ENJOY SAFER TECHNOLOGY™

saferkidsonline

Sicher in der Social Media Welt – Ein Leitfaden für Eltern

Einleitung

Erinnern Sie sich noch an die Zeiten, als unsere Kids draußen spielten und erst nach Hause kamen, wenn sie hungrig wurden? In unserer digitalisierten Welt gehört das längst der Vergangenheit an. Die Kids von heute können Stunden damit verbringen, in sozialen Netzwerken zu surfen oder mit ihren Freunden zu chatten.

Auch bei ESET gibt es viele Eltern. Umso mehr verstehen wir die Sorgen aller Mütter und Väter, ihr Nachwuchs könne sich in den Untiefen der Online-Welt verlieren. Und genau aus diesem Grund haben wir einen Ratgeber für Eltern zusammengestellt. Darin finden Sie nicht nur Wissenswertes über mögliche Gefahren und Stolpersteine in den Sozialen Netzwerken, sondern auch wertvolle Tipps und Lösungen, wie Sie Ihre Familie in der virtuellen Welt schützen können.

1. Vorsicht Schadprogramme!

Malware

Der Begriff setzt sich aus den englischen Wörtern malicious (schädlich) und software (Programm) zusammen. Daher wird im Deutschen auch oft der Terminus Schadsoftware verwendet. Viren, Würmer oder Trojaner sind wohl ihre bekanntesten Vertreter. Eine gängige Masche der Cyberkriminellen ist es, ahnungslose Anwender auf Facebook, WhatsApp & Co. dazu zu bewegen, mit Malware manipulierte Spiele und Software herunterzuladen.

Phishing

Phishing klingt nicht nur nach „Fischen", sondern stammt auch tatsächlich von diesem Wort ab (aus dem Englischen Password + fishing). Die Ableitung ist naheliegend, denn auch beim „Passwortangeln" wird ein Köder benutzt, um an sensible Daten zu gelangen. E-Mails, die gefälschte Links enthalten, zum Beispiel zur Webseite des bevorzugten Social Media – Kanals ihres Sprösslings, sind in diesem Fall eine beliebte Methode der Online-Kriminellen. Diese manipulierten Webseiten lassen sich kaum von den legitimen unterscheiden. Selbst als Erwachsener braucht man schon ein geschultes Auge, das Original von der Fälschung auseinanderzuhalten. Es ist also kein Wunder, dass Kids häufig in diese Falle tappen und ihre Logindaten preisgeben, ohne es zu merken.

Identitäts-Diebstahl

Gefälschte Social-Media-Profile, Missbrauch des Namens in Foren und Blogs oder bei der Warenbestellung - Identitäts-Diebstahl ist mittlerweile eine der am weitesten verbreiteten Formen der Cyberkriminalität. Hierbei verwenden die Betrüger die persönlichen Daten von Anwendern, um sich finanziell zu bereichern oder ihnen anderen Schaden zuzufügen (z.B. Verleumdung). Damit die Kriminellen an die sensiblen Daten der Profile gelangen, nutzen sie meist zwei Wege: Zum einen über Social Engineering, bei dem sich der Betrüger als Freund oder Bekannter Ihres Sprösslings ausgibt. Zum anderen geschieht dies über die öffentlich zugänglichen Daten des Social Media Profil Ihres Kindes.

Tipp: Stellen Sie sicher, dass Ihr Kind niemals sensible Informationen wie Adresse, Telefonnummer, Schuladresse oder Geburtstag in Netzwerken postet, über die man es identifizieren kann. Achten Sie darauf, dass die Daten Ihres Sprösslings in sozialen Netzwerken nicht öffentlich zugänglich sind. Dies lässt sich über entsprechende Datenschutz-Einstellungen bei Facebook, Instagram & Co. regulieren.

Online-Stakling und Cyber-Grooming

Nicht alle Gefahren in sozialen Netzwerken müssen zwangsläufig von Cyberkriminellen ausgehen. Auch das Verhalten der Mitschüler Ihres Kindes kann zu einem Problem werden. Das Thema Mobbing hat das Internet längst erreicht und ist hier genauso gefährlich und schmerzvoll wie im realen Leben.

Ein weiteres, sehr ernstes Thema ist das sogenannte Cyber-Grooming, besonders wenn jüngere Kinder davon betroffen sind. Dabei versucht ein Erwachsener, das Vertrauen des Kindes zu gewinnen und eine Art Beziehung zu ihm aufzubauen. Ziel ist es, das Kind zu sexuellen Handlungen zu bewegen, beispielsweise anzügliche Bilder zu senden. Oftmals beinhaltet Cyber-Grooming auch Sexting, also das Verschicken von Nachrichten mit unangemessenen Inhalten an oder durch das Kind.

2. Welche Maßnahmen können Sie ergreifen, um Ihren Nachwuchs zu schützen?

Mit Blick auf die potentiellen Risiken erscheint die Nutzung sozialer Netzwerke als ein gefährliches Unterfangen. Doch ein striktes Verbot wird das Problem nicht lösen. Im Gegenteil: Ihre Kids werden heimlich einen Weg finden, um an ihre Social Media – Profile zu kommen. Anstelle von Restriktionen sollen Ihnen unsere Tipps für einen sicheren Umgang mit Facebook, TikTok, Instagram & Co. helfen, Ihre Schützlinge sicher durch die Social Media Welt zu navigieren.

Suchen Sie das Gespräch mit ihren Kindern

Reden Sie offen mit Ihrem Nachwuchs über die Gefahren Sozialer Netzwerke. Wenn Sie darauf achten, ehrlich und auf Augenhöhe mit Ihrem Kind zu kommunizieren, steigt das Vertrauen zu Ihrem Urteilsvermögen und die Chance, dass es Ihren Ratschlägen folgt.

(Ein gutes Beispiel wäre hier die Vorbeugung gegen Cyber-Mobbing. Wenn Ihr Kind so etwas beobachtet – auch wenn es nicht direkt davon betroffen ist – sollte es das umgehend einer Vertrauensperson mitteilen. Dabei ist es völlig unerheblich, ob es sich um sie selbst, einen Lehrer oder einen anderen vertrauenswürdigen Erwachsenen handelt.)

Verwenden Sie einen guten Virenschutz

Viren, Trojaner & Co. gehören zu den häufigsten Gefahren im Cyber-Space. Hier sollten Sie auf technologische Hilfe zurückgreifen und grundsätzlich eine starke Schutzlösung auf den Geräten Ihrer Kids installieren. Sicherheitslücken und Einfallstore für Malware werden so auf ein Minimum reduziert. Vergessen Sie nicht, auch den Virenschutz regelmäßig zu aktualisieren (falls Updates nicht automatisch eingespielt werden).

Achten Sie darauf, dass der Account Ihres Sprösslings niemals Administratoren-Rechte besitzt, vor allem, wenn er häufig in sozialen Netzwerken unterwegs ist. Erstellen Sie ihm ein eingeschränktes User Profil, um die Gefahr einer Infektion zu minimieren.

Setzen Sie ggf. eine Kindersicherung ein

Je nach Alter Ihres Kinders empfiehlt es sich, eine Kindersicherung zu benutzen. Sie gibt Ihnen bspw. die Möglichkeit, unangemessene Webseiten zu blockieren oder Bildschirmzeiten einzurichten. Denken Sie daran: Die Kids sollten dabei auch immer ein Mitspracherecht haben.

Nutzen Sie starke Passwörter und eine Zwei-Faktor-Authentifizierung

Haben Sie schonmal mit Ihren Kindern über Passwörter gesprochen? Nein? Dann fangen Sie am besten gleich damit an. Zumindest wäre es wichtig, dass keine leicht zu erratenden Passwörter wie „12345“ oder „Passwort“ verwendet werden. Die Mindestlänge sollte 10 Zeichen umfassen und sowohl Ziffern als auch Sonderzeichen wie @ oder # enthalten. Kleine Eselsbrücken können dabei durchaus helfen.

Aus „Papa ist der Beste“ wird so das Passwort P@p@1stder8este.
Erinnern Sie Ihr Kind daran, die Passwörter niemals mit anderen Personen zu teilen – auch nicht mit ihren besten Freunden.

Wenn Ihre Schützlinge Facebook, Twitter und Co. benutzen, sollten sie grundsätzlich die Zwei-Faktor-Authentifizierung verwenden, die in den dortigen Sicherheitseinstellungen integriert ist. Das zusätzliche Einmal-Passwort erschwert es Cyber-Kriminellen erheblich, auf die Daten Ihres Kindes zuzugreifen.

Setzen Sie die Profil-Einstellungen auf „privat“

Die standardmäßigen Datenschutzeinstellungen in sozialen Netzwerken garantieren keine Sicherheit der Daten Ihres Kindes. Es ist daher ratsam, etwas Zeit zu investieren und zu überprüfen, welche Informationen unerwünscht nach Außen gelangen könnten. Lassen Sie uns das am Beispiel von Facebook einmal durchspielen:

Facebook

Stellen Sie sicher, dass Profil-Informationen Ihres Sprösslings nicht für alle Facebook-User sichtbar sind. Die Daten sollten lediglich für den engeren Familien- und Freundeskreis einsehbar sein.

Beschränken Sie die Anzahl an Nutzern, die Bilder, Status oder andere Inhalte sehen können, bei denen Ihr Kind markiert wurde. Anwendungen, die auf persönliche Informationen zugreifen oder Inhalte auf dem Profil Ihres Schützlings posten, sollten Sie keinesfalls zulassen.

Bringen Sie Ihrem Nachwuchs bei, ausschließlich Freundschaftsanfragen von Menschen anzunehmen, die er persönlich kennt. Machen Sie Ihren Kids klar, dass die Kontaktaufnahme bzw. ein Gespräch mit Fremden im Internet genauso gefährlich sein kann wie im realen Leben.

Wie Sie die entsprechenden Einstellungen bei Facebook richtig setzen, erfahren Sie in unserem Blog: https://www.welivesecurity.com/deutsch/2020/02/04/facebook-privatsphaere-einstellungen-datenschutz-tipps/

Twitter

Twitter hat durch die Beschränkung auf 280 Zeichen und das Verwenden verkürzter URLs spezifische Eigenschaften. Auf diese Besonderheiten sollten Sie Ihr Kind in einem ersten Schritt hinweisen, damit es auch bei Twitter sicher unterwegs ist.

Ihr Nachwuchs sollte ausschließlich Personen folgen, die er kennt und die Legitimität erhaltener Nachrichten prüfen. Andere Nutzer identifizieren häufig bösartige oder schädliche Nachrichten und warnen davor. Wenn Sie einen Teil des Tweets einfach in die Schnellsuche eingeben, werden Sie direkt fündig.

Installieren Sie ein vertrauenswürdiges Browser-Plug-In. Das ermöglicht Ihrem Kind, die komplette Adresse hinter der verkürzten URL zu lesen, ohne sie anklicken zu müssen.

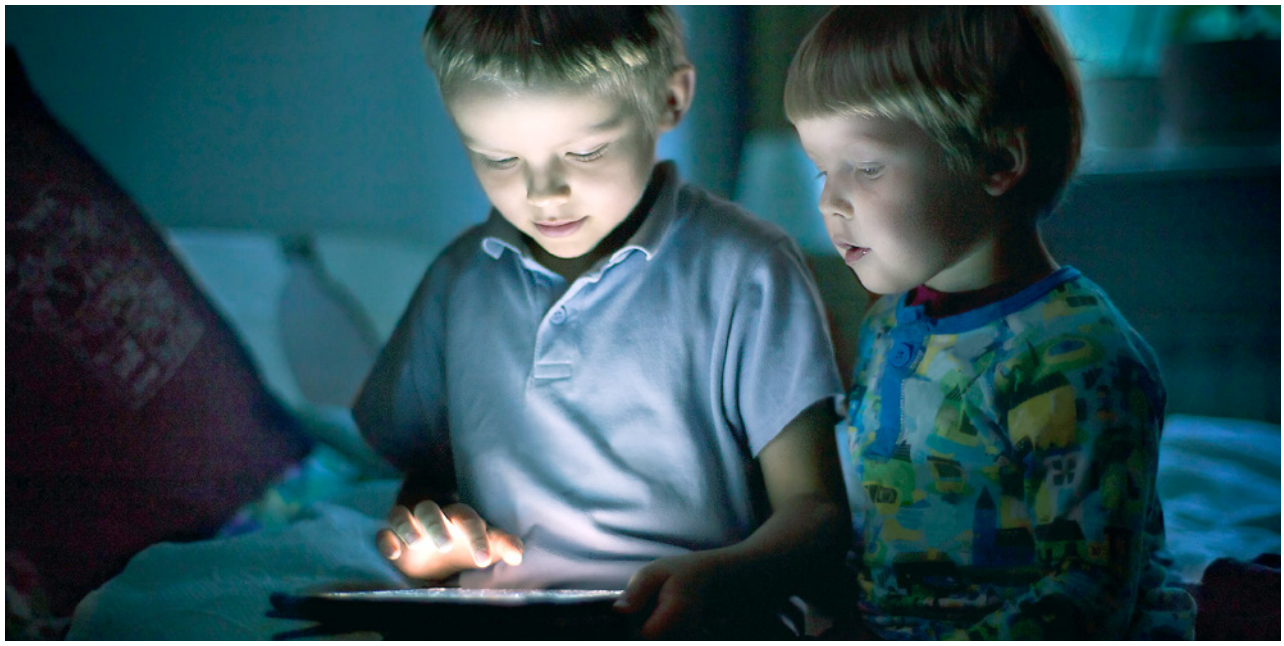
Weitere Soziale Netzwerke

Die Social Media Landschaft ist mittlerweile fast unüberschaubar geworden. Es gibt viele Anbieter für jegliche Altersgruppen und Interessen. Es ist wichtig, dass Ihre Kinder nur wirklich altersgerechte Plattformen nutzen. Als kleine Hilfestellung haben wir eine entsprechende Liste geeigneter sozialer Netzwerke zusammengestellt.

3. Zusammenfassung

Soziale Netzwerke können durchaus eine nützliche Informationsquelle sein. Doch wie dieser Leitfaden auch gezeigt hat, lauern auf Ihre Kids einige Gefahren darin. Unterschätzen Sie nie Cyber-Kriminelle oder andere Betrüger, denn ihre Methoden sind äußerst gewieft. Deshalb ist es umso wichtiger, dass Sie Ihren Nachwuchs sensibilisieren und zuverlässige Sicherheits-Tools verwenden, um Ihre Liebsten umfassend zu schützen.

Helfen Sie Ihren Kindern, ihre Profile richtig einzustellen und geben Sie ihnen einfache aber nützliche Tipps. Das kann entscheidend sein, um Ihre Schützlinge sicher durch das World Wide Web zu begleiten.



Unsere Top 10 Tipps

1. **Denken statt klicken:** Lernen Sie Ihrem Kind kurz innezuhalten und nachzudenken, bevor es auf Links oder Download-Buttons klickt.

2. **Weniger ist mehr:** Erklären Sie Ihrem Nachwuchs, dass man bei Online-Unterhaltungen immer vorsichtig bleiben sollte.

3. **Privat statt öffentlich:** Setzen Sie die Accounts Ihrer Kids immer auf „privat".

4. **Nicht von Fremden ansprechen lassen:** Lernen Sie Ihrem Sprössling, Freundschaftsanfragen von Fremden grundsätzlich abzulehnen.

5. **Stets up-to-date:** Halten Sie das Betriebssystem und die Sicherheitssoftware immer auf dem neuesten Stand.

6. **Dienen Sie als Vorbild:** Gehen Sie mit gutem Beispiel voran, indem Sie ihre eigene Online-Zeit nicht ausufern lassen.

7. **Aufmerksam bleiben:** Achten Sie auf Anzeichen, ob ein Kind möglicherweise Opfer von Cyber-Mobbing geworden ist.

8. **Kindersicher sein:** Nutzen Sie ggf. eine Kindersicherung, um unangemessene Webseiten zu blockieren.

9. **Machen Sie sich Passwort-stark:** Ermuntern Sie Ihre Kinder, starke Passwörter zu benutzen.

10. **Nicht zu viel verraten:** Bringen Sie Ihrem Kind bei, genaustens zu überlegen, welche persönlichen Informationen, Videos oder Fotos es wirklich teilt.