folder „Informationen betreffend unerwünschte Werbung mittels elektronischer Post (Spam)“ sowie eine Anleitung zur Eintragung in die E-Commerce-Gesetz-Liste.

Eine vorherige Zustimmung ist allerdings nicht erforderlich, wenn folgende Voraussetzungen gleichzeitig vorliegen:

1. Der Versender oder die Versenderin hat die Kontaktinformationen anlässlich eines Kaufes bzw. einer Dienstleistung vom Kunden oder der Kundin erhalten.
2. Der Versender oder die Versenderin verwendet diese Daten nur für Werbung für ähnliche Produkte und Dienstleistungen.
3. Der Empfänger oder die Empfängerin erhält die Möglichkeit, die Zusendung bereits bei der Erhebung der Daten oder anlässlich jeder weiteren Zusendung abzulehnen.
4. Der Empfänger oder die Empfängerin hat die Zusendung nicht von vornherein durch Eintragung in die sogenannte E-Commerce-Gesetz-Liste bei der Rundfunk- und Telekom Regulierungs-GmbH abgelehnt.

## Was kann ich gegen Spam tun?

Einen vollständigen Schutz gegen Spam gibt es nicht. Allerdings gibt es Werkzeuge, sogenannte Spamfilter, die eine gute Hilfe gegen Spams sind.

Spamfilter können im eigenen E-Mail-Programm und/oder beim Internetprovider aktiviert werden. Zusätzlich ist es empfehlenswert, einige vorbeugende Maßnahmen zu treffen:

1. Richten Sie eine zweite E-Mail-Adresse bei einem kostenlosen Anbieter ein, die Sie für die Weitergabe an unbekannte Personen verwenden. Wenn Sie über die zusätzliche Adresse zu viele Spam E-Mails erhalten, dann löschen Sie diese einfach und registrieren eine neue.



2. Spam-Versender verwenden oft Programme, die automatisiert nach E-Mail-Adressen im Internet suchen. Sie können das verhindern, indem Sie E-Mail-Adressen auf Ihrer Website für solche Suchprogramme verbergen. Fragen Sie Ihren Website-Administrator!

## Wie kann ich gegen Spam vorbeugen?

Gehen Sie vorsichtig mit Ihrer E-Mail-Adresse um und veröffentlichen Sie diese nur, wenn es notwendig ist. Es ist ratsam, sich bei kostenlosen E-Mail-Providern eine zusätzliche E-Mail-Adresse anzulegen. Ihre „private“ Adresse verwenden Sie nur für Freunde oder Freundinnen, Verwandte und Kollegen oder Kolleginnen. Ihre Zweitadresse können Sie dann beispielsweise für Einträge in Foren und Gästebüchern oder das Registrieren auf Websites benutzen. Wenn Sie dann über die zweite Adresse zu viele Spam-E-Mails erhalten, löschen Sie diese Adresse einfach bzw. lassen sie auslaufen und registrieren eine neue Adresse.

Antworten Sie nie auf Spam-E-Mails, auch nicht, um sich zu beschweren. Damit bestätigen Sie Spamversendern lediglich, dass Ihre E-Mail-Adresse tatsächlich aktiv ist und würden nur noch mehr solcher Zusendungen bekommen.



### TIPP

Praktische Informationen zum Thema „Spam“ finden Sie auf den Seiten von <http://saferinternet.at/themen/spam/>

# Illegale Inhalte im Internet

## Was sind illegale Inhalte?

In Österreich ist der Besitz kinderpornografischer Darstellungen und die Verbreitung nationalsozialistischer Inhalte gesetzlich verboten und daher strafbar. Besitz liegt dann vor, wenn eine solche Darstellung auf dem eigenen Computer gespeichert wird.

Die gesetzliche Grundlage zum Thema „Kinderpornografie“ ist im österreichischen Strafgesetzbuch festgehalten. Kinderpornografie ist die bildliche Darstellung von geschlechtlichen Handlungen, in die Minderjährige involviert sind. Als minderjährige Person gilt, wer das 18. Lebensjahr noch nicht vollendet hat.

In der Regel werden die Inhalte einer Seite schon beim bloßen Ansehen im Internet automatisch auf der Festplatte gespeichert (meist in einem Ordner für temporäre Dateien) – bereits das kann als Besitz eines Bildes gelten.

## Wo kann ich illegale Inhalte melden?

Melden Sie kinderpornografische und nationalsozialistische Inhalte

- online – auch anonym – bei der Meldestelle „Stopline“, [www.stopline.at](http://www.stopline.at),
- online mit Bürgerkarte unter Verwendung der Formulare „Kinderpornografie – Meldung“ bzw. „Wiederbetätigung – Meldung“ oder
- schriftlich, per Fax oder E-Mail bei den Meldestellen der Kriminalpolizei.



## Wie kann ich Kinder vor illegalen Inhalten schützen?

Sie können, gerade bei jüngeren Kindern, technische Hilfsmittel verwenden (z.B. Filterprogramme).

Eine Übersicht derartiger Programme finden Sie auf der Internetsite von <http://saferinternet.at/themen/unerwunschte-inhalte/>

Je älter Kinder werden, desto weniger stellen Filterprogramme einen verlässlichen Schutz dar, weil sie mit guten Computerkenntnissen unter Umständen umgangen werden können. Daher ist es empfehlenswert, Kinder gerade bei ihren ersten Entdeckungsreisen ins Internet zu begleiten und sich für ihre Onlineaktivitäten zu interessieren.

Gemeinsame Erfahrungen beim Internetsurfen erleichtern es in Zukunft, positive und negative Erfahrungen bei der Internetnutzung zu teilen. Damit können Sie Ihre Kinder bei der Internetnutzung gezielt anleiten.



**Achtung:** Eine hundertprozentige Garantie für einen Schutz vor illegalen Inhalten gibt es im Internet nicht, genauso wenig wie im „richtigen“ Leben. Aber mit einer Mischung verschiedener Maßnahmen können Sie problematische Interneterlebnisse Ihrer Kinder minimieren.

Vergessen Sie dabei nicht: Das Internet bietet großartige Möglichkeiten, ist aber gleichzeitig mit Risiken verbunden. Auf das Internet zu verzichten oder die Nutzung radikal einzuschränken, kann dabei keine Lösung sein. Daher ist es wichtig, Kinder auch aktiv auf die Risiken vorzubereiten und nicht zu kritisch bei ihren Entdeckungsreisen zu sein.



### TIPP

Weitere Informationen zum Thema „Unerwünschte Inhalte“ finden Sie auf den Seiten von <http://saferinternet.at/themen/unerwunschte-inhalte/>

# ☰ Schutz der persönlichen Daten

## Was kann mit meinen Daten passieren, die ich im Internet bekannt gebe?

E-Mail-Adressen und andere Kontaktdaten können gesammelt und illegal für Werbung oder Betrug verwendet werden. Unerwünschte und unerlaubte Zusendungen per E-Mail (z.B. Spam) sind dann die Folge.

Vergessen Sie nie, dass das Internet weltweiten Zugriff auf Informationen bietet und dass Sie – sobald Sie Informationen veröffentlicht haben – keine Kontrolle mehr über deren Weiterverwendung haben. Machen Sie sich bewusst, dass personenbezogene Angaben (Kontaktdaten, Partyfotos etc.) in ganz anderen, unerwünschten Zusammenhängen wieder auftauchen können.

Das gilt in besonderem Maße für Kinder. Diese sind oft leichtfertig bei der Veröffentlichung von Daten und es besteht die Gefahr, dass Erwachsene mit schlechten Absichten auf diese Weise Namen und Wohnort von Kindern ausfindig machen. Das ist durch die Verknüpfung von Angaben auf der eigenen Homepage, E-Mail-Adresse und dem elektronischen Telefonbuch leicht möglich.



### TIPP

Weitere Tipps zum sicheren Umgang mit Passwörtern finden Sie auf den Seiten von <http://saferinternet.at/themen/datenschutz/>

## Was kann ich tun, um meine Daten im Internet zu schützen?

- Wichtigste Regel: Falls nicht unbedingt notwendig, geben Sie keine personenbezogenen Daten (z.B. Name, Anschrift, Geburtsdatum, Alter, Telefonnummer) im Internet bekannt.
- Legen Sie sich bei einem Gratisanbieter eine E-Mail-Adresse zu, die keinen Rückschluss auf Ihren richtigen Namen zulässt. Verwenden Sie diese Adresse, um sich auf Websites zu registrieren, Beiträge in Gästebüchern zu verfassen oder in Foren mitzudiskutieren.
- Überprüfen Sie Ihre Homepage, ob sie Angaben über Sie enthält, die Sie eigentlich nicht öffentlich bekannt geben wollen. Ihre Website ist weltweit frei zugänglich und über Suchmaschinen einfach zu finden.
- Verwenden Sie sichere Passwörter, die aus mindestens acht Buchstaben, Zahlen und Sonderzeichen bestehen und keinen Bezug zu Ihnen aufweisen. Halten Sie Ihr Passwort geheim und teilen Sie es anderen nicht mit. Wenn Sie den Eindruck haben, dass eine unbefugte Person Ihr Passwort herausgefunden hat, sollten Sie sofort Ihr Passwort ändern.



## Was ist zu beachten, wenn ich persönliche Daten bekannt geben muss?

Oft ist es notwendig, persönliche Daten im Internet bekannt zu geben (z. B. beim Onlineshopping). Daher ist es wichtig zu wissen, ob Onlineanbieter seriös agieren und personenbezogene Daten wirklich nur auf Wunsch der Konsumenten und Konsumentinnen weitergeben.

Achten Sie darauf, dass sich der Anbieter auf seiner Website dazu verpflichtet, grundsätzlich keine Kundendaten an Dritte weiterzugeben.



### TIPP

Seriöse Shops erkennen Sie in Österreich beispielsweise am E-Commerce Gütezeichen, [www.guetezeichen.at](http://www.guetezeichen.at)

## Was kann ich tun, wenn ich ein unerwünschtes Foto von mir im Internet finde?

Ersuchen Sie zunächst den Websitebetreiber, das Foto zu entfernen. Falls dieser diesem Wunsch nicht nachkommt, müssen für das weitere Vorgehen die folgenden Fälle unterschieden werden:

- Foto, das jemand anderer gemacht hat: Vorausgesetzt, dass die Veröffentlichung gegen berechnete Interessen Ihrerseits verstößt, haben Sie einen Unterlassungsanspruch.
- Foto, das Sie selbst gemacht haben (mit beliebigem Motiv): In diesem Fall haben Sie einen unbedingten Unterlassungsanspruch und außerdem alle weiteren Ansprüche nach dem Urheberrechtsgesetz, insbesondere auch einen Schadenersatzanspruch.

In beiden Fällen ist die Beauftragung eines Rechtsanwalts oder einer Rechtsanwältin zur Einbringung einer Klage nach dem Urheberrechtsgesetz notwendig. Manchmal hilft aber auch bereits ein Schreiben Ihres Anwalts oder Ihrer Anwältin. Für Streitigkeiten nach dem Urheberrecht ist das Landesgericht zuständig (unabhängig vom Streitwert).



### TIPP

Weitere Informationen zum Thema „Datenschutz“ finden Sie auf den Seiten von <http://saferinternet.at/themen/datenschutz/>

# Urheberrechte im Internet (Tauschbörsen)

## Was ist das Urheberrecht?

Das Urheberrecht besagt, dass der Urheber oder die Urheberin das alleinige Recht hat, sein oder ihr Werk öffentlich zugänglich zu machen, zu vervielfältigen, zu verbreiten, zu senden, zu verleihen und aufzuführen. Bei Tauschbörsen und Websites sind vor allem zwei Rechte berührt: Einerseits wird das Werk meist anderen öffentlich zugänglich gemacht, andererseits durch die lokale Abspeicherung von Kopien vervielfältigt.

## Darf ich Musik oder Videos aus dem Internet downloaden (herunterladen)?

Ob der reine Download von Musik aus dem Internet (also ohne das Musikstück selbst wieder anbieten zu wollen) erlaubt ist, ist unter Juristen und Juristinnen umstritten. Die einen sehen darin eine erlaubte Vervielfältigung zum eigenen Gebrauch, die anderen meinen, auch diese Vervielfältigung zum Eigengebrauch sei

nicht erlaubt, wenn bereits die Vorlage selbst unrechtmäßig hergestellt wurde. Eine eindeutige Antwort auf diese Frage ist leider derzeit nicht möglich. Auf der sicheren Seite sind Sie jedenfalls, wenn Sie es nicht tun.

## Darf ich Musik oder Videos zum Download anbieten?

Tauschbörsenprogramme sind meistens so eingestellt, dass die Ordner, in welche die Dateien heruntergeladen werden, gleichzeitig auch zum Upload freigegeben sind. Die Programme können in den meisten Fällen zwar so eingestellt werden, dass die Uploads verhindert werden, aber dies hat zur Folge, dass Sie bei den Downloads benachteiligt werden.

Es werden – im Sinne des Tauschgedankens – meist jene Nutzer und Nutzerinnen bevorzugt, die auch selbst Dateien zur Verfügung stellen.



Der entscheidende Punkt ist jedoch, dass das Anbieten von Musikstücken oder Videos in Tauschbörsen ohne die Zustimmung des Urhebers oder der Urheberin nicht erlaubt ist.

### Können Tauschbörsenbenutzer oder -benutzerinnen überhaupt erwischt werden?

Ja, und zwar über die IP-Adresse Ihres Computers und den Zeitpunkt, wann sie mit dem Programm online waren.



#### TIPP

Nutzen Sie keine Tauschbörsen zum Download von Musik oder Filmen, Sie könnten damit das Urheberrecht verletzen!  
Weitere Informationen zum Thema „Tauschbörsen“ finden Sie auf den Seiten von <http://saferinternet.at/themen/tauschboersen/>

# Phishing

## Was ist Phishing?

Der Begriff „Phishing“ ist eine Wortkombination aus „Passwort“ und „Fishing“. Phishing bezeichnet den Versuch, Internetnutzern und Internetnutzerinnen Geheimdaten (z.B. für Onlinebanking, Auktionsplattformen oder Onlineshops) zu entlocken.

Sie erhalten dabei in der Regel eine E-Mail, in der Sie unter einem Vorwand aufgefordert werden, beispielsweise die Homepage Ihrer Bank aufzusuchen und dort die Kontodaten einzugeben. In der E-Mail ist meist eine Internetadresse angegeben. Wird diese angeklickt, gelangen Sie auf eine Seite, die der tatsächlichen Bankseite täuschend ähnlich sieht, aber in Wahrheit von Betrügern betrieben wird.

Die Betrüger hoffen darauf, dass Sie die Bankdaten dort eingeben, damit diese Zugang zu Ihren Konten erhalten und illegale Zahlungen von diesen veranlassen können. Die betrügerische Website verschwindet in der Regel nach wenigen Stunden oder Tagen wieder, jedoch können vorher auf diese Weise große finanzielle Schäden angerichtet werden.

## Wie sind Phishing-E-Mails zu erkennen?



**Die wichtigste Regel:** Seriöse Unternehmen werden niemals von Ihnen per E-Mail die Bekanntgabe vertraulicher Daten wie Passwörter oder Transaktionsnummern verlangen!



### TIPP

Um Ihre Onlinebanking-Aktivitäten sicher durchzuführen, können Sie auch zusätzlich die Bürgerkarte verwenden. Falls Sie doch Phishingopfer wurden, sollten Sie sofort Ihre Bank kontaktieren, um Ihr Konto sperren zu lassen.

Weitere Informationen zum Thema „Phishing“ finden Sie auf <http://saferinternet.at/themen/datenschutz/>

## Weitere Hinweise auf Phishing-E-Mails:

- Phishing-E-Mails enthalten oft Drohungen oder betonen die Dringlichkeit der von Ihnen geforderten Dateneingabe. Oft wird auf angebliche Sicherheitslücken auf den Seiten der Bank hingewiesen, die eine Eingabe Ihrer Zugangsdaten „zur Überprüfung“ erforderlich machen.
- Die in den Phishing-E-Mails angegebenen Internetadressen weichen von den tatsächlichen Internetadressen der betroffenen Unternehmen ab (z.B. [www.nelbanking.at](http://www.nelbanking.at) statt [www.netbanking.at](http://www.netbanking.at)).
- Die E-Mails sind oft in schlechtem Deutsch verfasst.
- Die Internetadresse wird beim Aufrufen der Seite ausgeblendet.
- Es sind überraschende Änderungen im Aussehen der vertrauten Login-Seite oder fehlerhafte Links zu erkennen.

## Schutzmaßnahmen zur Verhinderung von Phishing

- Bedenken Sie, dass seriöse Unternehmen Sie niemals per E-Mail auffordern werden, Ihre persönlichen Daten wie Passwörter oder Transaktionsnummern bekannt zu geben.
- Antworten Sie niemals auf Phishing-E-Mails, sondern leiten Sie diese an das betroffene Unternehmen weiter oder löschen Sie diese sofort.
- Geben Sie vertrauliche Daten ausschließlich über SSL-verschlüsselte Seiten bekannt (erkennbar am „https://“ in der Adresszeile und am geschlossenen Vorhangschloss am unteren Rand Ihres Internet-Browsers).
- Führen Sie regelmäßig Sicherheitsupdates des von Ihnen verwendeten Internet-Browsers durch.



# Computer- und Onlinespiele

## Empfohlene Spiele für Kinder und Jugendliche

Empfohlene Spiele für Kinder und Jugendliche finden Sie in der Spieledatenbank der Bundesstelle für Positivprädikatisierung von Computer- und Konsolenspielen (BuPP), [www.bupp.at](http://www.bupp.at). In einem eigenen Bereich finden Sie empfehlenswerte kostenlose Spiele zum Herunterladen.

Weitere Informationen bietet Ihnen auch der Informationsfolder „Tipps und Tricks für erfolgreiches Zocken am PC und an der Konsole“.

## Prädikatisierung und Alterskennzeichnung

Die Bundesstelle für Positivprädikatisierung von Computer- und Konsolenspielen (BuPP) des Bundesministeriums für Gesundheit, Familie und Jugend bietet Eltern und anderen Interessierten eine Entscheidungshilfe zum Kauf „guter Computerspiele“.

PEGI (Pan European Game Information) ist das erste europaweite Alterseinstufungssystem für Computer- und Videospiele. Es gibt Eltern und Konsumenten oder Konsumentinnen die Sicherheit, dass der Inhalt eines bestimmten Spiels für eine spezifische Altersgruppe geeignet ist. PEGI Online ist die Erweiterung für On-

linespiele.

USK (Unterhaltungssoftware Selbstkontrolle) ist das deutsche Alterskennzeichnungssystem für Computerspiele.



**Achtung:** Die beiden Kennzeichnungen PEGI und USK sagen nichts über sonstige Qualitäten des Spiels aus und auch nicht, ab welchem Alter das Spiel vom Schwierigkeitsgrad her passend ist. In Österreich ist eine Kennzeichnung mit PEGI oder USK derzeit noch nicht verbindlich vorgeschrieben.

Hier finden Sie weitere Informationen zum Thema „Kennzeichnung mit PEGI und USK“.

## Computerspielsucht

Beratungsangebot für Betroffene:

- Therapiezentrum Anton-Proksch-Institut Wien



### TIPP

Weitere Informationen zum Thema „Computer- und Onlinespiele“ finden Sie auf den Seiten von <http://saferinternet.at/themen/online-spiele/>



# ■ Belästigung im Internet („Cyber-Stalking“)

## Gesetzliche Lage

In Österreich ist am 1. Juli 2006 das sogenannte „Anti-Stalking-Gesetz“ (§ 107a Strafgesetzbuch, Tatbestand der „beharrlichen Verfolgung“) in Kraft getreten, das Opfer von Belästigungen besser schützt. Von „Stalking“ wird gesprochen, wenn folgende Vorgehensweisen eines Täters oder einer Täterin das Opfer unzumutbar beeinträchtigen und das Verhalten über längere Zeit hindurch fortgesetzt wird:

Der Stalker oder die Stalkerin

- sucht die räumliche Nähe des Opfers,
- stellt mithilfe von Telekommunikation oder durch sonstige Kommunikationsmittel oder durch Dritte den Kontakt zum Opfer her,

- bestellt unter Verwendung der persönlichen Daten des Opfers Waren oder Dienstleistungen in dessen Namen,
- bewegt unter Verwendung der persönlichen Daten des Opfers Dritte dazu, mit dem Opfer Kontakt aufzunehmen.

Die möglichen Maßnahmen gegen Stalker oder Stalkerinnen reichen von Wegweisung über Betretungsverbote bis hin zur Festnahme.

## Maßnahmen gegen Belästigung im Internet

Folgende Maßnahmen sind empfehlenswert:

- Lassen Sie sich von einer Anti-Stalking-Beratungsstelle über die weitere Vorgehensweise in Ihrer spezifischen Situation beraten.
- Sichern Sie die Beweise (z.B. SMS, E-Mails, Briefe).
- Weisen Sie zur Abschreckung den Täter oder die Täterin darauf hin, dass er oder sie möglicherweise eine strafbare Handlung setzt.
- Prävention: Seien Sie vorsichtig bei der Weitergabe von persönlichen Daten wie E-Mail-Adresse, Handynummer, Fotos etc.
- Reagieren Sie nicht mit einem Handy- oder Internetverbot. Internet und Handy spielen, auch wenn sie für Belästigungen missbraucht werden können, für die Betroffenen meist noch immer eine wichtige Rolle in der Freizeit und Schule. Wenn Kinder Opfer von Schikanen werden, ist eine Bestrafung nicht sinnvoll.
- Versuchen Sie den Täter oder die Täterin zu identifizieren.
- Kontaktieren Sie die Eltern des Täters oder der Täterin und/oder die Schule.
- Bei gefährlichen Drohungen kontaktieren Sie die Polizei.

Wenn Ihr Kind Opfer von „Cyber-Stalking“ geworden ist, sollten Sie Folgendes tun:

- Sprechen Sie mit Ihrem Kind und betonen Sie, dass es jederzeit mit Ihnen über Probleme reden kann. Belästigungen können zu einem großen Leidensdruck führen, besonders wenn Kinder mit niemandem darüber sprechen können.
- Informieren Sie sich über die Internet- und Handynutzungsgewohnheiten Ihres Kindes.
- Seien Sie sensibel für mögliche Verstörungen Ihres Kindes, gerade im Zusammenhang mit den Handy- und Internetaktivitäten Ihres Kindes.
- Geben Sie Ihrem Kind konkrete Tipps, wie es sich im Falle von Belästigungen verhalten kann (z.B. nicht antworten, Beweise sichern, nur moderierte, d.h. von einem Diskussionsleiter beaufsichtigte, Chats verwenden).



### TIPP

Weitere Informationen zum Thema „Cyber-Stalking“ finden Sie auf <http://saferinternet.at/themen/belaestigung/>



# Kinder vor ungeeigneten Inhalten schützen

## Gesetzliche Regelung des Jugendschutzes

Der Jugendschutz ist in Österreich durch die Jugendschutzgesetze der Bundesländer sowie durch das Pornographiegesetz geregelt. Das Bundesministerium für Gesundheit, Familie und Jugend, [www.bmgfj.gv.at](http://www.bmgfj.gv.at), hat die relevanten Auszüge der Jugendschutzgesetze der Länder für Sie zusammengefasst.

Daher ist es entscheidend, Themen wie Pornographie, Gewalt, Rechtsradikalismus etc. generell zu thematisieren und eine entsprechende Sensibilisierung und Reflexion zu fördern.

## Wie kann ich Kinder vor ungeeigneten Inhalten schützen?

Beginnen Sie schon mit Ihren Jüngsten, Regeln zur Internetnutzung zu vereinbaren, sich gemeinsam im Internet zu bewegen und sich ihre Lieblingsseiten zeigen zu lassen. Gemeinsame Erfahrungen beim Internetsurfen erleichtern es auch in Zukunft, positive und negative Onlineerlebnisse zu teilen. Und es ermöglicht Ihnen, Ihre Kinder bei der Internetnutzung gezielt anzuleiten. Vergessen Sie beim Festlegen von Regeln für Onlineaktivitäten in Ihrer Familie oder in der Schule nicht, dass Regeln nur wirksam sind, wenn Kinder und Jugendliche die Regeln verstehen und ihre Berechtigung akzeptieren.

Sie können, gerade bei jüngeren Kindern, technische Hilfsmittel verwenden (z.B. Filterprogramme). Je älter Kinder werden, desto weniger stellen diese Filterprogramme einen verlässlichen Schutz dar. Denn Jugendliche können diese umgehen oder an anderen Orten (z.B. bei Freunden oder Freundinnen oder in Internet-Cafés) das Internet nutzen.





Eine hundertprozentige Garantie für einen Schutz vor ungeeigneten Inhalten gibt es im Internet nicht, genauso wenig wie im „richtigen“ Leben. Aber mit einer Mischung verschiedener Maßnahmen können Sie die Risiken problematischer Interneterlebnisse minimieren.

Vergessen Sie dabei nie: Das Internet bietet großartige Möglichkeiten und eine kompetente Nutzung ist für Schule, Freizeit und Beruf eine unerlässliche Fähigkeit. Auf das Internet zu verzichten oder die Nutzung radikal einzuschränken kann daher keine Lösung sein. Daher ist es wichtig, Kinder aktiv auf die möglichen Risiken vorzubereiten.

## Wie kann ich Filterprogramme auf meinem Computer nutzen?

Links zu kostenlosen und kostenpflichtigen Filterprogrammen sowie technische Informationen finden Sie auf <http://saferinternet.at/themen/unerwueschte-inhalte/>

Dort finden Sie auch Hinweise zu Jugendschutzeinstellungen, die in Betriebssystemen und Internetbrowsern zu finden sind.

# Medienerziehung für Eltern

## TIPPS

- 1 Es ist wichtig, sich über die Onlineaktivitäten der Kinder zu informieren und – gerade am Anfang – gemeinsame Onlineerfahrungen zu machen. Eltern, denen die Internetvorlieben ihrer Kinder egal sind, können ihren Kindern dabei nicht genug Orientierungshilfen geben.
- 2 Leben Sie einen Umgang mit dem Internet vor, den Sie auch von Ihrem Kind erwarten.
- 3 Eltern sollten Grundkenntnisse über das Internet und dessen Risiken haben. Erwachsene, die nur verbieten oder das Internet bloß kritisieren, ohne selbst eine Ahnung davon zu haben, werden nicht ernst genommen.
- 4 Es ist aber auch nicht schlimm, wenn Erwachsene dabei einmal Erklärungen der Kinder benötigen. Gerade so kann es gelingen, eine gute Gesprächsbasis zu schaffen, die auch im Fall von Problemen hilfreich ist.
- 5 Regeln aufstellen, die Kinder auch verstehen und deren Sinnhaftigkeit sie anerkennen.
- 6 Kinder können im Internet auf unerwünschte Inhalte stoßen (z.B. Gewalt, Rassismus, Pornographie). Dies kann zu Irritationen führen. Kindern hilft es sehr, wenn Erwachsene mit ihnen darüber sprechen und auch ihre eigenen Gefühle dazu offenbaren.
- 7 Enttäuschungen und Frustrationen sind als normaler Bestandteil von Entdeckungsreisen anzusehen.
- 8 Achten Sie auf Alarmsignale (z. B. wenn sich keine Freunde und Freundinnen mehr melden oder Onlinebekanntschaften „richtige“ Freunde und Freundinnen zu ersetzen beginnen).
- 9 Gerade bei den Jüngsten können technische Maßnahmen wie Filterprogramme eine sinnvolle Ergänzung sein. Aber sie bieten keinen hundertprozentigen Schutz, da sie mit entsprechenden Computerkenntnissen umgangen werden können.

## TIPP

Informationen zum Thema bietet auch die Saferinternet.at Broschüre „Kein Stress mit Web und SMS – Fakten und Tipps für Eltern und Erziehungsberechtigte zum Umgang mit Internet und Handy“.

Nach Altersgruppen geordnete Tipps zur Medienerziehung sowie weitere Tipps für Eltern finden Sie auf den Seiten von <http://saferinternet.at/themen/medienerziehung/>

**Saferinternet.at**

Das Internet sicher nutzen!

c/o Österreichisches Institut für angewandte Telekommunikation (ÖIAT)

Margaretenstr. 70/2/10 1050 Wien

Tel.: +43 1 595 21 12-51

Fax: +43 1 595 21 12-99

Mail: [office@saferinternet.at](mailto:office@saferinternet.at)