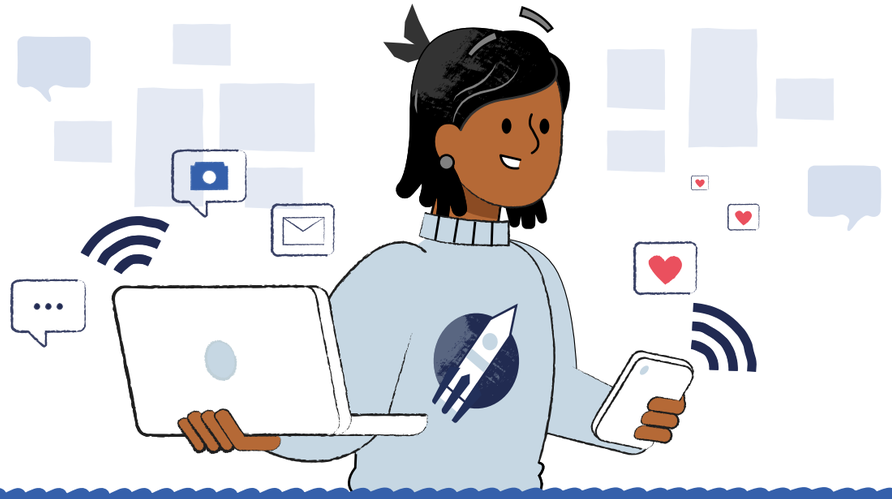
KAPITEL 8:

ONLINE SICHER UNTERWEGS

ONLINE SICHER UNTERWEGS



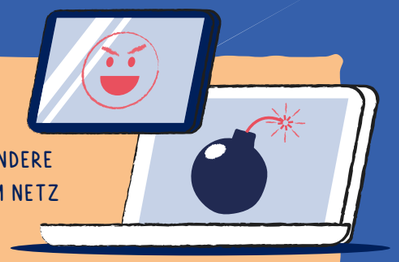
EINE VIELZAHL VON SATELLITEN DREHT SICH UM DIE ERDE, UND ES WERDEN IMMER MEHR.

Sie helfen uns, das Wetter vorherzusagen, Fernsehen auszustrahlen, Telefonanrufe und Internet an abgelegenen Orten zu ermöglichen, wissenschaftliche Experimente durchzuführen und vieles mehr. Wir können damit auch den Klimawandel beobachten.

Aber Satelliten sind offensichtlich in Gefahr: Es besteht nicht nur die Gefahr von Fehlfunktionen oder Kollisionen aufgrund der widrigen Bedingungen, unter denen die Satelliten betrieben werden. Sie können auch von Personen gehackt werden, die Daten stehlen oder Störungen verursachen wollen.

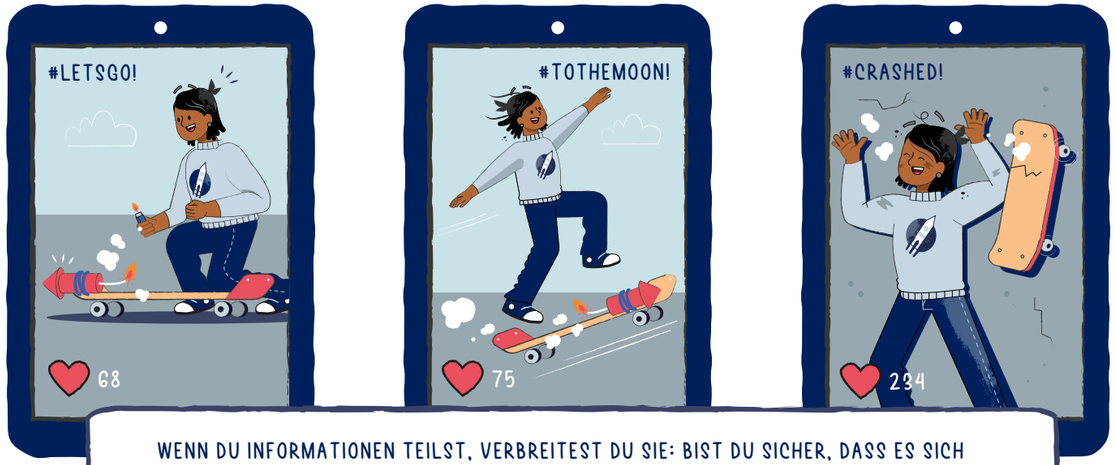
SATELLITEN SIND SICHER, SOLANGE WIR DAFÜR SORGEN, DASS DIESE GEFAHREN ABGEWENDET WERDEN. SIE KORREKT GENUTZT WERDEN UND WIR ENTSPRECHENDE WERKZEUGE (Z. B. PASSWÖRTER) UND VERHALTENSWEISEN ANWENDEN, UM SIE ZU SCHÜTZEN.

Dasselbe gilt für dich!



AUCH WENN DU ONLINE GEHST, KANNST DU DICH MIT EINIGEN TOOLS UND VERHALTENSWEISEN SCHÜTZEN. GANZ WICHTIG: PASSWÖRTER. SIE SIND DER SCHLÜSSEL FÜR DEIN DIGITALES LEBEN. DEINE PASSWÖRTER VERHINDERN, DASS ANDERE ALLES SEHEN, WAS DU TUST, UND HALTEN ANDERE DAVON AB, DEINE IDENTITÄT IM NETZ ZU MISSBRAUCHEN. DEINE ONLINE-KONTEN UND DEIN SMARTPHONE (FALLS DU EINS HAST) SOLLTEST DU IMMER MIT GUTEN PASSWÖRTERN SCHÜTZEN.

Doch beim Online-Verhalten geht es nicht nur um Sicherheit: Es geht auch um deine persönliche Verantwortung.



WENN DU INFORMATIONEN TEILST, VERBREITEST DU SIE: BIST DU SICHER, DASS ES SICH UM VERLÄSSLICHE INFORMATIONEN AUS EINER SERIÖSEN QUELLE HANDELT? WENN DU EIN FOTO VON DIR TEILST, IST ES ÖFFENTLICH ZUGÄNGLICH: IST ES IN ORDNUNG, WENN ANDERE, EINSCHLIEßLICH DEINEM ZUKÜNFTIGEN ARBEITGEBER UND DEINEN ZUKÜNFTIGEN KOLLEGEN UND KOLLEGINNEN, ES ZU SEHEN BEKOMMEN?

Würdest du das, was du geschrieben hast, auch jemandem ins Gesicht sagen? Wenn du auf einen Link klickst, zeichnet ein Server irgendwo da draußen deinen Klick auf, was normalerweise demjenigen, der sich hinter dem Link verbirgt, mehr Einfluss oder Geld verschafft. Welche Websites und Gruppen möchtest du unterstützen? Mit anderen Worten: Du solltest die Online-Welt als eine reale Welt betrachten, in der jeder Schritt Folgen für andere hat – und in der du Verantwortung trägst. Eine Welt, in der gut überlegte Schritte anderen helfen können, und in der schlechte Entscheidungen anderen Schaden zufügen können.

Wenn du einen Kommentar schreibst, wird dieser von echten Menschen mit echten Gefühlen gelesen.

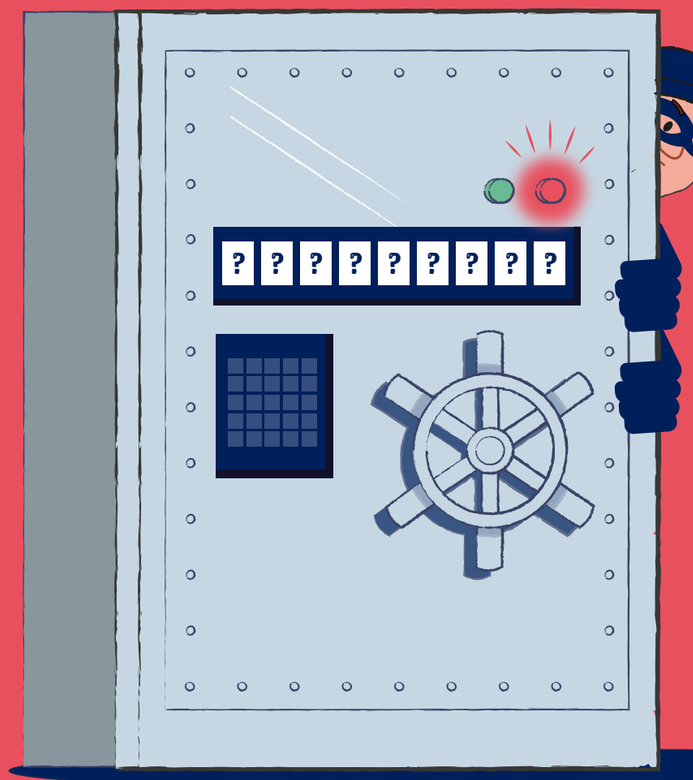
Und dir sollte auch bewusst sein, dass Mobbing und Hasskampagnen massive Online-Probleme sind. Wenn dich das Verhalten anderer verletzt, solltest du das sofort jemandem erzählen, dem du vertraust, zum Beispiel deiner Mutter oder deinem Vater, einem Lehrer oder einer Lehrerin oder einem Freund oder einer Freundin. Behalte das Problem nicht für dich. Such dir Hilfe. Du bist nicht schuld am Mobbing. Also brauchst du dich auch für nichts zu schämen. Du kannst die Nachrichten und Screenshots als Beweismaterial aufbewahren, aber versuch nicht, zu antworten oder zurückzuschlagen oder dich zu rächen. Es ist besser, wenn du dich zurückhältst und eventuell die Nachrichten von Menschen blockierst, die dich verletzen. In vielen Ländern gibt es Hotlines für „Cyber-Bullying“, also Mobbing im Netz. Suche nach einer Hotline in deinem Land und ruf an, um dir Rat zu holen.

SPEAK UP!
GEGEN MOBBING

WENN DU ZEUGE VON MOBBING BIST, IGNORIERE ES NICHT. BEZIEHE STELLUNG UND UNTERSTÜTZE DIE PERSON, DIE DAS ZIEL DES MOBBINGS IST. WENN DU EINE FREUNDLICHE NACHRICHT AN DIESE PERSON SCHICKST, KANN DAS SCHON EINE GROßE HILFE SEIN FÜR JEMANDEN, DER SICH ANGEGRIFFEN UND ALLEINE FÜHLT.

AKTIVITÄT 1

DEIN PASSWORT: MÖGLICHST LAAAANG SOLL ES SEIN



Einfache Wörter sind einfach zu knacken. Du musst also ein Passwort nehmen, das lang ist und für andere außer dir keinerlei Sinn macht. Es gibt verschiedene Methoden, ein Passwort zu erstellen. Das ist eine davon:

Denk dir einen Satz aus und schreibe nur jeweils die ersten beiden Buchstaben aller Wörter. Im Satz sollten einige Großbuchstaben auftauchen, damit dein Passwort Groß- und Kleinbuchstaben enthält.

Zum Beispiel: „Ich lese ein Booklet von der Airbus Foundation!“ wird dann zum Passwort: IcleeiBuvodeAiFo Gut!

PROFI-TIPP

ABER PASS AUF UND SCHREIBE DEIN PASSWORT NIE IRGENDWO AUF: ES SOLLTE NUR IN DEINEM KOPF GESPEICHERT SEIN ... ODER IN EINEM PASSWORT-MANAGER.

AKTIVITÄT 2

UND STARK STATT SCHWACH!

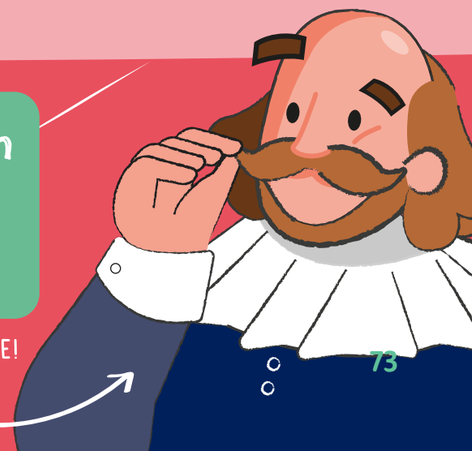
Du kannst einige Wörter durch Zahlen ersetzen, die sich ähnlich anhören. Im vorigen Beispiel könntest du „ein“ durch 1 ersetzen und das Passwort damit stärker machen: Icle1BuvodeAiFo. Und da der ursprüngliche Satz mit einem Ausrufezeichen endete, können wir das am Ende hinzufügen:

Icle1BuvodeAiFo!

Das ist ein Passwort, das nur schwer zu knacken ist! Und du kannst es dir einfach merken, während es andere unmöglich erraten können.

Kannst du raten, welcher Satz sich hinter dem Passwort 2beorno2be,thisthequ verbirgt?

WIR VERRATEN: ES IST DAS BERÜHMTESTE ZITAT VON SHAKESPEARE!



PRÜFE DICH SELBST

Was findest du online über dich heraus?

Stell dir vor, dass die Leiterin einer tollen Firma den besten Job aller Zeiten anbietet ... und zwar dir.

Doch zuvor will sie wissen, wer du bist.
Sie sucht im Internet nach sämtlichen Informationen, Bildern, Videos, Kommentaren usw., die sie über dich finden kann. Was wird sie finden?

Also, das findest du heraus, indem du selbst nach dir im Internet suchst. Gibt es etwas, das die Firmenleiterin nicht lesen soll? Etwas, das sie so überraschen würde, dass sie dich nicht in der Firma haben will? Wenn die Antwort „Ja“ ist, solltest du diese Bilder, Videos oder Kommentare schleunigst löschen. Denke auch daran, dass du deine Datenschutzeinstellungen in den sozialen Netzwerken ändern kannst, damit deine Posts nur eingeschränkt sichtbar sind.

Und am besten ist es natürlich, dass du keine möglicherweise peinlichen Dinge über dich selbst postest!

Zusätzliche Hilfen: Wenn du mehr Tipps über sicheres Verhalten im Internet lesen möchtest, stehen viele Quellen zur Verfügung wie: *Scroller* und *Datakid*.