DURCHBLICKT!
Digital in eine gesunde Zukunft.

Schutz der personenbezogenen Daten

9–10 Jahre

Handreichung für Lehrkräfte

- Informationen
- Arbeitsblätter
- Lösungen

DURCHBLICKT! www.durch-blickt.de

Klett MINT

Rechtliche Unterstützung
von CMS Hasche Sigle

Ein Präventionsprogramm der
BARMER

Schutz der personenbezogenen Daten

Handreichung für Lehrkräfte

9–10 Jahre
Dauer: 90 min

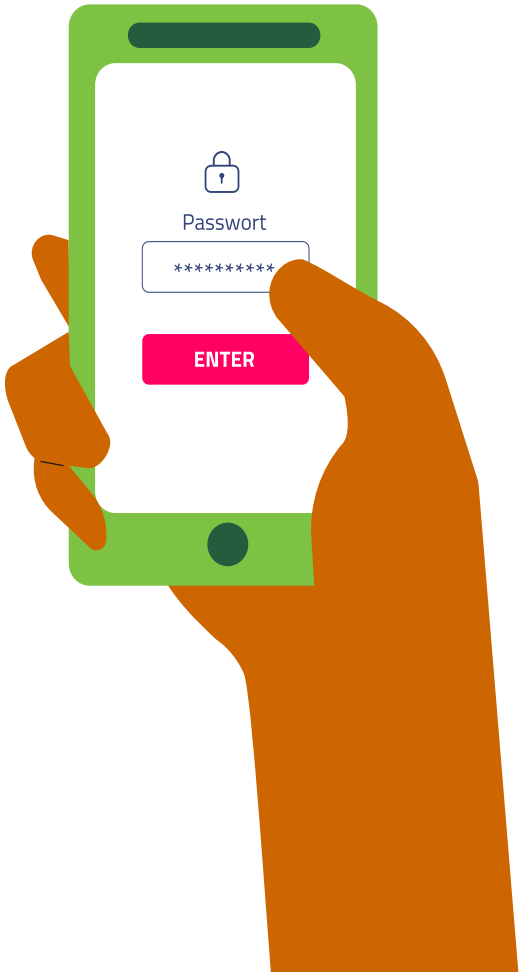
Die verwendeten Online Materialien/Tools sind DSGVO-konform.

Allgemeine Kurzbeschreibung des Themas

In dieser fächerübergreifenden Unterrichtseinheit sollen die Schülerinnen und Schüler die Bedeutung von personenbezogenen Daten (inklusive Gesundheitsdaten) verstehen und lernen, warum und wie sie diese im Alltag schützen können. Sie lernen zwei wichtige Möglichkeiten kennen, die eigenen sensiblen Daten vor unberechtigtem Zugriff und Missbrauch zu sichern und erkennen dabei auch die Notwendigkeit zur digitalen Verarbeitung von Daten. Sie bekommen einen Einblick, wie und wo ihre Daten gesammelt und genutzt werden können.

Ziel dieser Einheit ist es,

- aufzuzeigen, dass das Thema „personenbezogene Daten“ auch für diese Zielgruppe schon relevant ist.
- Datensparsamkeit zu fördern.
- die Schülerinnen und Schüler für einen vorsichtigen und umsichtigen Umgang mit ihren (Gesundheits-)Daten zu sensibilisieren.
- die zur Datensicherheit zur Verfügung stehenden Werkzeuge wie Passwort und Verschlüsselung zu verstehen und anzuwenden.
- die Alltagsrelevanz des Themas zu erkennen, um einen sichereren Umgang mit den eigenen Daten zu erreichen.



SCHULFÄCHER	BEZUG ZUM BILDUNGSPLAN
Religion/Ethik	▪ das eigene Handeln reflektieren ▪ Identität und Identitätsdiebstahl
Deutsch	▪ Lese- und Schreibkompetenz ▪ Verstehen von Texten zum Thema ▪ Üben von kritischem Denken
Biologie	▪ Gesundheitsförderung und -fürsorge ▪ Schutz- und Vorbeugemaßnahmen zum Erhalt der Gesundheit ▪ Förderung der Gesundheitskompetenz ▪ Wie funktioniert Wissenschaft und Forschung?
Informatik	▪ Grundlagen der Kryptographie (Verschlüsselung)
Mathematik	▪ mathematische Operationen, Muster und Strukturen ▪ Wahrscheinlichkeiten
Geschichte	▪ frühe Formen von Verschlüsselung und Kryptographie in der Geschichte (ausgehend von der Cäsar-Scheibe)
Wirtschaft/HSU	▪ Daten als „moderne Währung“
Geografie	▪ Wie reisen unsere Daten um die Welt? (z. B. via Amazon Bestellung, E-Mail schreiben, Online Spiele spielen)
Sport	▪ Gesundheitsdaten sinnvoll nutzen

KMK-Kompetenzen

- Risiken und Gefahren in digitalen Umgebungen kennen, reflektieren und berücksichtigen
- Strategien zum Schutz entwickeln und anwenden
- Maßnahmen für Datensicherheit und gegen Datenmissbrauch berücksichtigen
- Privatsphäre in digitalen Umgebungen durch geeignete Maßnahmen schützen
- Funktionsweisen und grundlegende Prinzipien der digitalen Welt kennen und verstehen
- Eigene Defizite bei der Nutzung digitaler Werkzeuge erkennen und Strategien zur Beseitigung entwickeln
- Anforderungen an digitale Werkzeuge formulieren

Schwerpunkt der Einheit nach den 7 Dimensionen der digitalen Gesundheitskompetenz:

Umgang mit personenbezogenen Informationen und Datenschutz:
verstanden als die Fähigkeit, Informationen über sich und andere Personen in digitalen Medien nicht zu teilen und zu entscheiden, wer Zugriff auf die personenbezogenen Daten und Informationen hat

Bestimmen der Alltagsrelevanz:
verstanden als die Fähigkeit, zu entscheiden, ob die gefundenen Informationen für die eigene Lebenslage und das eigene gesundheitsbezogene Anliegen nützlich sind

Weitere Informationen zu den 7 Dimensionen der digitalen Gesundheitskompetenz finden Sie im Exkurs und unter www.durch-blickt.de

Sozialform

- Plenum
- Gruppenarbeit
- 2er Gruppen
- Einzelarbeit

Link zur Einheit

- Startervideo, TaskCards und weitere Informationen unter www.durch-blickt.de

Kursmaterial (Lehrkraft)

- Tablet oder Laptop zur Ergebnissammlung
- Beamer, wenn nicht vorhanden: Tafel oder Flipchart
- Erwartungshorizont
- Möglichkeit Video zu zeigen
- eine kleine, mit Schloss verschließbare Box

Kursmaterial (Lernende)

- Schulheft für Notizen
- Tablet, Smartphone oder Schulgerät

Klasse(n) Meditationen und Achtsamkeitsübungen

7Mind@School bieten viele Übungen. Reinschauen und entspannen! Weitere Informationen unter www.durch-blickt.de

Online Material und Werkzeuge in der Einheit

- www.kits.blog (fakultativ)
- www.cryptoclub.org (fakultativ)
- www.taskcards.de (fakultativ)

Unterrichtsvorbereitung

- Video testen
- Arbeitsblätter ausdrucken
- evtl. Daten ausschneiden und im Klassenraum verstecken
- evtl. Schulgeräte besorgen
- evtl. Spreizklammern für die Cäsar-Scheibe besorgen

Ablauf

Einstieg	Startervideo zur Einheit
Hinführung zum Thema	Daten, Datenschutz, Datensicherheit?
Erarbeitung 1	Meine digitalen Daten
Vertiefung	Sensible Daten vor unberechtigtem Zugriff schützen
Erarbeitung 2	Daten mit Passwörtern sichern
Praxisphase 1	Sichere Passwörter erstellen und verwalten
Erarbeitung 3	Datenverschlüsselung
Praxisphase 2	Nachrichten verschlüsseln
Reflexion	Abschlussrunde

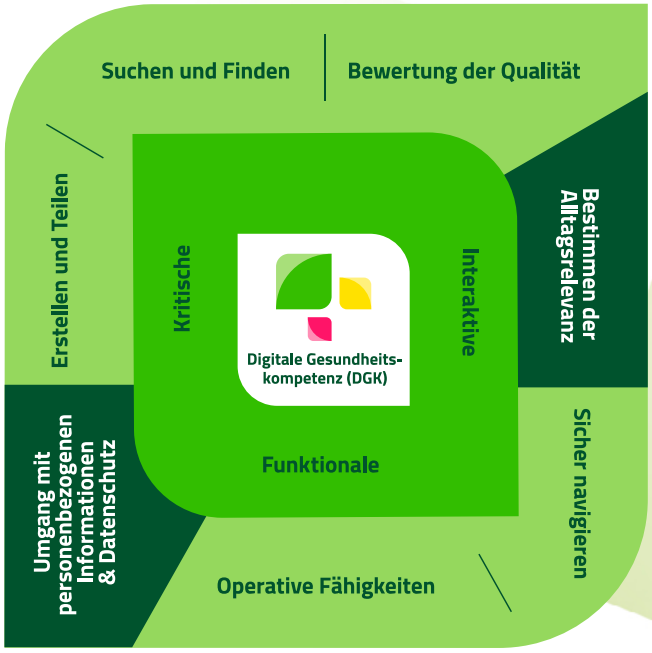
ZIEL UND FRAGESTELLUNG	METHODIK	MEDIUM
Einstieg Was hast du im Video gesehen?	Sammeln der Antworten im Plenum (Fragen und offene Antworten) und Überleitung zur Hinführung	▪ Video
Hinführung zum Thema Die Begriffe Daten, Datenschutz und Datensicherheit: Definitionen	Vortrag der Lehrkraft und Plenumsdiskussion Arbeit im Klassenverband oder in 2er Gruppen bei der Zuordnungsübung (je nach gewählter Form der Umsetzung)	**analog:** ▪ Tafel, Whiteboard oder Flipchart Definition fixieren: Daten, Datenschutz, Datensicherheit ▪ Arbeitsblatt 1 oder **digital:** ▪ www.kits.blog (Anleitung: siehe Anhang 5) ▪ Zuordnungsübung: www.learningapps.org *Weitere Informationen im folgenden Unterrichtsmaterial:* ▪ Ökonomischer Umgang mit Medien ▪ Personenbezogene Daten
Erarbeitung 1 ▪ Wer möchte deine Daten? ▪ Ist es immer erlaubt/legal, wenn jemand deine Daten sammelt und speichert? Ergänzende Fragen: ▪ Welche Daten sind von dir auf Computern gespeichert? ▪ Wo befinden sich diese Daten?	Plenum, am Ende abschließende Diskussion	▪ Tafel, Whiteboard oder Flipchart: Ergebnisse festhalten
Vertiefung **Phase 1:** Daten-Schatzsuche: Warum müssen gerade Gesundheitsdaten vor unberechtigtem Zugriff besonders geschützt werden? (siehe Erwartungshorizont)	Phase 1: Einzelarbeit	▪ Anhang 1 ▪ Schulheft oder Blatt zum Ideen sammeln

ZIEL UND FRAGESTELLUNG	METHODIK	MEDIUM
Phase 2: Was könnte passieren, wenn personenbezogene (Gesundheits-) Daten in die falschen Hände geraten?	Phase 2: Gruppenarbeit in 3er oder 4er Gruppen	*Weitere Informationen im folgenden Unterrichtsmaterial:* Umgangsregeln im Netz
Erarbeitung 2 Wichtige Methode, um Daten zu sichern: Passwörter ▪ Benutzt du Passwörter? ▪ Warum sind Passwörter wichtig? ▪ Wo nutzen z. B. deine Eltern Passwörter?	Plenum, danach Einzelarbeit oder 2er Gruppen (siehe Arbeitsauftrag im Erwartungshorizont)	▪ Anhang 2 ▪ Arbeitsblatt 2 (nur Checkliste)
Praxisphase 1 Sichere Passwörter erstellen und verwalten: ▪ Wie erstelle ich sichere Passwörter? ▪ Welche Methoden helfen mir dabei?	Einzelarbeit	▪ Arbeitsblatt 2: einen eigenen Passwortvorschlag erarbeiten
Erarbeitung 3 Neben der Passwort-Nutzung wird nun die zweite Säule vorgestellt: die Datenverschlüsselung ▪ Was bedeutet es, Daten zu verschlüsseln? ▪ Was ist mit „Verschlüsselung“ gemeint?	Vortrag und Diskussion anhand von Beispielen	–
Praxisphase 2 Auf einfache Weise Nachrichten mit der Cäsar-Scheibe verschlüsseln Fakultativ/Alternativ: Codebrecher oder eine Nachricht schreiben	im Plenum: Funktionsweise erläutern Arbeitsblatt: 2er Gruppen	**analog:** ▪ Arbeitsblatt 3: Cäsar-Scheibe basteln ▪ Anhang 4 oder **digital:** ▪ www.cryptoclub.org
Reflexion ▪ Was hast du in dieser Einheit gelernt? ▪ Welche Erkenntnisse hast du gewonnen? ▪ Was könntest du anders machen, um deine Daten sicher zu halten? ▪ Wie erkennst du, ob deine Daten sicher sind oder nicht? ▪ Was musst du tun, wenn deine Daten nicht sicher sind?	Diskussion im Plenum	▪ Arbeitsblatt 4 ▪ Anhang 3: Glossar

Über digitale Gesundheitskompetenz

Definition von digitaler Gesundheitskompetenz angelehnt an die HLS-Definition (2012):

Digitale Gesundheitskompetenz basiert auf dem allgemeinen Konzept von Gesundheitskompetenz und umfasst neben dem Wissen die Motivation und die Fähigkeiten, auch die digitale und Medienkompetenz von Kindern und Jugendlichen sowie relevante Informationen und Dienstleistungen für die Gesundheit in digitaler Form zu finden, zu verstehen, zu beurteilen und anzuwenden. Sie versetzt sie in die Lage, im Alltag in den Bereichen der Krankheitsbewältigung, Krankheitsprävention und Gesundheitsförderung Urteile fällen und Entscheidungen treffen zu können, die ihre Lebensqualität während des gesamten Lebensverlaufs erhalten oder verbessern. Während „Digitalkompetenz" als die Fähigkeit der angemessenen Nutzung von Medien- und Kommunikationstechnologien beschrieben wird, kann unter „digitaler Gesundheitskompetenz" die Fähigkeit der angemessenen Nutzung von digitalen Informationstechnologien zur Erschließung und Verarbeitung gesundheitsbezogener Informationen verstanden werden.



Dimensionen der digitalen Gesundheitskompetenz

Stufen der Gesundheitskompetenz nach Nutbeam (2000)

Sieben Dimensionen der digitalen Gesundheitskompetenz angelehnt an van der Vaart und Drossaert (2017):

- **Operative Fähigkeiten:** wird verstanden als die Fähigkeit, mit digitalen Endgeräten und digitalen Medien umgehen zu können (z. B. einen PC, ein Tablet oder eine Suchmaschine zu bedienen)
- **Suchen und Finden von Gesundheitsinformationen:** wird verstanden als die Fähigkeit, den gesundheitsbezogenen Informationsbedarf in eine geeignete Suchstrategie zu überführen (z. B. eine Frage zu formulieren, Suchanfragen entsprechend des Informationsbedarfs zu stellen) und die ermittelten Informationen auch zu verstehen
- **Bewertung der Qualität von Gesundheitsinformationen:** wird verstanden als die Fähigkeit, die Verlässlichkeit und Vertrauenswürdigkeit der ermittelten gesundheitsbezogenen Informationen zu bewerten (z. B. kritische Einschätzung, ob die gefundenen Informationen kommerziellen Charakter haben)
- **Bestimmen der Alltagsrelevanz:** wird verstanden als die Fähigkeit, zu entscheiden, ob die gefundenen Informationen für die eigene Lebenslage und das eigene gesundheitsbezogene Anliegen nützlich sind
- **Sicher im Internet navigieren:** gemeint ist die Fähigkeit, sich im Internet und in digitalen Medien gut zu orientieren (z. B. den Überblick auf einer Website zu behalten)
- **Erstellen und Teilen von Gesundheitsinformationen:** hierunter wird die Fähigkeit verstanden, eigene gesundheitsbezogene Anliegen mittels digitaler Medien (z. B. E-Mail) verständlich und klar zu formulieren
- **Umgang mit personenbezogenen Informationen und Datenschutz:** wird verstanden als die Fähigkeit, Informationen über sich und andere Personen nicht in digitalen Medien zu teilen und zu entscheiden, wer Zugriff auf die persönlichen Daten und Informationen hat

Lösungen/Erwartungshorizont

Einstieg.

Was hast du im Video gesehen?

Individuelle Antworten der Lernenden

Von der Lehrkraft sollten die Themen Daten und Datensicherheit in den Vordergrund gerückt werden und als Überleitung zum nächsten Punkt verwendet werden.

Hinführung zum Thema.

Lösungshinweise zu Arbeitsblatt 1 – Hinführung und konkrete Beispiele:

1. Was sind Daten?

Daten sind wie Informationen oder Geschichten über etwas. Es sind Details, die uns mehr über eine bestimmte Sache erzählen. Man kann sich hier z. B. ein Spielzeugauto vorstellen. Wann wurde das Auto gebaut, wo wurde es gebaut, wer hat es gebaut, welche Farbe hat es, wie lang und breit ist es, wie schnell fährt es? All das sind **Daten** über das Auto.

Es gibt verschiedene Kategorien von Daten.

→ Was sind personenbezogene Daten?

Personenbezogene Daten sind Informationen, die untrennbar zu euch gehören und die etwas über euch verraten. Das kann euer Name sein, eure Adresse, eure Telefonnummer oder E-Mail-Adresse, aber auch euer Geburtsort oder eure Hobbys. Wenn ihr zum Beispiel in einem Online Spiel euren echten Namen verwendet, dann ist das eine personenbezogene Information, die andere Leute nutzen könnten, um mehr über euch zu erfahren.

→ Was sind Gesundheitsdaten?

Es gibt personenbezogene Daten, die besonders geschützt werden, weil sie sensible Informationen über euch verraten. Dazu gehören unter anderem Gesundheitsdaten, die Informationen über eure Gesundheit preisgeben. Zum Beispiel können das Informationen sein, die zeigen, ob ihr gerade eine Erkältung habt, ob ihr gegen bestimmte Medikamente allergisch seid oder eine chronische Krankheit wie Diabetes, Asthma oder anderes habt. Wenn ihr eine Gesundheitsapp auf eurem Tablet oder Smartphone verwendet, dann könnte diese App solche Gesundheitsdaten sammeln.

→ Wozu können personenbezogene Daten genutzt werden?

Personenbezogene Daten können auf ganz verschiedene Arten verarbeitet werden. Beispielsweise können personenbezogene Daten genutzt werden, um euch zu identifizieren oder um Dinge über euch herauszufinden, die ihr lieber geheim halten möchtet. Personenbezogene Daten können auch gesammelt und an andere Personen weitergegeben werden, auch wenn ihr das nicht möchtet und ohne dass ihr das bemerkt. Zudem können personenbezogene Daten für eine lange Zeit gespeichert oder verändert werden. Schließlich können personenbezogene Daten auch offengelegt werden, also einer Vielzahl von anderen Personen gezeigt werden. Personenbezogene Daten können aber auch gelöscht oder vernichtet werden.

2. Was ist Privatsphäre?

Unter **Privatsphäre** versteht man den Teil des Lebens eines Menschen, der nur ihn etwas angeht. Dieser Bereich ist nicht öffentlich, sondern privat. In diesem Bereich kann jede Person leben, wie sie will – was sie dort tut oder denkt, geht niemanden außer sie selbst etwas an. Auch in der Privatsphäre muss man sich an Gesetze halten und darf insbesondere nicht die Persönlichkeitsrechte anderer Menschen missachten.

Die **informationelle Selbstbestimmung** bedeutet, dass jeder Mensch Informationen für sich behalten und entscheiden kann, was andere über ihn wissen dürfen. Es geht darum, dass man in Ruhe gelassen wird und es einen Bereich gibt, zu dem nicht jede Person Zugang hat. In der digitalen Welt bedeutet es auch, dass man die Kontrolle darüber behält, wer Daten oder Gespräche sehen oder hören darf, kann oder soll. Es ist eine geschützte Zone, in der jeder Mensch selbst entscheiden kann, wer eintreten darf.

3. Was ist Datenschutz?
Alle Menschen haben ein Recht auf den Schutz ihrer persönlichen Daten. Beim **Datenschutz** geht es vor allem darum, die Privatsphäre und personenbezogenen Daten vor missbräuchlicher Erhebung, Verwendung und Weitergabe zu schützen. Datenschutz bezeichnet also insbesondere das Recht jeder Person, selbst zu entscheiden, welche personenbezogenen Daten an wen weitergegeben werden und was mit diesen Daten gemacht werden darf. In den Datenschutzgesetzen ist daher festgelegt, dass jede und jeder darüber Auskunft erhalten kann, welche Daten von ihr oder von ihm gesammelt werden und was mit diesen Daten passiert. Wenn Daten zu Unrecht gesammelt werden, kann man fordern, dass sie gelöscht werden.

➔ Was hat das mit meiner Gesundheit zu tun?
Stellt euch vor, es gibt eine kleine Box mit all euren Gesundheitsdaten. Darin steht zum Beispiel, wann der letzte Besuch bei der Ärztin oder beim Arzt war, welche Medikamente einzunehmen sind oder Informationen wie eure Größe und euer Gewicht. Es geht darum, sicherzustellen, dass nur die Personen, denen ihr vertraut, wie den Eltern und/oder Erziehungsberechtigten, der Ärztin oder dem Arzt, diese sehr persönlichen Informationen sehen und verwenden können.

4. Was ist Datensicherheit?
Datensicherheit dient dem Schutz personenbezogener Daten vor einem unbefugten Zugriff von außen, einer Manipulation oder einer Zerstörung. Hierfür werden sogenannte technische und organisatorische Maßnahmen eingerichtet, um sicherzustellen, dass niemand ohne die Erlaubnis der betroffenen Person auf personenbezogene Daten zugreifen kann.

Während es beim **Datenschutz** vor allem darum geht, dass persönliche Daten nicht an Dritte weitergegeben werden dürfen, geht es bei der **Datensicherheit** insbesondere darum, die Daten vor dem Zugriff unberechtigter Dritter zu schützen.

➔ Was hat das mit meiner Gesundheit zu tun?
Stell euch wieder die kleine Box mit all den Gesundheitsinformationen vor. Datensicherheit ist wie ein Schloss an dieser Box. Sie stellt sicher, dass die Informationen in der Box sicher sind und nicht gestohlen oder versehentlich gelöscht werden können.

Zur Festigung des Verständnisses kann die Zuordnungsübung auf www.learningapps.org im Plenum über Beamer oder in 2er Gruppen mit Schulgeräten gemacht werden. So soll die Trennung von Datenschutz und Datensicherheit nochmal deutlich gemacht werden.

Erarbeitung 1.

In dieser Phase verstehen die Lernenden die Alltagsrelevanz der Thematik und bekommen ein Verständnis dafür, dass digitale Daten allgegenwärtig sind und nicht automatisch immer gesichert sind. Sie lernen, abzuwägen, wo digitale Daten sinnvoll genutzt werden und wo Gefahren sein könnten.

Wer will deine Daten? Ist es immer erlaubt/legal? – Vorschläge:
legal: Schule, Gemeinde, Verein, Praxis
ohne meine Einwilligung: Apps, Hacker, Leute, mit denen ich Streit hatte
Die beiden sich anschließenden Fragen können bei jedem der einzelnen Punkte geklärt werden, also „welche" Daten haben diese oder wollen diese Personen oder Einrichtungen haben und wo sind sie vermutlich gespeichert (PC, Handy, Tablet)?

Wo befinden sich diese Daten? Vorschläge:
Computer im Schulsekretariat, Smartphone, Praxis, Computer zu Hause (eventuell digitaler Kalender in der Familie)

Zusatzerklärung: Erklären Sie, dass es durchaus sinnvoll ist, dass Schule, Verein, Praxis (Arzt, Ärztin), usw. die Daten haben. Versäumen Sie aber nicht zu erwähnen, dass nicht jede Person, die nach personenbezogenen Daten fragt, gute Absichten hat und dass die Schülerinnen und Schüler immer vorsichtig sein und Erwachsene um Rat fragen sollten.

Abschließende Diskussion. Die besprochenen Inhalte der vorherigen Arbeitsphase werden hier wieder aufgegriffen. Als Überleitung zum nächsten Schritt fokussiert die Lehrkraft auf diejenigen Beiträge der Lernenden aus den vorigen Arbeitsphasen, die Gesundheitsdaten ansprachen.

Vertiefung.

In diesen beiden Phasen vergegenwärtigen sich die Lernenden an einem konkreten Beispiel, wie Daten einzeln nicht viel bedeuten müssen, wie aber das Verbinden und Verknüpfen von Daten dazu führen kann, ein „Profil" einer Person zu erstellen, das schon relativ viel über die Person aussagen kann. Sie lernen, zwischen unbedenklichen Daten und sensiblen Daten zu differenzieren.

Phase 1:

Warum müssen gerade Gesundheitsdaten vor unberechtigtem Zugriff geschützt werden?

Arbeiten mit Anhang 1:

Im Klassenzimmer sind Daten von Paul versteckt. Die Lernenden werden aufgefordert, die Daten zu suchen (eventuell mit Hilfe der Lehrkraft). Danach wird besprochen, warum die gefundenen Daten an einem sicheren Ort verwahrt werden müssen. Den Lernenden soll bewusst werden, dass offen zugängliche Daten von vielen Menschen ganz einfach gefunden werden können. Jede Information für sich, ist nicht sonderlich hilfreich (wenn also jemand die Information „Pikachu" findet, weiß diese Person nur, dass Paul Pokemon mag), wenn man aber alle Informationen zusammen betrachtet, ergibt sich ein recht konkretes Bild von Paul. Darunter auch Informationen, die für böswillige Zwecke genutzt werden können.

Hinweis für die Lehrkraft: „Verliebt in Paula" soll für die Lernenden unzugänglich, z. B. in einer kleinen Kiste mit einem Schloss versehen, versteckt werden. Dies dient als Beispiel für Passwort-Sicherheit. Die beiden kryptischen Informationen können von der Lehrkraft vielleicht so eingebaut werden: „Oh, da ist wohl was mit meinem Computer gewesen" oder „Oh, da habe ich wohl einen Fehler gemacht" und die beiden beiseitelegen, da sie beim Thema „Verschlüsselung" nochmal gebraucht werden. „Fxymrfynpjw" heißt entschlüsselt „Asthmatikerin" oder „Asthmatiker" und „qjxjxhmbfjhmj" heißt entschlüsselt „Leseschwäche".

Phase 2:

Welche möglichen Probleme können entstehen, wenn personenbezogene (Gesundheits-)Daten in die falschen Hände geraten?

Mögliche Daten: Name, E-Mail, Adresse, Familie, biometrische Daten (Finger, Gesicht), Fitnesstracker
Die Lehrkraft lässt Notizen erstellen und am Ende der Sequenz präsentieren die Lernenden ihre Ergebnisse.

Mögliche Probleme aus der Sicht der Schülerinnen und Schüler:

Mobbing, Identitätsdiebstahl, Doxing, Stalking, finanzieller Schaden bei Online Bestellungen, Benachteiligung im Verein oder im Schulleben, auch Eltern bzw. Erziehungsberechtigte können mit hineingezogen werden.
Doxing ist eine Praxis, bei der personenbezogene Daten über eine Person recherchiert, gesammelt und ohne deren Zustimmung im Internet veröffentlicht werden, oft mit schädlichen Absichten. Dies kann Informationen wie Namen, Adressen, Telefonnummern, E-Mail-Adressen und mehr umfassen. Das Hauptziel von Doxing besteht oft darin, die Privatsphäre einer Person zu verletzen oder sie online anzugreifen.

Erarbeitung 2.

In dieser Phase wird das Prinzip von Passwörtern verbildlicht. Kriterien für sichere Passwörter werden vermittelt und die Lernenden bewerten anhand dieser Kriterien ihre eigenen (fiktiven) Passwörter.

Benutzt du Passwörter?
Individuelle Antworten der Lernenden
Beispiele: Handy, Computer, Handyvertrag, E-Mail-Konto, Bankkonto usw.
Bei diesbezüglich schon versierten Kindern kann darauf hingewiesen werden, dass es Unterschiede gibt zwischen „Passwort" (also was man z. B. bei einer Webseite als Zugang zu einem Account hat), „PIN" (z. B. beim Zugang zum Smartphone) oder „TAN-Generator" (z. B. beim Online Banking). In den folgenden Arbeitsphasen liegt der Fokus auf „Passwort".

Warum sind Passwörter wichtig?
Erklären Sie, dass nicht alle Informationen über Paul (aus der vorherigen Arbeitsphase) zugänglich sind, da die Lehrkraft den Code für das Schloss nicht verraten hat. Passwörter sind also wie Schlüssel zu unseren digitalen „Häusern", die unsere personenbezogenen Daten und Online Konten schützen. Die Lehrkraft kann hier das Passwort verraten und eine weitere Information über Paul wird sichtbar.

Wo nutzen z. B. deine Eltern Passwörter?
Individuelle Antworten der Lernenden

Arbeitsauftrag: Erstelle ein Passwort, um Pauls digitale Daten zu schützen.
Individuelle Antworten der Lernenden

Die Lehrkraft lässt entscheiden, ob die genannten Passwörter sicher oder unsicher sind und diskutiert anschließend, warum jedes Passwort als sicher oder unsicher eingestuft wurde. Falls die Passwörter, die die Lernenden vortragen, „zu gut" sind, kann man die Liste der häufigsten Passwörter der Deutschen zeigen (siehe Anhang 2).

Erst jetzt wird Arbeitsblatt 2 ausgeteilt.
Anhand des Arbeitsblattes „Passwort-Checkliste" überprüfen die Schülerinnen und Schüler ihre erstellten Passwörter oder die ihrer Gruppenmitglieder.

Praxisphase 1.

In dieser Praxisphase wenden die Lernenden das Gelernte an.

Ziel dieser Aufgabe:
- Erstellung und Verwaltung von sicheren Passwörtern anhand der drei Methoden auf Arbeitsblatt 2.
- Festhalten des erarbeiteten Passwortes auf Arbeitsblatt 2 mit dem Hinweis darauf, dass dies ein Beispiel sein soll und im echten Leben nicht verwendet werden soll. Ein erwartbarer Einwand vonseiten der Lernenden kann sein, dass man sich die vielen Passwörter gar nicht merken kann. Hier bietet sich dann der Hinweis auf sogenannte „Passwort-Manager" (z. B. Bitwarden) an.
- Mit den älteren Schülerinnen und Schülern kann auch der Passwort-Schlüssel Automat genutzt werden (siehe Hinweis).

Mehr zum Thema Passwörter und Passwort-Sicherheit vom Bundesministerium für Familie, Senioren, Frauen und Jugend unter www.bmfsfj.de

Arbeitsblatt 2 – Mein sicheres Passwort / Warum ist es sicher?
Individuelle Antworten der Lernenden
Die Lernenden sollen hier mindestens eine Methode anwenden und ein beispielhaftes sicheres Passwort notieren.

Ergänzende Frage: Kennt ihr noch weitere Methoden, um Daten sicher vor Fremden zu schützen?
Hier können noch kurz die Möglichkeiten erwähnt werden, dass biometrische Daten (Fingerabdruck, Face ID) oder eine zusätzliche Sicherheitsstufe (2-Faktor-Authentifizierung) möglich sind. Somit gelingt die Überleitung zu der Erarbeitung 3.

Erarbeitung 3.

Aufbauend auf dem Verständnis zu Passwörtern, lernen die Schülerinnen und Schüler eine weitere wichtige Säule der Datensicherheit kennen: die Datenverschlüsselung.

Was bedeutet es, Daten zu verschlüsseln?
Passwörter sind also wie ein Schlüssel, um Daten zu schützen. Ihr könnt entscheiden, wem ihr den Schlüssel gebt. Wenn der Schlüssel aber gestohlen wird, können alle diese Daten lesen. Deshalb ist es eine gute Idee, Daten zu verschlüsseln. Das ist wie eine Geheimschrift. Selbst wenn jemand die Daten gestohlen hat oder sie verloren gehen, kann niemand sie verstehen, weil sie in Geheimschrift geschrieben sind und nur die Person, die die Daten verschlüsselt hat, weiß, wie man die Nachricht lesen kann.

Was ist mit „Verschlüsselung" gemeint?
Die **Verschlüsselung** bezieht sich auf den Prozess der Umwandlung von Informationen in eine Form, die nur von jemandem gelesen werden kann, der den speziellen „Schlüssel" zur Umwandlung der Informationen zurück in ihre ursprüngliche Form hat. Es ist eine Methode, Informationen zu schützen, indem sie für nicht autorisierte Benutzerinnen und Benutzer unlesbar gemacht wird.
Anhand der beiden „kryptischen" Informationen von Paul (aus den vorherigen Arbeitsphasen) erläutert die Lehrkraft das Prinzip der Verschlüsselung. Dabei handelt es sich um eine Methode, um Informationen so zu verbergen, dass sie nur von autorisierten Personen gelesen werden können.

Zwei einfache Beispiele:
- Röntgenaufnahmen werden oft zwischen Ärztinnen oder Ärzten und medizinischen Einrichtungen übertragen. Diese Bilder enthalten personenbezogene Gesundheitsdaten und werden daher verschlüsselt, um sicherzustellen, dass nur autorisierte Personen sie sehen können.
- Stell euch vor, ihr habt ein Bild von eurem Versteck gemalt und wollt es einer Freundin oder einem Freund zeigen, aber niemand anderem. Ihr nehmt das Bild und zerlegt es in verschiedene Puzzleteile, die ihr an verschiedenen Orten versteckt. Nur eure Freundin oder euer Freund weiß, wo man die Puzzleteile findet. So kann nur sie oder er das Bild zusammensetzen und sehen.

Praxisphase 2.

In dieser anwendungsorientierten Phase wird spielerisch die praktische Umsetzung einer verschlüsselten Nachricht geübt.
Analoge Version:
- Cäsar-Scheiben zum Ausschneiden (Arbeitsblatt 3)
- Bastelanweisung und Funktionsweise (Anhang 4)

Digitale Version: www.cryptoclub.org
(Klicken Sie auf „Cipher Tools“ und dann auf „Caesar“)
Für eine digitale Bearbeitung kann auch die oben genannte Seite genutzt werden. Mit einem Klick auf „Caesar" wird eine digitale Cäsar-Scheibe gestartet, mit der Nachrichten verschlüsselt und entschlüsselt werden können. Eine weitere Möglichkeit ist, dass die Schülerinnen und Schüler die gebastelte Scheibe nutzen und sie zusätzlich die Funktionsweise mithilfe der digitalen Variante demonstrieren können.

Jetzt können die letzten beiden Informationen zu Paul entschlüsselt werden. Weisen Sie darauf hin, dass aktuelle Verschlüsselungen im Internet auf diesem Prinzip basieren, aber weitaus komplexer sind.

Fakultativ/Alternativ:
1) Codebrecher: Teilen Sie die Klasse in kleine Gruppen und geben Sie jeder Gruppe eine verschlüsselte Nachricht. Die Aufgabe besteht darin, die Nachricht so schnell wie möglich zu entschlüsseln. Geben Sie die Verschiebezahl NICHT mit heraus, wenn sie die Aufgabe anspruchsvoll gestalten wollen. Die erste Gruppe, die es schafft, gewinnt.
Beispiel (Verschiebezahl ist 12, d. h.
Klartext A ist verschlüsselt M): YQUZQ PMFQZ EUZP EUOTQD
➔ Meine Daten sind sicher!

2) Nachricht schreiben: Lassen Sie die Lernenden verschlüsselte Nachrichten schreiben und untereinander austauschen. Zuhause sollen die Nachrichten dann entschlüsselt werden.

Reflexion.
Individuelle Antworten der Lernenden
Lösungen zu Arbeitsblatt 4: 1C, 2G, 3D, 4A, 5B, 6F, 7H, 8E (siehe auch Anhang 3)

Arbeitsblatt 1
Schutz der personenbezogenen Daten

Schütze deine digitalen Daten.

Kennst du diese Begriffe? Erkläre sie zuerst mit deinen eigenen Worten. Danach beantworte die Frage.

1. Daten

2. Privatsphäre

3. Datenschutz

4. Datensicherheit

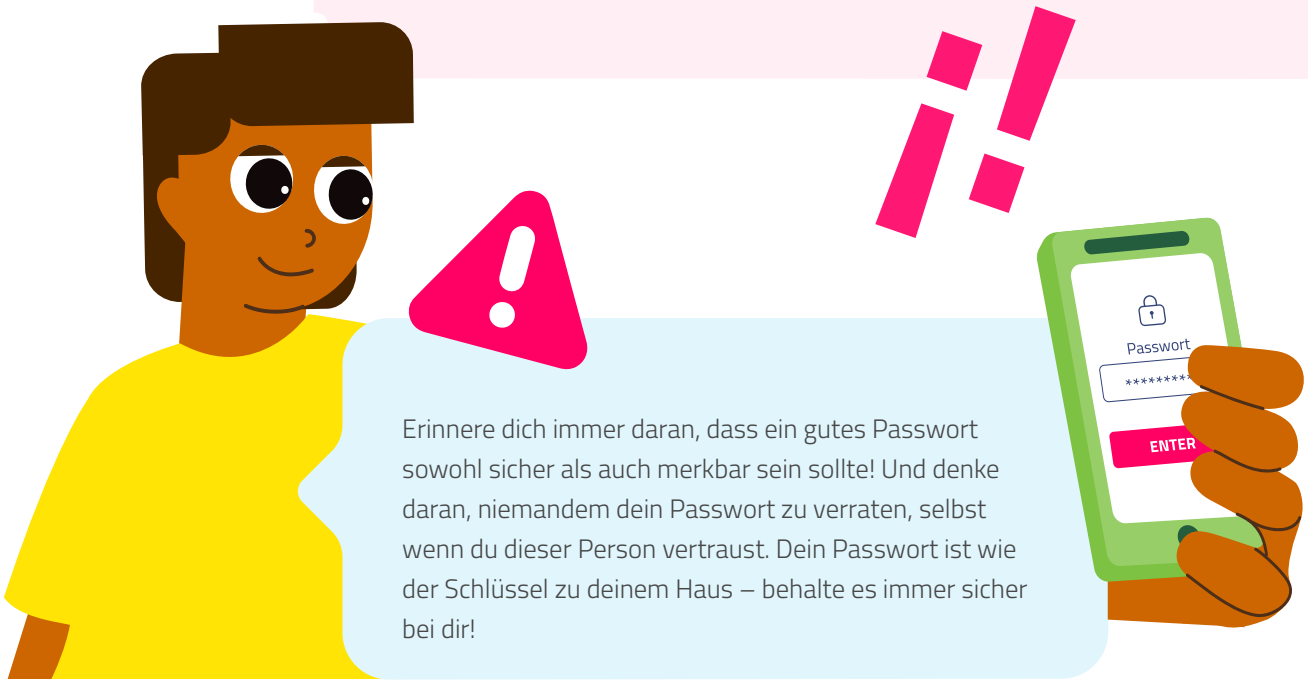
Was hat das mit meiner Gesundheit zu tun?

Ist mein Passwort sicher?

Wenn du ein Passwort erstellen musst, sollte das Passwort nach den folgenden Kriterien bzw. der Checkliste gestaltet werden:

A. Checkliste:

- **Passwortlänge:** Ist das Passwort mindestens 12 Zeichen lang? Je länger, desto besser!
- **Verschiedene Zeichentypen:** Enthält das Passwort eine Mischung aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen (z. B. @, #, $, %, &)?
- **Keine persönlichen Informationen:** Beinhaltet das Passwort keine offensichtlichen persönlichen Informationen, wie Geburtsdaten, Namen oder Adressen, die leicht von anderen erraten werden könnten?
- **Keine echten Wörter:** Enthält das Passwort keine echten Wörter, die im Wörterbuch gefunden werden können? Eine Möglichkeit, das zu erreichen, ist durch Einfügen von Zahlen und Sonderzeichen in Wörter.
- **Einzigartigkeit:** Wird dieses Passwort nur für diesen einen speziellen Account verwendet und nicht für andere?
- **Nicht vorhersagbar:** Ist das Passwort nicht zu offensichtlich oder leicht zu erraten, wie „123456" oder „passwort"?
- **Erinnerbarkeit:** Kannst du dich an das Passwort erinnern, ohne es aufschreiben zu müssen? Wenn du es aufschreiben musst, bewahre es an einem sicheren Ort auf, den niemand sonst kennt.



Erinnere dich immer daran, dass ein gutes Passwort sowohl sicher als auch merkbar sein sollte! Und denke daran, niemandem dein Passwort zu verraten, selbst wenn du dieser Person vertraust. Dein Passwort ist wie der Schlüssel zu deinem Haus – behalte es immer sicher bei dir!

B. Drei Methoden für das Erstellen sicherer Passwörter:

Methode 1:
Wörter mit Elementen verfremden

Kartoffelbrei → KartOff3lBr31 (Null statt Buchstabe o, 3 statt e, 1 statt i)
Schokolade → Sch0K0l4d3 (Null statt Buchstabe o, 4 statt a)
Computer → C0mPuT3r (Null statt Buchstabe, echte Buchstaben abwechselnd klein und groß)

Methode 2:
Lieblingssatz

Man merkt sich einen Lieblingssatz und nimmt davon jeweils immer den ersten Buchstaben jedes Wortes.
Beispiel: Im Sommer essen ich und meine Schwester am liebsten Vanilleeis mit Sahne.
→ ISeiumSalVmS

Methode 3:
Wortreihe

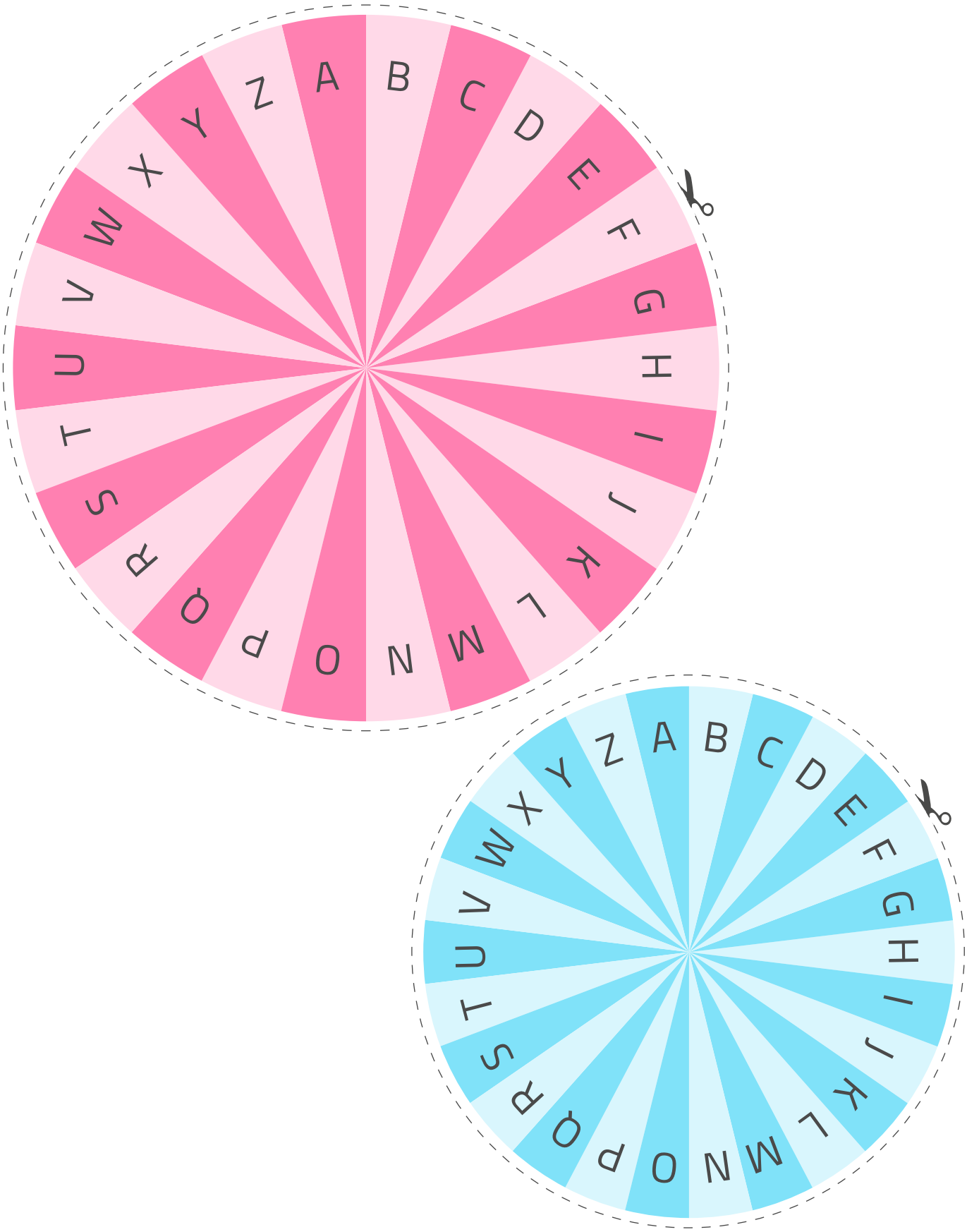
Man merkt sich eine Reihe von Wörtern, die eine persönliche Bedeutung für die Erstellerin oder den Ersteller haben. Die Sicherheit des Passwortes liegt hier in der Länge des Passwortes. So dauert es 23 Millionen Jahre, um ein Passwort mit 18 Kleinbuchstaben zu knacken. Durch Sonderzeichen und Großbuchstaben erhöht sich die Dauer noch.
Beispiel: der Wohnort, der Hund, das Lieblingsgericht, die Lieblingsfarbe
→ Hamburg.Layla.Spaghetti.Blau

Mein Vorschlag für mein persönliches, sicheres Passwort:

Warum ist es sicher?

Cäsar-Scheibe

Bastelanleitung: Beide Kreise ausschneiden, den kleineren auf den größeren legen, ein Loch in der Mitte machen und mit einer Spreizklammer aufeinander befestigen.



Was passt zusammen?

Finde die passenden Lösungen und trage die korrekten Antworten (Ziffern) in die Kästchen ein.

1. Datenschutz

2. Datensicherheit

3. Personenbezogene Daten

4. Privatsphäre

5. Doxing

6. Hacking

7. Verschlüsselung

8. Passwort

A. Teil des Lebens eines Menschen, der nur ihn etwas angeht. Dieser Bereich ist nicht öffentlich, sondern privat. In diesem Bereich kann jede Person leben, wie sie will – was sie dort tut oder denkt, geht niemanden außer sie selbst etwas an. ___

B. Eine Praxis, bei der personenbezogene Daten über eine Person recherchiert, gesammelt und ohne deren Zustimmung im Internet veröffentlicht werden, oft mit schädlichen Absichten. ___

C. Es geht insbesondere darum, dass jeder Mensch die Kontrolle über seine Daten hat und selbst entscheiden kann, an wen die Daten weitergegeben werden. ___

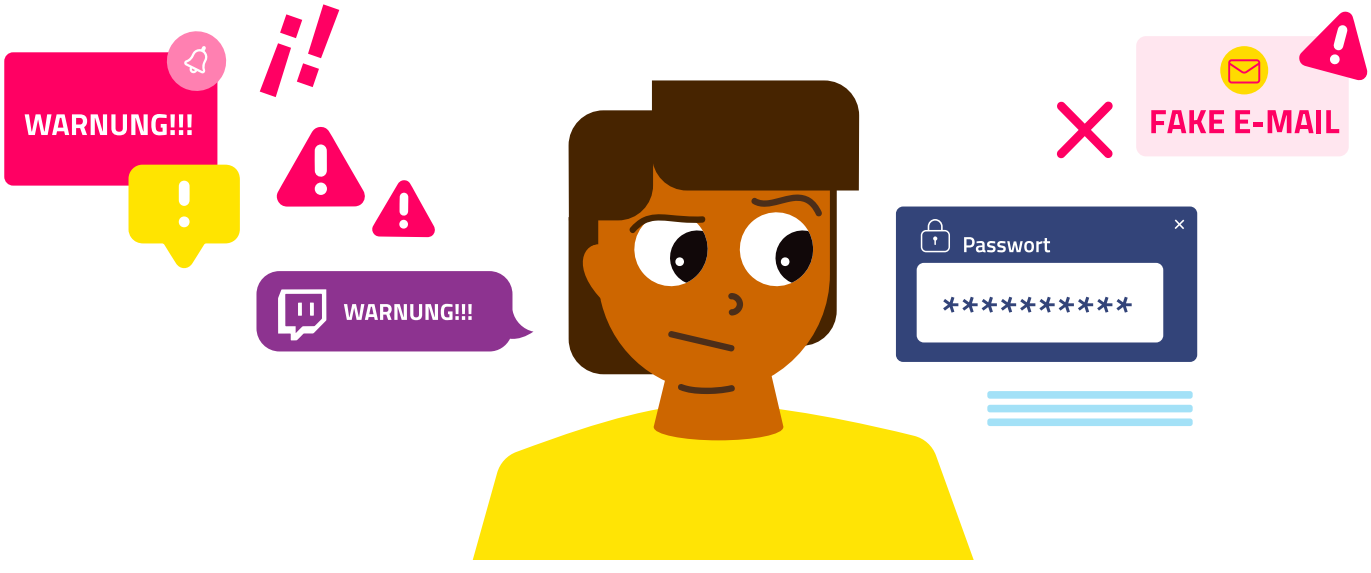
D. Informationen, die untrennbar zu einer Person gehören und die dazu genutzt werden können, eine Person zu identifizieren. ___

E. Eine geheime Kombination aus Zeichen, Zahlen oder Symbolen, die zum Schutz von Daten verwendet wird. ___

F. Der unerlaubte Zugriff auf Daten in einem System oder Computer. ___

G. Hier geht es darum, dass deine personenbezogenen Daten sicher aufbewahrt und geschützt werden, damit sie nicht gestohlen, manipuliert oder zerstört werden können. ___

H. Hiermit werden Informationen so umgewandelt, dass sie nur von Personen gelesen werden können, die den Schlüssel zur Umwandlung der Informationen kennen. ___



Anhang

Anhang 1

Pauls Daten

Verstecken Sie im Klassenzimmer (ruhig auch während der Einheit, sodass die Schülerinnen und Schüler sehen, wo die Informationen liegen) diese Daten zu Paul. 10 „normale“ Informationen. Eine davon („verliebt in Paula“) ist mit Passwort geschützt (z. B. in einer kleinen Kiste mit Vorhängeschloss), zwei davon („Asthmatiker“ und „Leseschwäche“) sind verschlüsselt.

Note 1 in Mathe	männlich
10 Jahre	Pikachu
13.6.	tanzen
Grundschule „Am Lindenbaum“	Brille

Paul

Fxymrfynpjw

lebt bei seiner Mutter

qjxjxhmbfjhmj

Blutgruppe AB

Migräne

verliebt in Paula

Anhang 2

Die 10 am häufigsten genutzten Passwörter der Deutschen

- 123456
- password
- 123456789
- 12345
- hallo
- passwort
- 12345678
- master
- qwertz
- 1Qay2ws3edc

Mehr zu den beliebtesten und meistverwendeten Passwörtern der Deutschen unter www.hpi.de und unter www.welt.de

Anhang 3
Glossar

Datenschutz: Ein Begriff, der sich auf den Schutz von personenbezogenen Daten bezieht. Es geht insbesondere darum, dass jeder Mensch die Kontrolle über seine Daten hat und selbst entscheiden kann, an wen die Daten weitergegeben werden.

Datensicherheit: Hier geht es darum, deine personenbezogenen Daten durch technische und organisatorische Maßnahmen vor einem unbefugten Zugriff oder einer Manipulation durch Dritte zu schützen.

Personenbezogene Daten: Informationen, die untrennbar zu einer Person gehören und die dazu genutzt werden können, eine Person zu identifizieren.

Informationelle Selbstbestimmung: Jeder Mensch hat das Recht, Informationen für sich zu behalten und zu entscheiden, was andere über ihn wissen dürfen. Es bezieht sich auf das Recht, personenbezogene Daten und Aktivitäten vor den Blicken und dem Eingriff anderer zu schützen. Privatsphäre im digitalen Kontext bedeutet, dass man auch online entscheiden kann, was man teilt, was privat bleibt und wer welche Informationen sehen oder hören darf – genau wie im eigenen Zuhause.

Privatsphäre: Teil des Lebens eines Menschen, der nur ihn etwas angeht. Dieser Bereich ist nicht öffentlich, sondern privat. In diesem Bereich kann jede Person leben, wie sie will – was sie dort tut oder denkt, geht niemanden außer sie selbst etwas an. Auch in der Privatsphäre muss man sich an Gesetze halten und darf insbesondere nicht die Persönlichkeitsrechte anderer Menschen missachten.

Doxing: Eine Praxis, bei der personenbezogene Daten über eine Person recherchiert, gesammelt und ohne deren Zustimmung im Internet veröffentlicht werden, oft mit schädlichen Absichten.

Hacking: Der unerlaubte Zugriff auf Daten in einem System oder Computer.

Verschlüsselung: Eine Methode, um Daten für nicht autorisierte Benutzerinnen und Benutzer unlesbar zu machen. Dabei werden Informationen so umgewandelt, dass sie nur von Personen gelesen werden können, die den Schlüssel zur Umwandlung der Informationen kennen.

Passwort: Eine geheime Kombination aus Zeichen, Zahlen oder Symbolen, die zum Schutz von Daten verwendet wird.

Anhang 4
Bastelanleitung und Funktionsweise der Cäsar-Scheibe

A. Anleitung Cäsar-Scheibe:

1. Stellen Sie sicher, dass alle Schülerinnen und Schüler ihre Cäsar-Scheibe vor sich haben. Die Scheibe besteht aus zwei Teilen: einem äußeren Kreis, der das Klartextalphabet zeigt, und einem inneren Kreis, der das verschlüsselte Alphabet darstellt.

2. Wählen Sie eine Verschiebungszahl (auch bekannt als Schlüssel). Diese Zahl bestimmt, wie viele Stellen das Alphabet für die Verschlüsselung verschoben wird. Legen Sie fest, ob die innere Scheibe mit oder gegen den Uhrzeigersinn gedreht werden soll. Zum Beispiel könnte die Verschiebungszahl „3 gegen" sein, was bedeutet, dass die innere Scheibe 3 Stellen gegen den Uhrzeigersinn gedreht wird. Dadurch wird jedes 'A' in der Nachricht durch ein 'D' ersetzt, ein 'B' durch ein 'E' und so weiter.
Zu Beginn steht ganz oben im inneren und äußeren Kreis der Buchstabe A.

3. Drehen Sie den inneren Kreis um so viele Stellen in die Richtung, wie die Verschiebungszahl angibt. Wenn Ihre Verschiebungszahl zum Beispiel „3 mit" ist, drehen Sie den inneren Kreis so, dass dem äußeren 'A' das innere 'X' gegenübersteht.

4. Beginnen Sie mit der Verschlüsselung Ihrer Nachricht. Für jeden Buchstaben in Ihrer Nachricht finden Sie diesen auf dem äußeren Kreis und schauen Sie dann, welcher Buchstabe ihm auf dem inneren Kreis gegenübersteht. Dieser Buchstabe ist die verschlüsselte Version des ursprünglichen Buchstabens.

5. Schreiben Sie den verschlüsselten Buchstaben auf und wiederholen Sie diesen Schritt für jeden Buchstaben in Ihrer Nachricht.

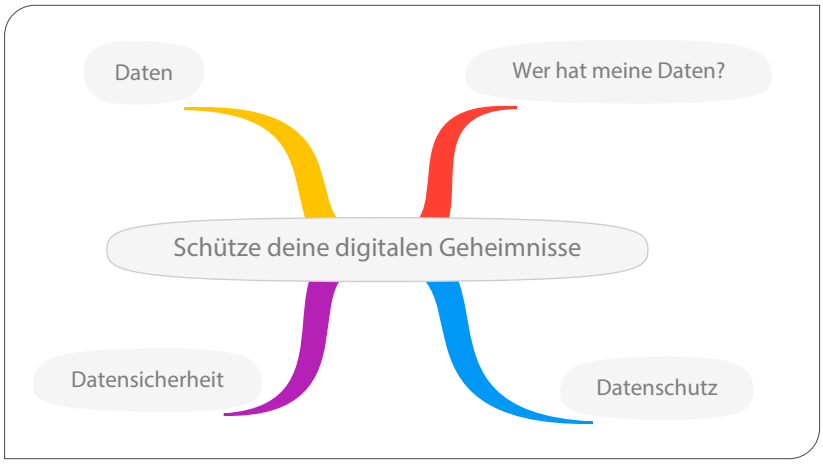
B. Schritte zum Entschlüsseln einer Nachricht:

1. Nehmen Sie die verschlüsselte Nachricht und die Verschiebungszahl, die zum Verschlüsseln der Nachricht verwendet wurde.

2. Stellen Sie Ihre Cäsar-Scheibe wieder so ein, dass 'A' auf dem äußeren Kreis gegenüber der entsprechenden Verschiebungszahl auf dem inneren Kreis steht.

3. Für jeden Buchstaben in der verschlüsselten Nachricht, finden Sie diesen auf dem inneren Kreis und schauen Sie dann, welcher Buchstabe ihm auf dem äußeren Kreis gegenübersteht. Dieser Buchstabe ist die entschlüsselte Version des ursprünglichen Buchstabens.

4. Schreiben Sie den entschlüsselten Buchstaben auf und wiederholen Sie diesen Schritt für jeden Buchstaben in Ihrer Nachricht. Die vollständige Abfolge der entschlüsselten Buchstaben ist die ursprüngliche Nachricht



Anhang 5
Digitale Mindmap

Wie lege ich eine Mindmap mit TeamMapper an, um digital Ideen zu sammeln?

- Rufen Sie die DSGVO-konforme Internetseite www.kits.blog auf.
- Sie und Ihre Schülerinnen und Schüler brauchen keinen Account oder Anmeldung auf dieser Seite.
- Klicken Sie auf „Mindmap erstellen" und gehen Sie mit einem Doppelklick in den Text „Thema" und passen Sie ihn an.
- Mit der + Schaltfläche fügen Sie neue Elemente zum aktuell aktiven Element hinzu, mit der – Schaltfläche können Sie Elemente wieder entfernen.
- Wenn Sie mit dem Erstellen der Mindmap fertig sind, klicken Sie oben links auf das Teilen-Symbol. Nun können Sie den QR Code oder Link an die Lernenden weitergeben.
- Wenn sie die Mindmap kollaborativ erstellen möchten, geben sie den QR Code gleich nach dem Erstellen der Mindmap an die Lerngruppe. Dann können Sie gemeinsam im Unterricht die Mindmap erstellen.

Interessante Links zum Thema „Schutz der personenbezogenen Daten"

- „Passwortschlüssel Automat" unter www.schooltools.at
- „Sichere Passwörter erstellen" unter www.bsi.bund.de
- „Ihr denkt, euer Passwort ist sicher?" unter www.mein-mmo.de

Weiterführende Hilfsangebote:

- Nummer gegen Kummer: 116 111
  Anonyme und kostenlose telefonische Beratung, Mo–Sa von 14 Uhr bis 20 Uhr
- www.krisenchat.de
  24/7 Krisenberatung per Chat

DURCHBLICKT!

Digital in eine gesunde Zukunft.

Impressum

Autor: Michael Kohl, Rieden
Redaktion und Projektkoordination: Fabienne Schmaus, Fellheim
Projektleitung: Petra Wöhner, Klett MINT GmbH
Layout und Satz: We are Family GmbH & Co. KG, Stuttgart
Eine Zusammenarbeit der BARMER und der Klett MINT GmbH

Dieses Unterrichtsmaterial wurde mit rechtlicher Unterstützung von CMS Hasche Sigle erstellt.

Digital in eine gesunde Zukunft.

Wir wollen die Chancen und Potenziale der Digitalisierung für unsere Gesundheit nutzen, indem wir digitale Kompetenz für selbstbestimmte Entscheidungen in allen Gesundheitsfragen vermitteln.

Ein Präventionsprogramm der BARMER

Klett MINT

Hochschule Fulda
University of Applied Sciences

Technische Universität München