McAfee®

Protect What You Value

Ein Leitfaden für die ganze Familie über sicheres Surfen im Internet

Warum?

Die sorglose Zeit, als Leute das Internet lediglich zum Sammeln von Informationen und zum Verschicken von E-Mails benutzten, gehört der Vergangenheit an. Heutzutage erschaffen die meisten Internetnutzer komplette virtuelle Lebenswelten und bewegen sich darin. Millionen von Familien weltweit sind versiert im Umgang mit dem Internet und nutzen es unter anderem zum Lernen, Recherchieren oder Einkaufen, für Online-Banking und Geldanlagen, für Spiele oder zum Herunterladen von Videos und Musik sowie um alte Bekannte wiederzufinden oder neue Bekanntschaften zu knüpfen.

Doch obwohl das Netz eine aufregende virtuelle Welt ist, die unzählige Vorteile und neue Möglichkeiten bietet sowie vieles einfacher und bequemer macht, ist es auch eine immer gefährlichere Umgebung, in der fast jeden Tag neue Bedrohungen aufkommen.

Ebenso ist es unverzichtbar, mit Kindern und anderen unerfahrenen Familienmitgliedern über Internetsicherheit zu sprechen. Um ein solches Gespräch zu führen und Ihr Wissen über Online-Sicherheit mit Anderen zu teilen, müssen Sie beileibe kein Technik-Experte sein. Als Hilfe für ein solches Gespräch haben wir Ihnen im Folgenden einen schrittweise aufgebauten und für die jeweilige Altersklasse geeigneten Leitfaden erstellt.

Die Bedrohungslage im Internet

Das Risiko, dass Sie Opfer eines Internetverbrechens werden könnten, liegt bei etwa 25 %.

Im Durchschnitt wird ein PC mit Internetanschluss alle 39 Sekunden von Hackern angegriffen.

Hacker-Angriffe

- Laut McAfee® Avert® Labs sind mittlerweile 222.000 bekannte Computerviren im Umlauf, und die Bedrohungen werden täglich mehr.
- Jeder fünfte Internetnutzer in den USA hatte bereits ein ernsthaftes, in vielen Fällen kostspieliges Virenproblem.
- Virusinfektionen haben bei 1,8 Millionen Haushalten in den letzten zwei Jahren zur Anschaffung eines neuen PC geführt.
- 83 % aller Teenager laden Musik herunter; 64 % nutzen illegale Seiten; „digital music“ ist einer der gefährlichsten Suchbegriffe im Internet.

Identitätsdiebstahl

- Im letzten Jahr (2006) sind in den USA 8,9 Millionen Menschen Opfer von Identitätsdiebstahl geworden.
- Der durchschnittliche Verlust für jedes Opfer ist dabei 2006 mehr als doppelt so hoch gewesen wie im Vorjahr.
- Die Anzahl einzelner Phishing-Webseiten ist im April 2007 gegenüber dem Vormonat um 35.000 auf 55.643 hochgeschnellt.

Sittliche Bedrohungen

- 71 % der Jugendlichen zwischen 13 und 17 Jahren haben schon einmal Nachrichten von Leuten erhalten, die sie nicht kannten.
- Die Bedrohungen beim Instant Messaging (IM) haben 2007 im Vergleich zu 2006 um 79 % zugenommen.
- 32 % der 13- bis 17-Jährigen sagten aus, dass sie normalerweise niemandem von Online-Nachrichten erzählen, die sie von Unbekannten erhalten haben.

Ein Leitfaden zum sicheren Surfen im Internet für kleine Kinder

Schritt 1. Sprechen Sie mit Ihrem Kind

- Lassen Sie den Computer ausgeschaltet, so dass Sie die ungeteilte Aufmerksamkeit Ihrer Kinder haben, und erklären Sie ihnen, dass der Computer ein Werkzeug ist und dass man sich das Internet wie eine riesige elektronische Bücherei voller Informationen vorstellen kann.
- Erklären Sie ihnen, dass es wichtig ist, sich im Internet zu schützen, weil der Computer ungeschützten Zugang zu wichtigen persönlichen Informationen bieten kann. Sprechen Sie darüber, dass böse Menschen die Kontrolle über den PC an sich reißen und ihn unbrauchbar machen können, so dass Sie ein neues Gerät kaufen müssen.
- Erklären Sie ihnen, warum es wichtig ist, unbekannten Personen im Internet keine persönlichen Informationen mitzuteilen. Schärfen Sie ihnen ein, nicht ihren echten Namen zu benutzen und nicht darüber zu sprechen, wo sie wohnen und auf welche Schule sie gehen.

Schritt 2. Stellen Sie zusammen mit dem Kind/den Kindern eine Liste mit Regeln auf

In dieser Liste sollten folgende Regeln enthalten sein:

- Ohne Erlaubnis der Eltern keine Musik- oder Programmdateien aus dem Internet herunterladen
- Nur beaufsichtigte Chaträume wie Disney's Virtual Magic Kingdom (oder in Deutschland den Kinderseiten-Chat von Seitenstark oder den „Schwatzraum") aufsuchen, wo Erwachsene den Chat überwachen. Ein Filter gegen grobe oder vulgäre Sprache reicht nicht aus.
- Keine Benutzernamen verwenden, die Rückschlüsse auf die echte Identität zulassen
- Niemandem die Passwörter verraten
- Niemals die eigene Telefonnummer oder Adresse nennen
- Niemals ohne Erlaubnis der Eltern ein Foto von einem selbst verschicken
- Keine grobe oder vulgäre Sprache benutzen
- Niemals Webseiten für Erwachsene ansehen
- Nur mit Menschen Informationen austauschen, die aus dem echten Leben bekannt sind, etwa Klassenkameraden, Freunde und Familienmitglieder
- Niemals ohne Hilfe der Eltern Online-Formulare ausfüllen oder an Umfragen teilnehmen
- Niemals Internet-Bekanntschaften persönlich treffen
- E-Mails und Instant Messages von Unbekannten ignorieren
- Den Computer immer abschalten, wenn er nicht verwendet wird
- Nur spezielle Suchmaschinen für Kinder wie Ask for Kids und Yahooligans (oder in Deutschland Blinde Kuh oder Trampeltier) benutzen.

Schritt 3. Überwachen Sie die Internetnutzung Ihrer Kinder

Positionieren Sie den Computer an einer Stelle, an der möglichst häufig Familienmitglieder vorbeikommen, und schränken Sie seine Nutzung ein. Ziehen Sie neben den Kindersicherungseinrichtungen, die Sie zum Beispiel in Sicherheitssoftware von McAfee® vorfinden, auch die Verwendung einer speziellen Überwachungssoftware für Kinder im Internet wie IMSafer™ in Betracht. Laden Sie sich ein Programm herunter, das vor gefährlichen Webseiten schützt und entsprechende Warnungen ausgibt. McAfee SiteAdvisor™ zum Beispiel bewertet Webseiten anhand von intuitiv verständlichen Signalen (Rot, Gelb, Grün).

Schritt 4. Verwenden Sie kindgerechte Browser und Suchmaschinen

Stellen Sie sicher, dass Ihre Kinder Browser verwenden, die anstößige Worte oder Bilder nicht darstellen. Bei diesen Browsern sind kindersichere Webseiten bereits geladen und Wortfilter voreingestellt. Sie müssen die Standard-Webseiten und Begriffe nur überprüfen und genehmigen.

Schritt 5. Sichern Sie Ihren Computer mit leistungsfähiger Sicherheitssoftware ab

Stellen Sie sicher, dass Sie über zuverlässige Sicherheitssoftware zum Schutz gegen Viren, Hacker und Spyware verfügen. Die Software sollte auch anstößige Inhalte, Bilder und Webseiten filtern. Sie muss häufig auf den neuesten Stand gebracht werden, weil jeden Tag neue Bedrohungen hinzukommen. Die beste Wahl ist Software, die sich nach einmaliger Einrichtung immer automatisch selbst aktualisiert.

Schritt 6. Aktivieren Sie die Kindersicherung des Computers

Alle führenden Anbieter von Sicherheitssoftware bieten auch eine Kindersicherung an. Diese sollten Sie unbedingt benutzen. (Wenn Sie Freeware oder sonstige Software einsetzen, die keinerlei Kindersicherung bietet, erwägen Sie bitte die Anschaffung einer entsprechenden Software.) Lesen Sie das Handbuch in Ruhe durch und nutzen Sie die zur Verfügung stehenden Kindersicherungsmaßnahmen.

Die Kindersicherung einer Sicherheitssoftware sollte die folgenden Möglichkeiten bieten:

- Schutz der Kinder vor gefährlichen Websites
- Begrenzung der Zeit im Internet
- Filterung von Schlüsselwörtern
- Blockierung von möglicherweise ungeeigneten Bildern

Ein Leitfaden zum sicheren Surfen im Internet für Jugendliche

Schritt 1. Sprechen Sie mit Ihrem Kind

Genau wie Ihre Kinder zunächst etwas über Sicherheit im Straßenverkehr lernen müssen, bevor sie ein Auto fahren dürfen, müssen Sie ihnen auch etwas über Sicherheit im Netz beibringen, bevor Sie sie unbeaufsichtigt im Internet surfen lassen. Wenn man sich nach der ursprünglichen und heute etwas angestaubten Beschreibung des Internet als „Datenautobahn" richtet und bei dieser Auto-Metapher bleibt, dann ist es leicht einzusehen, dass es nur vernünftig ist, Ihren Teenagern etwas über sicheres, defensives Fahren beizubringen, bevor Sie sie ans Steuer eines Computerboliden lassen.

Bevor Sie einem neugierigen, aber unerfahrenen Jugendlichen das Kommando über Maus und Keyboard übergeben, möchten Sie sich sicherlich darauf verlassen können, dass dieser versteht, worauf er achten muss und welche „Verkehrsregeln" gelten. Ein großer Unterschied zwischen der ersten Autofahrt und der ersten Reise ins Internet besteht darin, dass im Netz keine festen Regeln gelten. Dies macht aus dem Internet eine Welt, die enorme Möglichkeiten bietet, aber zugleich zahlreiche Gefahren birgt. Um einen „Crash" oder Schlimmeres zu vermeiden, müssen Sie also Regeln aufstellen und dafür sorgen, dass sie auch eingehalten werden. Hierbei liegt das Ziel darin, Teenagern gesunden Menschenverstand beizubringen, damit Sie im Netz selbständig Gefahren aus dem Weg gehen können.

Übrigens, sollten Sie auf den irrigen Gedanken kommen, Ihren Kindern den Zugang zum Internet verwehren zu wollen, dann erreichen Sie damit nur, dass diese von ihrem Umfeld unter Druck gesetzt und gesellschaftlich isoliert werden – nur um dann hinter Ihrem Rücken doch heimlich online zu gehen.

Sprechen Sie mit Ihren Kindern darüber, warum es wichtig ist, sich im Internet zu schützen. 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, dass es wichtig ist, sich im Internet zu schützen, weil der Computer ungeschützten Zugang zu wichtigen persönlichen Informationen bieten kann.
- Besprechen Sie, wie Identitätsdiebstahl vor sich geht.
- Sprechen Sie darüber, dass ein Computerexperte (wenn Sie selbst keiner sind) alles nachvollziehen kann, was auf einem Computer geschehen ist.
- Sprechen Sie darüber, dass Kriminelle die Kontrolle über den PC an sich reißen und ihn unbrauchbar machen können, so dass Sie ein neues Gerät kaufen müssen.

Besprechen Sie mit Ihrem Kind genau, was in Bezug auf die folgenden Fragen in Ordnung ist und was nicht:

- Welche Webseiten sind geeignet?
- Welche Chaträume dürfen besucht werden?
    - Nur beaufsichtigte Chaträume aufsuchen
    - Meiden Sie „.alt"-Chaträume – sie konzentrieren sich auf öfter auf Themen, die für Jugendliche eventuell nicht geeignet sind.
- Welche Themen sind im Chat tabu?

Schritt 2. Überwachen Sie die Internetnutzung Ihrer Kinder

Positionieren Sie den Computer an einer Stelle, an der möglichst häufig Familienmitglieder vorbeikommen, und schränken Sie seine Nutzung ein. Ziehen Sie neben den Kindersicherungseinrichtungen, die Sie zum Beispiel in Sicherheitssoftware von McAfee® vorfinden, auch die Verwendung einer speziellen Überwachungssoftware für Kinder im Internet wie IMSafer™ in Betracht. Laden Sie sich ein Programm herunter, das vor gefährlichen Webseiten schützt und entsprechende Warnungen ausgibt. McAfee SiteAdvisorTM zum Beispiel bewertet Webseiten anhand von intuitiv verständlichen Signalen (Rot, Gelb, Grün).

Schritt 3. Sichern Sie Ihren Computer mit leistungsfähiger Sicherheitssoftware ab

Stellen Sie sicher, dass Sie über zuverlässige Sicherheitssoftware zum Schutz gegen Viren, Hacker und Spyware verfügen. Die Software sollte auch anstößige Inhalte, Bilder und Webseiten filtern. Sie muss häufig auf den neuesten Stand gebracht werden, weil jeden Tag neue Bedrohungen hinzukommen. Die beste Wahl ist Software, die sich nach einmaliger Einstellung immer automatisch selbst aktualisiert.

Schritt 4. Aktivieren Sie die Kindersicherung des Computers

Alle führenden Anbieter von Sicherheitssoftware bieten auch eine Kindersicherung an. Diese sollten Sie unbedingt benutzen. (Wenn Sie Freeware oder sonstige Software einsetzen, die keinerlei Kindersicherung bietet, erwägen Sie bitte die Anschaffung einer entsprechenden Software.) Lesen Sie das Handbuch in Ruhe durch und nutzen Sie die zur Verfügung stehenden Kindersicherungsmaßnahmen.

Die Kindersicherung einer Sicherheitssoftware sollte die folgenden Möglichkeiten bieten:

- Schutz der Kinder vor gefährlichen Websites
- Begrenzung der Zeit im Internet
- Filterung von Schlüsselwörtern
- Blockierung von möglicherweise ungeeigneten Bildern

Neben Internetkriminalität sollten Sie auch ein Auge auf Belästigungen im Internet haben. Wenn Schüler das Schulgelände verlassen, lassen Sie damit nicht unbedingt auch ihre Klassenkameraden und ihre Konflikte hinter sich. Mit Computern, Pager-Meldungen und Handys können Schüler jederzeit in Verbindung bleiben und diese Technologie auch nutzen, um Andere zu belästigen, zu schikanieren und zu verletzen.

Auch wenn noch kein Anbieter von Sicherheitssoftware über ein Produkt verfügt, mit dem sich solche Belästigungen komplett aus der Welt schaffen lassen, bietet ein Großteil der Sicherheitssoftware den Eltern zumindest einige Hilfsmittel, mit denen sie das Problem abschwächen können. Software von führenden Sicherheitsanbietern wie McAfee kann bei Online-Belästigungen helfen, indem sie den Eltern die folgenden Maßnahmen ermöglicht: (1) Begrenzung der Zeit, die das Kind im Internet verbringen darf; (2) Blockieren des Zugriffs auf anstößige Webseiten; und (3) Herausfiltern von grober oder vulgärer Sprache.

Natürlich sind diese Hilfsmittel nur begrenzt wirksam. Aufmerksame und verantwortungsbewusste Eltern, die einschreiten, wenn ihr Kind online oder offline belästigt wird, sind durch nichts zu ersetzen. Gleichermaßen sollten Sie darauf achten, dass Ihr Kind nicht seinerseits andere Kinder belästigt.

Schritt 5. Erinnern Sie Ihr Kind daran, dass Leute in Chaträumen immer Fremde sind

Egal wie oft Ihre Kinder mit Anderen chatten und egal, wie gut sie ihre Chatpartner zu kennen glauben, Online-Bekanntschaften sind Fremde. Personen können falsche Angaben über sich machen, und der neue Freund Ihres Kindes könnte eventuell ein 40-jähriger Mann statt eines 13-jährigen Mädchens sein.

Schritt 6. Lernen Sie, wie Chat-Sitzungsprotokolle gespeichert, Anwender blockiert und Probleme gemeldet werden.

Sie können Sitzungen speichern, indem Sie den Nachrichtentext kopieren und in ein Textverarbeitungsprogramm einfügen. Bei den meisten Chat-Programmen können Sie einen Anwender blockieren, indem sie mit der rechten Maustaste auf dessen Namen in Ihrer Kontaktliste klicken und die Funktion „Blockieren“ oder „Ignorieren“ wählen. Wenn Ihr Kind mit einem anderen Chat-Teilnehmer ein Problem hat, senden Sie das kopierte Protokoll an den Chatroom-Moderator oder -Administrator. Die Kontaktinformationen finden Sie im Hilfe- oder Berichtsabschnitt des Programms.

Schritt 7. Überprüfen Sie alle Profile, die Ihr Kind bei Social Networking Seiten eingetragen hat

Stellen Sie sicher, dass Ihre Kinder auf Seiten wie MySpace oder Facebook nicht zu viele persönliche Informationen preisgeben. Achten Sie auch darauf, dass sie keine provokanten oder allzu freizügigen Bilder einstellen, die Aufmerksamkeit erregen oder einen schlechten Eindruck bei potentiellen späteren Arbeitgebern machen könnten.

Ein Leitfaden zum sicheren Surfen im Internet für Neulinge im Netz

Ihre Ehegatten, Partner, Eltern oder Großeltern sind vielleicht schon älter, aber auch sie interessieren sich sicherlich für das Internet - aus den gleichen Gründen wie Sie. Allerdings sind sie unter Umständen nicht sehr computererfahren und könnten daher leicht Betrügereien und Angriffen im Internet zum Opfer fallen. Sie werden ein bisschen Hilfestellung benötigen und Ihr Gespräch über Sicherheit im Internet sollte sich an folgenden Schritten orientieren:

Schritt 1.

Sprechen Sie über Viren, Spyware und Hacker (gute Definitionen für diese Begriffe sind leicht per Online-Recherche zu finden, oder im Glossar auf www.mcafee.com/advice).

Schritt 2.

Stellen Sie sicher, dass Sie über zuverlässige Sicherheitssoftware zum Schutz gegen Viren, Hacker und Spyware verfügen. Die Software sollte auch anstößige Inhalte, Bilder und Webseiten filtern. Sie muss häufig auf den neuesten Stand gebracht werden, weil jeden Tag neue Bedrohungen hinzukommen. Die beste Wahl ist Software, die sich nach einmaliger Einrichtung immer automatisch selbst aktualisiert.

Schritt 3.

Sprechen Sie über das Risiko von Identitätsdiebstahl und darüber, wie Phishing funktioniert. Unter Umständen empfiehlt es sich, ein Programm zur Überwachung von Kreditauskünften wie Experian Triple AdvantageSM zu abonnieren. Überprüfen Sie auch Kreditkartenabrechnungen und Kontoauszüge regelmäßig.

Schritt 4.

Gehen Sie sorgfältig auf „kostenlose“ Downloads ein. Erinnern Sie Ihre Partner oder Angehörigen an das alte Sprichwort, dass alles seinen Preis hat, auch wenn es kostenlos ist! Beim Softwaredownload zum Beispiel gelangt schnell unerwünschte Adware oder Spyware auf den Rechner.

Schritt 5.

Achten Sie darauf, dass Passwörter auch genug Sicherheit bieten. Ein gutes Passwort ist mindestens 8 Zeichen lang und besteht aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen. Auch müssen Passwörter regelmäßig geändert werden, um die Wahrscheinlichkeit zu verringern, dass eines davon nach einer Zeit geknackt wird.

Schritt 6.

Stellen Sie sicher, dass die internen Sicherheitsvorkehrungen Ihres Computers aktiviert sind.

Schritt 7.

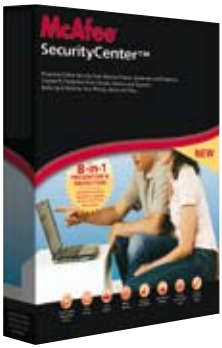
Installieren Sie zuverlässige Sicherheitssoftware, die integrierte Antiviren-, Antispyware-, Antiphishing- und Firewall-Technologien umfasst.

Schritt 8.

Schauen Sie sich im McAfee Advice Center nach Lerninhalten zum Thema Computer- und Internetsicherheit um: www.mcafee.com/advice.

McAfee® SecurityCenter™

Präventiver Online-Schutz für Ihre Familie



Die McAfee SecurityCenter ist ein präventives 8-in-1 Sicherheitspaket, das ständig aktualisiert wird und das schützt, was Sie schätzen. Mit Kinderschutz für mehrere Nutzer, Schutz vor Identitätsdiebstahl, E-Mail- und IM-Schutz sowie automatischem Backup. Es bietet Ihnen Sicherheit beim Surfen im Netz, beim Einkaufen, bei der Erledigung von Bankgeschäften, beim Chatten und beim Herunterladen von Dateien.

Weitere Gründe, warum Sie als Dell-Kunde McAfee kaufen sollten

Vorinstalliert: McAfee SecurityCenter wird von Dell-Technikern vor der Auslieferung der Computer vollständig installiert. Eine weitere Konfiguration ist nicht erforderlich, der Schutz steht Ihnen unmittelbar zur Verfügung.

Regelmäßige Aktualisierungen und Updates - jeden Tag. McAfee® Avert® Labs, das Weltklasse-Forschungszentrum von McAfee, liefert Ihnen rund um die Uhr Updates und Schutz vor Angriffen. Während der Abo-Laufzeit erhalten Sie kostenlos Software-Upgrades und Erweiterungen.

Regelmäßige Aktualisierungen und Updates - jeden Tag. McAfee® Avert® Labs, das Weltklasse-Forschungszentrum von McAfee, liefert Ihnen rund um die Uhr Updates und Schutz vor Angriffen. Während der Abo-Laufzeit erhalten Sie kostenlos Software-Upgrades und Erweiterungen.

Für mehr Informationen Besuch: www.dell.com

McAfee GmbH, Ohmstr. 1, 85716 Unterschleißheim, 089-3707 0, www.mcafee.de