SCHOOL-SCOUT.DE

Unterrichtsmaterialien in digitaler und in gedruckter Form

Auszug aus:

Datensicherheit - Medienkompetenz entwickeln

Das komplette Material finden Sie hier:

School-Scout.de

Inhaltsverzeichnis

Vorwort

Sehr geehrte Kolleginnen und Kollegen,

Handy, Smartphone, Tablet und Computer: Sie sind aus der Welt der Jugendlichen nicht mehr wegzudenken. Sie gehören zum Lebensalltag dazu.

- Auf dem Weg zur Schule werden noch einmal kurz die Mails gecheckt.
- Hat mir die Freundin eine WhatsApp geschickt?
- Gibt es etwas Neues in meiner Facebook-Gruppe?
- Hat die Straßenbahn Verspätung oder ist sie heute einmal pünktlich?
- Findet der Unterricht heute nach Plan statt oder fallen Stunden aus?
- Soll es heute Nachmittag regnen? Ich wollte doch mit meinem Freund eine Radtour machen.

Diese und viele andere Fragen werden heute von Jugendlichen in Windeseile mit dem Smartphone erledigt, und zwar ohne weitere Rückfragen und meist auch ohne weitere Vorsichtsmaßnahmen. Viele Jugendliche gehen mit diesen Medien sorglos um, meist zu sorglos. Sind sie sich der Gefahren bewusst, die mit der Nutzung der sozialen Medien, der Messenger-Dienste, des Internets allgemein verbunden sind oder sein können?
Diese Frage und andere sollen in diesem Arbeitsheft beantwortet werden. Der vorliegende Band wird jedoch keine Anleitung zum hundertprozentigen Schutz im Internet geben; dazu gibt es umfangreichere Werke. Er soll auch nicht dazu führen, dass man sich nur noch ängstlich in den digitalen Medien bewegt. Er will aber aufzeigen, welche Gefahren mit der Nutzung verbunden sind und wie man sich weitgehend davor schützen kann, indem man die Möglichkeiten der Absicherung ausreichend nutzt.

Mit diesem Heft sollen Jugendliche sensibilisiert werden, auf ihre Daten besser zu achten, indem sie die digitalen Geräte möglichst gut vor fremden Zugriffen schützen.
Vorfälle in den letzten Wochen, Monaten und Jahren zeigen immer wieder, wie anfällig die Netze für Angriffe von außen sind. Sie müssen nicht jedes Smartphone, nicht jeden Computer treffen, aber man sollte die vorhandenen Mittel einsetzen, um größeren Schaden zu verhindern. Gerade die Angriffe auf die öffentlichen Netze zeigen, wie empfindlich die gesamte Computerstruktur ist. Professionelle Hacker greifen die Netze von Firmen und Verwaltungen an, um Informationen zu gewinnen; sie greifen in private Netze ein, um an persönliche Daten zu gelangen, die dann für kommerzielle Zwecke genutzt werden.

Für Anregungen und Hinweise bin ich dankbar.

Heinz Strauf

heinz@strauf.de

Grundsätzliche Überlegungen zum Schutz meiner Hardware

Noch heute gibt es genügend Menschen, die sich zu wenig Gedanken über den Schutz ihrer Hardware machen. Und das obwohl die fest installierte Hardware als Desktop-Computer im Alltag und in privaten Haushalten immer mehr zugunsten von flexibleren Geräten verschwindet, die über offene Netzwerke dauerhaft mit dem Internet verbunden sind. Das Smartphone als Allroundprodukt birgt neben vielen Vorteilen immer die Gefahr, die sensibelsten Informationen zu einem selbst oder den Kontakten zugänglich zu machen. Da also Smartphones, Smartwatches oder Tablets fast immer online sind, sind auch die Anforderungen an die notwendigen Sicherungsmaßnahmen sehr hoch.

Smartphones, Tablets etc. sind aber auch beliebte Objekte für Diebstähle, gerade weil es stetig neue Modelle gibt, die darüber hinaus schon seit Langem sehr hochpreisig sind. Von daher muss man sich als Nutzer Gedanken darüber machen, wie man die Daten, die sich auf dem Smartphone befinden und die über Datendienste mit dem Gerät gekoppelt sind, sichern kann.

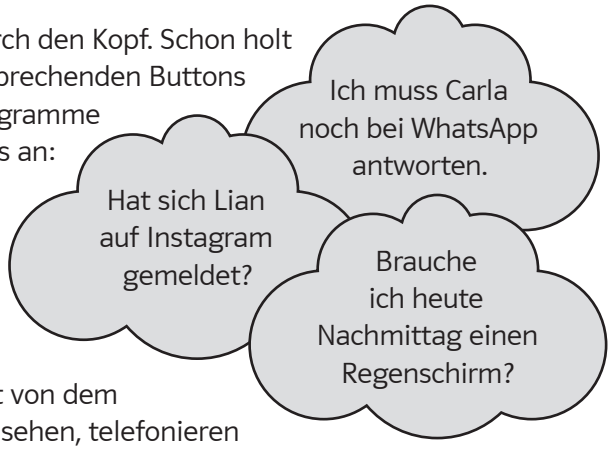
Hier ergeben sich vielfältige Aufgaben für jeden Nutzer, über die sich viele jedoch gar nicht im Klaren sind oder die sie nicht mit der notwendigen Sorgfalt erledigen.

Darüber hinaus darf auch nicht der richtige Schutz der Daten auf dem heimischen PC in Vergessenheit geraten, denn auch dort lauern stetig Gefahren, dass Daten gehackt werden oder sogar der Zugang zu einem Gerät aufgrund eines Virus verweigert wird.

Grundsätzlich gilt hier, man sollte vor allem E-Mails, Links etc. niemals blind vertrauen. Außerdem muss ein guter Virenschutz etc. nicht immer teuer sein, sodass es jedem möglich ist, seine Geräte und Daten zu schützen. Denn bei einem vollständigen Hack geht es ja häufig nicht mehr nur um die eigenen Daten, sondern auch um Daten, Dateien, Bilder, Nachrichten etc. von Kontakten.

Bildschirmsperre – so schütze ich mein Smartphone

Diese Gedanken gehen Mia auf dem Weg zur Schule durch den Kopf. Schon holt sie ihr Smartphone raus und schaut nach. Über die entsprechenden Buttons auf der Oberfläche kann sie sofort die gewünschten Programme aufrufen. Tom, der neben Mia läuft, guckt sie fassungslos an: „Mia, bist du irre? Hast du gar keine Bildschirmsperre?“



Mia geht tatsächlich sehr leichtfertig mit ihrem Smartphone um. Wenn man sofort nach dem Einschalten auf die einzelnen Programme zugreifen kann, ist das Smartphone bei einem Verlust oder einem Diebstahl überhaupt nicht geschützt. Das Smartphone kann sofort von dem Finder oder Dieb genutzt werden, er kann alle Daten einsehen, telefonieren und surfen.

Das ist natürlich gar nicht in Mias Sinne, so informiert sie sich über die verschiedenen Möglichkeiten, ihr Smartphone besser zu sichern.

Eine ganz einfache erste Möglichkeit ist die Bildschirmsperre durch Wischen bzw. Streichen. Dies dient jedoch vor allem dazu, dass, während das Smartphone in der Tasche ist, nicht wahllos irgendwelche Tasten betätigt werden. Zum Datenschutz ist diese Methode natürlich nicht geeignet.

Eine effektivere Methode der Sperre ist ein **Code** aus vier oder sechs Ziffern (Abb. 1).

Eine andere Variante ist das **Muster** (Abb. 2). Man verbindet auf der Tastatur einige Zahlen; nur mit dieser Zahlenkombination ist nun der Bildschirm des Smartphones wieder zu öffnen.

Einige Smartphones können als Bildschirmsperre auch einen **Fingerabdruck** einrichten (Abb. 3). Dies stellt eine nur schwer zu überwindende Sperre dar, denn nur über die bei der Installation gespeicherten Abdrücke lässt sich später der Bildschirm öffnen.

Ganz allgemein gilt: Die automatische Sperre sollte schon nach recht kurzer Zeit einsetzen. Auch wenn sich das Smartphone so sehr häufig automatisch sperrt, was nervig sein kann, ist es jedoch immer sicherer.

Abb. 1

Abb. 2

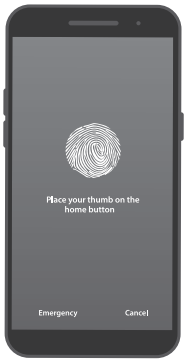


Abb. 3

AUFGABEN

1 **Welche Methoden nutzt ihr? Erstellt eine Strichliste.**

2 **Findet Vor- und Nachteile der Methoden. Diskutiert darüber.**

SCHOOL-SCOUT.DE

Unterrichtsmaterialien in digitaler und in gedruckter Form

Auszug aus:

Datensicherheit - Medienkompetenz entwickeln

Das komplette Material finden Sie hier:

School-Scout.de