So schütze ich mein Ich im Internet

Online verraten Menschen Dinge, die sie im richtigen Leben nie erzählen würden. Hier sagt BILD, wie Sie Ihre Privatsphäre schützen, wenn Sie durchs Web surfen. Wer diese **77 TIPPS** beherzigt, kann in sozialen Netzen sein Herz ausschütten, ohne sich dabei bloßzustellen

Von CORDULA POSDORF und MARTIN EISENLAUER

Internet-Kriminalität ist ein Milliarden-Geschäft: Laut aktueller Schätzungen erwirtschaften Hacker, Spammer und Datendiebe im Web mehr Umsatz als Hollywood und der internationale Drogenhandel zusammen. Der Anwender ist dieser Industrie allzu oft schutzlos ausgeliefert. „Internet-Kriminalität ist ein Profigeschäft. Die Täter handeln nach streng ökonomischen Gesichtspunkten und entwickeln so ständig neue Strategien, mit denen sie ahnungslose Internet-Nutzer immer wieder erfolgreich in die Falle locken“, weiß Ralf Benzmüller, Leiter der Sicherheitslabors beim Anti-Viren-Anbieter G-Data.

Doch wie erkennen Internetsurfer, wo ihre Daten sicher sind und wann sie besser aufpassen müssen? Wie wehren sie sich gegen Spam, Phishing und Identitätsdiebstahl? BILD am SONNTAG beantwortet mit Unterstützung des Bundesamts für Sicherheit in der Informationstechnik (BSI) die wichtigsten Fragen zur Datensicherheit und gibt Ihnen 77 Tipps für sicheres Surfen.

Worauf müssen Anwender achten, damit sie nicht Opfer von Cyberkriminellen werden?

„Wichtig ist immer die Mischung aus technischen Maßnahmen und dem umsichtigen Verhalten des Nutzers“, sagt Nora Basting vom BSI. Zu den wichtigsten Schutzmaßnahmen am PC gehört neben einem Virenschutz und einer Firewall unbedingt die regelmäßige Aktualisierung aller verwendeten Programme. Denn häufig gelangt Schadsoftware über Sicherheitslücken auf den PC. Ebenso wichtig ist aber auch eine gesunde Skepsis bei der Nutzung des Internets. Nicht alle Angebote sind vertrauenswürdig und persönliche Daten sollten nicht für jeden zugänglich sein.

Ist die Bedrohung aus dem Internet wirklich real oder ist das nur Propaganda der Hersteller von Sicherheits-Software?

BITTE BLÄTTERN SIE UM

COMPUTER: Neun Tipps, die Sie schützen

93 Prozent der Computer werden von Antiviren-Programmen geschützt. Trotzdem wurden laut einer aktuellen Studie schon knapp die Hälfte der Rechner von Schädlingen befallen. Den besten Schutz bietet eine Kombination aus Wissen und guter Software. Auf diese Dinge sollten Sie achten, bevor Sie lossurfen:

Virenschutz installieren

Wirksamen Basis-Schutz bieten Gratis-Programme wie avast! Free Antivirus (www.avast.de). Gekaufte Programme wie Norton 360 5.0 (20 Euro) schützen umfangreicher, sie bieten etwa Backup-Programme und bessere Phishing-Filter. Bei Downloads aus dem Web sollten Sie Virenschutzsoftware nur beim Hersteller laden, um Fälschungen zu vermeiden.

Anti-Spyware installieren

Windows Vista und 7 werden mit dem Anti-Spyware-Programm Defender ausgeliefert. Für Windows XP muss man bei Microsoft gratis herunterladen. Alternativ kann auch Spyware-Schutz genutzt werden, der mit Anti-Viren-Paketen geliefert werden.

Firewall aktivieren

Die Firewall entscheidet, wie Programme auf das Internet zugreifen. Sie hilft damit, Viren und Trojaner abzuwehren. Windows wird mit einer einfachen Firewall ausgeliefert, die standardmäßig aktiviert ist. Sie sollte nur ausgeschaltet werden, wenn eine andere Firewall installiert wird. Versucht ein Programm, auf das Internet zuzugreifen, fragt die Firewall nach, ob der Zugriff gestattet werden soll. Lesen Sie die Frage sorgfältig und geben Sie nur Programmen Zugriffrechte, die Sie kennen.

Regelmäßig aktualisieren

Egal ob Windows, Office, Virenscanner oder Browser – alle Programme, sollten auf dem aktuellen Stand sein. Nur so ist sicher, dass alle Sicherheitslücken auf Ihrem System so schnell wie möglich geschlossen werden. Viele Programme bieten dafür eine automatische Update-Funktion an. Wenn Sie eine Internet-Flatrate haben, sollte das Auto-Update auf jeden Fall aktiv sein. Unter Windows 7 aktivieren Sie das Auto-Update unter „Start“, „Systemsteuerung“, „System und Sicherheit“ im Bereich „Windows Update“ mit einem Klick auf „Automatisches Update ein- oder ausschalten“. Bei allen anderen Programmen, speziell bei Plug-ins und Erweiterungen wie Java müssen Sie regelmäßig prüfen, ob sie auf dem neusten Stand sind.

Gute Passwörter wählen

Ein gutes Passwort sollte mindestens acht Zeichen lang sein und neben Buchstaben auch Zahlen und Sonderzeichen enthalten. Oft helfen Eselsbrücken dabei, sich das Passwort zu merken. Beispielsweise können Sie sich einen Satz ausdenken und nur die jeweils ersten Buchstaben jedes Wortes nutzen. So wird etwa aus „Ich nutze Facebook seit '10“ das einfach zu merkende und sichere Passwort „IchuFase'10“.

Nehmen Sie sich Zeit

Klicken Sie Fragen von Programmen nicht einfach weg, um schnell etwas anderes erledigen zu können. Windows belästigt Sie nur, wenn wichtige Einstellungen geändert werden sollen. Dafür sollten Sie sich Zeit nehmen, die gestellte Frage aufmerksam lesen und prüfen, welche der angebotenen Antworten die richtige ist.

Das gleiche gilt für den Umgang mit allen anderen Programmen und das Surfen im Internet. Wenn Sie nicht wissen, was Sie da gerade „wegklicken“, öffnen Sie Hackern Tür und Tor.

Backups erstellen

Egal wie sehr Sie aufpassen – irgendwann wird mal was passieren. Dann ist es gut, wenn wichtige Daten regelmäßig gesichert worden sind. Backups macht man am einfachsten auf einer externen Festplatte. Viele Anti-Viren-Pakete liefern dafür Hilfen.

Verschlüsselung im WLAN aktivieren

Wenn Sie per Funk mit dem Internet verbunden sind, sollten Sie Ihr WLAN-Signal unbedingt verschlüsseln. Sonst können Hacker Ihre Daten abfangen oder Ihren Internet-Zugang für illegale Aktivitäten nutzen. Das dabei genutzte Passwort sollte komplex und mindestens 20 Zeichen lang sein. Wie Sie die Verschlüsselung an Ihrem DSL-Anschluss aktivieren, erfahren Sie im Handbuch Ihres Internet-Routers. Die sicherste Verschlüsselungsvariante für den privaten Bereich ist derzeit WPA2.

Immer abmelden

Egal ob Webmailkonto, Online-Banking oder Soziales Netz – wenn Sie es nicht mehr benutzen wollen, melden Sie sich aktiv ab. Meist gibt es dafür einen Link der „Abmelden“ oder „Logout“ heißt. Nur so ist sichergestellt, dass keine anderen Nutzer später am gleichen PC auf Ihre Daten zugreifen können.

BROWSER: So wird Ihr Surfbrett nicht zum Verräter

Der Internet-Browser ist das Fenster zur WWWelt und damit auch das wichtigste Einfalltor für Schädlinge. Ärgerlich: Wer sich schützen will, verliert Surf-Spaß. Denn praktisch alle Sicherheits-Einstellungen, führen dazu, dass man beim Surfen von nervenden Nachfragen des Browsers gestört wird, Seiten nicht angezeigt werden oder Komfort-Funktionen nicht klappen.

Die größte Gefahr dabei geht von sogenannten aktiven Inhalten aus. Die sorgen dafür, dass während des Surfens Programme laufen können, ohne dass man es bemerkt. Sie sollten ausgeschaltet und nur bei bekannten Seiten aktiviert werden.

Cookies sorgen dafür, dass Seiten einen Surfer „wiedererkennen“. Das kann bequem sein, hinterlässt aber Datenspuren, die zum Ausspionieren oder für Spam-Versand benutzt werden können.

Außerdem lohnt es sich, regelmäßig den Verlauf des Browsers zu löschen und unerwünschte Werbe-Fenster (Pop-ups) automatisch blockieren zu lassen. Auch sollte der Browser warnen, wenn er Phishing und Malware (Schad-Programme) vermutet.

Wie das alles bei Ihrem Browser geht? Genau so:

Internet Explorer

Microsofts Internet-Browser gilt als langsam und unsicher. Trotzdem wird er von über einem Drittel der Surfer benutzt – wahrscheinlich weil er unter Windows vorinstalliert ist.

Aktive Inhalte und Cookies blockieren

Unter „Extras“, „Internet-Optionen“ gibt es in der Karteikarte „Sicherheit“ einen Schieberegler. Er steuert, welche aktiven Inhalte ausgeführt werden und von welchen Webseiten Cookies angenommen werden. Der Regler sollte mindestens auf „Mittelhoch“ gesetzt werden. Außerdem sollten ein Häkchen vor „Geschützten Modus aktivieren“ stehen (nicht unter Windows XP).

Verlauf löschen

Geht am einfachsten unter „Extras“, „Internet-Optionen“ in der Karteikarte „Allgemein“. Ein Häkchen vor „Browserverlauf beim Beenden löschen“ sorgt dafür, dass beim Beenden alle Daten entfernt werden. Was genau gelöscht werden soll, kann unter „Einstellungen“ definiert werden.

Pop-up-Blocker aktivieren

Unter „Extras“, „Internet Optionen“ finden Sie in der Karteikarte „Datenschutz“ im Bereich „Popupblocker“ das Häkchen „Popupblocker einschalten“.

Firefox

Knapp die Hälfte der Surfer nutzen den vielseitigen und stabilen Browser von Mozilla.

Aktive Inhalte blockieren

Unter „Extras“, „Einstellungen“ sollten im Bereich „Inhalte“ keine Häkchen vor „JavaScript aktivieren“ und „Java aktivieren“ stehen. Funktionieren einige Webseiten danach nicht mehr, hilft das Firefox-Add-on „NoScript“ weiter, das unter https://addons.mozilla.org heruntergeladen werden kann. Es erlaubt die Aktivierung von JavaScript auf einzelnen, vertrauenswürdigen Websites.

Pop-ups verhindern

Unter „Inhalte“ in „Extras“: Bei „Einstellungen“ müssen Häkchen vor „Pop-up-Fenster blockieren“ und „Grafiken laden“ gesetzt werden. Mit einem Klick auf „Ausnahmen . . .“ können Sie die automatisch aufgehenden Fenster auf einzelnen Seiten zulassen.

Cookies blockieren

Im Menü „Extras“, „Einstellungen“, im Bereich „Datenschutz“ entfernen Sie das Häkchen vor „Cookies akzeptieren“. Falls Webseiten damit nicht mehr funktionieren, kann unter „Ausnahmen . . .“ einzelnen Seiten erlaubt werden, Cookies zu speichern.

Verlauf löschen

Ein Häkchen vor „Die Chronik löschen, wenn Firefox geschlossen wird“ im Menü unter „Extras“, „Einstellungen“ im Bereich „Datenschutz“ sorgt für sichere Spurenlöschung nach dem Surfen.

Phishing- und Malware-Schutz aktivieren

Firefox warnt vor unsicheren Webseiten, wenn im Menü unter „Extras“, „Einstellungen“ im Bereich „Sicherheit“ Häkchen vor „Webseiten anzeigen, falls die besuchte Webseite als attackierende Webseite eingeschätzt wird“ und vor „Hinweis anzeigen, falls die besuchte Webseite als Betrugsversuch eingeschätzt wird“ stehen.

Chrome

Den Browser von Google nutzen derzeit zwar nur etwas mehr als 5 Prozent der Surfer, aber hohe Geschwindigkeit und einfache Bedienung sorgen für eine rasch wachsende Fan-Gemeinde.

Cookies abwehren

Ein Klick auf das Werkzeugsymbol rechts des Adressfensters, dann auf „Optionen“ und in der Karteikarte „Details“ erlaubt einen weiteren Klick auf „Content-Einstellungen . . .“ im Bereich Datenschutz. In der Karteikarte „Cookies“ muss der Marker vor „Festlegen von Daten für Websites blockieren“ gesetzt werden. Außerdem müssen Häkchen vor „Alle Drittanbieter-Cookies ohne Ausnahme blockieren“ und „Cookies und andere Websitedaten beim Schließen des Browsers löschen“ stehen.

Aktive Inhalte deaktivieren

Nach dem Klick auf das Werkzeugsymbol klicken Sie auf „Optionen“, dann in „Details“ auf „Content-Einstellungen . . .“. Im Bereich „JavaScript“ setzen Sie den Marker auf „Ausführung von JavaScript auf keine Website zulassen“. Gibt es damit Probleme, kann JavaScript unter „Ausnahmen . . .“ auf einzelnen Seiten aktiviert werden.

Pop-ups und Plug-ins stoppen

Die Bereiche „Plug-ins“ und „Pop-ups“ finden Sie unter dem Werkzeugsymbol in „Optionen“. Dort gibt es im Bereich „Details“ „Content-Einstellungen . . .“. Hier sollten die Marker auf „Verwendung von Plug-ins für keine Webseite zulassen“ und „Anzeige von Pop-ups für keine Webseite zulassen (empfohlen)“ gesetzt werden. Bei Bedarf können hier auch jeweils „Ausnahmen“ definiert werden.

Phishing- und Malware-Schutz aktivieren

Klicken Sie auf das Werkzeugschlüssel-Symbol rechts vom Adressfenster, dann auf „Optionen“ und hier auf „Details“. Vor „Phishing- und Malware-Schutz aktivieren“ muss ein Häkchen stehen.

ILLUSTRATIONEN: RADE PETRASEVIC

Verlauf löschen

Geht mit Klicks auf „Werkzeugsymbol“, „Optionen“, „Details“ und „Internetdaten löschen . . .“. Im folgenden Menü kann gewählt werden, welche Daten aus welchem Zeitraum gelöscht werden sollen. Hier am besten vor alle Optionen ein Häkchen setzen und dann auf „Internetdaten löschen“ klicken.

SOZIALE NETZE: So verlieren Sie bei Facebook nicht Ihr Gesicht

50 Prozent der Surfer sind bei Facebook & Co. die versprechen, immer und überall mit Freunden und Bekannten zu verbinden. Damit aus dem Versprechen kein persönlicher Datenskandal wird, sollten Sie in Communitys diese Tipps beherzigen.

Persönliche Daten nicht leichtfertig veröffentlichen

Prüfen Sie vor dem Einstellen von Daten und Kommentaren, ob Sie die jeweiligen Informationen wirklich veröffentlichen wollen. Als Faustregel gilt: Nur Dinge posten, die Sie ohne Bedenken auf eine Postkarte schreiben würden. Das gilt besonders bei Informationen, die nicht nur Sie betreffen, sondern Freunde oder Ihren Arbeitsplatz. Wichtig: Das Netz vergisst nichts. Einmal eingegebene Daten sind teils nach Jahren noch abrufbar.

Auf Datenschutz und Rechte achten

Wie geht das gewählte soziale Netzwerk mit Ihren Daten um? Prüfen Sie die allgemeinen Geschäftsbedingungen und die Datenschutz-Richtlinien. Genauso wichtig ist die Frage nach den Rechten, die Sie dem Betreiber an Ihren Informationen und eingestellten Fotos, Videos oder Texten geben. Prüfen Sie, ob Sie die Rechte auf Ihre Inhalte sogar verlieren, wenn Sie Ihr Profil im Netzwerk gelöscht haben.

Freunde sollten Freunde sein

Wenn Sie Personen nur aus der virtuellen Welt kennen, sollten Sie bei Kontaktanfragen vorsichtig sein. Dahinter könnten sich Personen verbergen, die Ihre Gewohnheiten ausspionieren wollen.

Stalker melden

Werden Sie dauerhaft in sozialen Netzen von Personen belästigt oder fühlen Sie sich verfolgt, sollten die Stalker bei der Community melden. Dafür gibt es meist spezielle Links. Der Netzwerk-Betreiber prüft dann weitere Schritte. In besonders schweren Fällen von Cyberstalking sollten Sie auch die Polizei einschalten.

Nicht nur dem Netz trauen

Wenn Sie im Internet eine Anfrage bekommen, die Ihnen seltsam vorkommt, versichern Sie sich im realen Leben, ob sie wirklich stimmt. Vielleicht steckt hinter der Bitte nach einer Blitzüberweisung gar nicht Ihr bester Freund, sondern ein Hacker, der dessen Anmelde-Daten gestohlen hat.

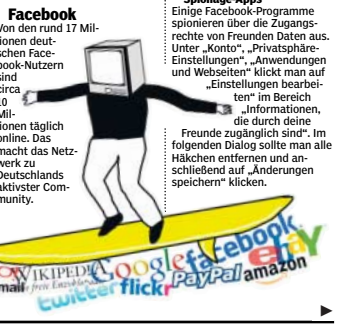
Vorsicht beim Klicken auf Links

Klicken Sie nicht auf Links oder Programme (Apps) in sozialen Netzen, wenn Sie nicht sicher sind, ob schädliche Inhalte dahinterstecken. Oft wird in sozialen Netzen versucht, Daten auszuspionieren oder Schadprogramme wie Viren oder Trojaner auf einem PC einzuschleusen.

Neben diesen allgemeinen Tipps, zeigen wir Ihnen hier, wie Sie bei den fünf am meisten genutzten sozialen Netzen Ihre Daten vor Unbekannten schützen:

Facebook

Von den rund 17 Millionen deutschen Facebook-Nutzern sind circa 10 Millionen täglich online. Das macht das Netzwerk zu Deutschlands aktivster Community.



Private Daten schützen

Wer von Ihren Freunden welche Daten sehen darf, steuern Sie unter „Konto“, „Privatsphäre-Einstellungen“. Die sicherste Variante ist ein Klick auf „Nur Freunde“, allerdings können unter „Benutzerdefiniert“ auch einzelne Informationen für „Alle“ oder „Freunde von Freunden“ freigegeben werden.

Schutz vor Spionage-Apps

Einige Facebook-Programme spionieren über die Zugangsrechte von Freunden Daten aus. Unter „Konto“, „Privatsphäre-Einstellungen“, „Anwendungen und Webseiten“ klickt man auf „Einstellungen bearbeiten“ im Bereich „Informationen, die durch deine Freunde zugänglich sind“. Im folgenden Dialog sollte man alle Häkchen entfernen und anschließend auf „Änderungen speichern“ klicken.

▶

Vorsicht: Taschendiebe im Webshop!

FORTSETZUNG VON SEITE 16

„IT-Kriminalität wird mittlerweile sehr professionell und arbeitsteilig betrieben. Schadprogramme werden heute industriell gefertigt, sodass alle zwei Sekunden eine neue Variante einer Schadsoftware im Netz auftaucht“, erklärt Nora Basting. Die Bedrohung ist real, Privatnutzer sind ebenso betroffen wie Unternehmen oder Behörden.

Braucht man neben einer Firewall wirklich noch einen Virenscanner und ein Anti-Spyware-Programm?

Ein Virenscanner sollte in jedem Fall zur Grundausstattung gehören und unter Windows auch ein Anti-Spyware-Programm.

Einige Browser bieten die Möglichkeit, „privat“ oder „inkognito“ zu surfen. Reicht das nicht als Schutz aus?

„Datenschutzeinstellungen im Browser schützen nicht vor Schadsoftware. Auch wenn Sie den Browser gar nicht geöffnet haben, ist Ihr Rechner möglicherweise online und kann über andere Wege infiziert werden“, so die BSI-Expertin.

Wie soll ich mir all die verschiedenen Passwörter und Zugangsdaten merken?

„Wer sich sehr viele Online-Zugangsdaten merken muss, für den kann sich ein Passwort-Verwaltungsprogramm empfehlen“, weiß Nora Basting. „Hier muss man sich nur ein Passwort merken, das alle anderen in einem verschlüsselten Programm auf dem PC schützt. Wer sich Passwörter doch notieren muss, sollte sie in jedem Fall unter Verschluss halten und gerade auf dem PC nie unverschlüsselt abspeichern.“

Worauf müssen Eltern achten, wenn ihre Kinder allein im Web unterwegs sind?

Viele Kinder und Jugendliche sind sich oft nicht bewusst, welche Gefahren im Internet lauern. Eltern sollten ihren Kindern im Internet wie im „echten Leben“ ein gesundes Misstrauen beibringen. Hilfen für Eltern und Kinder gibt es zum Beispiel unter www.klicksafe.de.

Wo bekomme ich mehr Informationen darüber, wie ich mich schützen kann?

Das BSI bietet auf der Webseite www.bsi-fuer-buerger.de Tipps, wie man PC, Internet und zum Beispiel auch Smartphones sicher nutzen kann. Hier werden auch Begriffe erklärt, die der Privatnutzer vielleicht nicht kennt. Unter www.buerger-cert.de können Nutzer sich per Mail über aktuelle Sicherheitslücken und Updates informieren lassen.

wer-kennt-wen

In dem Netzwerk sind über 9 Millionen Deutsche aktiv. Anmelden kann sich jeder, der über 14 Jahre alt ist.

Private Daten schützen
Unter „Einstellungen“, „Privatsphäre“ können Sie die Freigaben anpassen. Der Fragezeichen-Link liefert Informationen darüber, wie Sie das am besten machen.

Gästebucheinträge verbieten
Unter „Einstellungen“, „Privatsphäre“ können Sie Ihre Gästebucheinstellungen ändern. Ist „Nur ich selbst“ angeklickt, wird das Gästebuch unsichtbar. Weitere Optionen: „Nur Leute, die ich kenne“ und „Alle Leute innerhalb von wer-kennt-wen“. „Nur Leute, die ich kenne“ ist die sicherste Wahl.

Nachrichten schicken einschränken
Bei Nachrichten können Sie unter „Privatsphäre“ zwischen „Nur Leute, die ich kenne“ und „Alle Leute innerhalb von wer-kennt-wen“ wählen. Die erste Einstellung ist die sicherste.

XING

Die Community wendet sich anders als Facebook & Co. nicht so sehr an Privatpersonen, sondern will vor allem Geschäftskontakte pflegen.

Google aussperren
Im Menü „Start“, „Einstellungen“, „Meine Privatsphäre“ auf den Button „bearbeiten“ und dann „Mein Profil darf in Suchmaschinen auffindbar sein“ den Haken entfernen.

Persönliche Daten schützen
Geburtsdatum, Mailadresse etc. können Sie für jeden neuen Kontakt einzeln freischalten. Auf dem jeweiligen Profil steht rechts: „Einstellungen“, „Datenfreigabe bearbeiten“, „Geschäftliche Kontaktdaten“ oder eben „private Kontaktdaten“. Über das kleine Plus-Symbol rechts auffächern und bei „E-Mail“, „Adresse“ etc. das Häkchen setzen, wenn die Information für den Kontakt freigegeben sein soll.

Schutz vor Apps, die spionieren
Bevor eine Applikation erstmals genutzt wird, können Sie diese unter „Start“, „Applikationen“, „Applikation aussuchen“, „Applikation hinzufügen“ rechts bei „Ansichts- und Zugriffsoptionen“ freischalten. Diese Berechtigung können Sie unter „Start“, „Einstellungen“, „Externe Applikationen“ mit einem Klick auf „bearbeiten“ wieder entziehen.

Schutz vor unerwünschten Nachrichten
Bei „Start“, „Mein Profil“ unter „Profileinstellungen“, „Privatsphäre“, „Nachrichten und Gästebucheinträge schreiben“ können Sie wählen, ob „nur meine direkten Kontakte“ oder „alle Mitglieder“ Ihnen Nachrichten schicken oder in Ihr Gästebuch schreiben dürfen. Sie können auch einzelne Personen bestimmen, die Ihnen Nachricht schicken dürfen: Auf dem Profil der Person gehen Sie dafür rechts auf „Einstellungen“, „Datenfreigabe bearbeiten“ und bei „Kontakt XY darf Ihnen Nachrichten schreiben“ das entsprechende Häkchen setzen oder entfernen. Um Gästebucheinträge zuzulassen, muss das Gästebuch aktiviert sein. Das geht so: „Start“, „Mein Profil“, „Gästebuch“, „Gästebuch aktivieren/deaktivieren“.

VZ-Netzwerke

Die deutsche Community startete ursprünglich als Studenten-Netzwerk, ist heute aber auch als SchülerVZ und MeinVZ für alle Nicht-Studis verfügbar. Angemeldet sind rund 17 Millionen Menschen.

Privatsphäre schützen
Um sämtliche persönlichen Informationen zu blocken, gehen Sie in „Privatsphäre“ auf dem Reiter „Meine Privatsphäre“ und wählen dann „Nichts“ aus. Wer einzelne Infos freigeben will, wählt „Ich bestimme selbst“ und ändert etwa unter „Wer darf mein Profil sehen?“ den Punkt „Alle“ in „Nur meine Freunde“.

Schutz vor unerwünschten Nachrichten
Unter „Meine Privatsphäre“ in den „Benutzerdefinierten Einstellungen“ „Ich bestimme selbst“ unter „Wer darf mir Nachrichten schicken?“ einstellbar.

Daten für Apps sperren
Was Apps wissen dürfen, legen Sie fest, indem Sie die entsprechende App anklicken und dort unter „App-Einstellungen“ etwa wählen, ob die App „Benachrichtigungen schicken“ darf.

Werbung verhindern
Bei „Privatsphäre“ unter dem Reiter „Werbe-Einstellungen“ können Werbenachrichten abgeschaltet werden.

Twitter

Der Kurznachrichten-Dienst bietet zwar weniger Möglichkeiten als Facebook, ist dafür aber wesentlich aktueller und schneller.

Privatsphäre schützen
Klicken Sie zunächst oben rechts auf Ihren Profilnamen, dann auf „Einstellungen“. Im Bereich „Account“ setzen Sie ein Häkchen vor „Meine Tweets schützen“ und bestätigen die neue Einstellung mit einem Klick auf „Speichern“. Dann können nur noch Freunde und Bekannte Ihre Updates lesen.

Hier sollten übrigens auch die Häkchen vor „Tweets mit Ortsangabe versehen“ und „Show photos and videos from everyone“ entfernt werden.

Programme blockieren
Der Bereich „Verbindungen“ unter dem Profilnamen, „Einstellungen“ zeigt, welche Programme (etwa vom Handy) Zugriff auf Ihr Twitter-Profil haben. Hier sollten nur Apps stehen, die Sie tatsächlich benutzen. Andere Programme werden per Mausklick auf „Zugriff widerrufen“ entfernt.

Flickr

Hier laden Millionen Menschen weltweit Fotos hoch, um sie mit Freunden und Bekannten zu teilen oder direkt online Abzüge zu bestellen.

Berechtigungen einrichten
Unter „Sie“, „Ihr Account“ finden Sie im Bereich „Datenschutz & Berechtigungen“ viele Einstellungen, mit denen Sie auswählen, wer was mit Ihren Bildern machen darf. Diese Berechtigungen sollten Sie aufmerksam bearbeiten. Wichtig: Hinter „Wer darf Ihre Fotos und Videos weitergeben“ sollte „Nur Sie“ stehen. Hinter „Wer kann Sie auf einem Foto markieren?“ sollte höchstens „Ihre Freunde und/oder Familie“ stehen und hinter den Einträgen „Eigene Inhalte bei der öffentlichen Suche ausblenden“ und „Ihr Profil bei der öffentlichen Suche ausblenden“ sollte jeweils „Ja“ stehen.

Daten schützen
Auch die „Standardeinstellungen für neue Uploads“ sollten Sie kritisch bearbeiten, bevor Sie Fotos hochladen.

Daten schützen
Damit Ihr Name und Ihre Kontaktdaten nicht von allen Flickr-Mitgliedern gefunden werden können, klicken Sie unter „Sie“, „Ihr Profil“ auf „Datenschutz Ihres Profils bearbeiten“. Im folgenden Dialog stellen Sie in allen vier Fenstern die Option „Freunde und Familie“ ein und bestätigen mit einem Mausklick auf „Änderungen speichern“.

Google aussperren
Damit Suchmaschinen nicht Ihre Fotosammlung durchsuchen können, klicken Sie unter „Sie“, „Ihr Profil“, auf „Ihr Profil bei Suchvorgängen ausblenden“. Im folgenden Fenster setzen Sie in alle drei Kästen Häkchen (zwei unter „Ihre Fotos“, eines unter „Ihr Profil“) und bestätigen mit „Speichern“.

Stayfriends

Über 11 Millionen Deutsche bleiben über Stayfriends.de mit ihren ehemaligen Klassenkameraden in Kontakt.

Kontaktdaten sichern
Die von Ihnen eingegebenen Daten können Sie unter „Ich“ unter „Kontaktdaten“ mit einem Klick auf „Kontaktdaten bearbeiten“ vor unerlaubten Zugriffen schützen.

In den Bereichen „Sichtbarkeit Adresse“, „Sichtbarkeit Telefon“ und „Sichtbarkeit Instant Messaging“ klicken Sie dafür jeweils auf „ändern“ und wählen dann im folgenden Menü am besten „Freunde und Familie“ oder „Kontakte“ aus. Wichtig: anschließend immer auf „Speichern“ klicken, um die Veränderungen zu bestätigen.

Google aussperren
Unter „Ich“, „Einstellungen“ können Sie im Bereich „Gefunden werden“ mit einem Klick auf „bearbeiten“ wählen, wer Ihre Daten finden kann. Hier sollten am besten alle fünf Häkchen entfernt werden (besonders wichtig ist „von Personen, die nicht bei Stayfriends sind“). Danach mit „Alle Änderungen speichern“ bestätigen.

SHOPPING: Sechs Tipps fürs sichere Kaufen

Es geht so schön schnell auf Knopfdruck, und das Tütenschleppen fällt auch weg. 80 Prozent der Deutschen kaufen im Internet ein. Vor allem Musik, Bücher und Videos werden bestellt, aber auch Mode, Waschmaschinen und Lebensmittel. In einer aktuellen Untersuchung gaben allerdings 8 Prozent der Surfer an, beim Online-Einkauf schon betrogen worden zu sein. Sicherer geht es mit diesen Tipps:

Auf Anbieter achten
Unseriöse Anbieter erkennen Sie häufig daran, dass auf der Webseite kein Impressum mit Adresse und Namen von Geschäftsführern steht. Prüfen Sie bei unbekannten Anbietern diese Angaben und auch die Allgemeinen Geschäftsbedingungen (AGB). Bewertungssysteme, wie sie etwa Preisvergleichsseiten bieten, helfen, seriöse Anbietern zu finden.

Beschreibungen genau lesen
Gerade bei Online-Auktionshäusern wird gern mal eine leere Verpackung versteigert. Prüfen Sie genau, wie das Produkt beschrieben ist.

Vorsicht Schnäppchen
Kostet die gesuchte Ware in einem Shop nur die Hälfte des handelsüblichen Preises, steckt wahrscheinlich kein seriöser Anbieter dahinter. Nutzen Sie Preisvergleichsseiten wie etwa idealo.de, um ein Gefühl für „normale“ Preise zu bekommen.

Vorsichtig bezahlen
Generell gilt: Überweisen Sie nie Geld, ohne eine Gegenleistung dafür erhalten zu haben. Seriöse Händler bieten meist die Möglichkeit, per Kreditkarte, Bankeinzug oder Nachnahme zu bezahlen. Wichtig: Achten Sie beim Eingeben persönlicher Daten (wie etwa Kreditkartennummern) darauf, dass eine verschlüsselte Übertragungsart (https) benutzt wird. Dies erkennen Sie bei den meisten Internet-Browsern daran, dass ein kleines Schloss-Symbol im Adressfeld oder der Menüleiste eingeblendet wird. Kaufen Sie Waren auf einer Auktionsplattform wie Ebay, lohnt es sich bei größeren Beträgen, den dort angebotenen Treuhandservice zu nutzen. Der stellt sicher, dass die Bezahlung erst beim Verkäufer eingeht, wenn die Ware beim Käufer ist.

Im Zweifel zurückschicken
Im Internet gekaufte Ware dürfen Sie innerhalb von 14 Tagen ohne Angabe von Gründen zurückschicken. Aber: Liegt der Kaufpreis unter 40 Euro, darf Ihnen der Händler die Rücksendekosten berechnen.

Alles dokumentieren
Egal ob Rechnung oder Bestätigung – im Zweifelsfall brauchen Sie diese Dokumente. Archivieren Sie den Mailverkehr, oder drucken Sie sich die Webseite mit der Bestellbestätigung aus.

ILLUSTRATIONEN: RADE PETRASEVIC

BITTE BLÄTTERN SIE UM

19 von 20 Mails sind Spam

BANKING: So sparen Sie sich Datenklau

26 Millionen Deutsche nutzen Online-Banking. Ein wunderbarer Markt für Betrüger: 17 Millionen Euro fischten sie mit sogenannten Phishing-Mails 2010 ab. Diese Tipps helfen, sich gegen Banking-Betrüger zu schützen.

Adresse prüfen
Damit Sie immer auf der echten Bankwebseite landen, tippen Sie am besten die Internetadresse vor jedem Einloggen neu ein oder legen Sie sich selbst ein Lesezeichen auf Ihrem PC an. Vorsicht: Werden Sie bereits beim Login nach einer TAN oder anderen persönlichen Daten gefragt, ist die Seite mit Sicherheit gefälscht. Schon eine kleine Abweichungen der Internetadresse, zum Beispiel ein Trennstrich zu viel, ist ein Zeichen für eine Fälschung. Meiden Sie zudem Webadressen, die mit einer Nummer beginnen (wie http://4457.816/ . . .) und Seiten, in deren Adresse der Name nur „eingebaut" ist (wie http://XYZ-bank.Domainname.de). Achten Sie auch auf eine verschlüsselte Verbindung (meist gekennzeichnet durch ein „https" oder das Schlosssymbol in der Browserzeile).

Fremde PCs meiden
Fremde Rechner fürs Banking zu nutzen, birgt das Risiko, dass andere Benutzer auf Ihre persönliche Bankseite zugreifen können. Beenden Sie die Banking-Sitzung immer mit „Logout", schließen Sie nicht einfach das Browserfenster. Wichtig: Zwischenspeicher (Cache) löschen. Wie das geht, lesen Sie in unserem Kapitel zu den Internet-Browsern auf Seite 16.

Schaden begrenzen
Vereinbaren Sie mit der Bank einen Höchstbetrag (z. B. 500 Euro), der täglich online abgebucht werden darf. So halten Sie den Missbrauchs-Schaden möglichst gering.

Regelmäßig Kontoauszüge ziehen
Auch wenn Sie Ihren Kontostand online abrufen, holen Sie sich trotzdem regelmäßig gedruckte Auszüge. Die Online-Kontoauszüge könnten manipuliert sein.

Notfalls Konto sperren
Stellen Sie etwas Verdächtiges fest, sperren Sie sofort Ihr Konto. Das geht bei Ihrer Hausbank. Kreditkarten können Sie unter der bundesweiten Notfallnummer 116 116 sperren.

TANs geheim halten
Ihre Bank fragt nie per Mail oder Telefon nach vertraulichen Daten wie Zugangscodes, PINs, TANs oder Kontonummern. Bekommen Sie eine solche Mail, sagen Sie Ihrer Bank bescheid.

E-MAILS: 15 Tipps gegen böse Botschaften

Täglich bekommt jeder Internet-Nutzer im Schnitt 28 Mails. Hochgerechnet sind das 1,1 Milliarden Nachrichten, die täglich in deutschen Postfächern landen. Doch E-Mails sind nicht nur Nachrichten von Freunden, sondern oft auch Verstecke für Trojaner und aggressive Werber. Diese Tipps sorgen dafür, dass Sie keine unliebsamen Überraschungen im digitalen Briefkasten finden.

Spam nicht anklicken
Die meisten E-Mail-Anbieter filtern unerwünschte Werbemails schon aus Ihrem Posteingang. Kommt dennoch mal Spam durch, gilt: Auf keinen Fall antworten oder in der E-Mail enthaltene Links anklicken! Dies gilt auch für Links, unter denen der Nutzer sich angeblich „abmelden" kann. Denn mit dem Klick zeigen Sie dem Versender der Mail: „Diese E-Mail-Adresse wird regelmäßig genutzt!" Er wird Ihnen nur noch mehr Mails schicken.

Spam melden
Markieren Sie Spam-Nachrichten, die in Ihrem Postfach landen als Spam. Nur so kann Ihr Mail-Anbieter den Schutz vor den Werbenachrichten weiter verbessern.

Mehrere Mail-Adressen nutzen
Verwenden Sie je nach Art der Nachricht mehrere Mail-Adressen, etwa für Privates, Geschäftliches und die Anmeldung bei Newslettern oder Online-Shops. Einige Mail-Betreiber wie Yahoo! und Hotmail bieten die Möglichkeit, „Wegwerf"-Adressen zu nutzen. Die sind dann sinnvoll, wenn man die Adresse braucht, um sich für einen Dienst zu registrieren, bei dem man nicht sicher ist, ob der dahintersteckende Anbieter seriös ist.

Vorsicht bei Gewinnen!
Auch wenn die Nachricht, die einen Lotteriegewinn verspricht, verlockend ist: Prüfen Sie genau, bevor Sie auf den eingebauten Link klicken. Hacker versuchen, Sie mit diesen Mails auf unsichere Seiten zu locken, oder über Anhänge Viren auf Ihrem PC einzuschleusen. Klicken Sie nur auf Links und Anhänge von Absendern, die Sie kennen. Und fragen Sie im Zweifelsfall beim Absender nach, ob der Anhang tatsächlich von ihm stammt.

Neben diesen allgemeinen Tipps sollten Sie bei Ihrem Anbieter die folgenden Einstellungen vornehmen.

Yahoo!
Der Mailanbieter Yahoo hat in Deutschland 6,5 Millionen Nutzer und wurde 2010 vom Fraunhofer Institut für Sichere Informationstechnologie (SIT) ausgezeichnet, als kostenloser Maildienst mit dem besten Spamfilter.

Spam stoppen
Und genau dieser Spamfilter muss eingeschaltet sein. Das überprüft man unter: „Optionen", „Weitere Optionen". Dann aus der Liste „Spam" auswählen. Vor „SpamGuard" müsste bei „Spamverdächtige Mails automatisch in meinem Spam-Ordner ablegen" ein Haken sein. Dann ist der SpamGuard aktiv.

Sollte jemand Ihre Adresse benutzen, um Spam zu verschicken, müssen Sie zunächst Ihr Passwort ändern. Ob Sie als Spamverteiler missbraucht werden, erkennen Sie, wenn Sie regelmäßig den Ordner „Gesendete Mails" kontrollieren.

Mails blockieren
Unter „Optionen" auf „Spam" klicken und in dem leeren Feld unter „Blockierte Adresse" die entsprechende Mail-adresse eingeben. Mit „Hinzufügen" bestätigen. So können Sie bis zu 500 Adressen abwehren. Um eine Adresse wieder freizuschalten, klicken Sie in der Liste der blockierten Adressen auf den gewünschten Absender und dann auf „Entfernen" neben der Liste.

Wegwerfadresse einrichten
Wegwerfadressen können Sie etwa bei Gewinnspielen angeben. Die Mails, die Sie über die Wegwerfadressen bekommen, landen in Ihrem Yahoo!-Postfach. Der Clou: Haben Sie keine Lust mehr auf Gewinnspielbenachrichtigungen, können Sie einfach die Adresse löschen. Erstellen Sie eine Wegwerfadresse unter: „Option", „Mail-Optionen", „Spam", „Wegwerfadressen". Klicken Sie dann auf „Adresse hinzufügen". Nachdem Sie eine Grundadresse erstellt haben, können Sie die Wegwerfadressen hinzufügen.

GMX
Früher stand der Name synonym für Webmail und auch heute nutzen noch Millionen den Dienst.

Spam stoppen
Die „Blacklist" schützt vor Werbemails. Gehen Sie dafür auf „Mein GMX", „E-Mail", „Optionen", „Spamschutz", „Erweiterte Einstellungen vornehmen" und dann „Blacklist bearbeiten". Hier können sowohl genaue E-Mail-Adressen als auch bestimmte Worte in den Absender-Adressen wie zum Beispiel „Casino" eingegeben werden. So landen alle Mails eines bestimmten Absenders oder mit dem Wort „Casino" im Ordner „Spamverdacht". Dort können sie geprüft und gelöscht werden.

Oder Sie verweigern die Annahme der E-Mails ganz. Einfach einen Häkchen bei „Annahme verweigern, E-Mails nicht zustellen" unter „Erweiterte Einstellungen vornehmen", „Blacklist" setzen. Der Absender bekommt die Meldung, dass der Nutzer keine E-Mails von ihm empfangen möchte.

GoogleMail
Weltweit nutzen über 200 Millionen Menschen den Postdienst, dessen ursprüngliche Version ein Google-Programmierer unter dem Namen Gmail in seiner Freizeit entwickelt hatte. Der Spamfilter (automatisch aktiviert) funktioniert wegen der großen Nutzerzahl sehr gut.

Postfach absichern
Die Sicherheits-Einstellungen finden Sie unter „Einstellungen" im Bereich „Allgemein". Setzen Sie unter „Externer Content" den Marker vor „Vor dem Anzeigen von externem Content fragen", den Marker bei „Browserverbindung" vor „Immer https verwenden" und unter „Mein Bild" vor „Nur für Chat-Kontakte sichtbar". Danach mit einem Klick auf „Änderungen speichern" bestätigen.

Verdächtige Mails melden
Der Spamfilter von Googlemail ist automatisch aktiv. Finden Sie trotzdem Spam im Posteingang, können Sie die Nachricht per Klick auf „Spam melden" in der Mailansicht entfernen. Bei Phishing-Mails ist der Melde-Button etwas besser versteckt: Klickt man auf den Pfeil oben rechts neben „Antworten", gibt es dort die Option „Phishing melden".

Google-Profil absichern
Wichtig: Wer Googlemail nutzt, hat automatisch auch ein Google-Profil. Das sollte unter www.google.com/profiles/me mit einem Klick auf „Profil bearbeiten" vor der Öffentlichkeit versteckt werden. Dazu entfernen Sie im Bereich „Über mich" das Häkchen vor „Meinen vollen Namen anzeigen, damit . . ." und klicken dann auf „Änderungen speichern".

Hotmail
Microsofts Gratis-E-Mail-Dienst Windows Live Hotmail bietet neben Spam und normalem Posteingang noch einen Greymail-Ordner. Hier landen Nachrichten, wie etwa Newsletter, die kein klassischer Spam sind, aber vom Anwender auch nicht mehr regelmäßig gelesen werden.

Verbindung verschlüsseln
Klicken Sie im Posteingang auf das Menü „Optionen", dort auf „weitere Optionen", dann auf „Konto Verwalten" und „Kontodetails". Im folgenden Fenster wählen Sie unter „weitere Optionen" „Mit HTTPS verbinden" aus und aktivieren dort „HTTPS automatisch verwenden" anmarkern und mit „Speichern" bestätigen.

Spams filtern
Spam heißt bei Hotmail Junk-E-Mail. Wie kritisch Nachrichten geprüft werden, können Sie unter „Optionen" unter „weitere Optionen" im Bereich „Filter und Berichte" wählen. Optimalen Schutz bietet der Marker im Feld „Exklusiv". Wählen Sie die, sollten Sie aber von Zeit zu Zeit den Junk-Ordner anschauen, um zu verhindern, dass dort auch Mails landen, die kein Spam sind.

Werbung verbieten
Hotmail ist standardmäßig so eingestellt, dass Nutzer Werbung bekommen. Das können Sie unter „Optionen", „weitere Optionen" im Bereich „Kontoübersicht" mit einem Klick auf „Marketingeinstellungen" ändern. Setzen Sie hier in alle drei Kästen Häkchen und bestätigen Sie mit „Speichern".

WEB.DE
Schutz vor Phishing-Mails
Die kostenlose WEB.DE-Toolbar biete Schutz vor Phishing-Mails und kann direkt über die WEB.DE-Homepage heruntergeladen werden. Klicken Sie dazu auf „Alle Inhalte" unter dem WEB.DE Logo. Danach wählen Sie unter dem Buchstaben M den Punkt „Mail-Check" aus. Klicken Sie je nach Browser auf den Button „Für Mozilla Firefox jetzt hinzufügen" oder „Für Internet Explorer jetzt hinzufügen". Danach den Installationshinweisen folgen.

VIVA DIGITALIA

News aus der digitalen Welt und was sie bedeuten

Von MARTIN EISENLAUER

30 Millionen Android Birds

Das Handy-Spiel Angry Birds gibt es seit rund fünf Monaten für Googles Handy-Betriebssystem Android. Seither wurde es über 30 Millionen Mal heruntergeladen, meldete Hersteller Rovio diese Woche. Die App ist werbefinanziert, spült Rovio also ständig Geld in die Kassen.

Twitter angeblich 7,7 Milliarden Dollar wert

Twitter soll laut Unternehmensangaben rund 7,7 Milliarden US-Dollar wert sein. Der Kurznachrichten-Dienst soll Gerüchten zufolge in Verkaufsverhandlungen mit Google und Facebook stecken. Twitter-Gründer Biz Stone beteuert derweil öffentlich, dass er gern unabhängig bleiben würde.

Amazon wird im März zum Android-App-Store

Schwerer Schlag für Apple: Amazon steht offenbar kurz davor, Android-Apps über den eigenen Webshop zu verkaufen. Das eröffnet den Programmen für das Google-Betriebssystem eine riesige neue Käuferschaft. Marktstart könnte (zumindest in den USA) noch im März sein.

Nintendo 3DS in zwei Stunden ausverkauft

In Japan startete Nintendo am Montag den Verkauf der neuen mobilen Spielkonsole 3DS – zumindest für zwei Stunden. Denn danach waren die 400 000 Stück der ersten Lieferung des 250 Euro teuren Geräts komplett ausverkauft. Deutschland-Start für den 3DS ist der 25. März.

Opera erst ab 17 Jahren

Der Internet-Browser Opera wurde von Apple im App Store mit einer Altersbeschränkung versehen. Anwender müssen 17 Jahre alt sein, um ihn herunterzuladen. Opera-Chef Jan Standal nahm es mit Ironie: „Ich bin mir nicht sicher, ob 17-Jährige schon bereit sind, so ein schnelles und gutes Programm zu benutzen."

Webvideo der Woche

US-Komiker Conan O'Brien hat einen erstaunlich ehrlichen Werbefilm für das iPad 2 gemacht. Köstlich! Link: **bit.ly/e0aLEN**

Lesen Sie auch die Tech-Freak-Kolumne auf Seite 58

ILLUSTRATIONEN: RADE PETRASEVIC FOTOS: PR, INTERNET