



Wie schütze ich mein Kind vor den Gefahren im Internet?



Wie schütze ich mein Kind vor den Gefahren im Internet? Wie bewahre ich den Familien- oder Kinder-PC effektiv vor Angriffen? Das "Sicher-Stark-Team" gibt Grundinformationen für Eltern, Sorgeberechtigte, Betreuer oder Erzieher von Grundschulkindern:

Virenschutzprogramm

Das A und O, auf das Sie keinesfalls verzichten dürfen, ist ein Virenschutzprogramm. Es sollte immer im Hintergrund mitlaufen. Mit dem Programm können Sie auch gezielt Dateien/Downloads/Anhänge vor dem Öffnen auf Viren scannen. Kostenpflichtige Programme bieten mehr Funktionen als kostenlose, sind aber nicht unbedingt besser. Bei neu gekauften Computern sind meist Testversionen solcher Programme vorinstalliert und müssen später gekauft werden. Wenn Sie mit ihnen nicht zurechtkommen, treffen Sie lieber Ihre eigene Wahl im Vorfeld.

Zusätzliche Schutzsoftware, z. B. gegen Spyware, Malware, Adware. Sie hat den Vorteil, dass die Programme auf die jeweilige Schadsoftware spezialisiert ist, jedoch den Nachteil, dass sich verschiedene Schutzprogramme gegenseitig stören können. Gelegentliches Verfolgen von Neuheiten auf Seiten wie Computerbild.de oder chip.de helfen, den Überblick zu behalten.

Verwenden Sie für den Download, insbesondere von Gratisprogrammen, immer seriöse Seiten, um nicht Ihr System zu schädigen. Eine Auswahl von Seiten bietet kostenlose Firewall- und Port-Checks.

Welche Arten von Schadsoftware gibt es und welche Aktionen sind besonders gefährlich?

Malware, Trojaner sind bösartige Programme, getarnt als harmlose Software. Sie werden zumeist durch E-Mail-Anhänge und Webdownloads verbreitet und installieren sich ohne Ihr Wissen auf dem PC. Sie können Dateien verwalten, neue erzeugen, löschen, umbenennen, aufrufen, verschieben oder senden. Trojaner können ein Programm installieren, das es zum Beispiel Hackern erlaubt, Software zu installieren, auszuführen, zu öffnen oder zu schließen oder volle Kontrolle über den infizierten Rechner zu erhalten.

Würmer

Die meisten Infektionen erfolgen über E-Mail. Startet man eine angehängte Datei, wird der Wurm aktiviert und verbreitet sich anschließend selbst weiter. Bei Outlook und Outlook Express von Microsoft ist es sogar möglich, die verseuchten E-Mails ohne Wissen des Benutzers an Personen aus dem Adressbuch zu versenden. Weil die Empfänger den Absender der E-Mail kennen, geraten sie in Versuchung, den Anhang zu öffnen, und der Wurm pflanzt sich fort. Würmer infizieren jedoch keinen fremden Code, um sich fortzupflanzen. Viren versuchen, eine normale Programmdatei, z. B. eine Word-Datei, zu infizieren, indem sie dem normalen Programmcode ihren eigenen hinzufügen. Das heißt, das Programm hat nun zusätzliche Vireneigenschaften. Es ist der "Wirt".

Da Computerprogramme nicht wie biologische Zellen leben, kann sich ein Virus nur dann vermehren, wenn das Programm gestartet wird. Es dauert nicht lange und schon bald sind alle Ihre Dateien mit dem Virus infiziert. Der Melissa-Virus löschte beispielsweise MP3-Dateien. Spyware ist eine bösartige Software, die ohne Ihr Einverständnis zum Beispiel Werbung auf dem Kinder-PC anzeigt, persönliche Daten erfasst oder Einstellungen am Kindercomputer verändert. Adware sollte nicht damit verwechselt werden. Nicht jede Software ist schädlich, die Werbung aufruft. Beispielsweise kann Ihr Kind sich für einen kostenlosen Musikdienst anmelden, für den Sie durch das Akzeptieren von gezielter Werbung "bezahlen". Andere Spyware-Varianten nehmen Änderungen an Computern vor, die lästig sein und PCs verlangsamen oder gar zum Absturz bringen können.

Pharming ist das neue Phishing: mit Hilfe betrügerischer Software wird Ihr Browser trotz korrekter URL auf eine falsche Seite umgeleitet, ohne dass Sie das merken. So können zum Beispiel beim Online-Banking Ihre PIN und TAN in die Hände von Kriminellen gelangen – obwohl Sie die Adresse Ihrer Bank manuell eingetippt haben. Auch Sicherheits-Zertifikate von Internetseiten können manipuliert sein und Sie so "umleiten".

Wie schaffe ich für mein Kind einen sicheren Raum zum Surfen?

Das Familienministerium des Bundes fördert seit Februar 2013 die Einrichtung eines Kinderservers. Unterhalten wird dieser von namhaften Kinderseitenbetreibern, Jugendschutzverbänden und dem Verband der deutschen Internetwirtschaft. Nähere Informationen und Anleitungen sind unter www.kinderserver-info.de/die-ag-kinderserver abrufbar.

Bieten Sie Ihrem Kind interessante und sichere Seiten zum Surfen an. Kinderbrowser, Kindersuchmaschinen, Kinderchats und -foren, Freundebücher – es gibt Vieles im Netz zu entdecken. Gute Anbieter wie seitenstark.de, fragfinn.de und blindekuh.de halten viele kindergeeignete Inhalte bereit und verlinken nur auf sichere Unterseiten.

Mit den richtigen Überwachungseinstellungen in Ihrem Jugendschutzprogramm steuern Sie Zeit und Zugriffsmöglichkeiten Ihres Kindes beim Surfen, ohne dass Sie immer dabeisitzen müssen. Nehmen Sie jedoch trotzdem so viel wie möglich Anteil an den Erfahrungen Ihres Kindes im Netz und seien Sie der erste Ansprechpartner, wenn Fragen oder Probleme auftreten.

Ralf Schmitz ist Buchautor und führender Experte in der Gewaltprävention für die Primarstufen. Er wird für Vorträge und als Seminarleiter gebucht und arbeitet seit Jahren für das Sicher-Stark-Team.

Die Zielsetzung

Das Sicher-Stark-Team möchte helfen, mit präventiven Sicher-Stark-Kursen, Vorträgen und Webinaren Kinder vor Gewalt und Missbrauch zu schützen. Das Sicher-Stark-Team verfügt über ein hochkarätiges Expertenteam mit über 15-jähriger Erfahrung. Es wurden eine halbe Million Kinder mit dem Sicher-Stark-Konzept in den Jahren bereits geschult. Gegen alle diese Gefahren können Sie sich mit den Sicher-Stark-DVD-Serie (3 DVDs) und den Schutzprogrammen wirkungsvoll schützen.

Weitere Informationen unter

- www.sicher-stark-team.de
- E-Mail info@sicher-stark.de
- Bundesweite Servicenummer: 01 80/55 50 13 33
<http://www.hamburg-magazin.de/hamburg-fuer/kinder-familien/artikel/detail/wie-schuetze-ich-mein-kind-vor-den-gefahren-im-internet.html>