

Mit McAfee in 10 Schritten zur Internetsicherheit für die ganze Familie

So verstehen kleine Kinder, Kids,
Teenager und Internet-Anfänger jeden
Alters das Thema Online-Sicherheit

A large, semi-transparent red circle is overlaid on the image. Inside the circle, the number "10" is written in a white, bold, sans-serif font. The circle is positioned in the lower-left quadrant of the page, partially overlapping the laptop and the child's hands.

10

Inhaltsverzeichnis

- 3 Einleitung
- 4 Internet heute:
Lassen Sie Vorsicht walten
- 5 Ein 10-Schritte-Sicherheitsplan zum
Schutz der ganzen Familie
- 17 Das ABC der Online-Sicherheit:
 - 17 Für kleine Kinder (3 bis 7 Jahre alt)
 - 21 Für Kids (8 bis 12 Jahre alt)
 - 26 Für Teenager (13 bis 19 Jahre alt)
 - 30 Für Anfänger jeden Alters
- 33 Über McAfee

10





Einleitung

Millionen Familien auf der ganzen Welt nutzen das Internet jeden Tag – sie lernen, recherchieren, kaufen ein, nutzen Online-Banking, tauschen Fotos aus, spielen, laden Filme und Musik herunter, kommunizieren mit Freunden, lernen neue Leute kennen und gehen einer Vielzahl anderer Tätigkeiten nach. Der sogenannte Cyberspace bietet Vorteile und Möglichkeiten und macht vieles einfacher, stellt jedoch auch ein immer größeres Risiko dar – denn **täglich gibt es neue Bedrohungen**.

Kein Wunder, dass sich dort Cyberkriminelle tummeln und Menschen schaden, die das Internet nutzen. Bei jedem Besuch im Internet sollte man auf der Hut sein. Sie sollten nicht nur eine zuverlässige Sicherheitssoftware eines vertrauenswürdigen Unternehmens installieren, um Ihre Familie vor Hackern, Identitätsdieben, E-Mail-Betrügern und anderen Personen mit bösen Absichten zu schützen, Sie müssen auch **einige Grundregeln der Internetsicherheit befolgen** und sich auf Ihren gesunden Menschenverstand verlassen. Ein „Internetsicherheitsplan“ für Ihre Familie hilft.

Sobald ein Familienmitglied online aktiv ist, sollte mit der jeweiligen Person —ungeachtet ihres Alters— über Internetsicherheit gesprochen werden. **Auch wenn Sie zuhause keinen Computer haben**, gibt es inzwischen fast überall PCs—in der Schule, in der Bibliothek, bei Freunden zuhause und in öffentlich zugänglichen Räumen. Es ist wichtig, jeden grundlegend darüber zu informieren, wie er sich im Cyberspace schützen kann.



Internet heute: Lassen Sie Vorsicht walten

- 50 % der Teenager, die online unterwegs sind, haben personenbezogene Daten bekannt gegeben¹
- Alle 39 Sekunden greifen Hacker einen PC mit Internetanschluss an²
- Laut McAfee® Avert Labs®, gibt es gegenwärtig 222.000 bekannte Computerviren und der Umfang an Bedrohungen nimmt täglich zu
- 30 % der Teenager wurden während der Schulzeit einmal oder mehrmals durch Cyberbullying belästigt³
- Die Internetkriminalität hat 2008 im Vergleich zu 2007 um 33 % zugenommen⁴
- 31 % der Kinder sind bereits mit schädlichen Inhalten in Berührung gekommen¹
- Weltweit werden jährlich 3,2 Millionen Menschen Opfer von Betrug im Internet⁵

1 EU Kids Online, Comparing children's online opportunities and risks across Europe (2006–2009)

2 Hackers Attack Every 39 Seconds – James Clark School of Engineering der University of Maryland

3 theage.com.au

4 2008 Internet Crime Report, IC3

5 National Fraud Strategic Authority der USA

A woman with dark hair is smiling and looking towards a man whose profile is visible on the left. The image is overlaid with a large, semi-transparent blue geometric shape that covers the right side and bottom. The text is white and positioned on the blue background.

Ein 10-Schritte- Sicherheitsplan zum Schutz Ihrer Familie im Internet



Schritt 1

Überlegen Sie, wo Sie den Computer aufstellen

Sind Kinder im Haus, ist die Entscheidung, wo der Computer steht, sehr wichtig. Wir empfehlen, den Computer an einem **stark frequentierten Ort** aufzustellen. Sie sollten festlegen, wie lange und wann ein Kind den PC nutzen darf. Achten Sie darauf, dass Sie Computer-**Sicherheitssoftware** mit einer Kindersicherung verwenden, wie sie in McAfee-Produkten enthalten ist oder benutzen Sie spezielle Software, die für den Schutz von Kindern online bestimmt ist, wie z.B. McAfee Family Protection.

Schritt 1



Schritt 2

Legen Sie gemeinsam Grenzen fest

Legen Sie genau fest, was OK und was nicht OK ist, und zwar in Bezug auf folgende Punkte:

- Die Art von Websites, die bedenkenlos besucht werden können
- Die Chatrooms und Foren, an denen man sich bedenkenlos beteiligen kann:
 - Nur beaufsichtigte Chaträume aufsuchen
 - Stellen Sie sicher, dass Ihre Kinder Chatrooms mit der Bezeichnung „alt“ meiden, die alternativen Themen gewidmet und folglich möglicherweise ungeeignet sind für junge Menschen
- Die Themen, über die Ihre Kinder online diskutieren können und die Ausdrucksweise, die als unangemessen angesehen wird

Schritt 2



Schritt 3

Einigen Sie sich gemeinsam auf PC-Regeln für die ganze Familie

Wir empfehlen folgende Verhaltensweisen:

- Unter keinen Umständen mit Benutzernamen anmelden, die die wahre Identität preisgeben oder provozierend sind
- Niemals Passwörter herausgeben
- Unter keinen Umständen Telefonnummern oder Adressen preisgeben
- Unter keinen Umständen Informationen veröffentlichen, die die eigene Identität preisgeben
- Unter keinen Umständen anstößige Fotos oder Fotos veröffentlichen, die Rückschlüsse über die eigene Identität zulassen (z. B. Name einer Stadt oder Schule auf T-Shirts)
- Unter keinen Umständen irgendwelche Informationen mit unbekanntem Personen austauschen, die man online kennen gelernt hat
- Unter keinen Umständen persönliche Treffen mit unbekanntem Personen ausmachen, die man online kennen gelernt hat
- Niemals Anhänge öffnen, die man von Fremden erhalten hat

Nachdem Sie die Regeln festgelegt haben, drucken Sie diese aus und hängen Sie sie in der Nähe des Computers auf.

Schritt 3



Schritt 4

Unterzeichnen Sie eine Vereinbarung über angemessenes Online- Verhalten

Arbeiten Sie schriftlich eine Vereinbarung (einen sog. „Verhaltens-Kodex“) aus **oder nutzen Sie die Vereinbarung auf der nächsten Seite**, um allen Familienmitgliedern verständlich zu machen, wie man sich **im Internet verhalten soll**.

Schritt 4



Erklärung zum Schutz von Kindern im Internet

Ich möchte nicht auf den Computer und das Internet verzichten und verspreche Folgendes:

- Immer, wenn ich online bin, werde ich mich beim Surfen, Suchen, Arbeiten, Spielen und **Chatten so verhalten, dass kein Sicherheitsrisiko besteht**
- Ich werde **alle Regeln befolgen**, auf die wir uns geeinigt haben
- Ich werde Folgendes nicht preisgeben:** meinen richtigen Namen, meine Telefonnummer, meine Adresse oder meine Kennwörter, auch nicht für „Freunde“, die ich online kennen gelernt habe
- Ich werde mich mit Personen, die ich online kennen gelernt habe, **nie persönlich treffen**
- Wenn ich online in eine Situation gerate, in der ich mir nicht sicher bin oder mich unbehaglich fühle, **verspreche ich, es dir (meinem Elternteil/meiner Aufsichtsperson/meinem Lehrer) zu sagen**, damit du mir helfen kannst
- Ich bin an dieses Versprechen gebunden** und weiß, dass jede von mir getroffene Entscheidung Konsequenzen hat

Unterschrift des Kindes _____

- Als dein Elternteil/deine Aufsichtsperson/dein Lehrer verspreche ich, mir Zeit für dich zu nehmen wenn du um Hilfe bittest, und dich bei der Lösung jeglicher Probleme nach Kräften zu unterstützen

**Unterschrift des Elternteils/
der Aufsichtsperson/des Lehrers** _____



Schritt 5

Sicherheitssoftware installieren

Stellen Sie sicher, dass Sie über zuverlässige Sicherheitssoftware verfügen, die Ihren Computer vor Viren, Hackern und Spyware schützt. Die Software sollte auch anstößige Inhalte, Bilder und Websites filtern. Diese Software **sollte regelmäßig aktualisiert werden**, da jeden Tag neue Bedrohungen auftauchen. Ideal ist Sicherheitssoftware, die automatisch aktualisiert wird, etwa Software von McAfee, **bei der nach der einmaligen Konfiguration keine weiteren Schritte erforderlich sind**.

Schritt 5



Schritt 6

Nutzen sie die Kindersicherung

Kindersicherung ist bei allen großen Anbietern von Sicherheitssoftware Standard. Aktivieren Sie sie unbedingt. Wenn Sie derzeit mit Freeware oder Software arbeiten, die keine Kindersicherung bietet, ziehen Sie den Kauf entsprechender Software in Betracht. **Machen Sie sich in Ruhe mit der Funktionsweise der Kindersicherung vertraut** und aktivieren Sie Optionen zum Filtern und Blockieren ungeeigneten Materials.

Verwenden Sie für einen kompletten Schutz Ihrer Kinder online zusätzlich zur Kindersicherung in Ihrer Sicherheitssoftware die McAfee Family Protection-Software. Die McAfee Family Protection trägt zum Schutz von Kindern aller Altersgruppen vor unangemessenen Inhalten, Risiken des Social Networking, unbekanntem Personen und anderen Online-Gefahren bei.

Natürlich sind diese Hilfsmittel nur begrenzt wirksam. Nichts kann bei der Beaufsichtigung von Kindern, die online sind, ein aufmerksames Elternteil ersetzen, das jederzeit ansprechbar ist.

Schritt 6



Schritt 7

Schritt 7

Machen Sie den Familienmitgliedern klar, dass Online-Bekanntschafte Fremde sind

Jeder, der im Internet unterwegs ist, muss sich über Folgendes im Klaren sein:

Egal, wie oft man mit Online-„Freunden“ chattet, egal, wie lange man schon miteinander chattet, und egal, wie gut man den anderen zu kennen glaubt, Personen, die man online kennen lernt, sind und bleiben Fremde. **Es ist ein Leichtes, online zu lügen und vorzugeben, jemand anderer zu sein.** Besonders Kindern muss klar sein, dass es sich bei einem neuen „Freund“ statt um einen Gleichaltrigen in Wirklichkeit um einen 40-jährigen Mann handeln kann.

Social Networking Websites wie Bebo, Orkut und Facebook sind ideal, um online neue Bekanntschaften zu machen. Aus diesem Grund müssen Sie diese Sites besuchen und **sich das Profil Ihrer Kinder ansehen**, um sicherzustellen, dass keine unangemessenen Gespräche geführt und keine unangemessenen Fotos veröffentlicht werden. Sie sollten ebenfalls die Instant Messaging-Aktivitäten ihrer Kinder überwachen, um sicherzustellen, dass sie nicht von Personen mit bösen Absichten belästigt werden.



Schritt 8

Erstellen Sie komplizierte Passwörter

Um zu gewährleisten, dass ein Kennwort schwer zu „knacken“ ist, sollte es mindestens 8 Zeichen umfassen und aus einer Kombination aus Buchstaben, Ziffern und Symbolen bestehen. **Kennwörter sollten in regelmäßigen Abständen geändert werden**, um die Wahrscheinlichkeit zu verringern, dass ein bestimmtes Kennwort im Lauf der Zeit geknackt wird.

Techniken für starke Kennwörter:

- Verwenden Sie ein so genanntes Vanity-Nummernschild: „GR8way2B“
- Verwenden Sie mehrere kurze Wörter und Interpunktionszeichen: “Bindi#the^jungle@girl”
- Setzen Sie Interpunktionszeichen in die Mitte eines Wortes: “Beck%ham”
- Kürzen Sie Worte auf ungewöhnliche Weise ab: “ftblplyr”
- Nehmen Sie den ersten Buchstaben jedes Wortes in einem Satz, mit einer beliebigen Zahl: „hard to crack this password“ = „htc5tp”
- Geben Sie Ihre Kennwörter nicht preis!

Schritt 8



Schritt 9

Schritt 9

Sicherheitssoftware des Computers prüfen

Öffnen Sie die Sicherheitssoftware, die Sie momentan installiert haben und vergewissern Sie sich, dass Ihr Computer durch folgende **drei Kernelemente geschützt ist: Anti-Viren-Software, Anti-Spyware und Firewall.**

Dieser essenzielle Schutz sollte durch Anti-Spam-Software und Software für sichere Suchvorgänge erweitert werden; empfehlenswert ist beispielsweise McAfee SiteAdvisor®, da diese Software vor Phishing-Angriffen schützt und Sicherheitsbewertungen vornimmt. Familien wird ebenfalls ans Herz gelegt, auf privat genutzten PCs eine Suite mit Schutzmaßnahmen zu installieren, die Dienstprogramme für die Kindersicherung, wie z.B. die McAfee Family Protection-Software, und zum Schutz vor Identitätsdiebstahl bieten.



Schritt 10

Bleiben Sie auf dem Laufenden

Je mehr Sie wissen, desto sicherer sind Sie. Im McAfee Security Advice Center finden Sie leicht verständliche und lehrreiche Informationen zum Schutz bei der Computernutzung und im Internet: www.mcafee.com/advice

Schritt 10



Das ABC der Online Sicherheit

für Kinder im Alter von
3-7 Jahren



A

Beim Gespräch mit kleinen Kindern

Wenn Sie mit kleinen Kindern über Sicherheit im Internet sprechen, sollte der Computer ausgeschaltet sein, damit Ihnen ihre ungeteilte Aufmerksamkeit sicher ist. Erklären Sie zunächst, dass ein Computer ein Werkzeug und das Internet wie eine riesige elektronische Bibliothek voller Informationen ist.

Erklären Sie, warum es wichtig ist, online keine Risiken einzugehen - der Computer kann wie eine offene Tür zu wichtigen persönlichen Daten sein. Erzählen Sie ihnen, wie böse Menschen die Kontrolle über den PC übernehmen und ihn kaputt machen können. Wenn das passiert, muss man einen neuen Computer kaufen.

Erklären Sie ihnen, warum es wichtig ist, unbekanntem Personen im Internet keine persönlichen Informationen mitzuteilen. Sagen Sie ihnen, dass sie keinesfalls ihren tatsächlichen Namen verwenden und nicht darüber sprechen sollen, wo sie leben bzw. in welche Schule sie gehen.



B

Spezielle Regeln für Eltern kleiner Kinder, die den PC nutzen

In dieser Liste sollten folgende Regeln enthalten sein:

- Ohne elterliche Erlaubnis keine Musik- oder Programmdateien von Websites herunterladen
- Nur überwachte Chatrooms besuchen, wo tatsächlich ein Erwachsener den Chat beaufsichtigt
- Erst mit den Eltern sprechen, bevor man ein Foto von sich versendet
- Keine Schimpfwörter usw. verwenden
- Keine Websites besuchen, die für Erwachsene bestimmt sind
- Nur mit Menschen Informationen austauschen, die aus dem echten Leben bekannt sind, etwa Klassenkameraden, Freunde und Familienmitglieder
- Ohne elterliche Unterstützung online keine Formulare ausfüllen oder sich an Umfragen beteiligen
- Nur spezielle Suchmaschinen für Kinder verwenden, beispielsweise Blinde Kuh und Kidsweb



C

Speziell für Kinder konzipierte Browser und Suchmaschinen verwenden

Stellen Sie sicher, dass Ihre Kinder Browser und Suchmaschinen verwenden, in denen keine unangemessenen Wörter oder Bilder angezeigt werden. Vergewissern Sie sich, dass sie mit sicheren Websites und vordefinierten Wortfiltern vorkonfiguriert sind. Sie müssen lediglich die standardmäßigen Websites und Wörter prüfen und genehmigen.

Wenn Ihre Kinder eine Standardsuchmaschine verwenden, aktivieren Sie unbedingt die Kindersicherungen in der Suchmaschine, um zu verhindern, dass bei den Suchergebnissen unangemessene Bilder und Inhalte angezeigt werden.



Das ABC der Online Sicherheit

für Kinder im Alter von
8-12 Jahren



A

Beim Gespräch mit Kids

Kids zwischen acht und zwölf sind heutzutage viel erfahrener als früher in dieser Altersgruppe. Im Englischen werden sie als „Tweens“ bezeichnet, also Kinder, die nicht mehr als „klein“ gelten, aber auch noch keine Teenager sind (abgeleitet von „between“ - „dazwischen“). Sie sollten sich im Klaren darüber sein, dass Kinder in diesem Alter im Umgang mit dem PC bereits recht routiniert sind, weil sie mit Computern daheim oder in der Schule aufgewachsen sind.

Vor dem Gespräch mit Kids müssen Sie einige Entscheidungen treffen, um der Internetnutzung Grenzen setzen zu können. Sie müssen die Regeln erst definieren, um klar vermitteln zu können, wie sie lauten. Deshalb sollten Sie die Antworten auf folgende Fragen kennen:

- Ist der Computer in einem Raum, der von allen Familienmitgliedern genutzt wird?
- Welche Websites können Kids ohne Bedenken besuchen?
- Wie lange sollten sie ins Internet dürfen?
- Was können sie im Internet machen?
- Mit wem dürfen sie kommunizieren?
- Wenn Sie nicht vorhaben, Ihre Kids zu überwachen, in welchen Fällen sollten sie sich zwecks Hilfe und Erlaubnis an Sie wenden?



Wenn Sie die Antworten darauf kennen, beginnen Sie das Gespräch. Erklären Sie Ihrem Kind (bei ausgeschaltetem Computer, damit Ihnen die ungeteilte Aufmerksamkeit sicher ist), dass ein Computer ein Werkzeug ist und es wichtig ist, online keine Risiken einzugehen.

Die folgenden Aspekte sollten unbedingt Teil des Gesprächs sein:

- Sprechen Sie über Viren, Spyware und Hacker
- Erklären Sie, wie Sexualstraftäter Kinder dazu bringen, über sich selbst zu reden
- Erklären Sie, warum es wichtig ist, online keine Risiken einzugehen - der Computer kann wie eine offene Tür zu wichtigen persönlichen Daten sein
- Erklären Sie, was Identitätsdiebstahl ist
- Sprechen Sie darüber, dass ein Computerexperte (wenn Sie selbst keiner sind) alles nachvollziehen kann, was auf einem Computer geschehen ist
- Gehen Sie darauf ein, dass Kriminelle die Kontrolle über den PC übernehmen und ihn kaputt machen können. Wenn das geschieht, muss ein neuer Computer angeschafft werden



B

Erinnern Sie Ihr Kind daran, dass es um Hilfe bittet, wenn es online auf beunruhigende Inhalte stößt

Machen Sie Ihren Kids eindringlich klar, dass sie es Ihnen sagen müssen, wenn sie beim Online-Chat eine seltsame oder beunruhigende Nachricht erhalten, und dass Sie in einem solchen Fall weder böse auf sie sind, noch ihnen die Nutzung des Internets verbieten. Ihrem Kind muss klar sein, dass Sie wissen, dass es keinen Einfluss darauf hat, was andere Menschen zu ihm sagen, und dass es keine Schuld trifft, wenn ein solcher Fall eintritt.

Vergewissern Sie sich zudem, dass Ihr Kind weder online belästigt wird noch andere belästigt. Wenn Schüler das Schulgelände verlassen, lassen Sie damit nicht unbedingt auch ihre Klassenkameraden und ihre Konflikte hinter sich. Mithilfe von Computern, Pagern und Handys können Schüler ständig miteinander in Kontakt sein. Diese Technologien werden unter Umständen dazu genutzt, andere zu belästigen, zu schikanieren oder ihnen anderweitig Schaden zuzufügen.



C

So blockiert man Benutzer und meldet Probleme

Wenn es mit Ihrem Kind online beim Chat zu einem Zwischenfall kommt, können Sie das Problem melden und den Anwender blockieren. Kopieren Sie zunächst die Chat-Nachrichten und fügen Sie den Text dann in ein Textverarbeitungsprogramm ein. Senden Sie die Kopie des Protokolls dann an den Moderator oder Administrator des Chat-Raums. Kontaktinformationen zum Moderator oder Administrator finden Sie in dem Abschnitt des Programms, der der Hilfe oder der Meldung gewidmet ist. Bei den meisten Chat-Programmen können Sie einen Anwender auch blockieren, indem sie mit der rechten Maustaste auf den Namen in der Kontaktliste klicken und die Funktion „Blockieren“ oder „Ignorieren“ wählen.



Das ABC der Online Sicherheit

für Jugendliche im Alter von
13-19 Jahren



A

Beim Gespräch mit Teenagern

Genau wie man Teenagern Sicherheit im Straßenverkehr beibringen muss, bevor sie Auto fahren, muss man ihnen Sicherheit im Internet beibringen, bevor man sie ohne Überwachung im Web surfen lässt.

Der Hauptunterschied zwischen dem Fahren eines Autos und der Navigation im Internet besteht darin, dass es im Internet keine richtigen „Verkehrsregeln“ gibt. Dies macht aus dem Internet eine Welt, die enorme Möglichkeiten bietet, aber zugleich zahlreiche Gefahren birgt. Um also Computerabstürze oder Schlimmeres zu vermeiden, müssen Sie Regeln aufstellen und für ihre Einhaltung sorgen. Ziel ist es hier, Teenagern beizubringen, sich auf ihren gesunden Menschenverstand zu verlassen und so Online-Gefahren zu meiden.



Sprechen Sie mit Ihrem Teenager darüber, warum es wichtig ist, online kein Risiko einzugehen.

Die folgenden Aspekte sollten unbedingt Teil des Gesprächs sein:

- Sprechen Sie über Viren, Spyware und Hacker und wie sie vorgehen
- Gehen Sie darauf ein, dass es Leute mit bösen Absichten gibt, die Jugendliche dazu bewegen, über sich zu sprechen
- Erklären Sie, warum es wichtig ist, online keine Risiken einzugehen - der Computer kann wie eine offene Tür zu wichtigen persönlichen Daten sein
- Erklären Sie, was Identitätsdiebstahl ist
- Sprechen Sie darüber, dass ein Computerexperte (wenn Sie selbst keiner sind) alles nachvollziehen kann, was auf einem Computer geschehen ist
- Gehen Sie darauf ein, dass Kriminelle die Kontrolle über den PC übernehmen und ihn kaputt machen können. Wenn das geschieht, muss ein neuer Computer angeschafft werden



B

Machen Sie dem Teenager bewusst, dass Personen, die er online kennen lernt, Fremde sind

Egal, wie oft sie mit ihnen chatten oder wie gut sie sie zu kennen glauben: Personen, die Teenager online kennen lernen, sind und bleiben Fremde. Menschen können hinsichtlich ihrer wahren Identität lügen, bei dem neuen „Freund“ eines Teenagers kann es sich statt um einen Gleichaltrigen in Wirklichkeit um jemand ganz anderen handeln.

C

Prüfen Sie das Profil des Teenagers auf den Social Networking Sites

Stellen Sie sicher, dass Ihre Kinder auf Seiten wie Bebo, Orkut oder Facebook nicht zu viele persönliche Informationen preisgeben. Vergewissern Sie sich, dass die Fotos, die sie veröffentlichen, nicht provokant sind. Machen Sie ihnen klar, dass sie möglicherweise das Interesse von Personen mit bösen Absichten auf sich ziehen. Sie können dadurch Freunde und Familie in Verlegenheit bringen, bei einer Bewerbung scheitern oder bei einem künftigen Arbeitgeber einen schlechten Eindruck hinterlassen.



Das ABC der Online Sicherheit

für Anfänger jeden Alters



Ihr Mann/Ihre Frau, Ihr Partner, Ihre Eltern, Ihre Schwiegereltern oder Ihre Großeltern hat/ haben vielleicht noch keine Erfahrung im Umgang mit Computer und Internet. Sie haben möglicherweise nur geringe Kenntnisse und könnten deshalb Opfer von Online-Betrug und Cyberangriffen werden. Sie benötigen also ein wenig Hilfestellung. Erklären Sie die Sicherheit im Netz folgendermaßen:

A

Viren, Spyware und Hacker

Suchen Sie die genaue Definition dieser Begriffe, dann werden Sie schnell und einfach im Internet oder im Glossar unter www.mcafee.com/advice (in englischer Sprache) fündig.



B

Risiko Identitätsdiebstahl und Phishing

Phishing heißt, Kriminelle fälschen die Website und E-Mail-Adresse eines seriösen Unternehmens und versuchen so, an Kennwörter und Kreditkartennummern zu gelangen. Überprüfen Sie auch Kreditkartenabrechnungen und Kontoauszüge regelmäßig.

C

Warum es wichtig ist, beim Herunterladen „kostenloser“ Software Vorsicht walten zu lassen

Rufen Sie den Nutzern den alten Grundsatz ins Gedächtnis, dass alles seinen Preis hat, auch wenn man nicht gleich bezahlen muss. Weisen Sie außerdem darauf hin, dass sie beim Herunterladen von Software neben der eigentlichen Anwendung auch Adware und Spyware „bekommen“ können.

Weitere Tipps und Ratschläge zur sicheren Nutzung von PC und Internet

Weitere Informationen und Ratschläge zur PC- und Internet-Sicherheit finden Sie im McAfee Security Advice Center auf www.mcafee.com/advice.

Über McAfee

McAfee (NYSE: MFE) ist einer der weltweit größten dedizierten Spezialisten für IT-Sicherheit. McAfee ist stets bestrebt, die weltweit größten Sicherheitsherausforderungen kompromisslos zu bewältigen. Das Unternehmen bietet präventive und bewährte Lösungen und Dienstleistungen an, die weltweit sowohl Systeme als auch Netzwerke schützen und Anwendern das sichere Surfen sowie Shoppen im Internet ermöglichen. Unterstützt von einer preisgekrönten Forschungsabteilung, entwickelt McAfee innovative Produkte, die Privatnutzern, Firmen und Behörden helfen, ihre Daten zu schützen, einschlägige Gesetze einzuhalten, Störungen zu verhindern, Schwachstellen zu ermitteln und die Sicherheit ihrer Systeme laufend zu überwachen und zu verbessern.

<http://www.mcafee.com/de>

McAfee GmbH Ohmstraße 185716 Unterschleißheim Deutschland Telefon: +49 (0)89 3707 0 www.mcafee.com/de

McAfee und/oder andere genannte McAfee-Produkte in diesem Dokument sind eingetragene Marken oder Marken von McAfee, Inc. und/oder seinen Niederlassungen in den USA und/oder anderen Ländern. McAfee Red in Verbindung mit Sicherheit kennzeichnet McAfee-Markenprodukte. Alle anderen nicht zu McAfee gehörenden Produkte sowie eingetragene und/oder nicht eingetragene Marken in diesem Dokument werden nur als Referenz genannt und sind Eigentum ihrer jeweiligen Rechtsinhaber.

© 2009 McAfee, Inc. Alle Rechte vorbehalten.