IT-Basisschutz für Kinder und Jugendliche

Zum Familienleben gehören digitale Medien inzwischen selbstverständlich dazu. Computer, Laptop, Spielekonsole, Smart Speaker und vor allem mobile Geräte wie Smartphone und Tablet sind in den meisten Haushalten präsent, häufig sogar Teil des Alltags und werden bereits von den Jüngsten gerne genutzt. Die meisten dieser Geräte bieten einen einfachen und nahezu unbegrenzten Zugang zum Internet. Viele Kinder nutzen digitale Medien oftmals alleine – ohne entsprechende Einstellungen birgt dies Gefahren und Sicherheitsrisiken. In modernen Betriebssystemen sind Basis-Kindersicherungen meist integriert, müssen aber erst aktiviert und an die jeweiligen Bedürfnisse angepasst werden.

8 Tipps für den digitalen Familienalltag

Wer Kinder und Jugendliche begleitet, steht vor der Herausforderung, den bewussten Umgang mit digitalen Medien zu fördern und eine sichere Online-Umgebung zu schaffen. Dazu gehören auch technische Schutzmaßnahmen, um sie online vor potenziellen Gefahren zu schützen. Mit folgenden Basistipps legen Sie den Grundstein für einen sicheren digitalen Familienalltag.

Disclaimer: Kinderschutz ist grundsätzlich auf allen Geräten möglich, die von Kindern genutzt werden. Dazu zählen neben PC und Laptop, worauf sich dieser Wegweiser fokussiert, auch Smartphones, Tablets, Spielekonsolen, smarte Kinderuhren und smartes Spielzeug.

1. Richten Sie ein eigenes Benutzerkonto für Kinder ein
2. Nutzen Sie ein Virenschutzprogramm
3. Überprüfen Sie die Firewall
4. Nutzen Sie einen Router mit Kinderschutzfunktionen
5. Verwenden Sie eine Suchmaschine für Kinder
6. Legen Sie Zeitbeschränkungen fest
7. Sensibilisieren Sie frühzeitig für wirksamen Accountschutz
8. Sprechen Sie regelmäßig offen über Gefahren im Internet sowie über Schutzmaßnahmen

Tipps für den digitalen Familienalltag

Für PC und Laptop

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Schon gewusst?

Kinder und Jugendliche haben ein Recht auf Privatsphäre

Viele moderne Betriebssysteme bieten einige integrierte Kindersicherungsfunktionen, die an die jeweiligen Bedürfnisse angepasst werden können. Zudem gibt es eine große Auswahl an zusätzlichen Kinderschutzprogrammen von Drittanbietern.

Diese Funktionen und Programme ermöglichen es Eltern, den Zugriff auf bestimmte Websites, Apps und Inhalte zu beschränken und auch die Onlineaktivitäten ihrer Kinder zu kontrollieren. Aber auch Kinder und Jugendliche haben nach Artikel 16 UN-Kinderrechtskonvention ein Recht auf Privatsphäre. Passen Sie die Kinderschutzsoftware an das Alter des Kindes an, informieren Sie es über die hinterlegten Einstellungen und halten Sie ein angemessenes Maß zwischen Privatsphäre und technischen Schutzmaßnahmen.

Weiterführende Informationen und Anleitungen

Weitere Informationen

Risiken und Schutzmaßnahmen - Kinder im Internet

Eltern-Kind-Gespräch

Schritt für Schritt zu Jugendschutzeinstellungen bei Apps, Spielen & Co.

Impressum

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 87, 53175 Bonn

Kontakt:
E-Mail: service-center@bsi.bund.de
Internet: www.bsi.bund.de
Service-Center: +49 (0) 800 274 1000

Artikelnummer:
BSI-IFB 23/253

1. Richten Sie ein eigenes Benutzerkonto für Kinder ein

Ganz gleich, ob Familienrechner oder eigenes Gerät – legen Sie ein eigenes Benutzerkonto mit „Kindersicherung“ bzw. eingeschränkten Zugriffsrechten für Kinder an.

Die Einrichtung eines separaten **Benutzerkontos ohne Administratorenrechte** am PC ist ein erster wichtiger Schritt. In den **Einstellungen** des Computers können Sie unter **Konto** einen **Benutzer hinzufügen**. Durch die Einrichtung eines separaten Kinderkontos beschränken Sie zum Beispiel den Zugriff auf sensible Daten und Einstellungen des Hauptkontos. Dadurch wird beispielswiese verhindert, dass sich Schadsoftware Administratorberechtigungen zunutze macht und Dateien im System infiziert oder beschädigt.

2. Nutzen Sie ein Virenschutzprogramm

Eine Antivirensoftware überprüft neue Dateien (zum Beispiel Anhänge von E-Mails oder Downloads von Spieledateien) und den gesamten Computer auf Anzeichen einer Infektion.

Eine zuverlässige **Virenschutzsoftware** ist in der digitalen Welt, in der Bedrohungen durch Schadsoftware ständig präsent sind, ein unverzichtbarer Schutz. Unsichere Downloads, z. B. von Spielen, können schädliche Software auf dem Computer des Kindes installieren.
Ein Virenschutzprogramm erkennt und blockiert Malware und Sicherheitsbedrohungen. In den meisten Betriebssystemen ist bereits ein Virenschutzprogramm integriert. **Aktivieren** Sie die **Software** in den **Sicherheitseinstellungen** des Computers und halten Sie diese mit **automatischen Updates** auf dem neuesten Stand.

3. Überprüfen Sie die Firewall

Die Firewall schützt den Computer vor Angriffen von außen. Dazu kontrolliert sie alle Verbindungen in andere Netzwerke und überprüft sowohl die Anfragen ins Internet als auch die Daten, die an den Rechner gesendet werden.

Die meisten Betriebssysteme verfügen über eine integrierte **Firewall**. Überprüfen Sie unbedingt in den **Einstellungen** des Systems, dass diese **aktiviert** ist. Falls nicht, aktivieren Sie die Firewall und passen Sie diese auf Ihre individuellen Bedürfnisse an, um das eigene System und das der Kinder vor unbefugten Zugriffen und potenziellen Gefahren von außen zu schützen. Die Firewall können Sie außerdem zum Beispiel so konfigurieren, dass nur bestimmte Programme und Anwendungen auf das Internet zugreifen können. Dadurch wird das Risiko minimiert, dass Kinder schädliche Anwendungen, Programme oder Spiele herunterladen.

4. Nutzen Sie einen Router mit Kinderschutzfunktionen

Manche Router bieten verschiedene Einstellungsmöglichkeiten zur Kindersicherung, mit denen das Heimnetzwerk kindersicher eingerichtet werden kann.

Mit modernen **Routern** lässt sich der Internetzugang für alle Geräte, die im **Heimnetzwerk** angemeldet sind, einzeln regeln. Jedem Gerät wird dafür über den Router ein **Zugangsprofil** zugewiesen, in dem zum Beispiel die Online-Zeit begrenzt, Netzwerkanwendungen freigegeben bzw. beschränkt oder bestimmte Internetseiten gesperrt werden können. Die Einstellungen können bei allen Geräten der Kinder vorgenommen werden, während die Geräte der Eltern den vollen Zugriff behalten. Sichern Sie Ihr drahtloses Netzwerk zudem mit einem **starken Passwort**, um unbefugten Zugriff zu verhindern und die **Kontrolle** darüber zu behalten, wer auf das Internet zugreifen kann.

5. Verwenden Sie eine Suchmaschine für Kinder

Es gibt spezielle Suchmaschinen und Webbrowser für Kinder, die altersgerechte Suchergebnisse und einen begrenzten Zugriff auf Webseiten bieten.

Um Kinder bei der sicheren Online-Suche zu unterstützen, gibt es spezielle **Kindersuchmaschinen**. Diese zeigen nur **kindgerechte** und sogar **redaktionell gefilterte Inhalte**. Außerdem unterdrücken die meisten Kindersuchmaschinen auch **Werbung oder (gefälschte) Pop-ups**. Das minimiert das Risiko, dass Kinder auf gefälschte Webseiten geleitet werden, Malware herunterladen oder für Sie **ungeeignete Inhalte** sehen. Wenn Sie sich für eine Suchmaschine entschieden haben, legen Sie diese im **Browser als Startseite** fest. Auch die meisten Browser bieten Kinderschutz durch **Browser-Erweiterungen** an, mit denen z. B. einzelne Webseiten gesperrt werden können.

6. Legen Sie Zeitbeschränkungen fest

Das Einrichten von Zeitbeschränkungen für die Internetnutzung kann sicherstellen, dass Kinder und Jugendliche nicht mehr Zeit als vereinbart oder unbeaufsichtigt Zeit im Internet verbringen.

Diese Funktion ist oft in Kindersicherungssoftware, aber auch in Betriebssystemen integriert. Mit **Zeitlimits** können Sie festlegen, wie lange Kinder ihre Geräte nutzen und online sein können. Dabei geht es nicht nur darum, für die gesamte Woche die Dauer der **Bildschirmzeit zu begrenzen**, sondern sie auch auf verschiedene **Tageszeiten zu beschränken**, um zu verhindern, dass Kinder bis spät in die Nacht oder **unbeaufsichtigt online** sind. Manche Betriebssysteme und Softwarelösungen bieten auch die Möglichkeit, Limits für bestimmte **Spiele und Apps** zu vergeben.

7. Sensibilisieren Sie frühzeitig für guten Accountschutz

Richten Sie Accounts gemeinsam mit Kindern und Jugendlichen sicher ein und sprechen Sie mit ihnen über potenzielle Gefahren, wie z.B. Phishing.

Sobald Kinder und Jugendliche online unterwegs sind, können auch sie Opfer von **Phishingangriffen** werden. Erklären Sie Kindern die Bedeutung von **sicheren Passwörtern** und wie man sie erstellt und beispielweise mit einem **Passwortmanager** verwaltet. Richten Sie, wann immer möglich, die **Zwei-Faktor-Authentisierung** ein. Kinder sollten zudem wissen, dass sie **Passwörter niemals** mit anderen **teilen** und **keine persönlichen Informationen** an Unbekannte weitergeben sollen.

8. Sprechen Sie über Gefahren und Schutzmaßnahmen im Internet

Die Sicherheit von Kindern und Jugendlichen im Internet erfordert neben technischen Schutzmaßnahmen auch umfassende Medienkompetenz, die Sie in Gesprächen vermitteln können.

Damit Kinder zu souveränen und selbstbestimmten Onlinenutzerinnen und Onlinenutzern werden, müssen sie in einem **kritischen** und **verantwortungsbewussten Umgang** mit digitalen Medien unterstützt und gefördert werden. Genauso wichtig wie technische Schutzmaßnahmen ist eine **offene und vertrauensvolle Gesprächsbasis**. Bieten Sie sich als **Ansprechpartner** auf Augenhöhe an, zeigen Sie **Interesse und Verständnis** – auch in schwierigen Situationen. Verbote, Strafen oder der Entzug der Geräte können dazu führen, dass sich die Kinder und Jugendlichen Ihnen nicht mehr anvertrauen.