Unterrichtskonzept

Passwörter

Von Datensicherung
bis Passwortsafe

MEDIEN MONSTER
Medien kreativ begreifen

Inhaltsverzeichnis

3	Willkommen
3	Das Fundament der Module
5	Einordnung des Themas *Passwörter* in den thematischen Gesamtkontext
6	Lernziele
7	Überblick
9	Fachlicher Kontext und didaktische Reduktion
12	Wissensinput
14	Beschreibung der Schritte und Durchführung des Moduls
21	Facts Sheet: Hintergrundwissen
26	Arbeitsblätter, Checklisten, Barometer als Materialsammlung
63	Impressum

Willkommen

Schön, dass Sie sich für unsere Module zur Medienpädagogik interessieren. Wir, die MedienMonster, möchten Sie unterstützen, Kinder fit für unsere digitalisierte Welt zu machen und damit Chancen zu eröffnen und Teilhabe zu fördern. Ihnen liegt eines von mehreren Modulen vor. Wir haben aus unserer bisherigen Arbeit eine Reihe von zentralen Themen ausgewählt und für Sie aufbereitet. So können Sie die Module ohne intensive Vorbereitung direkt nutzen:

Die Module bieten Arbeitsmaterial für Lehrformen, die auf Individualiesierung und Eigenverantwortung hinarbeiten.

Kurz einlesen, sich mit den Materialien vertraut machen, den Ablauf anschauen – und loslegen. Der Technikaufwand ist überschaubar.

Die Konzepte lassen sich in den regulären Unterricht der Grundschule integrieren, zu diesem ergänzend nutzen oder in der außerschulischen Bildung einsetzen. Das Material ist in Unterricht und Arbeitsgemeinschaften erprobt worden.

Das Fundament der Module

Die Auswahl der Themen und die damit verknüpften Lernziele sind nicht nur erfahrungsgestützt, sie orientieren sich auch an bildungspolitischen Verlautbarungen und Lehrplänen. Klassische Lehrpläne haben häufig ein Manko: Sie können vielfach der raschen Entwicklung der Lebenswirklichkeit nicht standhalten. Das gilt besonders für den Themenkomplex Medien und Digitalisierung. Darauf haben die Kultusminister der Länder im Jahr 2016 in ihrer Strategie der Kultusministerkonferenz: „Bildung in der digitalen Welt“ reagiert, die als Beschluss verabschiedet wurde. Darin heißt es:

Präambel

„Die zunehmende Digitalisierung aller Lebensbereiche führt zu einem stetigen Wandel des Alltags der Menschen. Der Prozess betrifft nicht nur die sich zum Teil in hoher Dynamik verändernden beruflichen Anforderungen, sondern prägt in zunehmendem Maße auch den privaten Lebensbereich [...] Digitale Medien, Werkzeuge und Kommunikationsplattformen verändern nicht nur Kommunikations- und Arbeitsabläufe, sondern erlauben auch neue schöpferische Prozesse und damit neue mediale Wirklichkeiten. [...] Die Digitalisierung unserer Welt wird hier im weiteren Sinne verstanden als Prozess, in dem digitale Medien und digitale Werkzeuge zunehmend an die Stelle analoger Verfahren treten und diese nicht nur ablösen, sondern neue Perspektiven in allen gesellschaftlichen, wirtschaftlichen und wissenschaftlichen Bereichen erschließen, aber auch neue Fragestellungen z. B. zum Schutz der Privatsphäre mit sich bringen. Sie ist für den gesamten Bildungsbereich Chance und Herausforderung zugleich.“

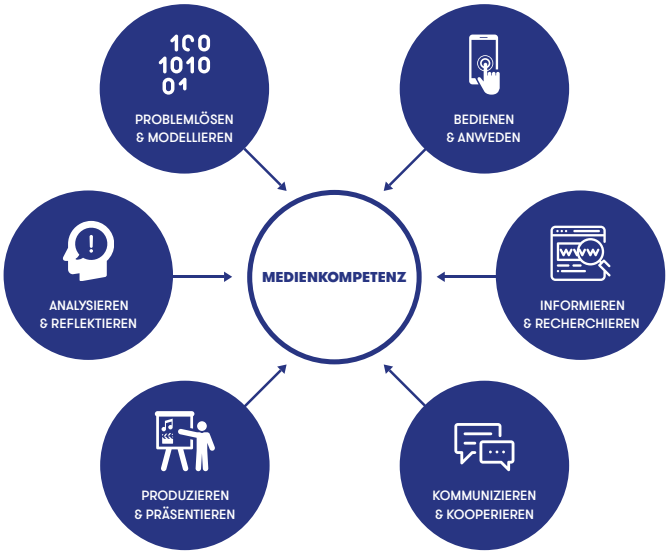
(Zitiert nach https://www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2018/Digitalstrategie_2017_mit_Weiterbildung.pdf)

Schulen sind aufgefordert, den Herausforderungen zu begegnen und die Chancen aufzugreifen. Was dazu gelehrt und gelernt werden und wie dies erfolgen soll, wird jedoch nicht länger in einen festen Bildungskanon gefasst, sondern es werden Ziele abgesteckt und Kompetenzen benannt, die erworben werden sollen. Die Bundesländer werden aufgefordert, kompetenzorientierte Lehr- und Bildungspläne zu erarbeiten, und zwar nicht für ein eigenes Fach, sondern als integrative Bestandteile der Fachcurricula aller Fächer. Dabei sollen digitale Lernumgebungen, in denen die Lehr- und Lernprozesse erfolgen, dem Primat des Pädagogischen folgen. Angestrebt sind ferner Individualisierung des Lernens und die Übernahme von Eigenverantwortung der Lernenden soll gestärkt werden.

Für die Umsetzung in die notwendigen länderbezogenen Regelungen ist eine Frist bis zum Jahr 2021 vorgesehen. Eine Bilanz des aktuellen Umsetzungsstandes in allen Bundesländern findet man auf dem Deutschen Bildungsserver in einer Rubrik „Konzepte und Portale der Bundesländer zur Medienerziehung“ unter dieser URL:

https://www.bildungsserver.de/Konzepte-und-Portale-der-Bundeslaender-2884-de.html

Wir betrachten im Folgenden kurz exemplarisch den „Medienkompetenzrahmen Nordrhein-Westfalen“. Er bietet das, was der Name bereits aussagt: Einen Rahmen, der Kompetenzbereiche absteckt und näher beschreibt, die in den Curricula der einzelnen Unterrichtsfächer aufgegriffen werden sollen. Der Medienkompetenzrahmen ist in sechs Teilkompetenzen aufgeteilt und bietet eine gute Orientierung im medienpädagogischen (Schul-) Alltag.



Die Kompetenzbereiche sprechen alle Ebenen von Medienkompetenz an u.a.:

- **den vielfältigen Einsatz von Medien und Tools in der Lebenswelt und auch als Instrument zum Arbeiten und Lernen in der Schule selbst,**
- **die Medien als Gegenstand der kritischen Betrachtung und Reflexion in den einzelnen Unterrichtsfächern, sowie**
- **die informationstechnische Grundbildung und Qualifikation in Informatik.**

Die Konzepte der MedienMonster lassen sich jeweils in mehreren der Kompetenzbereiche und dort in jeweiligen Unterbereichen verorten.

Das vorliegende Konzept Passwörter, das für Datensicherung sensibilisiert und die Handhabung bis hin zu einem selbst gebauten Passwortsafe zeigt, fällt in zwei Kompetenzbereiche.

Es werden folgende Kompetenzen des *Medienkompetenzrahmen NRW* gefördert:

Für weitergehende Informationen zum Medienkompetenzrahmen NRW ist die dazugehörige Broschüre zu empfehlen: https://medienkompetenzrahmen.nrw/fileadmin/pdf/LVR_ZMB_MKR_Broschuere.pdf

Passwörter dienen der Datensicherheit und diese gehört zu absoluten Grundlagen, mit denen sich jeder befassen muss.

Einordnung des Themas „Passwörter“ in den thematischen Gesamtkontext, Lebensnähe und Handlungsorientierung

In unserer digitalen Welt spielen Datenschutz und Datensicherung eine extrem wichtige Rolle. Die Nachrichten, dass Kriminelle in Computersysteme von Behörden, Unternehmen oder Privatpersonen eingedrungen sind und Schäden verursacht oder Daten gestohlen haben, sind spektakulär. Und das ist nur die Spitze des Eisbergs. Was mit unseren Daten im Alltag geschieht, wissen wir oft auch nicht. Wer hat wirklich Zugriff auf unsere PINs und Codes, was kann er damit tun und ist das dann auch in unserem Sinn? Wir sehen es als wesentliche medienpädagogische Aufgabe, für diese Fragestellungen zu sensibilisieren.

Jeder, der ein digitales Endgerät nutzt, erzeugt Daten. Hängt er dieses Gerät ins Netz, gibt er Daten weiter. Der Datenschutz (nach Bundesdatenschutzgesetz) stellt ein Regelwerk dar, wer persönliche Daten anderer weiternutzen darf und wie. Die Datensicherung bezieht sich auf die Maßnahmen, mit denen dieser Schutz erreicht werden soll und darüber hinaus auf die Absicherung gegen technische Pannen.

Das öffnet auch für Kinder, die mit digitalen Endgeräten umgehen, ein weites Feld. Bei ihnen muss ein Bewusstsein für die Problematik geschaffen werden. Wenn ich nicht möchte, dass jemand aus der Klasse meine Fotos anschaut, darf ich mein Handy oder Tablet nicht ohne Zugangsschutz herumliegen lassen. Wenn ich nicht möchte, dass einer der Kommunikationsdienste, die ich nutze, meine Kontaktadressen oder meine Fotos kennt und damit „etwas“ machen kann, muss ich die Einstellungen bewusst konfigurieren. Das ist schon ein schwierigeres Thema – was können die Dienste überhaupt, was kann ich als Nutzer eigentlich steuern und wie geht das? Was ist das „etwas“, das „die“ damit machen könnten und stört mich das überhaupt? Und sollte es mich nicht doch dringend stören?

Diese Problemkreise können Sie einführend mit den Kindern ansprechen, mit dem Ziel einer vorbereitenden Sensibilisierung für Sicherheitsfragen. Als Thema, die Datensicherung handfest und handlungsorientiert einzuführen, haben wir jedoch „Passwörter“ gewählt. Denn mit sicheren Passwörtern (= Bestandteil der Datensicherung) können die Kinder schon sehr viel gegen Datenmissbrauch (also die Missachtung von Datenschutz) im eigenen Umfeld und erst Recht bei der Benutzung der vielfältigen Online-Dienste erreichen.

Jeder, der ein digitales Endgerät nutzt, erzeugt Daten.

Datensicherung umfasst Maßnahmen gegen Pannen und Datensmissbrauch

Das Modul startet spielerisch mit den einfachen Grundlagen von Kodierung und erklärt im Weiteren, was ein sicheres Passwort auszeichnet. Damit begegnen die Kinder der Kryptografie, die in ihren Anfängen die Wissenschaft vom Verschlüsseln und Entschlüsseln von Nachrichten war (Chiffrierung und Dechiffrierung) und heute erweitert als Wissenschaft von der Informationssicherheit verstanden wird. Sie umfasst die „Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind“ (https://de.wikipedia.org/wiki/Kryptographie). Die Verfahren und ihre Anwendung gleichen oft mathematischen Knobeleien, was vielen Kindern Spaß macht. Auch stellen verschlüsselte Texte eine Art Geheimnis dar und man kann das Geheimnisumwitterte vielleicht etwas betonen. Das ist zum einen motivierend, zum anderen wird zugleich auf elementarer und verständlicher Ebene sichtbar, dass hinter Computeranwendungen systematische Verfahren stecken. Am Ende des Moduls haben die Kinder dann gelernt, sichere Passwörter zu erzeugen, die sie direkt benutzen können. Das Modul verknüpft also elementare Theorie mit Praxis und mündet in sehr konkrete Handlungsorientierung.

In Deutschland werden jährlich ca. 25 Millionen Smartphones verkauft.

Lernziele und Kurzbeschreibung

Lernziele zu Datenschutz und Datensicherheit gehören zu den unabdingbaren Grundlagen und sind beispielsweise im Medienkompetenzrahmen NRW und Bildungsplänen anderer Bundesländer aufgenommen. Da bereits Grundschulkinder mit Medien und Computern arbeiten, müssen sie von Anfang an in die Thematik eingeführt werden, damit sie auf dem für sie leistbaren Niveau sachgerecht vorgehen können. Dazu gehören auch die Vergabe von Passwörtern und das Einloggen. Dafür bildet das Modul unmittelbare Handlungskompetenz aus. Zudem wird diese Kompetenz spielerisch und im Team erarbeitet. So fördert dieses Modul zugleich auch die soziale Kompetenz der Kinder.

Das Modul hat die folgenden Lernziele:

- **Allererste Grundlagen von Datenschutz und Datensicherung verstehen**
- **Wissen, was eine Verschlüsselung ist und ausgewählte, einfache Verfahren kennen, wie man Nachrichten verschlüsselt oder entschlüsselt**
- **Wissen, welche zentralen Eigenschaften sichere Passwörter haben**
- **Für sich selbst sichere Passwörter erzeugen können**

Fragen? Einfach melden!

Überblick

Kurzbeschreibung zum Ablauf

Das Modul umfasst mehrere Teileinheiten:

1. Eine spielerische Einführung mit Basteln einer Kodierungsscheibe und mit einer Schnitzeljagd, bei der eine verschlüsselte, geheimnisvolle Botschaft entschlüsselt wird

2. Erarbeitung der Eigenschaften sicherer Passwörter und Kennenlernen einfacher Verfahren zur Passwörtererstellung, was in Form einer Kryptoparty gestaltet wird

3. Erstellen eines Passwortsafes.

Die Durchführung der zweiten Einheit ist an die vielerorts bekannten Cryptopartys der Chaos Computer Clubs angelehnt, auf denen sich Menschen mit unterschiedlichem Kenntnisstand zur Datensicherheit und -sicherung austauschen und von erfahreneren Computernutzern lernen können. Die MedienMonster danken dem Chaos Computer Club für seine Unterstützung bei der Entwicklung dieser Einheit.

Auf einer CryptoParty kann man gut voneinander lernen!

Notwendiges Material und erforderliche Infrastruktur

Wie versprochen, können Sie fast sofort loslegen. Unter *Durchführung des Moduls und Beschreibung der Schritte* finden Sie eine Ablaufbeschreibung für die einzelnen Einheiten dieses Moduls. Um die notwendige Paperware brauchen Sie sich nicht zu kümmern. Denn das Modul enthält Fragekarten, Checklisten, Auswertungsbogen und insbesondere auch Vorlagen, um eine Kodierungsscheibe und einen Passwortsafe anzufertigen. Als Handwerkszeug werden Schere(n), Splinte, ein Teppichmesser und ein Laminiergerät benötigt.

Die in der 1. Einheit vorgesehene Schnitzeljagd muss natürlich vorbereitet werden.

Für die Schnitzeljagd müssen Sie als Veranstalter sieben Botschaften verstecken, die schon vorbereitet sind (siehe Materialteil). Wir schlagen sieben Orte vor, die es in der Regel an jeder Schule gibt. Auf einem Arbeitsblatt werden als Rätsel formulierte Hinweise auf diese Orte gegeben. Dieser Teil der Vorbereitung muss eventuell individuell auf die Gegebenheiten an Ihrer Schule angepasst werden.

Für die weiteren Einheiten, müssen Sie sich Buchstaben- und Zeichenwürfel beschaffen. Denn die vorgeschlagenen Verfahren zum Erstellen wirklich sicherer Passwörter erfordern das „Auswürfeln“ von Zeichenketten (aus Buchstaben, Ziffern und Sonderzeichen). Dafür nicht geeignet sind Würfel, die auf allen sechs Seiten den gleichen Buchstaben haben und in der Regel für Lege- oder auch für Fädelspiele gedacht sind. Vielmehr werden Würfel benötigt, die auf jeder Seite andere Zeichen haben. Das gesamte Würfelset muss alle Buchstaben in groß und in klein, die Ziffern 0 bis 9 und wesentliche Sonderzeichen (+, *, %, § etc.) durchmischt abbilden. Solche Würfel gibt es auch zu kaufen, man findet sie aber viel seltener im Handel, und sie sind meist recht teuer. Eine Alternative stellen Blankowürfel dar, die Sie selbst mit den betreffenden Zeichen beschriften. Dazu eignet sich ein wasserfester Tafelschreiber mit feiner Linienstärke.

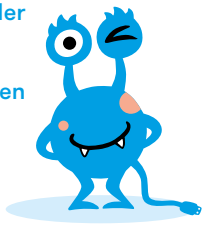
Der folgende Punkt *Wissensinput* erläutert zu Ihrer eigenen Information noch einiges zum fachlichen Kontext. Außerdem werden hier die Verfahren zur Erstellung von Passwörtern erklärt, die Sie mit den Kindern dann erarbeiten und anwenden sollen. Bitte überspringen Sie diese Informationen also nicht! Sie sind eine Voraussetzung, um die dann folgende Ablaufbeschreibung zu verstehen.

Verfahren für sichere Passwörter machen sich den Zufall zunutze - und den kann man gut durch Würfeln herstellen.

- 3 Teileinheiten á 1.5 Stunden

- Laminiergerät zum laminieren der Arbeitsmaterialien
- Schere(n)
- Splinte/Musterbeutelklammer
- Teppichmesser

- Allererste Grundlagen von Datenschutz und Datensicherung verstehen
- Wissen, was eine Verschlüsselung ist und ausgewählte, einfache Verfahren kennen, wie man Nachrichten verschlüsselt oder entschlüsselt
- Wissen, welche zentralen Eigenschaften sichere Passwörter haben
- Für sich selbst sichere Passwörter erzeugen können



Fachlicher Kontext und didaktische Reduktion

Der Themenkomplex Datenschutz und Datensicherheit ist umfassend und mündet zu konkreten Sicherungsmaßnahmen in Spezialwissen. Für Ihren Informationshintergrund als Gruppenleiter/-in finden Sie nachfolgend eine Zusammenfassung zur Unterscheidung von Datenschutz und Datensicherung. Ferner werden das Verschlüsseln sowie die Passwortnutzung in die grundsätzliche Struktur von Datensicherungsmaßnahmen eingeordnet. Sie können und sollten situativ entscheiden, was Sie von diesem Theorieanteil bei der Durchführung des Moduls in Ihre Gruppe einbringen.

- **Der Datenschutz ist ein rechtliches Regelungssystem, das festlegt, welche Daten wie genutzt werden dürfen. Rechtliche Verordnungen und Gesetze benennen Maßnahmen, die jemand ergreifen muss, um den Missbrauch von Daten zu verhindern. Bei solchen Maßnahmen geht es nicht nur darum, Hacker fernzuhalten. Sie reglementieren auch Unternehmen und Einrichtungen, die fremde Daten in ihren Computern speichern: Das reicht von Behörden über Arztpraxen, Krankenkassen, Versicherungen (die sensible Daten führen) bis zu Unternehmen jeder Branche, die Kundendaten speichern. Ein Beispiel: In einer Arztpraxis muss gewährleistet sein, dass nur der Arzt und die Mitarbeiter, die damit zwingend arbeiten müssen, Zugang zu den Patientendaten haben. Weder darf ein anderer Patient Einblick nehmen, noch Mitarbeiter, die nicht-medizinische Dienstleistungen für die Praxis erbringen (wie zum Beispiel die Reinigungsfirma).**

  Das Regelungssystem steht im Bundesdatenschutzgesetz (BDSG), das die auch die Datenschutz-Grundverordnung (DSGVO) der EU berücksichtigt, die am 25. Mai 2018 neu in Kraft getreten ist. Es bezieht sich auf alle personenbezogenen Daten und gilt für die Erhebung, Verarbeitung und Nutzung dieser Daten. Dieses Gesetz ist für den Bund und für nicht öffentliche Stellen (alle nicht staatlichen Einrichtungen und Unternehmen) gültig. Die Bundesländer haben zusätzliche Gesetze ausgearbeitet. Zu beachten ist: Das BDSG bezieht sich auf alle personenbezogenen Daten, egal ob sie digital oder in klassischer Form vorliegen.

- **Die Datensicherung umfasst alle Maßnahmen, die den gesetzlich geforderten Datenschutz gewährleisten sollen und darüber hinaus weitere, die im eigenen Interesse liegen. Dies betrifft Maßnahmen gegen technische Störungen (zum Beispiel das turnusmäßige Kopieren von Daten zur Vorbeugung eines totalen Datenverlusts) und Maßnahmen gegen den Missbrauch – sowohl zur Erfüllung der Datenschutzgesetze als auch im wirtschaftlichen Interesse (zum Beispiel um Werkspionage zu verhindern). Bei den Maßnahmen kann es sich um rein mechanische Vorkehrungen wie zum Beispiel das Abschließen sensibler Räume handeln. Sie können aber auch organisatorische Abläufe betreffen – zum Beispiel wenn der Weg von Daten in einem Unternehmen über Zugangsberechtigungen für bestimmte Mitarbeiter geregelt wird. Außerdem dienen (hard- oder software-)technische Sperren dazu, Daten zu schützen.**

Datenschutz liegt im Interesse aller. Wir sind darauf angewiesen, dass Datenverarbeiter ihn einhalten und unsere Daten verlässlich schützen. Die Maßnahmen beginnen auf unserem eigenen Rechner. Wir können, bezogen auf die Verarbeitungskette von Daten, zwar nur bescheidene Abschnitte sichern. Denn sobald Daten unseren Rechner verlassen haben – nach dem Versendeklick fürs Foto, nach Betätigen des Kauf-Buttons im Shop, nach dem Auslösen einer Online-Banking-Transaktion – endet unser Einfluss. Dennoch liegt es an uns, das erste Glied der Verarbeitungskette so sicher wie möglich zu machen.

Datenschutz beginnt immer schon auf dem eigenen Rechner und dem eigenen Smartphone.

Diese Verarbeitungskette sieht wie folgt aus:

Um den Datenschutz zu gewährleisten, muss es Datensicherungsmaßnahmen bei allen drei Schritten geben. Diese Maßnahmen können auf unterschiedlichen Ebenen liegen; Beispiele sind:

- **mechanische Sperren (Computerraum wird abgeschlossen),**
- **arbeitsorganisatorische Maßnahmen (Daten werden gezielt nur über berechtigte Personen in einer Behörde/Einrichtung/Unternehmen geleitet),**
- **softwareseitige Schutzmechanismen.**

Beim Übertragungskanal erfolgt bevorzugt die Verschlüsselung der Nachrichten („sichere Verbindung"), damit jemand, der unbefugt auf die Leitung zugreift, die Nachrichten nicht offen lesen kann. Der Schutz steht und fällt damit, wie schnell sich die Verschlüsselung „knacken" lässt. Im Internet werden als Protokolle http (HyperText Transfer Protocol) und https (HyperText Transfer Protocol Secure) unterschieden. Letzteres überträgt Daten verschlüsselt. Die Protokollangabe gehört zwar zu einer Webadresse dazu, wird aber in der Praxis oft weggelassen. Verbindet man sich mit einer Seite im Internet, erkennt man im Browser, ob die Verbindung verschlüsselt ist. Machen Sie den Test mit www.medien-monster.info! Wenn Sie die Seite mit dieser Adresse aufrufen, wird sie dennoch über eine Verschlüsselung geladen. Das kann man in den verschiedenen Browsern an spezifischen Kennzeichnungen sehen. Bei Mozilla Firefox zum Beispiel erscheint oben links ein kleines, grünes Schloss; diese Kennzeichnung liefert, wenn man sie anklickt, zusätzlich noch Informationen über die Verifizierung der Seite.

An den Endstellen, das heißt beim eigenen Rechner beziehungsweise beim eigenen Netzwerk und bei den Fremdrechnern und Servern, mit denen wir uns verbinden, erfolgt die Sicherung in erster Linie durch Anmelde- und Legitimationsverfahren. Wird eine Datei angeklickt, ein Programm geöffnet oder ein Dienst gestartet, muss ein Passwort eingegeben werden und in vielen Fällen zugleich auch ein Benutzername. Manche Dienste verlangen auch im weiteren Verlauf des Nutzungsprozesses eine erneute Legitimation – zum Beispiel eine TAN-Nummer wie beim Online-Banking (siehe *Facts Sheet*).

Auch „Dateneinbrecher" werden abgeschreckt, wenn der Einbruchsversuch zu lange dauert.

Wer diese Sicherung über Passworte überwinden will, hat dafür etliche Möglichkeiten. Er kann:

- **Passworte stehlen – (zum Beispiel wenn es diese aufgeschrieben und unachtsam aufbewahrt wurden.)**
- **sich mit einem Trick das Passwort verschaffen – (zum Beispiel mithilfe einer gefälschten Mail die Zusendung verlangen.)**
- **alle möglichen Passworte durchprobieren. Zum Beispiel wählen manche Menschen einfach ihr Geburtstagsdatum als Passwort. Wer das Datum kennt und es als Passwort vermutet, erlangt sehr schnell Zugang. Manchmal sind Systeme auch anfangs auf ein Standardpasswort – zum Beispiel die Ziffernfolge 123456 – eingestellt. Wurde dies nie durch etwas Individuelles ersetzt, bietet man beste Angriffsflächen.**
- **computergestützt alle theoretisch nur möglichen Passworte durchprobieren. Das erfordert Rechnerleistung und Zeit. Diebe, die zum Beispiel im großen Stil Kundendaten von Händlern oder Banken stehlen, arbeiten mit solchen Methoden. In vielen Softwareprogrammen ist gegen diese Angriffe eine Sperre eingebaut: Nach drei vergeblichen Versuchen kann man erst nach einer bestimmten Wartefrist – zum Beispiel nach fünf Minuten – wieder fortfahren.**
- **komplette Kundendatenbanken stehlen.**

Diebe und Trickbetrüger machen vor der digitalen Welt nicht Halt.

Eine Schutzmaßnahme gegen das Knacken kompletter Kundendatenbanken ist das Passwort-Hashing. Dabei werden die Passwörter nicht im Original, sondern verschlüsselt in einer Datenbank abgelegt. Bei jeder Eingabe wandelt das Programm das „offene" Passwort in einen Code, dieser wird vom Programm abgeglichen und bewirkt die Legitimation. Die Codierungsverfahren funktionieren nur in eine Richtung. Das heißt, dass sich das Passwort nicht aus dem Code rekonstruieren lässt. Wird nun eine komplette Datenbank gestohlen, verfügen die Diebe zwar über alle Codes, nicht jedoch sofort über die Passwörter. Sie können aber nun „in Ruhe" alle erdenklichen Passworte durchtesten. Sie wählen also ein beliebiges Passwort, codieren es neu und gleichen das Ergebnis mit der Datenbank ab. Sobald sich eine Übereinstimmung ergibt, können sie Rückschlüsse ziehen, welches Passwort auf welchen Code führt. Ausführlicheres dazu können Sie im *Facts Sheet* nachlesen.

Diese Zusammenhänge sollten den Kindern in Grundzügen verdeutlicht werden. Denn sie zeigen, dass Leichtfertigkeit schnell zu Schaden führt, während schon ein mittelmäßig komplexes Passwort sehr gut vor Schäden im Alltag schützt. Es ist – und hier erfährt das Spielerische rund um Geheimnisse wirklich Bedeutung –, sehr wichtig, dass man seine Daten „versteckt" und den Zugangsweg (das Passwort) geheim hält („Geheimzahl"). Um sich gegen die Computerkriminalität im großen Stil abzusichern, bedarf es allerdings professionell erstellter Datenbanken. Und gegen den Gau eines Datenbankdiebstahls sind wir als Nutzer letztlich machtlos.

Wissensinput: Verschlüsselung und Methoden zur Passworterstellung

Verschlüsselung bedeutet, dass Texte zeichenweise in andere Zeichen übersetzt werden, sodass der Text anschließend weiterhin aus bekannten Buchstaben, Zahlen und sonstigen Zeichen besteht, aber nicht mehr lesbar ist. Um den Text wieder entschlüsseln zu können, muss dies systematisch mithilfe einer Zuordnungstabelle erfolgen. Eine einfache Verschlüsselung ist die Cäsar-Verschlüsselung. Dabei werden die Buchstaben im Alphabet um eine bestimmte Anzahl von Stellen verschoben. Bei einer Verschlüsselung über die Zahl 2 wird zum Beispiel aus dem „a“ das „b“, aus dem „b“ das „c“ usw. Entsprechend wird bei der Verschlüsselung über die Zahl 10 aus dem „a“ das „j“ (= der 10. Buchstabe des Alphabets). Diese Verschlüsselung ist im Grunde relativ „leicht“ zu „knacken“.

Denn in deutschen Texten kommt der Buchstabe „e“ mit Abstand am häufigsten vor. Zudem gibt es Analysen über die Frequenz weiterer Buchstaben. Wenn man also im verschlüsselten Text das häufigste Zeichen sucht, muss dieses das „e“ sein. Darüber kann man sofort die Zahl der Verschiebung ermitteln. Das klappt natürlich bei extrem kurzen Texten nicht – wenn zum Beispiel lediglich einzelne Begriffe verschlüsselt wurden. Aber da die Anzahl der möglichen Kodierungen auf 25 (entsprechend der Anzahl der Buchstaben im Alphabet abzüglich eins) begrenzt ist, kann man bei kurzen Texten einfach alle Möglichkeiten durchprobieren. Handelt es sich um einen bekannten Begriff und nicht um ein Kunstwort oder einen außergewöhnlichen Namen, wird man ihn mit dieser Methode recht schnell entschlüsseln. In der Praxis werden deshalb komplexere Verschlüsselungen verwendet.

Zum Einsatz kommen Verschlüsselungen, wie oben schon erwähnt, beispielsweise

- **bei der sicheren Übertragung von Daten und**
- **beim Passwort-Hashing.**

Darüber hinaus werden in verschiedenen Verfahren der Passwörter-Erstellung Verschlüsselungen benötigt. Wenden wir uns also nun den Passwörtern zu.

Was Sinn gibt und leicht zu merken ist, kann auch leicht geknackt werden!

„Sinnfällige“ Passwörter sind die schlechtesten, weil sie leicht geknackt (das heißt durch einfaches Ausprobieren ermittelt) werden können. Wir verwenden aber gern sinnfällige Passwörter, weil wir uns diese gut merken können.

Man mag es kaum glauben: Untersuchungen renommierter Institute zeigen, dass „hallo“, „passwort“ oder mit Ziffern kombiniert „hallo1“ oder „hallo 123“ zu den am häufigsten verwendeten Passwörtern gehören. Auch „schatz“ findet sich oft in den Listen. Die Kunst besteht also darin, „komplizierte“ und damit „gute“ Passworte zu erstellen, die wir für uns wieder ableiten können, wenn wir sie einmal vergessen haben.

Was aber ist ein „gutes“ Passwort? Hier gilt das Folgende:

> „Gute“ Passwörter sind erstens lang und zweitens ohne erkennbare Systematik – also „chaotisch“; der Fachbegriff dafür heißt entropisch (abgeleitet von der physikalischen Größe Entropie als „Maß für Ungeordnetheit“).

Und nun kommt es darauf an, Verfahren zu entwickeln, mit denen wir Passwörter jederzeit für uns nachvollziehbar ableiten zu können. Einen Begriff einfach mithilfe der Cäsar-Verschlüsselung zu codieren, ist schließlich keine gute Lösung.

Wir stellen drei Verfahren näher vor:

Verfahren „Erlebu“

Erlebu steht für „erster und letzter Buchstabe“. Man nimmt einen Text, z.B. mit zehn Wörtern und verwendet von jedem Wort den ersten und den letzten Buchstaben. Groß- und Kleinschreibung wird beachtet und Satzzeichen werden mit eingefügt.

Ein Beispiel:

Erlebu ist eine einfache Methode: damit lassen sich Passwörter bilden.

Passwort: EuiteeeeMe:dtlnshPrbn.

Es müssen natürlich nicht zehn Worte sein, aber zehn Zeichen gelten als Mindestlänge für ein gutes Passwort. Am besten nimmt man einen Text, den man gut auswendig kennt.

Die Wortliste findet ihr unter medienmonster.info

Verfahren „Passwörter würfeln“

Das Verfahren benötigt eine Wortliste, die den Ziffern von (normalen Zahlen-)Würfeln Wörter oder Zeichen zuordnet (siehe betreffendes Arbeitsblatt unter *Materialsammlung*). Man nimmt dann fünf Würfel, würfelt damit und ordnet den fünf Würfelergebnissen (zum Beispiel: 12455) die betreffenden Wörter und Zeichen aus der Liste zu (die komplette Liste steht in *Materialsammlung*).

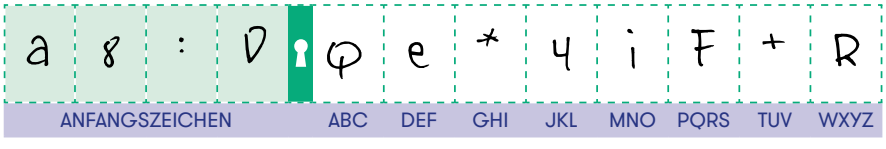
Diese Methode hat große Vorteile: Die Ergebnisse beruhen auf reinem Zufall. Das Passwort setzt sich aus Worten und Satzzeichen zusammen. Allerdings ist ein solches Passwort keineswegs „sinnfällig“. Wer kein gutes Gedächtnis hat, wird sich damit schwertun. Zusätzlich nutzen auch Kriminelle Wörterlisten bei einer Brute-Force-Attacke. So ist im schlechtesten Fall, ein Wort mit nur einem Zeichen gleichzusetzen (zum Beispiel fuerlaufengockelsaftgruen = 5 Zeichen, nicht 25).

Verfahren „Passwortkarte“

Dieses Verfahren kombiniert Würfeln mit Kodierung. Man erwürfelt zunächst mit Buchstaben-, Zahlen- und Zeichenwürfeln vier Anfangszeichen.

Dann denkt man sich ein normales Wort aus. Dieses Wort wird nicht notiert, sondern mit mithilfe einer Kodierungsliste („Passwortkarte“) verschlüsselt. Die Kodierung kann man sich ausdenken oder ebenfalls erwürfeln. Das Passwort besteht dann aus den ersten vier Zufallszeichen und dem kodierten Ausgangswort.

Beispiel für eine Passwortkarte



Die gewürfelten Anfangszeichen und die Kodierungsvorschrift stehen auf der Passwortkarte. Dort steht aber weder das Ausgangswort noch das Passwort. Die Passwortkarte ist vielmehr ein Hilfsmittel, um das fertige Passwort immer wieder aus dem Ausgangswort ableiten zu können. So geht das Passwort nicht verloren, auch wenn es nicht fertig – und damit „diebstahlgerecht“ – aufgeschrieben wird.

Durch die Zuordnung von je drei oder auch vier Buchstaben zu einem Passwortzeichen wird die Rückwärtscodierung deutlich erschwert. Sie gelingt nur demjenigen recht leicht, der ungefähr weiß, welches Wort herauskommen soll.

Durchführung des Moduls und Beschreibung der Schritte

1. Einheit

Schritt 1 Sie beginnen mit einem „Meinungs-Barometer“ („Passwörter Einstieg“). Bitten Sie die Kinder um Beantwortung der Fragen zum Thema und dessen Umfeld.

Eine Skala gibt Antwortmöglichkeiten mit drei Ausprägungen vor (JA/VIELLEICHT/NEIN bzw. HÄUFIG/SELTEN/NIE). Diese Skala wird als Plakat im Raum aufgehängt, so dass die Kinder beim Beantworten die Antwortalternativen immer vor Augen haben.

Dieser Einstieg erfüllt drei Funktionen:

- **Er dient als Warm-up und holt die Kinder im Bezug auf ihre eigenen Geräte und Dienste dort ab, wo sie aktuell stehen.**
- **Die Kinder beginnen, das Thema Sicherheit zu reflektieren.**
- **Die Gruppenleiterin/der Gruppenleiter erhält einen Überblick über die vorhandene Ausstattung, das Verhalten und das Grundwissen der Kinder.**

Schritt 2 Wissensquiz und Theoriesequenz

Als Grundlage führen Sie ein Wissensquiz mithilfe von Fragekarten durch. Dabei sollte auch das Thema Passwörter angesprochen werden. Zunächst erklären Sie anschaulich die schon beschriebene Verarbeitungskette – eigener Rechner, Übertragungskanal, fremder Rechner – und nennen mögliche Punkte, an denen Fremde in die Systeme eindringen können: den Zugang zum Rechner, die Schnittstelle zum Netzwerk, das Eindringen in Server. Das soll und braucht nicht systematisch erfolgen.

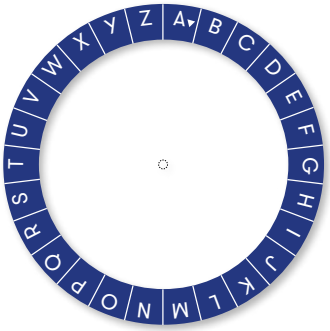
Vielmehr sollen die Kinder eine Vorstellung erhalten, wie umfassend diese Probleme sind. Beeindruckend sind auch immer Beispiele für große Schadensfälle, die Sie am besten der aktuellen Presseberichterstattung entnehmen. Dadurch bekommen die Kinder ein Gefühl dafür, wie weltumspannend und in welchem Tempo Daten bewegt werden. Das macht zudem verständlich, dass es extrem viele Angriffspunkte in den Systemen gibt. Verschlüsselungen und Passwörter sind wesentliche Maßnahmen zur Datensicherheit, aber sie können gehackt werden. Wo dies im großen Stil erfolgt, nutzen die Hacker maschinelle Verfahren des Durchprobierens. Dagegen helfen nur „sehr gut“ konstruierte Verschlüsselungen und Passwörter, deren Wirksamkeit darauf basiert, dass sie den Aufwand und die benötigte Zeit für das Durchprobieren extrem in die Höhe treiben.

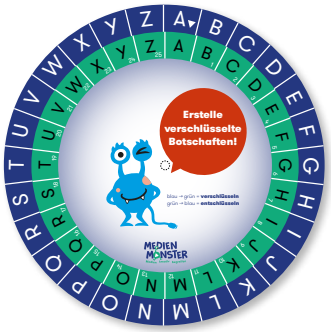
Welche Karten eingesetzt und ob weitere darüber hinaus gehende Themen hinzugezogen und im Lerngespräch behandelt werden, sollten Sie situativ entscheiden.

Anregungen finden Sie im *Facts Sheet*. Je nach Vorwissen kann es hilfreich sein, konkret zu benennen, für welche Art von Daten sich kriminelle Hacker interessieren und welche Schäden sie anrichten können. Kriminielle eignen sich zum Beispiel Daten von prominenten Personen oder Politikern an, um deren Karriere zu schaden oder Wahlen zu beeinflussen. Sie besorgen sich Daten aus dem E-Commerce, um Bestellungen auf Kosten anderer zu tätigen. Sie knacken Bankdaten, um Geld zu stehlen. Die Sequenz sollte nicht zu lang ausfallen, damit Zeit für die Schnitzeljagd bleibt. Bitte erklären Sie den Kindern aber den Unterschied zwischen Verschlüsselung (Nachricht als Schutz für die Übertragung in eine „Geheimsprache" bringen) und Passwort (analog einer Parole, die beim Zugang zu etwas überprüft wird).

Schritt 3 Kodierungsscheibe basteln

Als Beispiel dient die Cäsar-Verschlüsselung. Um keine Tabellen erstellen zu müssen, kann man sich eine Kodierungsscheibe bauen. Die MedienMonster haben für dieses Modul eine Bastelvorlage entwickelt. Die Vorlage besteht aus zwei Scheiben, auf der einen sind in einem blauen Außenring, auf der anderen – etwas kleineren – in einem grünen Ring die die Buchstaben des Alphabets gedruckt. Beide Scheiben ausdrucken, auf Pappe kleben, ausschneiden, laminieren und mit einem „Splint/Musterbeutelklammer" drehbar verbinden.





So kann man alle möglichen Verschlüsselungen einstellen, um mit der Scheibe Texte von Blau nach Grün zu verschlüsseln und von Grün nach Blau zu entschlüsseln (funktioniert natürlich auch in Schwarzweiß! Wichtig ist, die Arbeitsrichtung festzulegen und einzuhalten, damit niemand im Eifer der Schnitzeljagd durcheinanderkommt.)

Schritt 4 Schnitzeljagd durchführen

Die Schnitzeljagd als solche läuft klassisch ab. Das abgebildete Arbeitsblatt erklärt alles Notwendige.

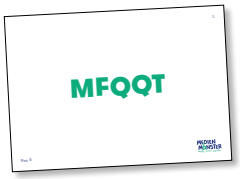
Das Blatt enthält sieben kleine Rätsel. Es gilt, jeweils einen spezifischen Ort in der Schule zu erraten. An jedem dieser Orte ist ein Zettel mit einer verschlüsselten Botschaft versteckt. Die Botschaft muss mithilfe der Kodierungsscheibe entschlüsselt und auf dem Lösungsbogen eingetragen werden. Aus den Buchstaben in den hervorgehobenen Kästchen ergibt sich das Lösungswort.

Die Zahlen geben jeweils die Verschiebung der Cäsar-Verschlüsselung an. Zettel mit den verschlüsselten Botschaften und das ausgefüllte Lösungsbeispiel (das natürlich nicht vor der Schnitzeljagd für die Schüler bestimmt ist!) finden Sie unter *Materialsammlung*.

Dann geht es, ausgestattet mit der Kodierungsschreibe, auf die Jagd. Die Kinder suchen die Orte und dort den Zettel mit der Botschaft, notieren diese und entschlüsseln sie jeweils. Am Ende können sie das Lösungswort zusammensetzen. Und schön ist es natürlich, wenn es für die richtige Lösung am Schluss auch eine kleine Belohnung gibt!

Die Schnitzeljagd muss vorbereitet werden:

- **Prüfen Sie, ob es die vorgeschlagenen Suchorte bei Ihnen gibt, sowie ob die Umschreibungen als Rätsel sinnvoll und für die Kinder lösbar sind (gegebenenfalls ändern/anpassen), und**
- **natürlich die Zettel mit den verschlüsselten Botschaften dort verstecken (rechtzeitig, aber nicht zu früh, damit sie nicht jemand anderes schon findet…)**



2. Einheit

Bei Bedarf kommt jetzt nochmals das Meinungsbarometer zum Einsatz. Dann wird etwas Theorie erläutert. Der Kern dieser Einheit ist jedoch die praktische Herstellung von Passwörtern mithilfe der unterschiedlichen Verfahren. Die Einheit kann als Cryptoparty gestaltet werden (was wir uns beim Chaos Computer Club anschaut haben, dem wir für seine fachliche Unterstützung auch nochmals danken).

Bei einer Cryptoparty geht es um Verschlüsselungen. Sie sollte nicht als Unterricht, sondern als lockeres Treffen angelegt sein, bei dem man sich zwanglos mit dem Thema befassen kann, miteinander arbeitet und auch voneinander lernt. Für die meisten Kinder werden die konkreten Inhalte neu sein, sodass der Gruppenleiter*in durchaus Wissensinput geben muss. Aber wo immer es sich anbietet, sollte vorhandenes Wissen von den Kindern aufgegriffen und integriert werden. Die betreffenden Arbeitsblätter dieses Moduls erfordern an manchen Stellen etwas Knobelei, sollten aber in erster Linie Spaß machen und vor allem selbstständig bearbeitet werden können.

Schritt 1 Theorie

Damit sich das Erstellen von Passwörtern wirklich mit Sinn füllt, sollten Sie mit den Kindern nochmals gemeinsam zusammenfassen, wo man Passwörter benötigt – als Zugang zu einem Gerät, zu einem Dienst, zu einem Programm oder einer App oder zu einer Datei (lassen Sie bitte konkrete Beispiele nennen!). Zudem sollte noch einmal deutlich werden, welchen Zweck sie erfüllen – nämlich den Zugang Unbefugter zu verhindern. Je nachdem, was Sie in Einheit 2 schon besprochen haben, formulieren Sie mehr oder weniger ausführlich, was ein gutes Passwort auszeichnet:

- **Es ist lang (mindestens zehn Zeichen, besser mehr),**
- **setzt sich aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen zusammen und**
- **hat keinerlei erkennbare Systematik (es ist „chaotisch").**

Ob Sie dies begründen oder tiefer erläutern, sollten Sie situativ entscheiden. Auf elementarer Ebene werden Kinder jeder Altersstufe sofort verstehen, dass es bei einem Passwort aus nur einer Ziffer nur zehn Möglichkeiten gibt, die ein krimineller Hacker ganz schnell durchprobiert hätte. Dass sich bei zwei Ziffern schon 100 Möglichkeiten ergeben, wird durch Aufschreiben in einer Matrix ebenfalls rasch deutlich. Da sehen die Kinder anschaulich, dass die Passwörter den Zahlen 0 (geschrieben als 00) bis 99 entsprechen. Je nach Alter beziehungsweise Klassenstufe lässt sich noch der Schluss auf drei Zahlen (0 bis 999, entsprechend 1.000 Möglichkeiten) und auf vier Zahlen (0 bis 9999, entsprechend 10.000 Möglichkeiten) ziehen. Das ist möglicherweise eine Rechnung, die die Mathecracks aus der Gruppe den anderen Kindern, die sich mit dem Rechnen (noch) schwerer tun, erklären können.

Ein gutes Beispiel zur Veranschaulichung: Das Zahlenschloss

Die Anzahl der Möglichkeiten für Passwörter aus zwei, drei oder mehr Ziffern zu errechnen, ist das eine. Das andere ist zu verstehen, warum längere Passwörter besser sind. Fragen Sie dies die Kinder konkret, d.h. stellen Sie ihnen eine Frage wie die folgende: „Warum ist es sicherer, wenn wir für ein Passwort eine lange Zeichenfolge verwenden, die besonders viele Möglichkeiten bietet?“ Es hängt naturgemäß von ihrem Entwicklungsstand und Vorwissen ab, ob die Kinder erfassen, dass dann Ausprobieren länger bzw. zu lange dauert. Entscheiden Sie gruppenbezogen

- **ob diese Erkenntnis klar ist oder**
- **ob sie diffus vorhanden ist und Sie sie nochmals nachempfinden und sichern wollen oder**
- **ob sie diese Erkenntnis erst noch erarbeiten müssen.**

Als Methode bietet sich „handelndes Lernen“ an und das können Sie einfach mit einem üblichen Zahlenschloss durchführen. Beim Zahlenschloss geht es analog zum Passwort darum, durch Eingabe einer Ziffernfolge den Zugang zu öffnen. Wer die Zifferenfolge nicht kennt, kann probieren, sie herauszufinden.

Vorgehen

Bringen Sie Zahlenschlösser mit. Gut sind mindestens zwei Muster, darunter eines, bei dem nur drei Ziffern einstellbar sind. Denn Sie sollten sich auf drei Ziffern beschränken, damit die Aufgabe praktikabel bleibt. Sie zeigen die Zahlenschlösser vor und erklären das Prinzip. Dann geben Sie den Kindern ein Schloss (mit drei Ziffern) und stellen die Aufgabe, es durch Ausprobieren zu öffnen. Lassen Sie bitte nicht einfach „wild“ probieren, sondern arbeiten Sie zunächst im kurzen Unterrichtsgespräch eine Strategie zum Vorgehen heraus. Dafür gibt es zwei grundlegende Möglichkeiten, die jeder „Cracker“ nutzt:

1. Man kann nach Wahrscheinlichkeiten vorgehen und z.B. Schnapszahlen (wie 333, 666 etc.) oder offensichtliche Zahlenfolgen (z.B. 123, 456 etc.) probieren. Der Fantasie sind keine Grenzen gesetzt. „Profis“, die Passwörter knacken wollen, probieren zunächst bereits verwendete oder häufig verwendete Passwörter (also solche die schon gehackt worden sind).

2. Man kann systematisch vorgehen und ein System ausdenken, wie man alle möglichen Zifferenkombinationen ausprobieren kann. Das „sture“ Durchprobieren aller Möglichkeiten wird auch als **„Brute Force Angriff“** bezeichnet.

Je nach Ihrer Gruppensiuation können Sie beide Strategien in je einer Teilgruppe ausführen lassen. Da der Brute Force Angriff bei drei Ziffern noch immer lange dauert, können Sie dies verkürzen, indem Sie die erste Ziffer vorgeben.

Die Kinder werden merken, dass die Strategie der Wahrscheinlichkeit nur bei gängigen Zahlen schnell Erfolg bringt und es andersfalls lange dauert. Hier sichern Sie als Erkenntnis, dass Passwörter nicht einfach und üblich, sondern kompliziert sein sollten. Auch der Brute Force Angriff dauert seine Zeit, aber man kommt immer zum Ziel. Als Erkenntnis lässt sich formulieren, dass man die Zeit hinauszögern kann – je länger ein Passwort ist, desto länger dauert das Probieren. Computer sind allerdings um ein Vielfaches schneller als Menschen und deshalb müssen Computerpasswörter sehr lang sein und möglichst viele Zeichen nutzen, wodurch es eine sehr große Anzahl von Möglichkeiten zur Bildung des Passwortes gibt.

Ein handelsüblicher Computer kann ca. 1,5 Milliarden (!) verschiedene Passwörter pro Sekunde errechnen.

Am Ende sollte klar werden: Je mehr Zeichen genutzt werden können, desto mehr Möglichkeiten gibt es. Deshalb nimmt man am besten noch Buchstaben und Sonderzeichen dazu.

Dass Passwörter möglichst keine Systematik erkennen lassen dürfen, ist schwieriger zu vermitteln. Zumindest den Sachverhalt, dass sinnfällige Wörter viel besser erraten werden können als zum Beispiel Fantasiewörter oder „Quatschwörter“ und erst Recht als völlig sinnleere, gemischte Zeichenketten, sollten Sie anführen. Wenn Sie die Frage vertiefen möchten, lesen Sie bitte dazu im *Facts Sheet* nach und entscheiden Sie, welche Inhalte Sie aufgreifen möchten.

Schritt 2 Praktischer Arbeitsteil: Passwörter bilden

Nun werden in der Gruppe die im voranstehenden Wissensinput erklärten drei Methoden mit den Kindern erarbeitet, nämlich

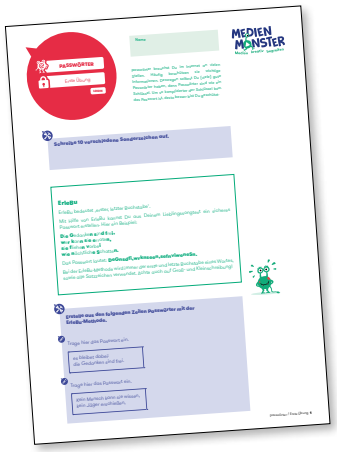
- **Erlebu (Verschlüsselung eines Textes über ersten und letzten Buchstaben pro Wort)**
- **Würfeln**
- **Passwortkarte**

Dazu stehen drei Arbeitsblätter zur Verfügung, die selbsterklärend sind.

Hinweis: Alle Arbeitsblätter stehen in *Materialsammlung* in Orginalgröße zum Ausdrucken/Kopieren zur Verfügung.

Arbeitsblatt „Erlebu“

Erklärung des Verfahrens anhand eines Beispiels, zur Selbst-erarbeitung; dazu zwei Aufgaben



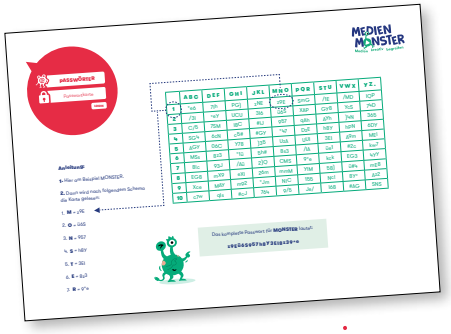
Arbeitsblatt „Passwörter Würfeln“

Benötigt werden einfache Zahlenwürfel, damit wird fünfmal gewürfelt. Die so erwürfelte fünfstellige Zahl wird als Passwort verschlüsselt, und zwar mithilfe einer Wortliste. Diese ist in *Material* enthalten. Das Prinzip ist also, dass hier Worte aus einer umfassenden Liste als Passwort mit dem „Zufallsverfahren Würfeln“ ausgewählt werden.

Passwortkarte

Die MedienMonster haben eine fertige Passwortkarte entwickelt. Mit ihr lassen sich unterschiedliche Übungen durchführen:

- **Um das Prinzip durch die praktische Ausführung zu verinnerlichen, können „Geheimwörter“ verschlüsselt werden.**
- **Dann folgenden Übungen für eine Entschlüsselung. Dabei müssen die Kinder das Problem bewältigen, dass die Rückcodierung nicht eindeutig ist. Es gibt jeweils mehrere Lösungen. Aus diesen soll das „sinnvolle“ Wort ausgewählt werden.**
- **Schließlich wird noch einmal die Codierung sinnfälliger Passworte geübt.**



3. Einheit

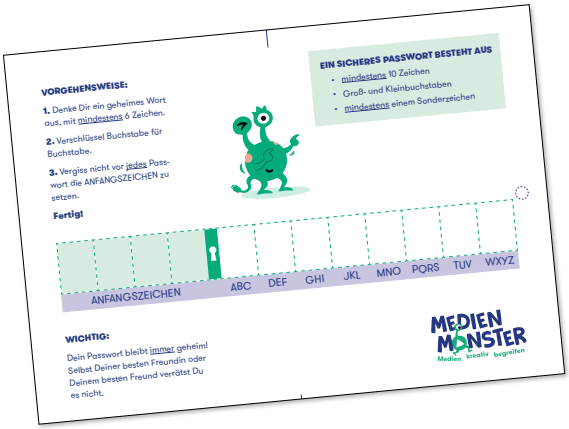
Die sichersten Passwörter liefert das Verfahren mithilfe der Passwortkarte. Es kombiniert Würfeln mit Verschlüsseln und führt auf lange sowie völlig zufällige Zeichenketten. Auch ist es das Verfahren, mit dem sich auf ganz praktischer Ebene eine größere Anzahl von Passwörtern relativ schnell erstellen und auch gut verwalten lässt.

Wenn die Kinder mögen, können sie nun in dieser Einheit die Passwörter, die sie tatsächlich in ihrem Alltag benötigen, (erstmals oder neu) erstellen. Dazu fertigen sie sich eine eigene, individuelle Passwortkarte an und erstellen damit ihre Passwörter.

Am Ende können sie ihre Passwortkarte in einem „Passwortsafe“ eintragen, in dem auch noch einmal die Anleitung zum Vorgehen aufgeführt ist. Dieser Passwortsafe ist eine zuammengeklappte Pappkarte, die mit einer Musterbeutelklammer verschlossen werden kann. Die Angaben stehen innen und sind so „im Safe“ sicher verwahrt. Dieser ist außen nett bedruckt und hat eine gute Symbolkraft für die Geheimhaltung und das „Wegschließen“ der Informationen, die niemand anderen etwas angehen.

MiniSafe

Bei unserer Variante eines kleinen Safes gibt es nur eine Verschlüsselungstabelle. Über diese lassen sich mehrere Ausgangswörter – wir können auch sagen „Geheimwörter“ – verschlüsseln. Dadurch reduziert sich die Sicherheit. Allerdings müssen sich die Kinder die Ausgangs-/Geheimwörter ja merken, und das funktioniert nur bei einer sehr kleinen Anzahl. Ab einer bestimmten Anzahl wird dies jedoch unpraktisch. Deshalb stellen die MedienMonster auch noch die Vorlage für einen großen Safe zur Verfügung.



Die Kinder sollten unbedingt darauf hingewiesen werden, dass ihre Ausgangswörter nicht mit im Safe stehen dürfen, sondern dass sie siese im Kopf behalten (oder woanders notieren) müssen. Für jüngere Kinder ist der kleine Safe völlig ausreichend.

Großer Safe

Da ältere Kinder/Schüler vielfach bereits eine größere Anzahl von Anwendungen nutzen und deshalb mehrere Passwörter benötigen, gibt es den Safe auch in einer großen Variante, um bis zu zehn Passwörter einzutragen. Die Unterschiede zum kleinen Safe:

- **optionaler Eintrag von bis zu zehn Passwörtern**
- **längere Passwörter (18 beziehungsweise 19 Zeichen)**
- **komplexere Verschlüsselung, indem jeder Buchstabe eines Ausgangs- beziehungsweise Geheimwortes anders verschlüsselt wird**
- **abweichend: keine Anfangszeichen**
- **stattdessen: Anhängen eines 19. Zeichens, das nirgends notiert ist und das die Information darstellt, die man im Kopf behalten muss.**

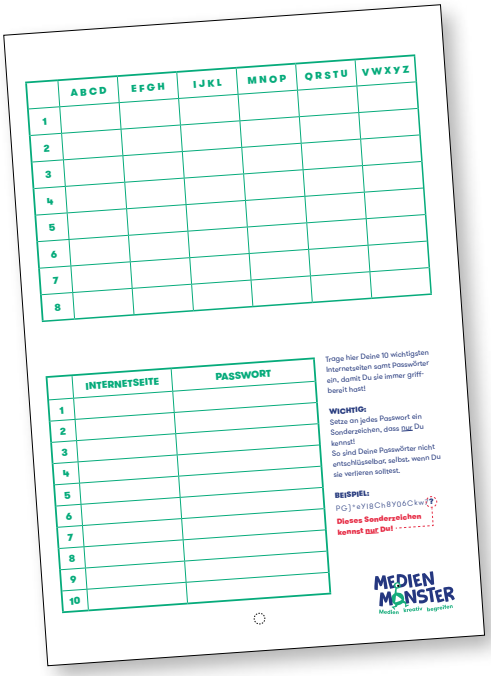
Dieses Schlusszeichen (ähnlich Prüfziffer) erhöht die Sicherheit, dass bei Verlust des Safes der Finder mit den Passwörtern nichts anfangen kann.

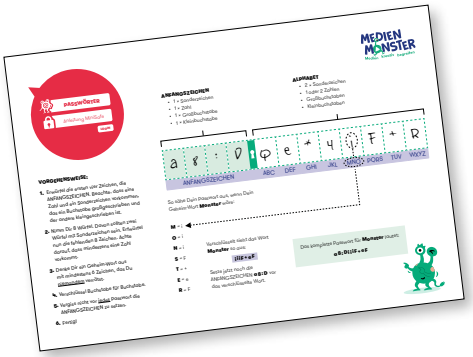
Ein Safe für jeden Bedarf - der kleine Passwortsafe für wenige, der große für viele Passwörter!

Die Kinder übernehmen natürlich nicht das obige Kodierungsbeispiel, sondern erwürfeln – Arbeitsschritte 1 und 2 – ihre individuelle Passwortkarte und tragen sie in ihren leeren Safe ein. Dazu werden die „gemischten" Würfel benötigt, die eingangs in diesem Modul als notwendige Ausstattung benannt wurden.

Der Safe hat Vorder- und Rückseite, wird in der Mitte gefaltet und ergibt so eine vierseitige „Karte". Drucken Sie bitte beide Seiten aus – es passt 1 Vorlage (bzw. 2 Vorlagen beim „MiniSafe") auf A4-Papier, legen Sie sie gegeneinander und laminieren Sie den „Safe" für bessere Haltbarkeit. Es entsteht eine „Doppelkarte" mit vier Seiten im Hochformat.

Zum „MiniSafe" gibt es auch eine Anleitung, wie dieser verwendet werden woll. Diese ist unter *Materialsammlung* zu finden.





Facts Sheet: Hintergrundwissen

Passwörter sind mit Schlüsseln vergleichbar

In der „analogen“ Welt ist es selbstverständlich, dass wir unsere Wohnung (oder unser Haus) durch ein gutes, sicheres Schloss mit entsprechendem Schlüssel sichern. Wir würden auch nie auf die Idee kommen, für verschiedene Häuser oder Wohnungen ein baugleiches Schloss und denselben Schlüssel zu verwenden. Seltsamerweise legen wir ein solches Verhalten aber im „virtuellen Raum“ an den Tag. Nicht selten verwenden User für verschiedenste Accounts immer dasselbe Passwort.

Im virtuellen Raum ist es – im Gegensatz zur analogen Welt – sogar möglich, dass jemand der im Besitz des richtigen „Schlüssels“ ist, sich auch als Schlüsselbesitzer ausgeben kann (im Falle des „Schlüsselverlusts“ bei einem E-Mail-Account kann das fatale Folgen haben). Da analoge und virtuelle Welt immer mehr verschmelzen, soll der folgende Text dazu anregen, sich systematisch um seine Passwörter zu kümmern.

Das Beruhigende ist, dass es jeder selbst in der Hand hat, wie sicher sein Schlüssel ist.

Man muss beides sichern: Das Device (Gerät) und den Account (Zugang zu einem Dienst, Programm usw.).

Es gibt zwei unterschiedliche Sicherungsnotwendigkeiten

Zunächst müssen wir zwei grundsätzlich verschiedene Szenarien unterscheiden. Zum einen geht es darum, ein Gerät – in der Fachsprache „Device“ (zum Beispiel ein Smartphone oder Tablet) – zu sichern. Zum anderen wollen wir uns damit beschäftigen, wie ein Zugang – in der Fachsprache „Account“ – gesichert werden kann. Dabei unterscheiden wir zwischen der Passwort-Eingabe per Hand und dem Berechnen von Passwörtern durch einen Computer.

Das erste Szenario kann man mit dem Nutzen einer Bankkarte vergleichen. Der Code für eine Bankkarte umfasst „nur“ eine vier Zeichen lange Zahlenfolge. Ist diese Sicherung ist wirklich ausreichend? Bei einer vier Zeichen langen Zahlenfolge gibt es 10.000, also 10^4 (zehn hoch vier) mögliche Zahlenfolgen (siehe auch im *Wissensinput*) – wenn man bedenkt, dass nach dem dritten Fehlversuch die Karte eingezogen wird, ist das sogar mehr als ausreichend. Über ähnliche Schutzmechanismen verfügen auch moderne Devices. Nach mehrmaligen falschen Versuchen, muss man mehrere Minuten warten, um die nächste Eingabe vornehmen zu können. Bei einigen Herstellern kann man auch einstellen, dass alle Daten des Devices nach zehn Fehlversuchen gelöscht werden. Auch hier reichen also vier bis sechs Zeichen lange Passwörter aus.

Ähnliche Schutzmechanismen sind auch bei modernen Accounts eingebaut. Auch dort muss nach einigen Fehlversuchen auf die nächste Eingabe gewartet werden. Auch hier werden die Passwörter per Hand eingegeben. Doch hier können Fehleingaben zu weitreichenden Folgen führen: dem Verlust der Datenbank auf dem Server beziehungsweise bei dem Dienst, in den man sich einloggen wollte.

Schwachstelle Datenbank

Die individuellen Passwörter der Nutzer/-innen sind nämlich bei jedem Anbieter in einer oder in mehreren Datenbanken gespeichert. Das muss auch so sein, weil die betreffende Software die eingegebenen Passwörter auf ihre Richtigkeit abgleichen muss. Zur Sicherheit sind diese Passwörter nicht nur (mehrfach) gehasht beziehungsweise verschlüsselt (Ausnahmen bestätigen leider die Regel), sie werden auch zusätzlich so gut „bewacht“ wie es nur geht. Trotzdem passiert es, dass solche Datenbanken gestohlen werden – und das auch bei großen, bekannten Anbietern (siehe zum Beispiel Yahoo oder LinkedIn). Spätestens jetzt kommt die Sicherheit des eigenen Passworts ins Spiel.

Gerät eine solche Datenbank in die Hände eines Menschen mit krimineller Energie, hat er viel Zeit, um die Passwörter zu errechnen. Die Zeit spielt hier eine besondere Rolle. Bei Einbrüchen, egal ob in der analogen oder der virtuellen Welt, ist die Zeit

der entscheidende Faktor. Es gibt kein Schloss, das unknackbar ist. Es ist nur eine Frage der Zeit. Egal ob bei der Wohnungstür, beim Fahrradschloss, beim Banksafe oder beim virtuellen Schloss, es geht darum, dass der Angreifer möglichst viel Zeit benötigt, um ein Schloss zu knacken. Je länger dieser braucht, desto höher ist die Wahrscheinlichkeit, dass der Einbruch bemerkt wird, beziehungsweise dass es für den Einbrecher so teuer wird, dass es sich nicht mehr lohnt. Zum Glück steht dem oder den Angreifern nicht unendlich viel Zeit zur Verfügung. Ein guter Schlüssel bedeutet also nicht totale Sicherheit, aber er verbessert den Schutz. Manche Schlüsselmodelle sind sogar so ausgefeilt, dass sie als „sicher" gelten können. Übrigens: Jeder kann selbst (mit-)beeinflussen, wie lange ein potenzieller Angreifer braucht, ein Passwort zu knacken.

Der Sicherungsmechanismus: Hashen

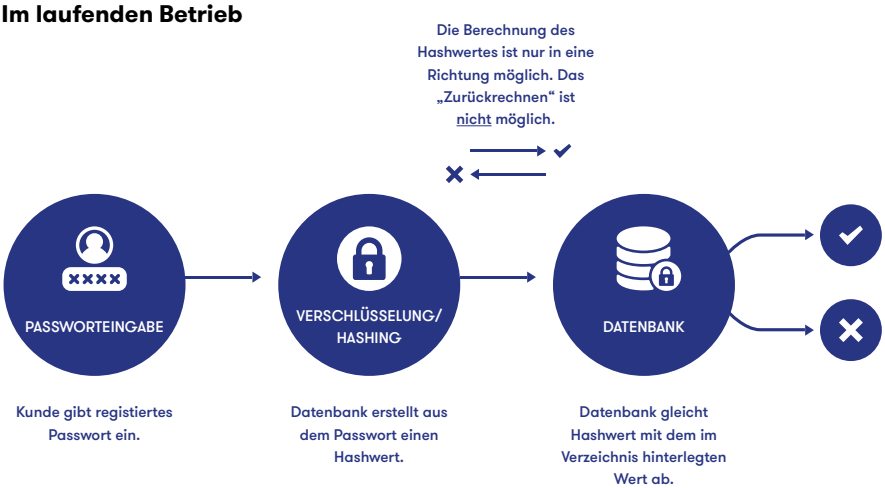
Passwörter stehen nicht im Klartext in einer Datenbank (auch wenn leider hier immer noch Ausnahmen die Regel bestätigen), sondern sind durch eine mathematische Berechnung transformiert worden. Diese Transformation erfolgt systematisch – und zwar über eine mathematische Funktion. Diese heißt Hashfunktion. Sie wandelt jedes Passwort in einen anderen Hashwert um. Hashfunktionen sind hochkomplizierte mathematische Funktionen. Gute Hashfunktionen sind so angelegt, dass, egal welche Zeichenlänge am Anfang eingegeben wird, am Ende eine gleich lange Zeichenlänge herauskommt (siehe Tabelle: Alle Hashwerte haben 64 Zeichen, obwohl die gehashten Wörter viel kürzer sind). Zusätzlich kann man Hashfunktionen nur in eine Richtung rechnen (außer sie wurden bereits „geknackt" – es gibt aber genügend Funktionen die „sicher" sind). Das heißt, dass man von den Hashwerten nicht zurückrechnen und das ursprünglich Wort herausfinden kann.

Sobald man aber Zugriff auf eine Datenbank hat, kann man alle möglichen Passwortkombinationen hashen und schauen, ob der Hashwert mit einem Wert aus der Datenbank übereinstimmt. Ist das der Fall, weiß man, von welcher Zeichenkombination aus der Hashwert errechnet wurde. Diese Zeichenkombination entspricht dann einem gültigen Passwort. Obwohl es viele verschiedene Hashfunktionen gibt und die jeweils verwendete nicht (zwangsläufig) in der Datenbank vermerkt sein muss, kann das ein erfahrener Informatiker erkennen.

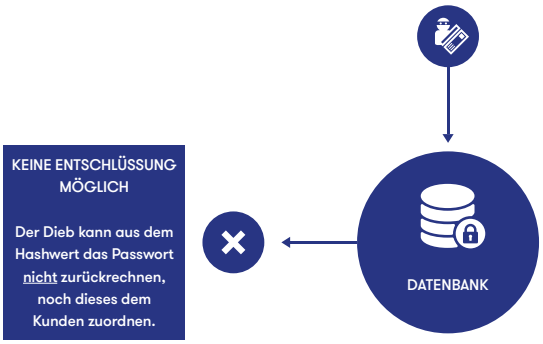
Daten zuverlässig zu sichern ist ein ständiger Wettlauf mit der technischen Weiterentwicklung - die Rechner werden immer schneller und damit können immer kompliziertere Passwörter schnell durchprobiert werden!

Anfangs

Im laufenden Betrieb



Im Fall des Diebstahls



Wort	**Hashwert** (Hashfunktion SHA256; alle Werte haben 64 Zeichen)
abc	ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad
Monster	3a241d59687b801ed1a519fd9acf1bad288e1cc9993b2d03a7974623483fa00a
Roland1234	6971a286f5d14a307ca15e47fdf7e209a4e8a643705cd4fba6b75a95bf8396a8
~Res#v4ZkT=xt44bH6&2	449252799bc73e0ac77026d17c3825bb2dea1cc0724b5326251804 3dbc69dee8

Wenn Sie sich die Beispiele für Hashwerte in der Tabelle anschauen und Sie kein Informatiker sind, werden Ihnen diese Zeichenketten wahrscheinlich wenig sagen. Sie werden sich sicherlich fragen, wie es möglich ist, aus den Kombinationen aussagekräftige Informationen zu gewinnen. IT-Experten – und die gibt es zunehmend unter den Kriminellen – sind dazu aber durchaus in der Lage! Wer das Prinzip beherrscht, für den ist es am Ende nur eine Frage der Zeit, ob er Erfolg hat.

Wie schnell ein Computer Hashwerte erstellen kann und wie wichtig Länge und Komplexität eines Passwortes sind, zeigt folgende Tabelle. Mit einem handelsüblichen Computer können circa 1.500.000.000 Hashwerte (Hashfunktion: SHA256) pro Sekunde (!) errechnet werden. Wir haben als Beispiel ein 5-stelliges, ein 8-stelliges und ein 12-stelliges Passwort gewählt. Außerdem haben wir drei Szenarien:

- **Groß- und Kleinschreibung: 52 verschiedene Zeichen**
- **Groß- und Kleinschreibung und Zahlen: 62 verschiedene Zeichen**
- **Alle im ASCII-Zeichencode darstellbaren Zeichen: 95 verschiedene Zeichen**

Stellen	**Anzahl der Möglichkeiten bei 52 verschiedene Zeichen** (bei Benutzung von Groß- und Kleinschreibung)	**Dauer des Errechnen aller Möglichkeiten** mit einem guten, handelsüblichen Computer (1.500.000.000 Haschwerte pro Sekunde). Die hier verwendete Hashfunktion: SHA256.
5	380 204 032	ca. 0,25 Sekunden
8	53 459 728 531 456	ca. 9,9 Stunden
12	390 877 006 486 250 192 896	ca. 8 263 Jahre

Das Errechnen aller Möglichkeiten nennt man Brute Force (deutsch: rohe Gewalt).

Stellen	**Anzahl der Möglichkeiten bei 62 verschiedene Zeichen** (bei Benutzung von Groß- und Kleinschreibung, sowie Zahlen)	**Dauer des Errechnen aller Möglichkeiten** mit einem guten, handelsüblichen Computer (1.500.000.000 Haschwerte pro Sekunde). Die hier verwendete Hashfunktion: SHA256.
5	916 132 832	ca. 6,1 Sekunden
8	218 340 105 584 896	ca. 40,4 Stunden
12	3 226 266 762 397 899 821 056	ca. 68 203 Jahre

Stellen	**Anzahl der Möglichkeiten bei 95 verschiedene Zeichen** (bei Benutzung von Groß- und Kleinschreibung, sowie Zahlen und Sonderzeichen; ASCII Zeichenkodierung)	**Dauer des Errechnen aller Möglichkeiten** mit einem guten, handelsüblichen Computer (1.500.000.000 Haschwerte pro Sekunde). Die hier verwendete Hashfunktion: SHA256.
5	7 737 809 375	ca. 51,6 Sekunden
8	6 634 204 312 890 625	ca. 51,2 Tage
12	540 360 087 662 636 962 890 625	ca. 17 134 705 976 111 015 Jahre

Die Beispiele zeigen deutlich: 8-stellige Passwörter ohne Sonderzeichen sind durchweg unsicher. Durch die Verwendung von Sonderzeichen wird ein Passwort hingegen komplexer und sicherer. Und auch bei einer Passwortlänge von 12 Zeichen steigt die Sicherheit rapide an.

Interpretiert man die erste der Tabellen näher, entsteht der Eindruck, dass ein Passwort mit zwölf Zeichen, das lediglich aus Groß- und Kleinbuchstaben (52 Zeichen) besteht, unknackbar sei. Denn wer hat schon die Zeit, 8.263 Jahre zu rechnen? Leider ist es nicht ganz so einfach. Denn diese Berechnungen beziehen sich, wie eingangs erwähnt, nur auf den Einsatz eines handelsüblichen Computers. Dank Cloud-Computing ist es jedoch möglich, für wenige Stunden oder Tage einen „Super-Computer“ zu mieten. Die Rechenleistung kann so um ein Vielfaches erhöht, die Rechenzeit gleichzeitig um ein Vielfaches gesenkt werden. Außerdem sind Kriminelle, die solche Methoden anwenden, vom Fach. Sie sind also sehr kompetent und clever.

Sie nutzen nicht nur hohe Rechenleistungen, sie rechnen auch mit Wahrscheinlichkeiten. Da viele Menschen zum Beispiel ihr Geburtsdatum oder ihr Geburtsjahr in ihr Passwort einbauen, ist das Passwort Roland1978 viel wahrscheinlicher als Roland1878. Solche Faktoren werden bei der Art und Weise des Berechnens berücksichtigt. Auch Wörterbücher und bereits bekannte, häufig verwendete Passwort-Kombinationen (die in bereits entschlüsselten Datenbanken vorkamen) kommen zum Einsatz.

Lange und zufällige Zeichenketten als Passworte bilden und diese verwalten - dabei hilft der Passwortsafe!

Deswegen ist die Unordnung (Entropie) eines Passwortes sehr entscheidend. Kann man sich sein eigenes Passwort nur schwer merken, ist es ein erstes Indiz für seine Sicherheit. Einige Experten gehen dazu über, den Begriff Passwörter durch Passphrasen zu ersetzen, um auch durch die Sprache auf die so wichtige Komplexität zu verweisen.

Eine weitere wichtige Faustregel lautet **longer = stronger**. Durch einfaches Verlängern des Passwortes erhöht sich auch die Anzahl möglicher Zeichenkombinationen. Das ist wirkungsvoller als das Steigern der Komplexität.

Hier ein Beispiel:

Bei einem 5-stelligen Passwort mit 52 verschiedenen Zeichen (52 hoch 5) gibt es 380.204.032 Möglichkeiten. Erhöht man die Komplexität und nimmt Zahlen hinzu (62 verschiedene Zeichen; 62 hoch 5) werden es 916.132.832 Möglichkeiten. Verlängert man das Passwort einfach um eine Stelle und bleibt bei 52 verschiedenen Zeichen (52 hoch 6) ergeben sich 19.770.609.664 Möglichkeiten. Also ein Vielfaches mehr.

Natürlich bleibt die sicherste Methode ein langes und komplexes Passwort. ;-)

Nachbemerkung

Dass Passwörter in der Praxis so oft mehrere oder sogar alle dieser Regeln verletzen, hat zum Teil mit Unkenntnis, zum Teil mit Bequemlichkeit, aber auch mit Effizienz zu tun.

Auf die Art und Weise, wie unsere meisten Devices abgesichert werden, haben wir keinen Einfluss, weil uns das der Hersteller vorgibt. Wir können aber eines tun: zumindest für jeden Device ein eigenes Passwort/einen eigenen PIN verwenden. Der Einbrecher, der es vielleicht zufällig schnell schafft, unseren PC oder Laptop zu knacken, sollte sich nicht auch gleichzeitig bequem noch am Tablet oder am Smartphone „bedienen" können.

Wie wir unsere Accounts schützen, haben wir – in Leitplanken (zum Beispiel durch die Beschränkung von Zeichenlängen oder Zeichenvorräten) – selbst in der Hand. Bei einer großen Anzahl von Accounts, die unterschiedliche Bedeutung für uns haben, können wirklich sichere Passwörter für alle Dienste vielleicht mühsam werden. Der erste Schritt ist hier, sich genau zu überlegen, wie wichtig welcher Account ist, und keinesfalls zufällig zu agieren, sondern zunächst die wichtigsten Accounts wirklich gut abzusichern. Wenn man dann in absteigender Folge für die Accounts am Ende der Liste einfachere Passwörter wählt (oder negativ ausgedrückt: nachlässiger vorgeht), ist das kein Beinbruch. Um zum Bild mit dem Haus zurückzukehren: Die Haustür und die Wohnungstür brauchen ein sicheres Schloss. Echte Wertsachen liegen im kleinen Safe. Weitere wichtige Unterlagen stecken in einer robusten Schublade, die abgeschlossen ist. Weiteres lässt sich lose verwahren.

In diesem Modul zeigen wir, wie Kinder ihren Passwortsafe anlegen können, wie sich also perfekt konstruierte Passwörter erstellen lassen. Aus praktischen Gründen haben wie uns auf zehn Zeichen beschränkt. Das sollte für die Anwendung in dieser Zielgruppe ausreichen.

Unser Tipp für das optimale Verwalten von Passwörtern:

Ein digitaler Passwortsafe!

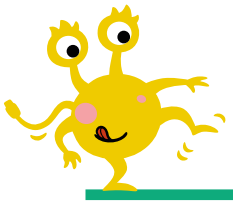
Tipps:

- **länger = sicherer**
- **umso unordentlicher, desto sicherer**
- **mindestens 10 Zeichen, gerne auch 20 ;-)**
- **Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen verwenden**
- **für jeden Account ein eigenes Passwort wählen**

Arbeitsblätter, Checklisten, Barometer als Materialsammlung

Im Folgenden finden sich alle Arbeitsmaterialien/Vordrucke um das Modul durchzuführen.

JA

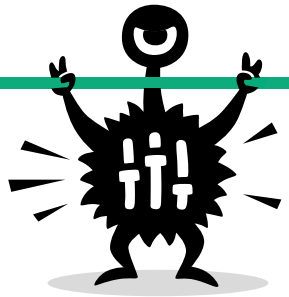


HÄUFIG

VIELLEICHT

SELTEN

NEIN



NIE

MEDIEN MONSTER
Medien kreativ begreifen

Klasse

Anzahl der Schüler

Hier kannst Du eintragen, wie die Kinder geantwortet haben.

Wofür braucht man Passwörter?

Wo hast Du einen Account?

	JA HÄUFIG	VIELLEICHT SELTEN	NEIN NIE
Hast Du eine eigene E-Mail-Adresse?			
Hast Du mehr als zwei Accounts?			
Hast Du mehr als zwei Passwörter?			
Hast Du schon einmal Dein Passwort vergessen?			
Soll man seiner besten Freundin, seinem besten Freund seine Passwörter sagen?			
Wie oft änderst Du Dein Passwort, Deine Passwörter?			
Magst Du Katzenvideos?			

Wie viele Zeichen sollte ein Passwort mindestens haben?

MEDIEN MONSTER
Medien kreativ begreifen

Aus welchen Zeichen-gruppen sollte ein Pass-wort bestehen?

MEDIEN MONSTER
Medien kreativ begreifen

10

Info:
Damit ein Passwort als „sicher“ gelten kann, sollte es mindestens 10 Zeichen haben. Es sollte aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Und: Warum nicht einmal ein passwort mit einer Zweichenlänge von 30 verwenden?!

Groß- und Kleinbuch-staben, Zahlen und Sonderzeichen

Ist
1qay2wsx3edc
ein gutes Passwort?

MEDIEN MONSTER
Medien kreativ begreifen

Ist
y6oru<Wf[{.6kCi*
ein gutes Passwort?

MEDIEN MONSTER
Medien kreativ begreifen

Nein.

Info:
Schaut man auf die Tastatur kann man ein Muster erkennen. So machen das viele, die ein scheinbar zufälliges, aber leicht zu merkendes Passwort wollen. Hacker wissen das.

Ja!

Info:
Es besteht aus Groß-/ Kleinbuchtsbane, aus Ziffern und Sonderzeichen und mehr als 10 Zeichen.

Wie viele Passwörter kann ein sehr guter Einzel-PC pro Sekunde ausrechnen?

MEDIEN MONSTER
Medien kreativ begreifen

Was sind persönliche Daten?

MEDIEN MONSTER
Medien kreativ begreifen

1 500 000 000

(eine Milliarde fünfhundert Millionen)

Info:
Ein guter Einzel-PC kann ca. 1,5 Milliarden Schlüssel pro Sekunde durchrechnen.

MEDIEN MONSTER
Medien kreativ begreifen

Name, Geburtstag, Anschrift, Telefon-nummer, E-Mail-Adresse

Info:
Persönliche Daten sind alle Angaben, die direkt zu einer Person gehören: Name, Geburtstag, Anschrift, Telefonnummer, E-Mail-Adresse. Personenbezogene Daten sind die persönlichen Daten und darüber hinaus auch weitere Angaben, die auf die Person „bezogen“ sind. Beispiele sind Kontonummer, Kreditkartennummer, Kundendaten, Beruf, Arbeitsplatz.
Wer sich unbefugt persönliche und personenbezogene Daten verschafft, erfährt sehr viel über die betreffende Person. Er kann diese Informationen leicht missbrauchen!

MEDIEN MONSTER
Medien kreativ begreifen

Was ist Phishing?

Wie viel Geld wurde beim größten Hack entwendet?

Beim Phishing versenden Datendiebe eine große Anzahl von E-Mails mit gefälschtem Absender.

Info:
Sie teilen den Empfängern mit, dass ein dringendes Problem besteht und fordern zu etwas auf. Beispielsweise sieht die Mail so aus, als käme sie von einer Bank und es wird mitgeteilt, dass das Passwort für den Online-Zugang ganz dringend überprüft werden muss. Dazu soll es sofort in ein Antwortfeld eingetragen werden. Die Antwort landet aber gar nicht in der Bank, sondern beim Absender, der ein Betrüger ist. Dieser hat daraufhin Zugang zum Konto. Und dieser Missbrauch wird noch nicht einmal bemerkt!

MEDIEN MONSTER
Medien kreativ begreifen

ca. 50 000 000 €
(fünfzigmillionen)

Info:
SheepMarket (eine annonymeer Verkaufsplattform) wurde zum Opfer eines Hackers, der die sagenhafte Summe von 96.000 Bitcoins – zu diesem Zeitpukt fast 60 Millionen Dollar – stahl und die User-Accounts gleichzeitig so manipulierte, dass sie zunächst nichts von dem Hack bemerkten.
https://bitcoinblog.de/2016/06/20/zwoelf-der-groessten-bitcoin-hacks/

MEDIEN MONSTER
Medien kreativ begreifen

Für Fortgeschrittene

Wie viele Kombinationen gibt es, bei einem 5-stelligen Passwort, bei der Nutzung von Groß- und Kleinbuchstaben?

(52 verschiedene Zeichen)

MEDIEN MONSTER
Medien kreativ begreifen

Für Fortgeschrittene

Wie lange braucht ein guter Einzel-PC, um alle Möglichkeiten eines 5-stelligen Passworts, bei der Nutzung von Groß- und Kleinbuchstaben, auszurechnen?

(52 verschiedene Zeichen)

MEDIEN MONSTER
Medien kreativ begreifen

380 204 032

(dreihundertachtzig Millionen zweihundertviertausendzweiunddreißig)

Info:
Groß- und Kleinbuchstaben sind 52 verschieden Zeichen. Das macht 52^5 (52×52×52×52×52) mögliche Kombinationen.

MEDIEN MONSTER
Medien kreativ begreifen

ca. 0,25 Sekunden

Info:
Bei einer Rechengeschwindigkeit von 1,5 Milliarden generierten Schlüsseln pro Sekunde (die gleichzeitig durch die Hashfunktion SHA-256 gehasht werden), was einem guten Einzel-PC entspricht.

MEDIEN MONSTER
Medien kreativ begreifen

Für Fortgeschrittene

Wie viele Kombinationen gibt es, bei einem 10-stelligen Passwort, bei der Nutzung von Groß-/ Kleinbuchstaben?

(52 verschiedene Zeichen)

MEDIEN MONSTER
Medien kreativ begreifen

Für Fortgeschrittene

Wie lange braucht ein guter Einzel-PC, um alle Möglichkeiten eines 10-stelliges Passworts, bei der Nutzung von Groß- und Kleinbuchstaben, auszurechnen?

(62 verschiedene Zeichen)

MEDIEN MONSTER
Medien kreativ begreifen

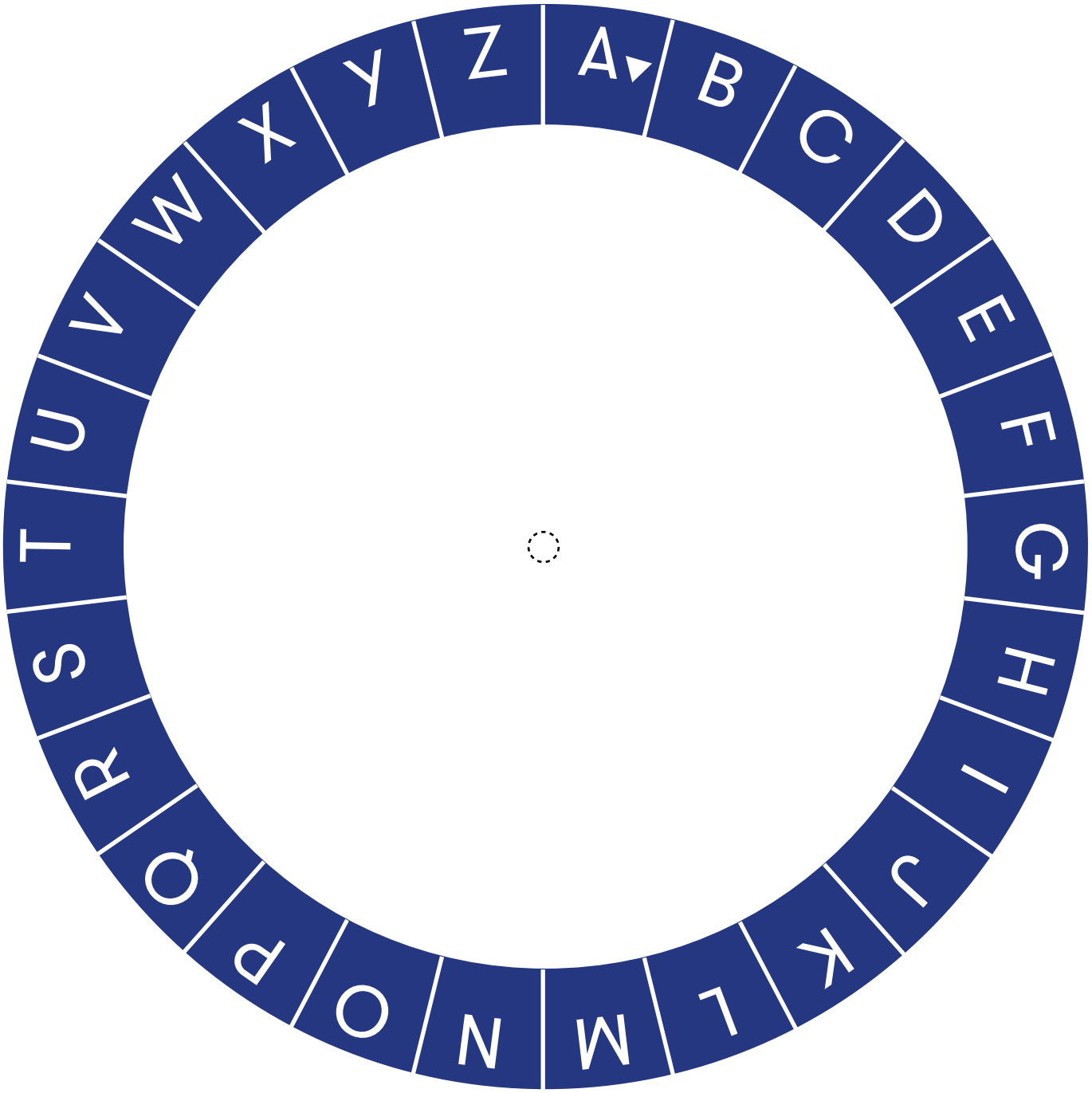
ca. 145 000 000 000 000 000 000

(hundertfünundvierzig Billiarden)

Info:
Groß- Kleinbuchstaben ergben 52 mögliche Zeichen. Das macht 52^{10} mögliche Kombinationen.

ca. 3 Jahre

Info:
Bei einer Rechengeschwindigkeit von 1,5 Milliarden generierten Schlüsseln pro Sekunde (die gleichzeitig durch die Hashfunktion SHA-256 gehasht werden), was einem guten Einzel-PC entspricht.


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z

A 1
B 2
C 3
D 4
E 5
F 6
G 7
H 8
I 9
J 10
K 11
L 12
M 13
N 14
O 15
P 16
Q 17
R 18
S 19
T 20
U 21
V 22
W 23
X 24
Y 25
Z
Erstelle verschlüsselte Botschaften!
blau → grün = verschlüsseln
grün → blau = entschlüsseln
MEDIEN MONSTER
Medien kreativ begreifen

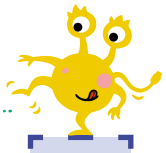
MEDIEN MONSTER
Medien kreativ begreifen

An verschiedenen Orten der Schule sind geheime Lösungswörter versteckt. Beantwortest Du die Frage richtig, weißt Du, an welchem Ort Du suchen musst. Bist Du dort angelangt, kannst Du mithilfe der Chiffrier-Scheibe die geheimen Wörter entschlüsseln. Trage die Lösungen in die entsprechenden Felder ein und erhalte das Master-Lösungswort.

Wer als erstes alle Rätsel gelöst hat, gewinnt!

Tipp: Du musst die verschiedenen Orte nicht der Reihenfolge nach suchen.

1. Welcher Raum ist entweder nur für Mädchen oder nur für Jungs?



2. Wo kommt man so richtig ins schwitzen?

3. Ein Raum, der nur für Lehrer ist.

4. Hier gehen alle durch, die in die Schule wollen.

5. Wo findest Du den Hausmeister?

6. Wer Hunger hat, bekommt hier etwas zu essen.

7. Wo kann man seine Kletterfähigkeiten unter Beweis stellen?

						2
7						
			4			
						3
	1					
						6
			5			

Master-Lösungswort

1	2	3	4	5	6	7

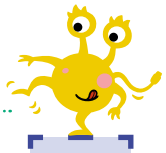
MEDIEN MONSTER
Medien kreativ begreifen

An verschiedenen Orten der Schule sind geheime Lösungswörter versteckt. Beantwortest Du die Frage richtig, weißt Du, an welchem Ort Du suchen musst. Bist Du dort angelangt, kannst Du mithilfe der Chiffrier-Scheibe die geheimen Wörter entschlüsseln. Trage die Lösungen in die entsprechenden Felder ein und erhalte das Master-Lösungswort.

Wer als erstes alle Rätsel gelöst hat, gewinnt!

Tipp: Du musst die verschiedenen Orte nicht der Reihenfolge nach suchen.

1. Welcher Raum ist entweder nur für Mädchen oder nur für Jungs?



H a l l o 2

.....

2. Wo kommt man so richtig ins schwitzen?

r 7 i e s i g

.....

3. Ein Raum, der nur für Lehrer ist.

T i s 4 c h

.....

4. Hier gehen alle durch, die in die Schule wollen.

l a u f e n 3

.....

5. Wo findest Du den Hausmeister?

M 1 a l e r

.....

6. Wer Hunger hat, bekommt hier etwas zu essen.

s c h u l e 6

.....

7. Wo kann man seine Kletterfähigkeiten unter Beweis stellen?

b i t 5 t e

Master-Lösungswort

M 1 O 2 N 3 S 4 T 5 E 6 R 7

MFQQT

Rot: 5

MEDIEN MONSTER
Medien kreativ begreifen

EVRFVT

Rot: 13

KZJTY

Rot: 17

ODXIHQ

Rot: 3

IWHAN

Rot: 22

MEDIEN MONSTER
Medien kreativ begreifen

LVANEX

Rot: 19

DKVVG

Rot: 2

MEDIEN MONSTER
Medien kreativ begreifen

DJFM!

Rot: 5

MEDIEN MONSTER
Medien kreativ begreifen

Name

MEDIEN MONSTER
Medien kreativ begreifen

Passwörter brauchst Du im Internet an vielen Stellen. Häufig beschützen sie wichtige Informationen. Deswegen solltest Du (viele) gute Passwörter haben, denn Passwörter sind wie ein Schlüssel. Um so komplizierter der Schlüssel bzw. das Passwort ist, desto besser bist Du geschützt.

Schreibe 10 verschiedene Sonderzeichen auf.

ErleBu

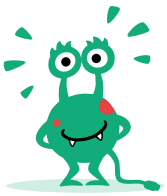
ErleBu bedeutet ‚erster, letzter Buchstabe'.

Mit Hilfe von ErleBu kannst Du aus Deinem Lieblingssongtext ein sicheres Passwort erstellen. Hier ein Beispiel:

Die **G**edanke**n** **s**in**d** **f**re**i,**
we**r** **k**an**n** **s**i**e** **e**rrate**n,**
si**e** **f**liehe**n** **v**orbe**i**
wi**e** **n**ächtliche **S**chatte**n.**

Das Passwort lautet: **DeGnsdfi,wrknseen,sefnviweneSn.**

Bei der ErleBu-Methode wird immer der erste und letzte Buchstabe eines Wortes, sowie alle Satzzeichen verwendet. Achte auch auf Groß- und Kleinschreibung!



Erstelle aus den folgenden Zeilen Passwörter mit der ErleBu-Methode.

Trage hier das Passwort ein.

es bleibet dabei:
die Gedanken sind frei.

Trage hier das Passwort ein.

Kein Mensch kann sie wissen,
kein Jäger erschießen,

Passwörter würfeln

Mit Hilfe von 5 Würfeln und einer Wortliste kannst Du ebenfalls sichere Passwörter erstellen. Dafür nimmst Du Dir 5 Würfel. Dann würfelst Du und legst die Würfel in eine beliebige Reihenfolge. Anschließend schaust Du in der Liste nach, welches Wort hinter der zufälligen Zahlenfolge steht.

Würfel 2 Passwörter, die aus 5 erwürfelten Wörtern bestehen.

Trage hier die beiden Passwörter ein.

Passwortkarte

Hast Du eine Passwortkarte, kannst Du sehr komplizierte Passwörter erstellen. Besonders dabei ist, dass Du mit einer Passwortkarte jederzeit, und an jedem Ort (falls Du sie bei Dir trägst) Dein Passwort wieder ablesen kannst, ohne es Dir merken zu müssen.

Erstelle mit Hilfe der ausliegenden Passwortkarte die Passwörter, für die Webseiten *kika.de* und *fragfinn.de*.

Trage hier das Passwort für *kika* ein.

Trage hier das Passwort für *fragfinn* ein.

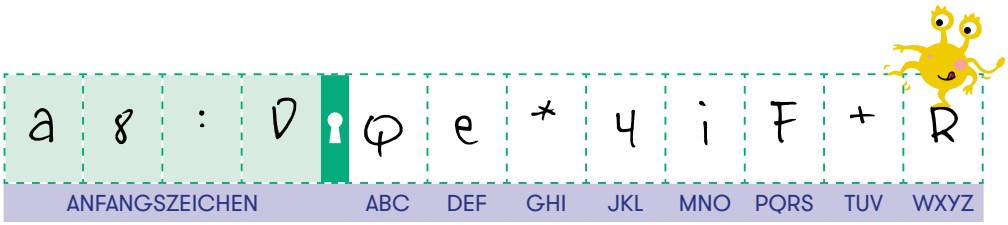
Tipps:

- länger = sicherer
- umso unordentlicher, desto sicherer
- mindestens 10 Zeichen, gerne auch 20 ;-)
- Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen verwenden
- für jeden Account ein eigenes Passwort wählen

Name

MEDIEN MONSTER
Medien kreativ begreifen

Passwörter braucht Du im Internet an vielen Stellen. Häufig beschützen sie wichtige Informationen. Deswegen solltest Du (viele) gute Passwörter haben, denn Passwörter sind wie ein Schlüssel. Um so komplizierter der Schlüssel bzw. das Passwort ist, desto besser bist Du geschützt.



Mithilfe der oben abgebildeten Passwortkarte kannst Du die verschlüsselten Worte entschlüsseln.

Entschlüssel das Wort ***4Q***

Entschlüssel das Wort ***e****

Entschlüssel das Wort ***R+****

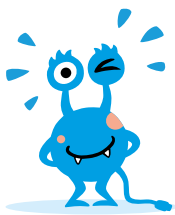
Entschlüssel das Wort ***ie*i***

Um die kurzen Worte zu entschlüsseln, nimmst Du einen verschlüsselten Buchstaben und schaust, welcher mögliche „echte“ Buchstabe dieser sein könnte. Dann nimmst Du den Nächsten, entschlüsseltst diesen und so weiter. Nachdem Du alle Buchstaben hast, fängst Du an zu kombinieren.

Hier das Beispiel für ***eQ***: ***e*** = D, E oder F

Q = A, B oder C

Die möglichen Worte wären: DA, DB, DC, EA, EB, EC, FA, FB, DC. Da das Wort aber einen Sinnn haben muss, kommt nur ***DA*** in Frage. ***„Da“*** ist also die Lösung!



MEDIEN MONSTER
Medien kreativ begreifen

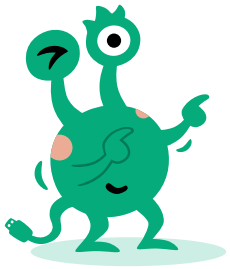
	ABC	DEF	GHI	JKL	MNO	PQR	STU	VWX	YZ.
1	*e6	7Ih	PG)	zNE	z9E	SmG	/1E	/MD	IQP
2	/3I	*eY	UCU	3I6	ü6S	XAP	GY8	YcS	74D
3	C/5	7SM	I8C	#IJ	957	qAh	AYh	)4N	365
4	SG4	6cN	c5#	#GY	*47	DzE	h8Y	hPN	6DY
5	AGY	06C	Y78	)35	UzA	UUI	3EI	A9m	MEI
6	MSs	8z3	*1ü	5h#	8s3	/IA	üe1	#2c	kw7
7	8!c	93J	/Aü	2)Q	CMS	9*e	kck	EG3	4YY
8	EG8	mX9	eXI	26m	mmM	Y!M	58)	ü#4	mE8
9	Xce	MAY	m92	*Jm	N!C	155	Nc!	8Y*	Az2
10	c7w	qIs	#cJ	764	9/5	Je/	I68	#AG	SNS

Anleitung:

1. Hier am Beispiel MONSTER.

2. Dann wird nach folgendem Schema die Karte gelesen:

1. **M** = z9E
2. **O** = ü6S
3. **N** = 957
4. **S** = h8Y
5. **T** = 3EI
6. **E** = 8z3
7. **R** = 9*e



Das komplette Passwort für **MONSTER** lautet:

z9Eü6S957h8Y3EI8z39*e

VORGEHENSWEISE:

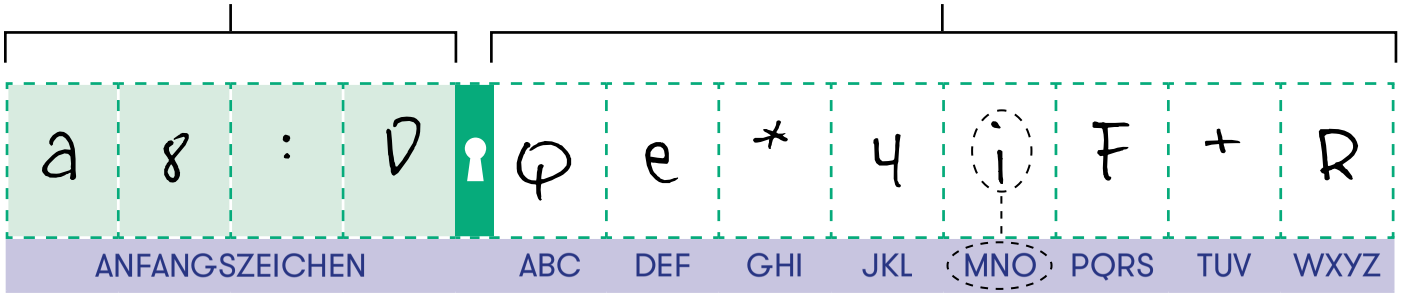
1. Erwürfel die ersten vier Zeichen, die ANFANGSZEICHEN. Beachte, dass eine Zahl und ein Sonderzeichen vorkommen, das ein Buchstabe großgeschrieben und der andere kleingeschrieben ist.
2. Nimm Dir 8 Würfel. Davon sollten zwei Würfel mit Sonderzeichen sein. Erfwürfel nun die fehlenden 8 Zeichen. Achte darauf, dass mindestens eine Zahl vorkommt.
3. Denke Dir ein Geheim-Wort aus mit mindestens 6 Zeichen, das Du niemandem verrätst.
4. Verschlüssel Buchstabe für Buchstabe.
5. Vergiss nicht vor jedes Passwort die ANFANGSZEICHEN zu setzen.
6. Fertig!

ANFANGSZEICHEN

- 1 × Sonderzeichen
- 1 × Zahl
- 1 × Großbuchstabe
- 1 × Kleinbuchstabe

ALPHABET

- 2 × Sonderzeichen
- 1 oder 2 Zahlen
- Großbuchstaben
- Kleinbuchstaben



So sähe Dein Passwort aus, wenn Dein Geheim-Wort **Monster** wäre:

M = i
O = i
N = i
S = F
T = +
E = e
R = F

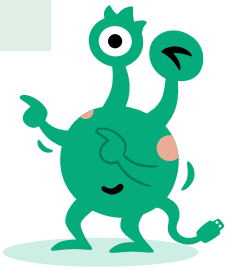
Verschlüsselt sieht das Wort **Monster** so aus:

iiiF+eF

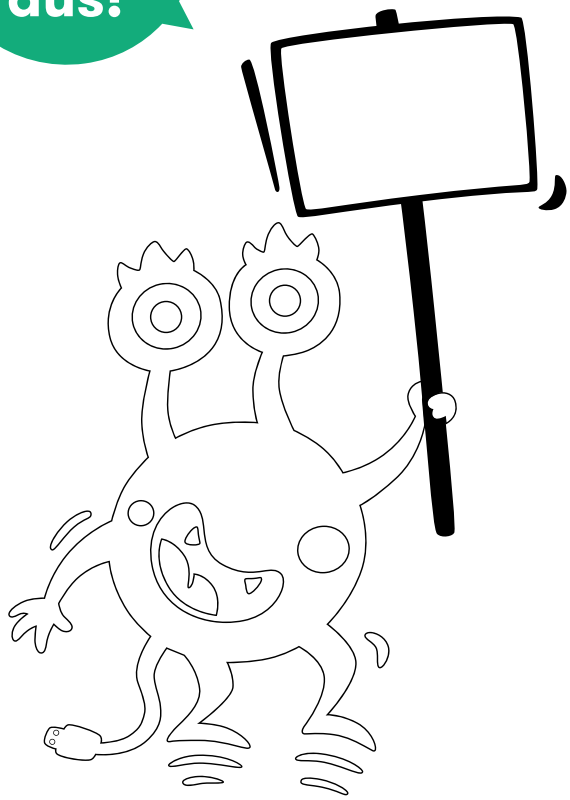
Setze jetzt noch die ANFANGSZEICHEN **a8:D** vor das verschlüsselte Wort.

Das komplette Passwort für **Monster** lautet:

a8:DiiiF+eF

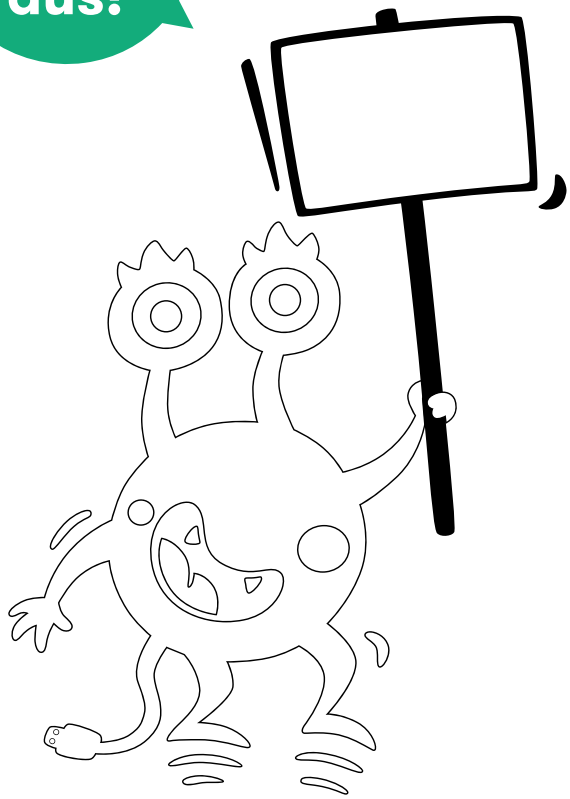


Mal mich aus!



MEIN MINI MONSTER SAFE

Mal mich aus!



MEIN MINI MONSTER SAFE

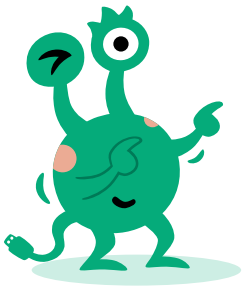
VORGEHENSWEISE:

1. Denke Dir ein geheimes Wort aus, mit mindestens 6 Zeichen.

2. Verschlüssel Buchstabe für Buchstabe.

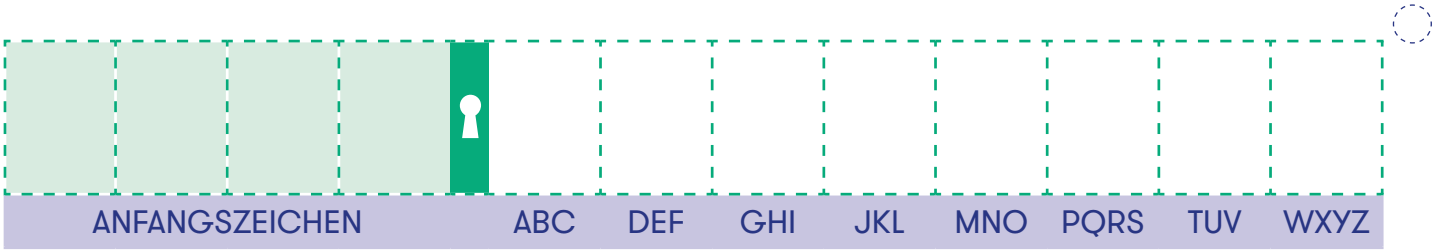
3. Vergiss nicht vor jedes Passwort die ANFANGSZEICHEN zu setzen.

Fertig!



EIN SICHERES PASSWORT BESTEHT AUS

- mindestens 10 Zeichen
- Groß- und Kleinbuchstaben
- mindestens einem Sonderzeichen



WICHTIG:

Dein Passwort bleibt immer geheim! Selbst Deiner besten Freundin oder Deinem besten Freund verrätst Du es nicht.

MEDIEN MONSTER
Medien kreativ begreifen

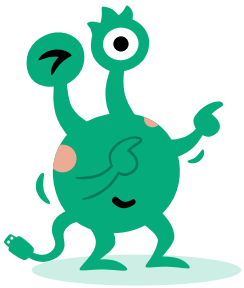
VORGEHENSWEISE:

1. Denke Dir ein geheimes Wort aus, mit mindestens 6 Zeichen.

2. Verschlüssel Buchstabe für Buchstabe.

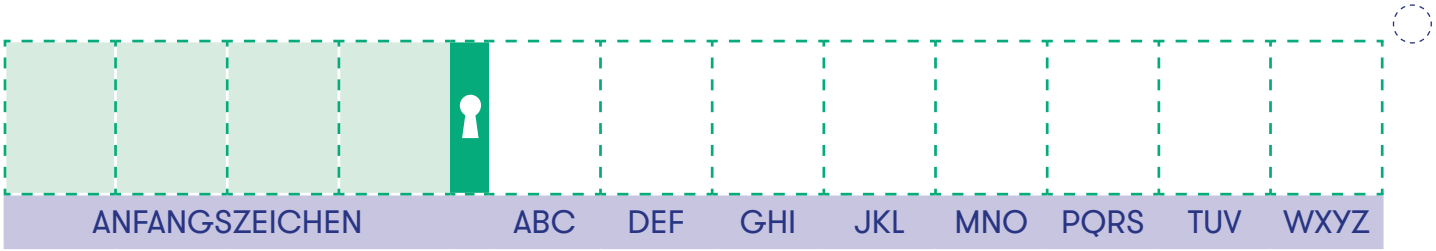
3. Vergiss nicht vor jedes Passwort die ANFANGSZEICHEN zu setzen.

Fertig!



EIN SICHERES PASSWORT BESTEHT AUS

- mindestens 10 Zeichen
- Groß- und Kleinbuchstaben
- mindestens einem Sonderzeichen

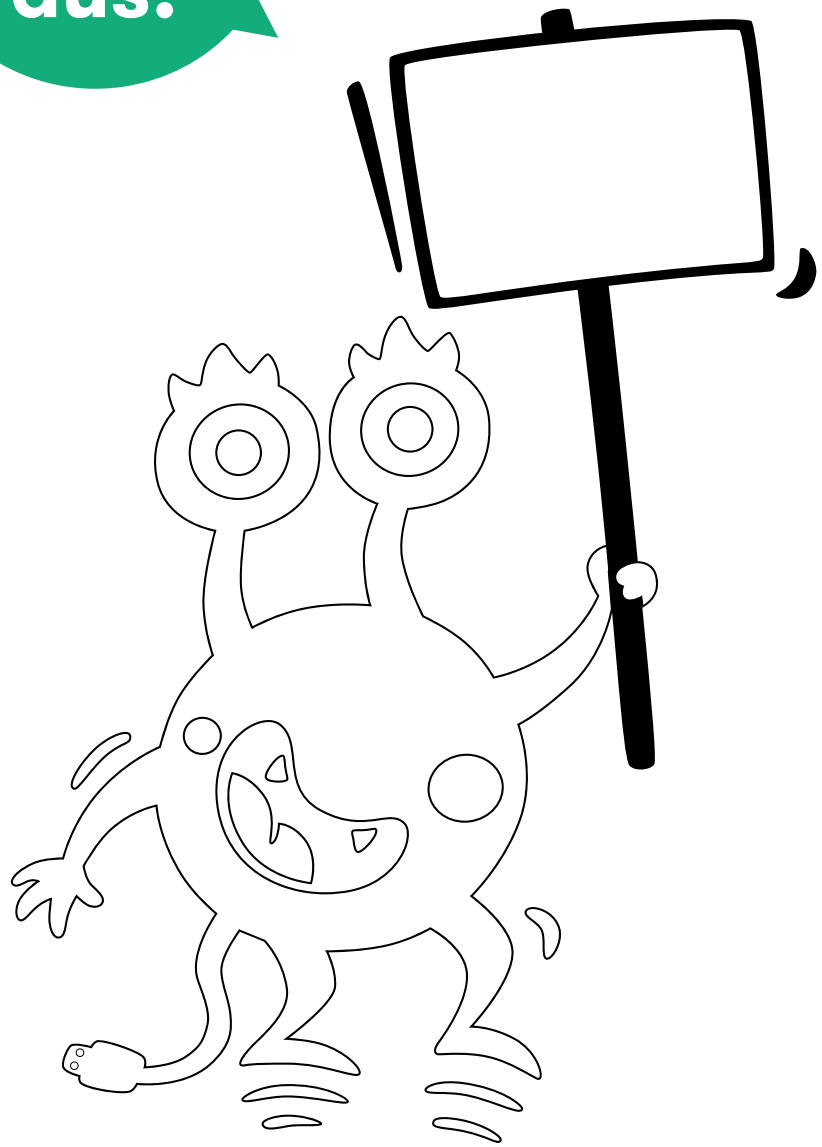


WICHTIG:

Dein Passwort bleibt immer geheim! Selbst Deiner besten Freundin oder Deinem besten Freund verrätst Du es nicht.

MEDIEN MONSTER
Medien kreativ begreifen

Mal mich aus!



MEIN MONSTER SAFE

	ABCD	EFGH	IJKL	MNOP	QRSTU	VWXYZ
1						
2						
3						
4						
5						
6						
7						
8						

	INTERNETSEITE	PASSWORT
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Trage hier Deine 10 wichtigsten Internetseiten samt Passwörter ein, damit Du sie immer griffbereit hast!

WICHTIG:
Setze an jedes Passwort ein Sonderzeichen, dass nur Du kennst!
So sind Deine Passwörter nicht entschlüsselbar, selbst, wenn Du sie verlieren solltest.

BEISPIEL:

PG)*eYI8Ch8Y06Ckw7**?**

Dieses Sonderzeichen kennst nur Du!

MEDIEN MONSTER
Medien kreativ begreifen

Impressum

Ohne die Hilfe und Mitarbeit von vielen Unterstützern, wäre dieses Modul nie zustande gekommen. Wir danken unseren Mitgliedern, Sponsoren und Ehrenamtler für ihr reichhaltiges Engagement. Ganz besonders danken wir:

Jennifer Fischer

Erich Schmidt-Dransfeld

Julia Münziger

Christian Roschow

Matthias Lindhorst

Maik Seehöfer

Jugendhilfe Essen

Chaospott

Adacor Hosting GmbH

kinoblau design

Konzeption

Jennifer Fischer, Christian Roschow, Julia Münziger, Marc Velten

Autoren

Erich Schmidt-Dransfeld, Marc Velten

Bildnachweis

MedienMonster

Projektleitung

Kiki Radicke, Marc Velten

MedienMonster e. V.
Medien kreativ begreifen
Emmastr 70 A
45130 Essen

www.medienmonster.info
hallo@medienmonster.info

Telefon 0201 857878 – 60
Telefax 0201 857878 – 61

CC BY ND