Norton Online-Security Leitfaden: Mit diesen Tipps und Erklärungen machen Sie Ihre Kinder fit für einen sicheren Umgang mit dem Internet

Für viele Eltern ist der Versuch, ihre Kinder über die Gefahren, die das Internet mit sich bringt, aufzuklären so ähnlich, als würden sie gegen eine Wand reden. Ihnen geht es damit kein Stück besser? Wie also können Sie Ihren Kindern den sicheren Umgang mit dem World Wide Web und den zahlreichen sozialen Plattformen, auf denen junge Menschen tagtäglich unterwegs sind, vermitteln?

Nachfolgend geben wir Ihnen anhand verschiedener Themen einen Überblick über die verschiedenen Bedrohungen, denen Ihre Kinder ausgesetzt sind. Gleichzeitig erhalten Sie einen Einblick zu Vorsichtsmaßnahmen, mit denen diesen Gefahren entgegenwirken können.

Soziale Medien

Kinder und Jugendliche tummeln sich in einer Vielzahl unterschiedlicher Social Media Plattformen. Die mit Abstand problematischste Frage dabei ist, ab welchem Alter es für Kinder und Jugendliche angemessen ist, einen Account bei einem sozialen Netzwerk zu haben. Sollten sie Bilder posten können? Wie kann ihre Kontonutzung überwacht werden, ohne ihre Privatsphäre zu verletzen?

Facebook, Twitter und Snapchat schreiben alle vor, dass Kontoinhaber mindestens 13 Jahre alt sein müssen. Ein Zehnjähriger sollte also auch keine zehn-Sekunden-Selfies via Snapchat an seine Freunde versenden.

Sexting

Die unverantwortliche Nutzung von Snapchat kann äußerst schädigende Auswirkungen haben, zum Beispiel beim *Sexting*. *Sexting* bezeichnet das Versenden sexuell eindeutiger Fotos, Bilder, Textnachrichten oder E-Mails per Handy oder über andere Mobilgeräte. Zahlen aus Großbritannien zeigen, dass sich zwischen 2013 und 2015 die Anzahl der Fälle mehr als verzehnfacht hat.

Der Grundgedanke von Snapchat ist, dass jemand ein Foto an einen Freund sendet, das dann eine bestimmte Zeit sichtbar ist, bevor es für immer verschwindet. Doch nichts im Internet ist jemals endgültig gelöscht. Es gibt Apps, mit denen Nutzer eine Bildschirmaufnahme des Fotos machen können, ohne dass der Absender davon weiß. Das bedeutet, dass das schlüpfrige Foto, das die Person bedenkenlos verschickt hat (in der Annahme es würde verschwinden) auf dem Gerät des Freundes gespeichert ist.

In den Augen des Gesetzes gilt es als Kinderpornographie, wenn Personen, die über 18 Jahre alt sind, sexuell eindeutige Bilder von jemanden unter 18 Jahren in ihrem Besitz haben – auch dann, wenn die betreffende Person ihr Einverständnis gegeben hat.

Sie sollten Ihrem Kind unbedingt klarmachen, dass alles, was es versendet, sofortige oder zukünftige Konsequenzen haben kann. Es ist wichtig, sehr vorsichtig dabei vorzugehen, was an andere geschickt wird – schließlich vergisst das Internet nie.

Grooming und Ausbeutung

Bedauerlicherweise sind soziale Medien außerdem zu einem Nährboden für *Grooming* (die Anbahnung von Kontakten zu Minderjährigen) und Pädophilie geworden. Deshalb gilt hier für Kinder ein ähnlicher Sicherheitsgrundsatz wie im realen Leben: Sprich online nicht mit Fremden, akzeptiere keine Freundschaftsanfragen von Leuten, die du nicht kennst und erzähle deinen Eltern von merkwürdigen Nachrichten oder E-Mails.

Ein Freund kommuniziert plötzlich anders oder merkwürdig mit Ihrem Sohn oder Ihrer Tochter oder fordert sie auf, sich mit ihm zu seltsamen Zeiten zu treffen: Dann könnte es sein, dass das entsprechende Konto gehackt wurde. Das sollte auf jeden Fall gemeldet werden. Wenn Ihr Sohn oder Ihre Tochter eine neue Online-Freundin bzw. -Freund hat, sollten sie in der Lage sein, die Identität dieser Person zu bestätigen. Andernfalls könnte es sein, dass sie zum Opfer von *Catfishing* werden. Bei dieser Vorgehensweise wird ein falsches Online-Profil erstellt, um jemanden in eine Beziehung zu locken.

Leider bietet die Beschaffenheit des Internets Kriminellen eine nützliche Fassade, hinter der sie sich verbergen können. Daher ist es ratsam, zunächst nichts, was dort gesagt wird, für bare Münze zu nehmen. Alles zu hinterfragen und zu überprüfen ist die beste Methode, um die Sicherheit Ihrer Kinder zu gewährleisten.

Darknet – das „Dunkle Netz“

Beim Darknet handelt es sich um eine Reihe von *Overlay*-Netzwerken, also Netzwerke, die auf einem anderen Netzwerk aufbauen. Diese existieren im World Wide Web, es kann jedoch nur mit bestimmten Softwareprogrammen oder Befugnissen zugegriffen werden. Es sollte nicht mit dem *Deep Web*, dem versteckten Web, verwechselt werden.

Warum könnte das dunkle Netz Ihrem Kind zur Gefahr werden?

Im *Darknet* wird absolut alles zum Kauf angeboten. Dort gibt es Kinderpornografie, Drogen, Waffen, Auftragskiller und sogar Menschenhandel. Zugegebenermaßen ist es nicht leicht, dorthin zu gelangen. Dennoch ist es durchaus vorstellbar, dass sich ein Fünfzehnjähriger mit technischen Know-how und genügend Neugierde Zugang zur illegalen und unmoralischen Welt des Darknet verschafft.

Zum einen würden Kinder und Jugendliche hier alle möglichen Dinge zu Gesicht bekommen, die sie in ihrem Alter nicht sehen sollten. Gleichzeitig besteht die Gefahr, dass sie an illegalen Transaktionen teilnehmen. Wer dabei ertappt wird, dem können Geldbußen oder sogar Gerichtsverfahren drohen.

Auch wenn das Darknet nicht oben auf der Liste potenzieller Bedrohungen steht, sollten Sie dennoch erwägen, Ihren Sohn oder Ihre Tochter über die damit verbundenen Gefahren aufzuklären. Vor allem dann, wenn sie sich besonders für Computer und das Internet interessieren. Bei ihren „angeborenen" Computerfertigkeiten ist es nicht auszuschließen, dass sie aus reiner Neugier dort landen.

Cybermobbing

Kinder gehen immer früher mit Laptops, Tablets oder Smartphones ins Internet. Daher ist es zunehmend wichtig, sie über *Cybermobbing* aufzuklären. Es besteht immer die Sorge, dass Ihrem Kind diese Art von schlechter Behandlung widerfahren könnte. Daher sollte es ermutigt werden, sofort einem Erwachsenen davon zu erzählen, falls es passiert. Was als ein kleiner Spaß beginnt, kann bald zu einer gezielten Online-Kampagne werden, bei der das Opfer unangemessene Bilder, Bedrohungen oder manipulierte Fotos erhält. Wird dieser anfängliche „Spaß" nicht unterbunden, kann er ganz schnell ausarten. Genau wie beim herkömmlichen Mobbing sollte Cybermobbing möglichst schnell Einhalt geboten werden, bevor etwas gesagt, gepostet oder gesendet wird, das nicht zurückgenommen werden kann.

Ein nicht so angenehmer Gedanke

Eher selten wird in Erwägung gezogen, dass das eigene Kind eventuell nicht das Opfer, sondern der Täter sein könnte. In einigen Fällen kann das auch völlig unbeabsichtigt geschehen, z. B. wenn jemand auf einer Party ein peinliches Foto gemacht hat, das Ihr Kind dann online postet oder unter seinen Freunden und Klassenkameraden verbreitet. Dabei ist es sich überhaupt nicht bewusst, dass es sich hierbei um Cybermobbing handelt. Folgende Fälle zählen bereits als Cybermobbing: Ein negativer Kommentar zu einem Foto, das in einem sozialen Netzwerk gepostet wurde, verletzende oder negative Kommentare an eine andere Person, sei es in einer Statusmeldung, einem Posting oder einer Chat-Nachricht.

Schadprogramme (Malware)

Viele sind nachlässig, was das eigene Computer- und Internetverhalten angeht. Wenn Sie selbst bei Ihrer Computer- und Internetsicherheit Risiken eingehen, liegt es nahe, dass Ihr Kind sich genauso verhält. Im Folgenden finden Sie einige unkomplizierte Richtlinien, die Sie selbst befolgen und für Ihre Kinder aufstellen sollten, um Schadprogramme fernzuhalten:

1. Vertrauen Sie nicht immer allem, was Freunde in sozialen Medien posten.
2. Geben Sie Passwörter niemals an Freunde weiter und aktualisieren Sie diese alle sechs bis acht Wochen.
3. Wenn Ihr Betriebssystem meldet, dass ein Update benötigt wird, heißt das meistens, dass eine Sicherheitslücke geflickt werden muss. Je eher Sie also das Update ausführen, desto geringer das Risiko, dass diese Sicherheitslücke von einem Schadprogramm ausgenutzt werden kann.
4. Haben Sie keine Angst, im Internet einzukaufen, aber gehen Sie dabei umsichtig vor. Vergewissern Sie sich immer, dass die Website SSL (Secure Socket Layer) verwendet. Diese zusätzliche Sicherheitsschicht sorgt dafür, dass Ihre sensiblen Informationen nicht von Dritten eingesehen werden können. Ob eine Website SSL verwendet, lässt

sich ganz leicht feststellen: Vor der URL wird entweder ein Vorhängeschloss oder ein Schlüsselsymbol anzeigt.

5. Öffnen Sie niemals E-Mails von unbekannten bzw. unerwarteten Absendern oder verdächtig aussehende E-Mails von Freunden.
6. Stellen Sie sicher, dass Ihre Internetsicherheitssoftware auf dem neuesten Stand ist und ständig ausgeführt wird.
7. Vermeiden Sie Websites mit unzähligen Anzeigen und Werbe-Popups, da diese ein Tummelplatz für Schadsoftware sein können.
8. Kindern lernen, nach rechts und links zu schauen, bevor sie über die Straße gehen. Bringen Sie ihnen ebenfalls bei, erst zu überlegen, bevor sie klicken!

Illegale Downloads und Pornographie

Illegale Downloads und Pornographie kann ein neugieriger Teenager im Internet in Hülle und Fülle finden. Eltern sollten Ihre Kinder darüber aufklären, worum es dabei geht und sie so schützen.

Pornographie

Pornographische Websites können mithilfe einer Kindersicherung blockiert werden, die verhindert, dass Ihre Kinder Websites mit sexuell eindeutigen Inhalten aufrufen. Diese Einstellung lässt sich relativ leicht ein- und ausschalten, indem Sie Ihren Service Provider kontaktieren.

Illegale Downloads

Illegale Downloads sind etwas schwieriger zu verhindern oder zu kontrollieren. Die einfachste Methode, um festzustellen, ob ein bestimmter Musiktitel oder Film legal ist, besteht darin, Ihr Kind zu fragen, wo es das Material erhalten hat und ob es dafür bezahlt hat oder nicht. Illegale Downloads wurden nicht von einer Aufsichtsbehörde oder einer Website als sicher bestätigt und sind daher eine weitere Möglichkeit, über die sich Ihr Computer mit Schadsoftware infizieren könnte.

Sprechen Sie offen mit Ihren Kindern

Eine der effektivsten Methoden, um die Online-Sicherheit von Kindern zu gewährleisten, besteht darin, das Internet zu entmystifizieren. Es ist wichtig, Kindern zu erklären, was gut und was schlecht ist, und ihnen die sichere Computernutzung beizubringen. Wenn Sie offen mit ihnen über das Internet sprechen und dann ein Problem auftritt – sei es ein Virus oder eine Website mit unangemessenen Inhalten – können sie entweder selbst damit umgehen oder wissen, dass sie damit zu Ihnen kommen können.