ÜBUNGS-NL NR. 2, MÄRZ 2014 SICHERHEIT IM INTERNET

Hintergrundinformation für Lehrkräfte

Fächerbezug 8./9. Schulstufe:

Berufsorientierung und Lebenskunde für PTS, Geografie und Wirtschaftskunde für PTS und AHS

Mathematik (Berechnung Prozentsätze und Darstellung als Balkendiagramm, arithmetisches Mittel und Median)

Zeitaufwand: 2 Unterrichtseinheiten

Die **erste Unterrichtseinheit** beschäftigt sich mit den **Internet-Gewohnheiten der SchülerInnen**, die zweite Einheit behandelt **Gefahren im Internet** und **die Erstellung sicherer Passwörter.**

Vorbereitung

1. Ausdruck der Datei „Arbeitsblatt Schülerinnen bzw. Schüler“ 1x pro Person.
2. Pro Gruppe auf 1 Bogen Packpapier jeweils einen Begriff aus der Übung „Gefahren im Internet“ (S. 7) schreiben.

Unterrichtseinheit 1

Aufgabe 1 Vortragsstoff „Internet-Gewohnheiten“

Lehrkraft: Einstieg über „Könnt ihr euch ein Leben ohne Internet vorstellen? Was wäre anders?“ Ideen an der Tafel sammeln! Beispiele:

- keine Freunde über Facebook
- niemand weiß, was ich gerade mache und wo ich bin
- keine Verbindung zu meinen Freunden über WhatsApp
- ich kann mir meine Hausübungen nicht mehr über Google erleichtern

Zeitaufwand: 10 Minuten

In der nun folgenden Aufgabe wird die Internet-Nutzung der Schülerinnen bzw. Schüler erhoben, im Anschluss daran werden die Vor- und Nachteile besprochen.

Aufgabe 2 „Internet-Nutzung für SchülerInnen“

Lehrkraft teilt die Klasse in Gruppen zu je 3 bis 5 ein und gibt folgende Aufgaben:

Diskussion

- Besprecht in der Gruppe, wie viel Freizeit ihr an einem normalen Schultag habt (24 Stunden minus Schlafen, Schule, Zeitaufwand für den Schulweg, Hausübungen usw.)?
- Wie viel davon verbringt ihr im Internet mit Surfen, Spielen, sozialen Medien usw.?

Zeitaufwand: 10 Minuten

Tragt nun das Ergebnis eurer Diskussion in der Tabelle unten ein, jede Schülerin bzw. jeder Schüler für sich:

- Schreibt zuerst euren Vornamen in das Feld ganz oben.
- Alle nun folgenden Zeitangaben in Minuten:
- Tragt nun die folgenden Werte ein: „Gesamte Freizeit“ an einem normalen Schultag und die gesamte Zeit, die ihr täglich im Internet verbringt („Internet gesamt“). Subtrahiert die beiden Zahlen und ihr erhaltet die „Restliche Freizeit“.
- Dann schreibt in der Zeile „Internet-Nutzung aufgeteilt“ im mittleren Teil der Tabelle die Mi-nuten, die ihr täglich für die einzelnen Internet-Anwendungen aufwendet. Die linke, grau gekennzeichnete Spalte „Internet gesamt“ muss wiederum die gesamte Anzahl in Minuten ergeben.

Zeitaufwand: 5 Minuten

Anmerkung für die Lehrkraft: In einer kürzlich in Deutschland veröffentlichten Studie gab ein Teil der Jugendlichen an, sie seien ständig online und könnten daher gar nicht sagen, wie viel Zeit sie im Internet verbringen, ihr „analoges“ Leben verschmelze völlig mit dem „virtuellen“. Trotzdem – oder vielleicht gerade deshalb – sollten Schülerinnen bzw. Schüler, bei denen das zutrifft, ihren Internet-Konsum kritisch hinterfragen und überlegen, wie lange sie tatsächlich täglich das Internet nutzen.

Berechnung Prozentsätze

Nun berechnet die Prozentsätze, den ihr durchschnittlich täglich für das Internet gesamt und für die einzelnen Anwendungen aufwendet, bezogen auf die gesamte Tagesfreizeit (= 100 %). Tragt diese Prozentsätze in die Tabelle ein.

Zeitaufwand: 5 Minuten

UE 1 Aufgabe 1											
Vorname											
An einem normalen Schultag:											
Gesamte Freizeit							..... **Minuten**				
Internet gesamt							– ..... **Minuten**				
Restliche Freizeit (= Gesamte Freizeit minus Internet gesamt)							= ..... **Minuten**				
Tägliche durchschnittliche Internet-Nutzung											
	Internet gesamt	Surfen		Internet-Spiele	Soziale Medien						Sonstiges
		für die Schule	Sonstiges		Face-book	Whats App	You Tube	Google+	Insta-gram	Sonstige	
Internet-Nutzung aufgeteilt (in Minuten)											
Prozentsätze											
in % der gesamten Tagesfreizeit (= 100 %)											

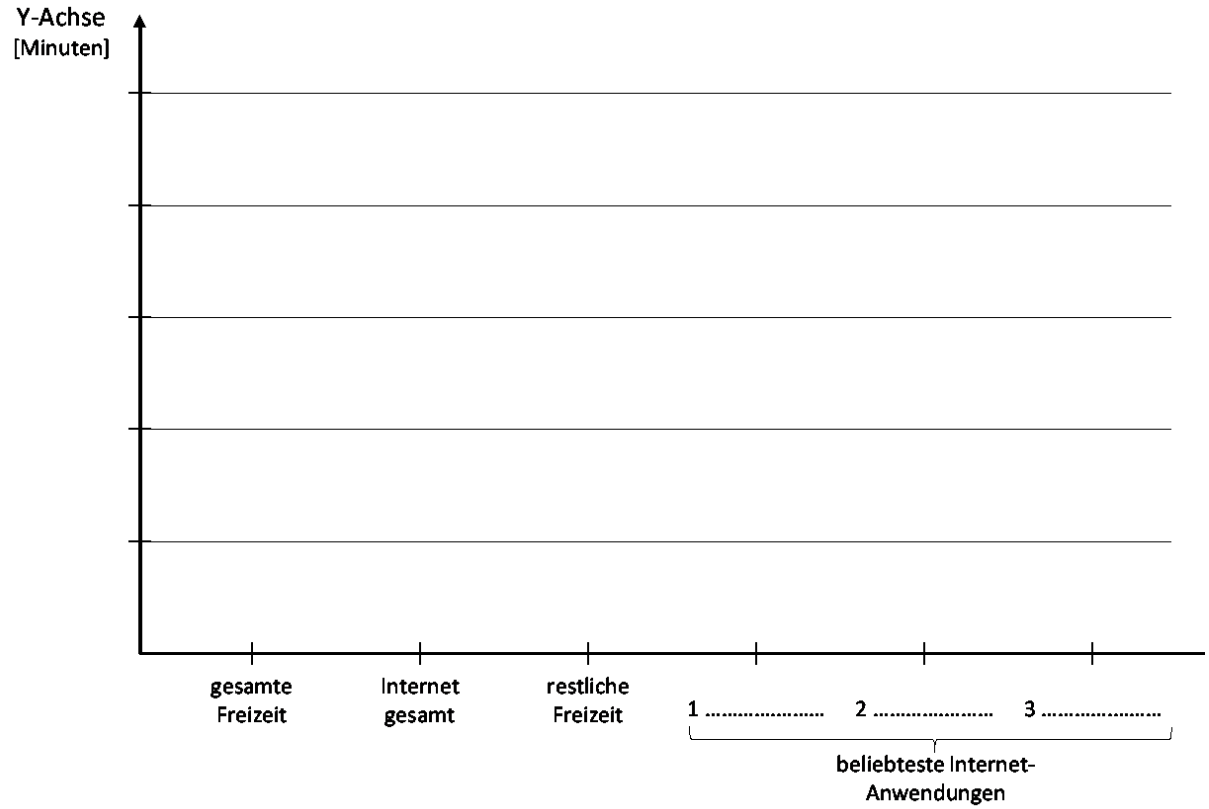
Zeichnung Balkendiagramm

Zeichnet nun ein Balkendiagramm mit folgenden Werten aus der Tabelle (Y-Achse in Minuten; den Maßstab der Y-Achse müsst ihr selbst festlegen):

- Gesamte Freizeit,
- Internet gesamt,
- restliche Freizeit und
- eure 3 beliebtesten Internet-Anwendungen (jene mit den höchsten Minutenwerten). Schreibt auch dazu, um welche Internet-Anwendung es sich handelt.
- Tragt bei jedem Balken auch den jeweiligen Minutenwert ein.
- Ein Tipp für die Festlegung des Maßstabes der Y-Achse: Beginnt mit dem größten Wert („Gesamte Freizeit“).

Zeitaufwand: 5 Minuten

Di



Aufgabe 3 „Mittelwert und Median der ganzen Klasse (Internet gesamt)“

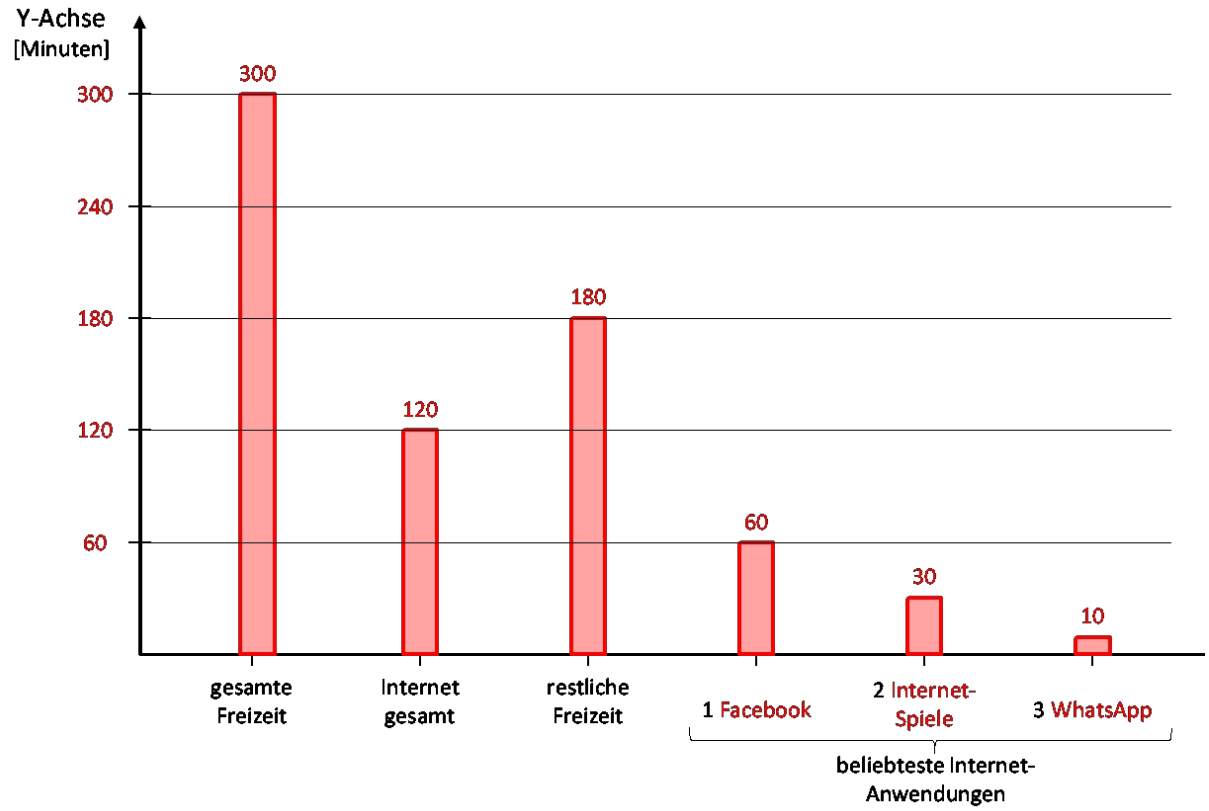
Lehrkraft fordert die Klasse auf, ihre tägliche gesamte Zeit, die sie im Internet verbringen, auf die Tafel oder eine Flipchart zu schreiben – am besten gleich in aufsteigender Reihenfolge, um den Median möglichst einfach berechnen zu können. Dann werden (arithmetischer) Mittelwert und Median der ganzen Klasse berechnet.

Zeitaufwand: 15 Minuten

Hintergrundinformation Berechnung und Balkendiagramm

Der jeweilige **Prozentsatz** wird durch Division der Minutenwerte der gesamten und der jeweiligen Internet-Anwendungen durch die Minuten der gesamten Tagesfreizeit (= 100 %) ermittelt.

Beispiel für das **Balkendiagramm** (in ***ROT*** alles, was die Schülerinnen und Schüler eintragen sollten):



Der **Mittelwert** (das arithmetische Mittel) ist der Quotient aus der Summe aller Werte und der Anzahl der Werte (hier der Summe der gesamten Internet-Nutzung der ganzen Klasse durch die Anzahl der Schülerinnen bzw. Schüler).

Der **Median** teilt eine Liste von Werten in zwei Hälften. Er kann auf folgende Weise bestimmt werden (hier wieder bezogen auf die gesamte Internet-Nutzung der ganzen Klasse):

- Alle Werte werden (aufsteigend) geordnet.
- Wenn die Anzahl der Werte ungerade ist, ist die mittlere Zahl der Median.
- Wenn die Anzahl der Werte gerade ist, wird der Median meist als arithmetisches Mittel der beiden mittleren Zahlen definiert, die dann Unter- und Obermedian heißen.

Unterrichtseinheit 2

Aufgabe 1 Vortragsstoff „Gefahren im Internet“

Folgender Fall beschäftigte kürzlich ganz Österreich:

Datenpanne in Österreich: Schülerdaten im Netz veröffentlicht

Österreichische Schulen können das Niveau ihrer Schüler testen lassen, online und geheim. Doch dann passiert eine Panne: Testergebnisse von Schülern und E-Mail-Adressen von Lehrern tauchen ungeschützt auf einem rumänischen Server auf.

Die vertraulichen Testergebnisse von 400.000 Schülern aus Österreich sind versehentlich im Internet öffentlich geworden. Auf einem Server in Rumänien fanden sich neben den Ergebnissen aus der sogenannten Informellen Kompetenzmessung (IKM) der Jahre 2011 und 2012 auch die E-Mail-Adressen von 37.000 Lehrern.

Quelle: n-tv technik ***http://www.n-tv.de/technik/Schuelerdaten-im-Netz-veroeffentlicht-article12350801.html*** , abgefragt am 17.3.2014.

Das zeigt, dass auch die Profis vom Bildungsinstitut BIFIE, das die PISA- und sonstigen Tests zu den Bildungsstandards durchführt, vor Datenlecks nicht sicher sind. Das Internet ist zwar eine unglaublich spannende Sache, trotzdem muss man sich schützen: Durch regelmäßige Updates der Viren-Software, durch die Verwendung sicherer Passwörter, durch eine regelmäßige Überprüfung der Einstellungen in den Sozialen **Medien** und vieles mehr. **Und noch etwas ganz Wichtiges**:

Das Internet vergisst nicht! Was einmal im Netz steht, kann nicht mehr „zurückgeholt“ werden. Und man kann es weltweit über Suchmaschinen abfragen. Zwar kann man die Löschung verschiedener Daten beantragen, allerdings: Kontrolle, ob diese Daten vollständig gelöscht wurden, gibt es keine. Und außerdem: In der Zwischenzeit könnte der eigene Eintrag von jemandem kopiert und weiterverbreitet worden sein. Diese Kopien entziehen sich ganz sicher jeglicher Kontrolle.

Daher: Vertrauliche persönliche Daten gehören nicht ins Internet - das schützt am besten vor Cyber-Mobbing. Vor jedem Posting sollte man genau überlegen, ob man diese Information wirklich öffentlich machen will, ob es für einen selbst oder jemand anderen sogar peinlich sein könnte, und ob man dazu – auch noch in der Zukunft – steht.

Aufgabe 2 Recherche „Gefahren im Internet“

Lehrkraft teilt Schülerinnen bzw. Schülern in **Gruppen zu je 3 bis 5** ein und gibt an jede Gruppe einen der vorbereiteten Bögen Packpapier, auf dem einer der folgende Begriffe geschrieben ist: Spam, Phishing, Viren, Scams, Grooming, In-App-Käufe, Bezahlen bei Internet-Auktionen.

Recherche

- Besprecht in der Gruppe, was der jeweilige Begriff bedeutet. Wie kann man sich dagegen schützen bzw. was muss man beachten?
- Schreibt das Ergebnis eurer Diskussion auf das Packpapier.

Optional: Nachdem die Schülerinnen und Schüler ihre Packpapierbögen beschriftet haben, können sie die Packpapiere der jeweils anderen Gruppen ergänzen.

Die Lehrkraft kontrolliert die Antworten und ergänzt sie gegebenenfalls.

UE 2 Aufgabe 1 Hintergrundinformation „Gefahren im Internet“

Zeitaufwand: 15 Minuten

UE 2 Aufgabe 1 Hintergrundinformation „Gefahren im Internet“

- Als Spam oder Junk versteht man jede Art von unerwünschten E-Mails – meist handelt es sich dabei um Massenaussendungen mit werbendem Inhalt. Spams sind zu einer echten Plage im Internet geworden: Nach einer Schätzung aus dem Jahr 2009 machten in den USA Spam-Mails 89 bis 97 % des gesamten E-Mail-Verkehrs aus. Diese rund 60 Billionen Spams verbrauchten ca. 30 Milliarden Kilowattstunden Energie, zum Sichten und Löschen der Mails waren 100 Milliarden Stunden Arbeitszeit erforderlich.

Wie kann man sich dagegen schützen?

> **Verwendung von 2 E-Mail-Adressen**: Während die berufliche Mailadresse, die nur schwer geändert werden kann, nur für „seriöse“ Anwendungen verwendet wird und damit öffentlich kaum einsehbar ist, nutzt man die zweite Mailadresse - die keine Rückschlüsse auf die Person zulässt - für Communities, Soziale Medien, Gästebücher, Gewinnspiele usw. Diese zweite Mailadresse sollte bei einem der großen Webmail-Provider registriert werden, da diese über einen üblicherweise guten Spamfilter verfügen (z.B. GMX, Yahoo, Google; siehe den folgenden Punkt).
> **Spamfilter eines Webmail-Providers**: Diese Spamfilter werden meist kostenlos angeboten und löschen im Idealfall die Spams nicht, sondern kennzeichnen diese lediglich oder verschieben sie in einen eigenen „Spamordner“.

Spamfilter des eigenen E-Mail-Programms am Computer: Diese Filter sind meist selbstlernend, d.h., sie können sich den Bedürfnissen der BenutzerInnen anpassen. Zusätzlich sind sie in der Regel engmaschiger als jene der Webmail-Provider. Wie das Anlernen erfolgt, entnimmt man am besten der Anleitung des E-Mail-Programmes.

Hat man trotz der Filter ein Spam erhalten, sollte man die Mail auf keinen Fall öffnen. Öffnet man die Mail nämlich, erhält der Spammer die Information, dass an diese Adresse gesendete Mails gelesen werden – was für ihn eine wichtige Information darstellt. Er wird daraufhin noch mehr Spams schicken. Einzige empfehlenswerte Vorgangsweise: Löschen der Mail.

- Unter **Phishing**, einem Kunstwort aus „password“ und „fishing“, versteht man Versuche von Betrügerinnen bzw. Betrüger, durch E-Mails oder gefälschte Websites an geheime Daten wie Passwörter, TAN-Codes des Bankkontos und ähnlichem zu gelangen. Betrugsopfer werden üblicherweise aufgefordert, ihre Zugangsdaten per Mail zu versenden oder sie werden auf täuschend echt nachgebaute Websites ihrer Bank umgeleitet.

Wie kann man sich dagegen schützen?

Sensible Daten niemals mittels Mail versenden! Banken, Online-Häuser und dergleichen fragen solche Daten keinesfalls per Mail ab.
Telefonische Rückfrage etwa bei der Hotline der Bank, ob die Mail echt ist.
Banken verwenden immer SSL-Verschlüsselung bei Internet-Verbindungen (am Schloss-Symbol und der Webadresse ***https://www*** erkennbar). Da auch kopierte Websites gelegentlich eine SSL-Verschlüsselung verwenden: Immer auch die Adresszeile (URL) kontrollieren!

Und noch eine Möglichkeit gibt es, falsche Webseiten aufzuspüren: „WOT“ (Web of Trust - Netz des Vertrauens; ***https://www.mywot.com***), eine der größten Bewertungsplattformen für Websites, gibt es gratis als Browser-Erweiterung. Ein Ampelsystem zeigt an, wie zuverlässig eine Website von den Nutzern bewertet wird.

- **Viren** (als Überbegriff, die Terminologie ist hier nicht einheitlich) sind Schadprogramme, die sich selbständig ausbreiten können und meist Schaden anrichten. Heutzutage haben sie gelegentlich auch noch eine andere Funktion: Sie übernehmen die befallenen Computer als „Zombies“, die ohne Wissen der Besitzer von außen ferngesteuert und etwa für die Aussendung von Spam- oder Phishing-Mails missbraucht werden.

Wie kann man sich dagegen schützen?

Keine unbekannten Dateianhänge in E-Mails herunterladen, öffnen oder ausführen.

Regelmäßige Updates des E-Mail-Programms, des Betriebssystems, der Antiviren-Software und der Firewall.

- Unter Scams (Vorschussbetrug) versteht man Handlungen, wo den E-Mail-EmpfängerInnen ein angeblicher Lottogewinn, eine Erbschaft oder ein anderes lukratives Geschäft mitgeteilt wird. Im Zuge der Mail-Konversation fordert dann der Scammer auf, Geld für entstandene Spesen, Flugtickets oder Steuern zu überweisen – dieses Geld ist unwiederbringlich verloren.

Wie kann man sich dagegen schützen?

Mails mit einem derartigen Inhalt einfach ignorieren – niemand hat etwas zu verschenken.

- **Grooming** ist das gezielte Ansprechen von Personen mit dem Ziel sexueller Kontakte. Pädophile Erwachsene geben sich dabei im Internet als Jugendliche aus, um das Vertrauen von Kindern zu erschleichen. Durch subtiles Vorgehen erhalten die Erwachsenen Informationen über Wohnort, Hobbys und Interessen der Kinder und bauen so eine Beziehung zu ihren Opfern auf. Die damit verbundenen Straftaten sind kinderpornografische Aufnahmen und sexueller Missbrauch. Seit 2012 ist Grooming bei unter 14-jährigen Personen durch § 208a StGB unter Strafe gestellt.
- **In-App-Käufe** können zur Kostenfalle werden: Vermeintlich als „kostenlos“ beworbene Spiele im Internet bieten häufig die Möglichkeit, kostenpflichtige Upgrades für neue Spielfiguren oder spannendere Spiellevel zu bestellen. Problematisch ist die Sache deswegen, weil die Aufforderung zum Kauf über Smartphone oder Computer direkt an die Kinder und Jugendlichen geht, und so die Genehmigung der Erziehungsberechtigten umgangen wird.
- Über **Internet-Auktionen** (z.B. auf eBay) werden täglich Unmengen an Waren gehandelt – Kleidungsstücke, Handys, Notebooks und was es sonst noch alles gibt. Wie im täglichen Leben gibt es aber auch hier Betrügereien. Deshalb sollte möglichst keine Vorauskasse vereinbart werden, sondern Bezahlung per Nachnahme, Zahlschein oder – bei persönlicher Abholung – auch Barzahlung. Vor allem bei größeren Beträgen empfehlen sich Treuhandsysteme: Hier wird das Geld an die Verkäufern erst überwiesen, wenn die Ware bei den Käufern eingelangt ist.

Aufgabe 3 Vortragsstoff „Sichere Passwörter“

Lehrkraft: Einstieg über „Wir reden nun über Passwörter. Was glaubt ihr: Ist „Karli1“ ein sicheres Passwort? Oder „Susi23“? Oder „12345“? – Nein, sie sind es ganz sicher nicht.“

Passwörter sind wichtig, weil sie den Zugang zum eigenen Computer oder Smartphone schützen. Wer möchte schon, dass andere unbefugt lesen können, was ich geschrieben habe, sich ohne meine Erlaubnis meine Fotos ansehen oder sich meine Lieder anhören? Damit Passwörter wirklich Schutz bieten, muss man einige Grundsätze zum Erstellen sicherer Passwörter beachten:

- Keine einfachen Wörter oder Namen (Passwort-Cracker verwenden häufig Programme, die alle Einträge eines Wörterbuchs durchprobieren), keine Geburtsdaten oder einfachen Zahlenfolgen. NICHT sicher sind .z.B.: „Schule“, „Karli“, „25.4.2001“, „12345“.
- Zeichenfolgen, die man sich selbst merkt, aber von niemand anderem erraten werden können. Diese sollten 6 bis 8 Zeichen umfassen und aus einer Kombination von Buchstaben, Sonderzeichen, Zahlen und Groß-/Kleinschreibung bestehen. Beispiel: „Ig$8Jid$“.

Wie kann man sich aber nun solche Zeichenfolgen merken? Eine Möglichkeit besteht darin, einen Satz, den man sich leicht merken kann zu nehmen, und jeweils nur die Anfangsbuchstaben aufzuschreiben. ZB wird dann aus „Ich gehe seit 8 Jahren in die Schule“ „Igs8JidS“. Ersetzt man nun noch einzelne Buchstaben durch Sonderzeichen, die dem Buchstaben ähneln (in diesem Fall wird etwa „s“ und „S“ durch „$“ ersetzt), ergibt sich vorhin erwähntes „Ig$8Jid$“.

- Unterschiedliche Passwörter für die diversen Anwendungen und Websites, denn: Wird ein Passwort geknackt, kann nur die jeweilige Anwendung missbräuchlich verwendet werden.
- Regelmäßige, möglichst vollständige Änderung der Passwörter.

Aufgabe 3 “Erstellen sicherer Passwörter“

Lehrkraft teilt an die Schülerinnen bzw. Schüler kleine Zettel aus und gibt folgende Aufgabe:

- Erstellt 2 sichere Passwörter, die ihr euch merken könnt.

Die Zettel werden dann eingesammelt, einzelne Beispiele vorgelesen und gefragt, wie man sich das jeweilige Passwort merken kann.

Zeitaufwand: 25 Minuten