8_1 Passwörter
8_2 Kritisches Surfverhalten
8_3 Browser und Internet-Café
8_4 Digitaler Fußabdruck
8_5 W-LAN
8_6 Datensicherung

Sachinformation

Passwortepidemie

E-Mail-Konto, Onlineshop, Onlinebanking oder Chat, egal, um welchen Internetdienst es sich handelt: Passwörter (sind übrigens synonym zu Kennwörtern) sind zur Identifizierung des Nutzers unerlässlich. Sie erlauben dem Nutzer, sich vor unerlaubten Eingriffen von Fremden zu schützen. Und wer ein Passwort sucht, sollte es zuerst mit den Namen des Partners/der Partnerin, den Kindernamen und dem Haustier versuchen, denn allzu viele vergeben leichtsinnig Passwörter und erleichtern es den „Bösen Buben" damit. Die Top Ten der Passwörter in Europa: Haustiername, Hobby, Geburtsname Mutter, Geburtstag Familienmitglied, eigener Geburtstag, Name des Partners, eigener Name, Lieblings-Fußballmannschaft, Lieblingsfarbe und Name der Grundschule (erhoben von MacAfee, veröffentlicht in Focus 42/2007 vom 15.10.2007, S.18)

Das Problem

Folgende Punkte sollte man im Umgang mit Passwörtern vermeiden:

- keine im Wörterbuch (Duden) zu findenden Wörter
- keine (Kose-) Namen
- nicht dasselbe Passwort für mehrere Webdienste nutzen
- Passwörter nicht in E-Mails oder Ähnlichem weitergeben
- Passwörter nicht auf einem Zettel in der Nähe des PCs aufbewahren
- vor der Eingabe des Passwortes sollte immer darauf geachtet werden, dass die Webseite nicht über einen Link, sondern selbst angewählt wird (Achtung: Phishing-Mails!)

Warum Passwörter nicht per Zettel am PC hängen oder in einer E-Mail weitergegeben werden sollen, ist leicht verständlich. Warum aber keine Dudenwörter? Dazu muss man wissen, wie manche Passwort-Knacker-Software arbeitet. Sie benutzen eine „brutale" Methode („Brute-Force" genannt) und probieren einfach alle im Duden vorkommenden Wörter aus, per Software geht das innerhalb von Minuten. Der Datenschutzbeauftragte des Kantons Zürich schreibt dazu: „Es existieren neben den reinen Brute-Force und den Hybrid-Attacken weitere Methoden, um Passwörter zu finden. Am Labor für Sicherheit und Kryptografie der ETH Lausanne wurde die Methode „Rainbow Table" entwickelt, bei welcher durch Vorausrechnen einer grossen Anzahl von Passworten ein erheblich schnelleres Finden des Kennworts möglich wird." (Quelle: **www.passwortcheck.datenschutz.ch**)

Vorbeugung

Der beste Schutz ist selbstverständlich die Wahl eines starken Passwortes. Aber wie sollte ein starkes Passwort aussehen? Ein starkes Passwort besteht bestenfalls aus Groß- und Kleinbuchstaben sowie aus verschiedenen Ziffern und Sonderzeichen wie z. B. */%#. Des Weiteren sollten Passwörter mindestens acht Zeichen haben. Damit ein Passwort schwer zu erraten ist, sollte es eine scheinbar sinnlose Zeichenfolge enthalten. Zusammenfassend kann Folgendes festgehalten werden:

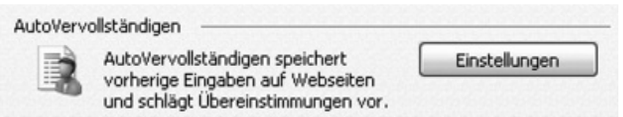
- Das Passwort sollte aus mindestens acht Zeichen bestehen.
- Dabei sollte es sich aus Zahlen, Buchstaben und Sonderzeichen zusammensetzen (Bsp.: 7uz6"Fb4); auf Groß- und Kleinschreibung achten!
- Das Passwort sollte dennoch gut zu merken sein und in angemessenen Zeitabständen gewechselt werden.
- Das Passwort geheim halten.

Ein guter Tipp für die Passworterstellung ist, ein System zu verwenden. So könnten sie bspw. alle „a" in Namen durch die Zahl „1" ersetzen, aus dem Passwort „Andrea" würde „1ndre1". Oder man fügt die Telefonnummer ein, nach jedem Buchstaben eine Ziffer, so würde aus „Willi" und „876530" das Passwort „W8i7l6l5i3". Oder sie merken sich kurze Sätze wie z. B. „Morgens stehe ich auf und putze meine Zähne." und verwenden nur jeweils die ersten Buchstaben: „MsiaupmZ". Welches System auch immer Verwendung findet, man sollte es sich selbst ausdenken, geheim halten und sich gut merken! Weitergehende und ausführlichere Informationen hat das Bundesamt für Sicherheit in der Informationstechnik unter **www.bsi-fuer-buerger.de** (unter „Schützen – aber wie?", „Passwörter") bereitgestellt.
Warum ausgerechnet acht Zeichen? Hier kommen die Mathematik-Kolleginnen und -Kollegen zum Zuge: Die

Menge aller Kleinbuchstaben, Großbuchstaben, Ziffern sowie einiger Sonderzeichen ergibt ca. 80 mögliche Zeichen und damit ca. 1 680 000 000 000 000 mögliche Kombinationen. Bei einem Computer, der eine Million Kombinationen pro Sekunde ausprobiert, dauert es rechnerisch 25 Jahre, die richtige Kombination zu knacken. Bei einer Länge von nur sechs Zeichen habe ich nur noch ca. 262 000 000 000 mögliche Kombinationen. Das ließe sich mit dem o. a. Computer in 36 Stunden schaffen.

Verwaltung der Passwörter

Eine der wohl gefährlichsten Funktionen ist die Möglichkeit, Passwörter vom Computer speichern zu lassen. So werden sie bspw. im Internet-Explorer gefragt, ob Sie das Passwort speichern möchten (Funktion „Auto-Vervollständigen").



Beim nächsten Aufruf der Seite brauchen sie es nicht mehr eingeben. Schön bequem und schön gefährlich. Selbstverständlich kann auch der nächste Benutzer des Computers diese Funktion nutzen und wie sicher ihre Daten auf dem heimischen PC sind, ist im Kapitel 7_2 „Viren, Würmer, Trojaner und Spyware" nachzulesen.

Screenshots: Im Internet-Explorer die Registerkarte „Extras – Internetoptionen – Inhalte – Autovervollständigen Einstellungen. Hier sollten keine Häkchen gesetzt sein.

Screenshots: Im Internet-Explorer 7 die Registerkarte „Extras – Internetoptionen – Allgemein – Browserverlauf löschen". Hier können sie mit einem Klick auf „Alle löschen" alle Passwörter (hier Kennwörter genannt) löschen. Beim Mozilla Firefox 2 ist diese Option unter „Extras – Private Daten löschen" sowie unter „Extras – Einstellungen – Datenschutz" zu finden.

Neben diesen browserinternen Verwaltungsmöglichkeiten bieten einige Hersteller Software zur Verwaltung von Passwörtern auf der Festplatte an. Mit einem „Master-Passwort" sind alle anderen zu sichern, d. h. man muss sich nur ein Einziges merken. Hier ist Vorsicht geboten: Nur wirklich seriösen Anbietern sollte man Vertrauen schenken.

Passwort-Check
Einige Webseiten bieten die Möglichkeit, sein Passwort zu testen. Man gibt es ein und erhält eine Beurteilung. Auch hier bitte Vorsicht! Nie das tatsächliche Passwort verwenden, sondern nur ein ähnlich aufgebautes, denn wer garantiert, dass die Seite das Passwort nicht speichert? Unter **https://passwortcheck.datenschutz.ch** kann man beim Datenschutzbeauftragten des Kantons Zürich in der Schweiz bspw. beliebige Passwörter auf ihre Sicherheit überprüfen lassen. Man erhält einen detaillierten Prüfbericht mit vielen Kriterien für eine sichere Wahl.

TIPP: Geben sie kein aktuell genutztes Passwort ein. Probieren sie zur Überprüfung ein Passwort aus, welches nach demselben Schema zusammengestellt ist, wie das Passwort, welches sie tatsächlich nutzen.

Captchas
Für Internetanbieter stellt sich das Problem, erkennen zu müssen, ob sich ein Mensch oder eine Software (automatisch) anmeldet. Der Vollständigkeit halber seien noch die bekannten Zerrbilder mit Zahlen- oder Buchstabenkombinationen erwähnt, die man inzwischen bei zahlreichen Anmeldeprozeduren eingeben muss. Diese Symbole heißen „Captchas" (übrigens das Akronym für Completely Automated Public Turing test to tell Computers and Humans Apart) und sollen sicherstellen, dass sich tatsächlich ein Mensch anmeldet und keine Software (sog. „Bots"). Auch diese sind nicht mehr 100%ig sicher und manche Firmen gehen dazu über, Bilder zu zeigen, die wirklich nur Menschen unterscheiden können, aber keine Maschinen.

Links

www.internet-abc.de (unter „Suchen und Finden von A-Z")	Glossar des Internet-ABC
www.sicherheit-macht-schule.de (unter „Schutz der Privatsphäre", „Starke Passwörter")	die Aktion „Sicherheit macht Schule" der Firma Microsoft zum Thema Passwörter
www.klicksafe.de	das Thema Passwörter bei klicksafe.de: „Wie sollte ein sicheres Passwort aussehen?"
www.lizzynet.de/dyn/106731.php	Hinweise zum sicheren Passwort bei Lizzynet von Schulen ans Netz (für Mädchen)
www.secure-it.nrw.de (Pfd-Datei zum Download unter „Angebote für die Schule")	Material der Initiative secure-it.nrw für die Grundschule, mit Thema Passwörter: „Internetfibel für die Grundschule", „Wie sicher ist mein PC?"

8_1 Passwörter
8_2 Kritisches Surfverhalten
8_3 Browser und Internet-Café
8_4 Digitaler Fußabdruck
8_5 W-LAN
8_6 Datensicherung

Methodisch-didaktische Hinweise

Arbeitsblatt	▶●●	▶▶●	▶▶▶
Zeitangabe (Unterrichtsstunden)	1–2	1	2
Ziele	Die Schülerinnen und Schüler nähern sich spielerisch dem Thema Passwortschutz, indem sie eigene Passwörter anhand verschiedener Systeme entwickeln.	Die Schülerinnen und Schüler wissen Regeln für den Passwortschutz und lernen ein System kennen, mit dem sie sich Passwörter merken können.	Die Schülerinnen und Schüler lernen die gängigsten Methoden zum Passwortknacken und die wichtigsten Bewertungskriterien für sichere Passwörter kennen.
Methode/n	Geheimsprache	Passwortsystem erfinden	Passwortcheck
Organisationsform/en	Einzel, Partner, U-Gespräch, Erwachsenenintegration	Einzel, U-Gespräch	Einzel, U-Gespräch
Zugang Internet **Zugang PC**	nein nein	ja ja	ja ja

Kommentare zu den Arbeitsblättern

▶●●

Mit diesem Arbeitsblatt sollen sich die Schülerinnen und Schüler dem Thema Passwortschutz spielerisch über den Einstieg „Geheimsprache“ nähern, der hier mit einer Nummerierung des Alphabets gemacht ist. Ihre Schülerinnen und Schüler erfinden sicherlich eine schwierigere Geheimsprache (s. Arbeitsauftrag). Die Tipps für gute Passwörter können auch die jüngeren Schülerinnen und Schüler nachvollziehen, vielleicht sollten sie die einzelnen Punkte verdeutlichen (siehe Sachinformationen oben).
Der letzte Punkt dient der Überprüfung, wobei selbstverständlich das Ziel sein sollte, dass niemand das Passwort „knacken“ kann. Hier ist der Spagat wichtig zwischen der Notwendigkeit, sich Passwörter gut merken zu können und ihrem Schutz.

Erfahrungsgemäß brauchen die Schülerinnen und Schüler ein wenig Unterstützung bei der „Geheimsprache“ des letzten Arbeitsauftrages. Hier sollen sie für sich ein System entwickeln, mit dem die Wörter gut zu merken sind. Ich verwende das Beispiel auf der nächsten Seite.
Danach können sie sehr schnell einsehen, dass man mit diesem System viele verschiedene, gute Passwörter erstellen kann, denn ich brauche nur den Ausgangsnamen verändern (eigener Name, Name der Mutter, des Vaters, der Haustiere etc.). In diesem Fall ist auch eine kleine Notiz wie „Mail=Hund“ nicht schlimm, denn niemand kennt das System. „Passwörter niemals verraten“ lautet der Lösungssatz.
Immer 2 Zahlen zusammen nehmen und den Buchstaben davor wählen (Bsp: 16=p;01=a)

Merken	Passwort	Beschreibung
Mein Hund heißt:	Naischa	Leicht zu merken.
Alle Vokale in Großschreibung:	nAIschA	Die Selbstlaute sind groß geschrieben, alles andere klein.
Meine Telefonnummer lautet 765499; immer abwechselnd ein Buchstabe und eine Zahl:	N7A6I5s4c9h9A	Die Telefonnummer ist eingebaut.
Das Ganze immer in Klammern, damit der Hund nicht wegläuft:	(N7A6I5s4c9h9A)	Es wurden Klammern gesetzt.

Mit der Adresse **https://passwortcheck.datenschutz.ch/check** steht ein Tool zur Verfügung, sein Passwort zu testen. Dabei sollte den Schülerinnen und Schülern klar gemacht werden, dass man nie sein tatsächliches Passwort dort eingibt, denn trotz der Seriosität des Schweizer Datenschutzbeauftragten sollte man im Internet nie auf einer unbekannten Webseite ein richtiges Passwort eingeben. Die Tabelle zum 1. Arbeitsauftrag ist oben erläutert.

Die Jugendlichen sollen die Bewertungskriterien für „starke" Passwörter einschätzen, wodurch sie hoffentlich einsichtiger werden. Bestenfalls geben sie sich anschließend sichere Passwörter, die viele der Kriterien erfüllen. Im 2. Arbeitsauftrag ist ein Problem angesprochen, das alle Passwörter haben, die z. B. „§1.C4QM0" lauten: Man kann sie sich schlecht merken. Wie oben erwähnt, Passwörter sollten möglichst in ein merkbares System eingebettet sein.

Möglichkeiten zur Weiterarbeit „Lust auf mehr"

„Sicherheit macht Schule" ist eine Initiative der Firma Microsoft. Sie bietet auf ihren Seiten zwei interessante Unterrichtsideen zum Thema. Die Erste basiert auf der ältesten bekannten Chiffrierung, der Cäsarverschlüsselung, einer Verschiebechiffre: **www.sicherheit-macht-schule.de**. Die zweite Unterrichtsidee behandelt sichere Passwörter: Auch ein historischer Ansatz ist sicherlich spannend, wie z. B. der im Zweiten Weltkrieg spielende Film „Enigma" zeigt.

Arbeitsblatt vom **Name:** .....

Kennst du eine Geheimsprache?

Die Kunst der Geheimsprache wird seit Jahrtausenden gepflegt. Früher war sie nur für Könige und Generäle interessant, aber im Computerzeitalter brauchen wir alle eine Geheimsprache. Wir brauchen sie für die vielen Passwörter. Übrigens … Kennwörter ist nur ein anderer Name für Passwörter!

Hier ist ein Beispiel für eine Geheimsprache:
160119192315051820051814090513011219 2205181801200514

1. Arbeitsauftrag:
Entschlüssle die Geheimsprache oben! Vergleicht eure Ergebnisse in der Klasse.

Zu einer Geheimsprache gehört immer ein „Schlüssel", mit dem man sie wieder „entschlüsseln" kann.
Hier der Schlüssel der Geheimsprache oben:
a01 b02 c03 d04 e05 f06 g07 h08 i09 j10 k11 l12 m13 n14 o15 p16 q17 r18 s19 t20 u21 v22 w23 x24 y25 z26

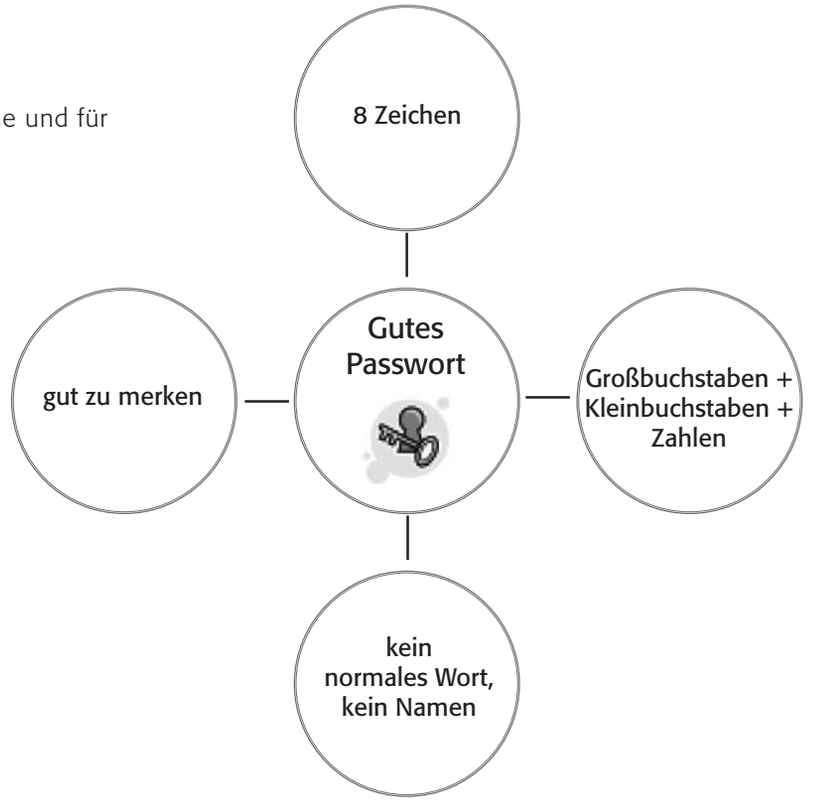
2. Arbeitsauftrag:
Erfinde eine eigene Geheimsprache, in der auch Zahlen vorkommen können.

3. Arbeitsauftrag:
Zeige sie deiner Nachbarin/deinem Nachbarn und lasse sie „entschlüsseln"!

Passwörter sind auch eine Art Geheimsprache und für gute Passwörter gibt es ein paar Tipps:

4. Arbeitsauftrag:
Erfinde gute Passwörter in einer Geheimsprache, die du dann auch für dein Postfach verwenden kannst. Diesmal darfst du sie aber niemandem verraten!

5. Arbeitsauftrag (Hausaufgabe):
Kontrolliere mit deinen Eltern ihre Passwörter! Denke daran: Sie müssen sich ein eigenes System überlegen!



Arbeitsblatt vom **Name:**

Sichere Passwörter – wie geht das?

„Statt vom Computerzeitalter sollte man lieber vom Passwortzeitalter sprechen", stöhnt Jasmin beim Abholen ihrer E-Mails. „Ich verwende immer das gleiche: Nicolo – so heißt mein Meerschweinchen und das vergesse ich niemals". „Danke für die Information", antwortet ihr jüngerer Bruder, „Ich habe mir ein todsicheres System ausgedacht". „Lass mal hören!" … „Liebste Schwester – dann wäre es kein todsicheres System mehr!"

Gute Passwörter erfüllen folgende Bedingungen:
- Gute Passwörter sind mindestens 8 Zeichen lang!
- Gute Passwörter enthalten sowohl Klein- und Großbuchstaben als auch Zahlen!
- Gute Passwörter enthalten Sonderzeichen (-+.,;:_#/*%&?${}[]()!
- Gute Passwörter bestehen nicht aus echten Wörtern oder Namen!
- Gute Passwörter sind trotzdem gut zu merken!

Aber wie soll das gehen? Wie kann man sich **IwidB_65uhJ** merken? Das funktioniert am besten über ein System, hier ist ein Satz abgekürzt: **„Ich wohne in der Bunsengasse _65 und heiße Jan".**

Merken	Passwort	Beschreibung der Veränderung
Mein Hund heißt:	Naischa	
?	nAIschA	
Meine Telefonnummer lautet 765499	N7A6I5s4c9h9A	
?	(N7A6I5s4c9h9A)	

Wie funktioniert folgendes System? Findest du es heraus?

1. Arbeitsauftrag:
Beschreibe das System oben! Probiere es mit zwei anderen Wörtern aus (zum Beispiel mit deinem eigenen Namen oder deinem Haustier)!

2. Arbeitsauftrag:
Erfinde ein eigenes System, wie du gute Passwörter machst und sie dir trotzdem merken kannst! Dann kannst du auch ein Stichwort notieren (oben dürfte man „Hund" notieren, oder?)

3. Arbeitsauftrag:
Ausnahmsweise darfst du dein System NICHT mit den anderen austauschen! Denke an Jasmin und ihren jüngeren Bruder! Teste es jedoch im Internet:

https://passwortcheck.datenschutz.ch/check.php

Denke jedoch daran, dass du nicht dein echtes Passwort hier testest!

Arbeitsblatt vom Name:

Passwort – ist deines sicher?

Passwörter sind allgegenwärtig. Es gibt kaum eine Anmeldung (und das nicht nur im Internet: Denke mal an die Girokontokarte oder Pin-Nummer beim Handy etc.), bei der ich nicht ein Passwort (= Kennwort) vergeben muss. Und ich muss sie mir alle merken und schützen. Aber wie gelangen Unberechtigte an mein Passwort?

Erraten

Die wohl einfachste Methode ist das Erraten. Noch immer vergeben viele Computernutzer ein Passwort, das sie sich gut merken können. Beliebt sind die Namen der Familienangehörigen, der Haustiere oder des Fußballvereins. Diese Methode heißt unter Experten „Password Guessing" und wird häufiger angewandt als man vielleicht denkt.

Brute-Force

Einfache Passwörter sind auch zu knacken über eine „brutale" Methode, dem „Brute-Force-Attack". Dabei werden die Wörter einfach aus einer Wortliste ausprobiert (z. B. alle Wörter des Dudens werden durchprobiert). Diese Methode funktioniert bei kurzen und einfachen Wörtern gut, hat aber Grenzen, wenn das System nur drei Fehlversuche zulässt (so beim Online-Banking).

Mitlesen

Über spezielle Programme (so genannte „Keylogger"), die auch als „Spyware" bezeichnet werden, kann mitverfolgt werden, welche Tastatureingaben der Nutzer macht.

Auslesen

Spezielle Programme lesen die hinterlegten Passwörter aus, z. B. in Skript- oder Konfigurationsdateien.

Phishing

Auf eine falsche Website gelockt, geben Nutzer ihr Passwort ein und damit weiter (Phishing ist ein Kunstwort aus Password und Fishing).

Proxy-Falle

Bei der Verwendung eines Proxyservers ist es möglich, bestimmte Log-Dateien auszulesen.

Sniffer

Mit diesen „Netzwerkschnüfflern" können Passwörter, die über das Netzwerk übertragen wurden, ausgelesen werden. Besondere Gefahren bergen hier unverschlüsselte E-Mails.

Software

Spezielle Programme können verschlüsselte Passwörter wieder in eine lesbare Form umwandeln.

Es gibt also zahlreiche Gefahren, trotzdem geben starke Passwörter einen besseren Schutz. Hier findest du eine von vielen Adressen mit einem „Passwortgenerator": **www.anonym-surfen.com/service/330-passwort-generator**

1. Arbeitsauftrag:
Probiere diesen (oder einen anderen Passwortgenerator) aus! Formuliere einen Satz, der erklärt, wie starke Passwörter aussehen!

2. Arbeitsauftrag:
Wenn ihr starke Passwörter habt, sind diese sicher, aber welches Problem haben sie dennoch? Besprecht diese Frage in der Klasse!

Arbeitsblatt vom **Name:**

Auf folgender Seite des Datenschutzbeauftragten des Kantons Zürich in der Schweiz kannst du deine Passwörter testen lassen (Aber Vorsicht! Benutze kein echtes, sondern nur ein ähnliches!):
https://passwortcheck.datenschutz.ch/check.php

Der Check benutzt folgendes Bewertungssystem:

Bewertungskriterien	**Spezifikationen**
Optimale Passwortlänge ist 10 Zeichen	pro fehlendes Zeichen
Fehlende Kleinbuchstaben	a-z
Fehlende Großbuchstaben	A-Z
Fehlende Interpunktions- und Sonderzeichen	-+.,;:_#/*%&?${}[]() usw.
Fehlende Zahlen	0-9
Leerzeichen, Umlaute oder nicht druckbare Zeichen enthalten	öäüéàèÖÄÜÉÀÈç usw.
identische Zeichen in Folge	ab dem 3. Zeichen
Zeichenfolgen auf der Tastatur	ab dem 3. Zeichen
ABC- und Zahlenreihen	ab dem 3. Zeichen
Passwort durch Wortliste erleichtert eruierbar	deutsch & englisch
Qualität des Passworts in Punkten:	

3. Arbeitsauftrag:
Erläutere das Bewertungssystem! Warum sind die einzelnen Kriterien wichtig!
Tausche dich mit einer Partnerin/einem Partner aus!

4. Arbeitsauftrag:
Überprüfe deine eigenen Passwörter nach dem Bewertungssystem oben! Beachte aber, dass du dich hierbei nicht mit einer Partnerin/einem Partner austauschst. Immerhin geht es um deine echten Passwörter!

5. Arbeitsauftrag:
Erstelle sichere Passwörter nach einem eigenen System! (Schließlich müssen Passwörter auch noch gut zu merken sein!)

TIPP: Wie kann man sich **IwidB_65uhJ** *merken? Das funktioniert am besten über ein System, hier ist ein Satz abgekürzt:* **„Ich wohne in der Bunsengasse _65 und heiße Jan"**.