



Wenn Computer, Tablet und Smartphone unter dem Weihnachtsbaum liegen

Aufklärung in Sachen Sicherheit: Sophos gibt Tipps für Informationen, die Eltern ihren Kindern unbedingt gemeinsam mit den neuen digitalen Begleitern auf den Weg geben sollten.

Wiesbaden, 24. November 2014 – Weihnachten steht vor der Tür und viele Kids und Teens werden wieder mit neuen digitalen Geräten beschenkt werden. Sind die Devices auch hilfreich und unterhaltsam und aus dem Alltag der jungen Leute nicht mehr wegzudenken, so kommt der Aspekt der Sicherheit leider oftmals immer noch zu kurz.

Damit das Chatten mit Freunden, fröhliche Posten auf Facebook, Twitter und Instagram, spannende Online Gamen oder auch intensive Suchen von Infos für die Hausaufgaben so unbeschwert und ungefährlich wie möglich bleibt, gilt es die Gefahren, die im Netz lauern, zu kennen. Sophos gibt einige Tipps, wie Eltern ihren Nachwuchs digital „aufklären“ können und sich selbst und ihre Kinder fit machen gegen die Gefahren und für den bestmöglichen Schutz:

Schneller sein als die Bösen Buben.

- Das Internet ist eine Schlangengrube, dort lauern Gefahren wie Hacker, Viren, Trojaner und böartige Mobber. Das weiß jedes Kind. Und jedes Kind sollte deshalb lernen, worauf es beim Schutz ankommt.

Sich fit machen für den Umgang mit den Gefahren. Austausch mit Eltern oder anderen Erwachsenen.

- Kinder sind häufig fitter im Umgang mit Computern und bei der Nutzung sozialer Netzwerke, als ihre Eltern. Das macht sie aber nicht fit genug, um alle Situationen auch tatsächlich alleine meistern zu können. Mit einer Kombination aus Technikwissen (der Kinder) und Erfahrung (der Eltern) lassen sich jedoch sichere und sinnvolle Wege für alle Beteiligten finden.
- Es lauern nicht nur technische Gefahren im Netz. Dort warten auch Pädophile, Mobber und andere, die Traumata auslösen können. Kinder müssen lernen, sich zu wehren, sich abzugrenzen. Hier helfen die Schulen, zahlreiche, spezielle Initiativen und natürlich eine gute Internet-Aufklärung zuhause.

Surfen und Chatten auf dem Smartphone – aber sicher.

- Öffentliche WLANs vermeiden. WLANs zuhause, bei Freunden oder in der Schule sind gesichert und relativ ungefährlich. Öffentliche WLANs jedoch können Hacker-Fallen sein, über die beispielsweise Fotos und Adressen geklaut oder das ganze Handy gesperrt werden können.
- Auf den mobilen Geräten sollten nur bekannte und geprüfte Apps installiert werden. Viele Apps versenden persönliche Daten ohne, dass man es bemerkt und schon weiß ein Fremder genau, was man macht, wo man ist oder wie die Freunde im Adressbuch heißen.

- Smartphones sollten mit einem pfiffigen Passwort geschützt sein. Wichtig ist, dass man es sich gut merken kann und kein Unbefugter es kennt. Wird das Telefon geklaut oder geht es verloren, kann niemand Chats, Mails, Freunde oder Spiele sehen.

Schütze Dich selbst und Deinen PC zuhause.

- Ein guter Virens Scanner hilft, den PC zu schützen. Nur so kann man beim Surfen oder Spielen sicher sein, dass kein Anderer den Computer mit einem Virus infiziert.
- USB-Sticks oder selbst gebrannte CDs können schädliche Viren transportieren. Externe Datenträger sollten daher erst von einem Virens Scanner geprüft werden.
- Surfen und Spielen macht Spaß und kann helfen, neue Dinge zu lernen. Nützliche Hilfsprogramme helfen, damit Kinder nicht versehentlich auf Internetseiten gelangen, wo Gefahren mit Trojanern und Viren lauern. Schalten Sie den den Internetschutz niemals aus.

Facebook und WhatsApp und was sind eigentlich Freunde?

- **Kinder brauchen ein soziales Netz**, das gilt für die digitale wie für die reale Welt. Das eigene Smartphone und mit installiertem whatsapp steht vielen Kindern bereits mit neun, zehn Jahren zur Verfügung, Facebook folgt zum 13. Geburtstag. Wichtiger Aspekt: für Kids sind digitale Freunde nicht weniger real als Nachbarn und Klassenkameraden, und ob man sich nun wie früher auf der Straße oder heute im Chatroom trifft, macht so gut wie keinen Unterschied. Die Kommunikation zwischen den Generationen über den Umgang mit „Freunden“ ist daher elementar. Ansprechen, nachfragen, erklären ist der Auftrag an die Eltern/Erwachsenen, zuhören, annehmen, befolgen heißt es für die Kids.
- **Wirklich alle?** Schnell mal mitteilen wo man ist, was man gerade macht oder kurz ein Foto für die Freunde posten – tolle Sache. Man sollte jedoch vorsichtig sein. Wer soll Einträge und das Profil lesen können? Nur die Freunde oder gleich die ganze Welt? Die Privatsphäre sollte immer so eingestellt sein, dass nur Freunde die persönlichen Einträge lesen können. So ist man auf der sicheren Seite.
- **Á propos Freunde.** Es ist für viele Jugendliche geradezu ein Sport, Freunde zu „sammeln“. Bei mehr als 500 Freunden ist es unwahrscheinlich, dass man jeden persönlich kennt. Vielleicht ist es sinnvoll, nicht jedes Posting allen 1325 Freunden (oder wie viele es auch tatsächlich im Einzelfall sind) zugänglich zu machen. Manch einer ist gar kein „Freund“ und das wertvolle Rennrad, die Xbox oder was auch immer einem am Herzen liegt, ist nach dem Urlaub verschwunden. Der Dieb wusste ja Dank Facebook, dass man weg war. Auch hier gilt es, mit den Kindern über den Umgang mit Sozialen Medien zu reden, aufzuklären und gegebenenfalls gemeinsam in die Sicherheitseinstellungen zu schauen.
- **Sicherheitstools einsetzen.** Wirksame Tools für die Sicherheit gibt es von zahlreichen Anbietern, sowohl kostenpflichtig als auch kostenlos. Sich zu informieren und je nach individuellem Bedarf zu vergleichen ist daher sinnvoll. Sophos stellt seine Sicherheitstools für Endverbraucher kostenlos zur Verfügung – unter folgendem Link gibt es mehr: <http://www.sophos.com/de-de/products/free-tools.aspx>

Über Sophos

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.

Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos

Jörg Schindler, PR Manager CEEMEA

joerg.schindler@sophos.com, +49-721-25516-263

TC Communications

Arno Lucht, +49-8081-954619

Thilo Christ, +49-8081-954617

Christiane Capps, +49-174-3335550

Ulrike Masztalerz, +49-30-55248198

sophos@tc-communications.de

<http://people.astaro.com/joergschindler/2014-q2-dirty-dozen-by-vol.png>