

WAS KANN ICH FÜR MEHR SICHERHEIT TUN?

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.

AUFGABEN

- 1 Welche Methoden nutzt ihr?
Erstellt eine Strichliste.
- 2 Findet Vor- und Nachteile der Methoden.
Diskutiert darüber.

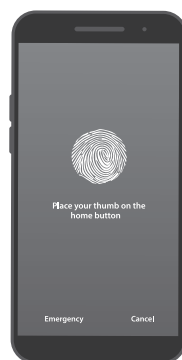


Abb. 3



Abb. 2



Abb. 1

Hat sich Lian auf Instagram gemeldet?

Ich muss Carla noch bei WhatsApp antworten.


Brauche ich heute Nachmittag einen Regenschirm?

Passwörter – so schütze ich meine Accounts

WAS KANN
ICH FÜR MEHR
SICHERHEIT TUN?

Bei diesen vielen Passwörtern, die man im Laufe der Zeit beim Erstellen von Profilen, Accounts und zum Schutz von Smartphone, PC etc. generiert hat, kann man schnell mal den Überblick verlieren. Da liegt der Gedanke doch nah, Passwörter zu verwenden, die man sich besonders gut merken kann, z. B.:

- das Geburtsdatum
- den Vornamen zusammen mit der Lieblingszahl
- 123456
- Test




123456

So leicht darf man es sich natürlich nicht machen. Das Passwort sollte aus einer Kombination von verschiedenen Typen bestehen: Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen. Einige Programme geben vor, aus wie vielen Zeichen in welcher Kombination das Passwort bestehen muss; manchmal erhält man dann bei der Eingabe einen Hinweis darauf, wie stark das eingegebene Passwort ist, sodass man es noch ändern und verstärken kann.

Eine gute Möglichkeit für ein starkes Passwort ist dieses Vorgehen:

Man merkt sich einen einfachen Satz: *Peter geht jeden Tag 1 Stunde um 5 Uhr joggen.* Mit den Anfangsbuchstaben (und Ziffern) bildet man das Passwort, in diesem Fall also: PgjT1Su5Uj. Ein solches Passwort ist für andere schwer herauszubekommen und es fällt auch schwer, sich dieses Passwort zu merken, wenn man nicht den dazugehörigen Satz kennt. Also selbst wenn jemand mal dein Passwort sieht, wird er es sich sicherlich nur schwer merken können – anders als 123456.



PgjT1Su5Uj

Ein weiterer Fehler, den viele in Bezug auf ihre Passwörter begehen, ist, das Passwort für alle Accounts etc. zu nutzen. So gut das Passwort dann auch sein mag, wenn es einmal jemand herausbekommt, hat derjenige Zugriff auf all deine Konten.

Die Passwortflut lässt sich also leider nicht vermeiden, allerdings gibt es allerlei Hilfsprogramme – sogenannte Passwortmanager –, die einem dabei helfen können, den Überblick zu behalten. Dort gibt man alle Passwörter, die man im Gebrauch hat, ein. Für die Öffnung dieses Programms muss man sich dann nur noch ein Passwort merken.

Das sind einige der kostenlosen Passwortverwaltungsprogramme:

DASHLANE

KEEPASS

TRUE KEY

ENPASS

1PASSWORD

AUFGABEN

- 1 **Sprecht über eure jetzigen Passwörter – natürlich ohne sie tatsächlich zu nennen. Was fällt euch auf? Zählen sie zu den einfach zu erratenden Passwörtern?**
- 2 **Überlegt euch je drei Passwörter nach dem Beispiel oben. Nutzt Sätze, die ihr euch gut merken könnt.**

WAS KANN ICH FÜR MEHR SICHERHEIT TUN?

Passwortcheck – wie sicher sind meine Passwörter?

Du kennst sicherlich schon einige Voraussetzungen für die Erstellung eines Passwortes und weißt auch, welche Kriterien ein gutes Passwort erfüllen muss. Oft wird dir in Apps und Programmen z. B. durch einen Balken von Rot nach Grün gezeigt, wie stark das von dir eingegebene Passwort ist. Das ist aber nicht immer der Fall.

Es gibt deshalb die Möglichkeit, Passwörter durch einen sogenannten Passwortcheck überprüfen zu lassen. Ein solches Programm findest du z. B. unter der Webadresse <https://www.passwortcheck.ch>.

Es öffnet sich dieses Fenster:

Hier wird das zu prüfende Passwort eingegeben.

Hier erfährt man während der Eingabe, wie stark das Passwort ist.

Bei dem Programm <https://checkdeinpasswort.de> ändert sich während der Eingabe des Passworts die Bildschirmfarbe von Rot nach Grün.



AUFGABE

Überprüft auf einer Seite eurer Wahl eure aktuellen Passwörter und kreiert neue.