

Liebe Schülerinnen und Schüler,

da ihr weiterhin die nächsten Wochen von zu Hause arbeiten müsst, schicke ich euch Aufgaben, die ihr bis zum 30.04. erledigen sollt.

Die fertigen Aufgaben schickt ihr bitte an folgende Adresse:

[Nina.Hecht@gmx.net](mailto:Nina.Hecht@gmx.net)

Bitte sendet mir ebenfalls, falls noch nicht geschehen, Eure letzte Aufgabe, die Digital Detox Pläne zu.

Falls ihr große Schwierigkeiten oder Rückfragen habt steht Euch meine E-Mail-Adresse natürlich ebenfalls zur Verfügung.

Freundliche Grüße, haltet weiter durch und bleibt gesund!

Nina Hecht

### **Arbeitsauftrag für die Wahlpflicht-Wirtschaftskurse 8a-f HEHT**

1. Lies dir das nachfolgende Arbeitsblatt zum Thema Passwörter durch.
2. Suche nach Gründen, warum es viele Menschen bei der Sicherheit von Passwörtern nicht allzu genau nehmen.
3. Nenne mindestens 3 Eigenschaften, die ein gutes Passwort haben soll.
4. Erstelle ein sicheres Passwort und überprüfe es mit einem Passwort-Checker, z.B. diesen hier:  
<https://www.passwortcheck.ch/passwortcheck/passwortcheck>  
Welche Merkmale hat dein Passwort und wie lange würde es dauern dieses zu hacken?
5. Schau dir deine bisherigen Passwörter an, prüfe diese im Passwort-Checker und nenne Gründe, warum sie eventuell zu unsicher waren.

# Passwörter richtig wählen

Dein Passwort besteht nur aus wenigen Buchstaben und heißt „Hund“, „Passwort“, „12345“, oder „Schatz“? Schlecht gewählt! Diese Passwörter lassen sich viel zu leicht, auch von Laien knacken.

Vielleicht hattest du bisher Glück und niemand hat versucht dein Passwort herauszufinden, um an deine ganzen Daten zu kommen. Vielleicht liest aber auch ein ehemaliger Freund deine privaten E-Mails, oder stöbert in deinen Social Media Accounts, dem du vor Urzeiten dein Passwort leichtsinnig verraten hast.

## Passwort-Checker gegen Hacker

Im Internet findest du Programme, mit denen du kontrollieren kannst, wie sicher dein Passwort ist. Dort gibst du dein gewähltes Passwort ein und das Programm sagt dir, wie leicht oder schwer dein Passwort zu knacken ist.

Einen kostenlosen **Passwort-Checker** findest Du unter: <https://www.passwortcheck.ch/>.

**Hacker** benutzen zum Knacken von Passwörtern selbst geschriebene Programme, die automatisch alle Wörter aus einem Wörterbuch durchprobieren. Diese Programme probieren in sekundenschnelle tausende von Wörtern aus, bis sie die richtige Kombination gefunden haben. Außerdem überprüfen diese Programme Vornamen und kurze, einfach Zahlenkombinationen wie Geburtstage.

Hierbei ist jetzt die Länge des Passwortes wichtig. Ein schneller Rechner benötigt ein paar Tage, um eine beliebige Buchstaben- und Zahlenkombination zu knacken, wenn sie nicht mehr als 7 Stellen hat. Besteht das Passwort jedoch aus **8 oder mehr Stellen**, bräuchte der Hacker, bzw. dessen Computer mehrere Jahre, um die richtige Kombination zu finden.

## Wie finde ich ein sicheres Passwort?

Aus diesem Grund sollte jedes Passwort mindestens **8 Zeichen** lang sein, je mehr Zeichen, desto sicherer wird es.

Außerdem sollte es eine Mischung aus **Groß- und Kleinbuchstaben**, sowie **Sonderzeichen und Ziffern** sein, um nicht sofort von den Hacker-Programmen durchschaut zu werden.

Weiterhin ist es immer ratsam keine persönlichen Begriffe aus deinem Leben zu nehmen, falls der Hacker dich kennen sollte und es gezielt ein Angriff gegen dich ist.

## Und wie soll ich mir das merken?

Hierbei gilt die Empfehlung sich Passwörter niemals aufzuschreiben. Besser ist es die Passwörter so zu gestalten, dass sie einen **Passwort-Merksatz** ergeben. Ein Beispiel wäre der Satz:

Muttis 3-Frucht Marmelade schmeckt um 12 am besten. Hierbei würde sich das Passwort ergeben:

**M3-FMsU12ab**

Dieses System kann individuell ausgebaut und verändert werden. Hierbei sind deiner Kreativität fast keine Grenzen gesetzt. Groß- und Kleinschreibung könnten vertauscht werden, oder der Satz wird rückwärts gelesen. Wichtig ist, dass du dir dein eigenes System merken und reproduzieren kannst.

