

***Woran und wie erkennt ein System ein gutes
Kennwort
(Kriterien, reguläre Sprache, Automat)?***

Autorin: Sabine Krzyzek

Matrikelnummer: XXXXXXXXXX

**Thema der
Unterrichtseinheit:**

Wie erkennt ein System ein gutes Kennwort?

Thema der Reihe:

Sicherheit im Internet

Klasse:

3

Zeitumfang (Min.):

90 Minuten

Inhaltsverzeichnis

Schriftliche Planung des Unterrichts

- | | |
|--------------------------------------|------|
| 1. Ziele und angestrebte Kompetenzen | S. 1 |
| 2. Didaktische Schwerpunkte | S. 3 |
| 3. Artikulationsschema | S. 6 |

| | |
|----------------------|------|
| Literaturverzeichnis | S. I |
|----------------------|------|

| | |
|--------|-------|
| Anhang | S. II |
|--------|-------|

| | |
|------------------------------------|-------|
| Versicherung und Verwertungsrechte | S. VI |
|------------------------------------|-------|

Schriftliche Planung des Unterrichts

1. Ziele und angestrebte Kompetenzen

Ein Stundenziel/Kernanliegen mit Indikator:

Die Schülerinnen und Schüler sollen die Notwendigkeit und den Aufbau von sicheren Kennwörtern verstehen. Mittels selbst entwickelter Kriterien erarbeiten sie sichere Passwörter und eine Möglichkeit, diese zu überprüfen. Schließlich wird ein Transfer zur Funktion von Automaten gezogen, die die SuS aus vorherigen Unterrichtsstunden kennen. Die SuS denken sich selber Kennwörter aus und kontrollieren sie auf Sicherheit mithilfe des selbst gebauten analogen Passwortprüfautomaten und der digitalen Version im Internet. Unsichere Passwörter werden überarbeitet und erneut getestet.

Drei bis fünf Teilziele mit Indikator:

- Die SuS identifizieren sich mit der Notwendigkeit von Passwortsicherheit, indem sie überlegen, welche ihrer Informationen (Spielstände, e-mails etc.) sie für sich behalten wollen und welche alle anderen Schüler generell einsehen dürfen.
- Die SuS erarbeiten mithilfe der Think-Pair-Share-Methode Kriterien für gute Passwörter und stellen diese vor.
- Die SuS entwickeln eigene neue Passwörter, die diesen Kriterien entsprechen.
- Die SuS entwickeln ein System, mit dem analog ein Kennwort auf seine Sicherheit überprüft werden kann. Sie nehmen die Rolle des Systems ein, überprüfen ihre eigenen Passwörter und überarbeiten sie ggfs.

Hierdurch sollen folgende Kompetenzen laut Lehrplan/Empfehlungen gefördert werden (je eine inhaltsbezogene und prozessbezogene Kompetenz):

Prozessbereiche:

Da in Grundschulen Informatik nicht als eigenes Fach unterrichtet wird, können die Inhalte der informatischen Bildung im Sachunterricht oder fächerübergreifend durchgenommen werden. Der Stundeninhalt steht in Zusammenhang mit der Logik, daher kann das Vorhaben sowohl in Mathematik als auch im Sachunterricht durchgeführt werden. Hier erkennbare prozessbezogene Kompetenzbereiche, die durch den Lehrplan für Mathematik an Grundschulen in NRW legitimiert werden, sind Modellieren und Kommunizieren/Darstellen [MSW08, S. 59F].

Die Prozessbereiche, die die Gesellschaft für Informatik (GI) beschreibt, sind in dieser Unterrichtsstunde neben Modellieren und Implementieren auch Kommunizieren und Kooperieren sowie Darstellen und Interpretieren. „Die Kinder tauschen sich über eigene Denkprozesse oder Vorgehensweisen mit anderen aus“ und „kooperieren zur bzw. bei der Bearbeitung informatischer Probleme“ [vgl. GI18, S. 8]. Außerdem wird der Bereich Darstellen und Interpretieren angesprochen, da die SuS Denkprozesse darstellen, die sie zuerst individuell und dann in der Gruppe entwickeln [vgl. ebd]. Vorrangig wird der **Prozessbereich Modellieren und Implementieren** angesprochen, denn die „Kinder wenden Informatik auf konkrete Aufgabenstellungen aus ihrer Erfahrungswelt an“ [ebd. S.9]. Die SuS erarbeiten ein analoges Modell zur Überprüfung von Passwörtern und führen die Arbeitsschritte selbst durch. Schließlich wird dieses Modell in die digitale Version übertragen und online getestet. Die SuS reflektieren so den selbstgebauten Automaten und erhalten eine sichtbare Vorstellung eines digital ablaufenden Prozesses. Hier wird eine praktische Vorstellung zu einem wichtigen Aspekt der Sicherheit im Internet geschaffen, sodass die SuS eigenverantwortlich und selbstbestimmt ihr Verhalten mit digitalen Medien gestalten können.

Inhaltsbereiche:

Die sachbezogene Kompetenz Methoden zur Generierung eines Passworts zu verstehen und anzuwenden

Der Inhaltsbereich, der in der vorliegenden Stunde behandelt wird, ist **Sprachen und Automaten** mit einem direkten Lebensweltbezug. Die Nutzung und die Grundlagen der Funktionsweisen von Automaten im direkten Umfeld (Fahrkartenautomat, Kaugummiautomat etc.) sind den SuS aus vorangegangenen Unterrichtsstunden bekannt. Die SuS erlernen nun mit der analogen Nutzung eines Automaten, den sie selber betreiben, die Grundlagen der Funktion eines Passwortüberprüfungsprogramm.

Insgesamt bedeutet „Die Orientierung an Kompetenzen [...], dass der Blick auf die Lernergebnisse gelenkt, das Lernen auf die Bewältigung von Anforderungen ausgerichtet und als kumulativer Prozess organisiert wird. Die Kinder haben Kompetenzen ausgebildet,

- wenn sie zur Bewältigung einer Situation vorhandene Fähigkeiten nutzen, dabei auf vorhandenes Wissen zurückgreifen und sich benötigtes Wissen aneignen,
- wenn sie die zentralen Fragestellungen eines Lerngebietes verstanden haben und angemessene Lösungswege wählen,
- wenn sie bei ihren Handlungen auf verfügbare Fertigkeiten zurückgreifen und ihre bisher gesammelten Erfahrungen in ihre Handlungen mit einbeziehen“ [ebd. S.8].

2. Didaktische Schwerpunkte

Die SuS haben noch kein Vorwissen zu dem speziellen Thema Passwortsicherheit. Im Rahmen des Themas Robotik und Automaten wurde bereits der BeeBot und das Treasure Island Spiel durchgenommen. Die Grundlagen der Robotik und der Funktionsweisen von Automaten sind also bekannt.

Die Klasse ist eine motivierte und wissbegierige Gruppe. Das Thema rund um Computer/Tablet etc. interessiert den Großteil der Klasse, weil viele Kinder selber auch schon Smartphones oder Tablets zu Hause nutzen. Die Think-Pair-Share-Methode ist den SuS aus dem bisherigen Unterricht bekannt. Kooperative Erarbeitungsmethoden wie Gruppenarbeiten werden häufig durchgeführt und auch die Ergebnissicherung im Plenum ist ein bekannter Teil des Unterrichts.

Der Schwerpunkt des Unterrichtsgegenstandes liegt im Schaffen eines Bewusstseins für die eigene Sicherheit im Netz sowie das Verständnis für die Funktion eines Passwortüberprüfungsprogramms. Im Rahmen einer Unterrichtsstunde ist ein Anfang der Sensibilisierung der SuS gegenüber der Datensicherheit in digitalen Medien realisierbar. Die Vorstellung, dass jemand Fremdes das eigene Tagebuch o.Ä. lesen oder verändern könnte, wird den SuS einen realistischen Einblick geben in den hohen Stellenwert von Passwörtern bei der Nutzung von digitalen Medien. Besonders wichtig ist hier die Kooperation mit den SuS und nicht eine ermahnende Lehrerstimme, die Angst schürt. Didaktisch ist hier also eine beratende Funktion des Lehrers von Nöten, damit die SuS sich in einer geschützten Atmosphäre mit dem Thema auseinandersetzen können, ohne unter Druck zu geraten.

Im Lehrplan für Grundschulen in NRW wird durchweg aufgegriffen, dass die Arbeit mit einer Vielzahl von Medien in den Unterricht mit eingebunden werden soll. „Umgang mit Medien“ ist nicht nur in den Fächern Englisch und Deutsch gefragt [vgl. MSW08, S.33, 83], sondern wird als ein übergreifendes Ziel des Lehrens so beschrieben: „Indem die Medien selbst zum Gegenstand der Arbeit im Unterricht werden, erfahren die Schülerinnen und Schüler Möglichkeiten und Beschränkungen einer durch Medien geprägten Lebenswirklichkeit. Die systematische Arbeit mit Medien trägt dazu bei, die Medienkompetenz der Schülerinnen und Schüler zu entwickeln“ [vgl. ebd. S. 15]. In den Richtlinien und Lehrplänen für die Grundschule in Nordrhein-Westfalen ist die informatische Bildung explizit noch nicht aufgeführt. Der Arbeitskreis »Bildungsstandards Primarbereich« der Gesellschaft für Informatik (GI) e. V. führt jedoch Kompetenzen für informatische Bildung im Primarbereich auf, die als Richtlinien geltend gemacht werden können um SuS ein Verständnis und Bewusstsein für den Umgang mit digitalen Medien zu vermitteln. Es werden „die informatischen Kompetenzen näher ausführt, die von Kindern entwickelt werden sollen, um ihre Zukunft eigenverantwortlich und kompetent gestalten und einordnen zu können.“ [GI, S. 1] Mit dem Thema Passwortsicherheit wird nur ein Teilthema der informatischen Bildung angesprochen, welches bei der Nutzung von digitalen Medien wichtig ist. Die Fähigkeit die, Sicherheit des eigenen virtuellen Ichs in digitalen sozialen Netzwerken zu gewährleisten und zu kontrollieren, wird in diesem Unterrichtsentwurf lebensweltnah an die SuS herangeführt.

**Lehr- und
Lernausgangslage
der SuS**

**Begrenzte
Sachanalyse
des U.-
gegenstandes**

**Legitimation
des Vorhabens
durch
curriculare
Vorgaben**

Der Gegenwartsbezug ist ggfs. bei den Drittklässlern noch nicht übergreifend vorhanden, aber in den Anfängen ist das Thema Passwortsicherheit sicherlich aktuell, denn es ist anzunehmen, dass die SuS Internetplattformen und das Prinzip von Spiele-Accounts auf Tablets uvm. kennen.

Ihr persönlichen Informationen, seien es nun z.B. Spielstände oder E-mails, sind ihnen wichtig und daher ist das Thema der Unterrichtsstunde mit direktem aktuellen und zukünftigen Lebensweltbezug von hoher Relevanz für die SuS. Um naiven Umgang mit persönlichen Informationen und dadurch möglichen Missbrauch derer zu vermeiden wird das Thema theoretisch und praktisch behandelt.

Relevanz für die SuS

Mit den drei Visionssätzen der GI „Ich kann das!“, „Ich entscheide mit!“ und „Hier wird mir geholfen!“ (GI, S.3) legitimiert sich die zentrale Unterrichtsmethode. Sie lässt eigene Überlegungen, Erfahrungen und Ideen zu - sie fordert sie sogar, damit der Unterricht stattfinden kann. Sie werden mit den Mitschülern bearbeitet und weiterentwickelt. Die Think-Pair-Share-Methode beinhaltet den Ausbau der Fähigkeit sich kritisch mit den eigenen aber auch den Ansichten der anderen auseinanderzusetzen. Die Methode bewirkt, dass alle SuS mitmachen und die Teamfähigkeit der SuS gefördert wird.

Begründung der wichtigsten Entscheidungen des geplanten Unterrichts

Der **Einstieg** mit der offenen Frage nach dem Nutzen von Kennwörtern im digitalen Leben der SuS holt die SuS an einem Wissensstand ab, an dem sich alle wiederfinden können, ob sie sich schon mit diesem Thema auseinandergesetzt haben oder nicht. Es wird also anfänglich eine Basis zum Thema gelegt, welche einen gemeinsamen Unterrichtsfortschritt ermöglicht. Die Vernetzung des Stundeninhalts im weiteren Verlauf mit dem Thema „Automaten“ bietet eine Erweiterung der Zusammenhänge im Bereich Informatik.

In der ersten **Erarbeitungsphase** werden die Notwendigkeit und die Kriterien von sicheren Passwörtern erarbeitet. Der Wechsel der Sozialformen (Einzel-, Partner- und Gruppenarbeit) ist bewusst gewählt, damit die Schüler ihre eigenen Gedanken entwickeln, sie aber dann auch mit anderen teilen und besprechen. Die Notwendigkeit des Austauschs mit den Mitschülerinnen und -schülern bewirkt den Ausbau sozialer und kommunikativer Kompetenzen. Kritikfähigkeit an den Aussagen anderer aber auch an sich selber wird geübt.

Das Medium Tafel ist in diesem Unterrichtsentwurf zentral, da es sich um Ideensammlungen handelt, die zu Regeln für sichere Passwörter aufgestellt werden. Alle SuS können ihre Überlegungen in der **Auswertung** beitragen und an der Tafel gesammelt betrachten. Eine Ergebnissicherung in Form eines Arbeitsblattes folgt im Laufe der Stunde.

Danach lässt eine kurze **Bewegungspause** die Schüler die theoretischen Überlegungen verarbeiten und frische Luft und Ablenkung sorgen für neue Konzentrationsfähigkeit im zweiten Teil der Stunde. Die theoretische Sammlung von Kriterien für sichere Passwörter wird dann praktisch umgesetzt in Form eines Passwortprüfautomaten, der von den SuS selbst „betrieben“ und benutzt wird. Hierfür wird in der zweiten **Erarbeitungsphase** das Tafelbild mit den Kriterien wiederholt und ein Passwortprüfautomat hergestellt. Hier wird nun der Transfer zur Funktionsweise von Automaten gezogen. Eine Liste der Kriterien und eine Auswertungsmethode wird im Plenum erarbeitet, Hilfestellungen der Lehrperson werden ggfs.

nötig sein. Die Liste ist als AB vorbereitet. Ein Umzugskarton mit Griffschlitzen als Ein- und Auswurfschlitze dient als Automatengehäuse.

Die finale **Auswertung** findet mit der Nutzung des analogen Passwort-

prüfautomaten statt. Ein Kind übernimmt die Prüferfunktion im Karton, erhält von den Mitschülerinnen und -schülern Passwörter durch den Einwurfschlitz, überprüft sie mittels der Liste, trägt die Sicherheit der Kennwörter auf dem Zettel ein und wirft sie wieder aus dem Auswurfschlitz heraus. Hier werden Ampelfarben eingesetzt, da sie für die SuS bekannt sind und klare Ergebnisse bedeuten:

Grün = sicheres Passwort

Gelb = das Passwort könnte noch sicherer sein

Rot = unsicheres Passwort

Hat ein SuS ein gelbes oder rotes Ergebnis, soll er/sie das Passwort überarbeiten. An welchem Kriterium er/sie noch etwas verändern muss, muss er möglichst selbst mithilfe des Tafelbildes erkennen. Dann soll das Passwort erneut überprüft werden.

Die SuS handeln mit den zuvor entwickelten Ideen und erschließen so Zusammenhänge zur digitalen Version der Passwortüberprüfung. Schließlich wird die Passwortüberprüfung online durchgeführt. Die Online-Version des Passwortprüfautomaten ist schneller, genauer und differenzierter. Es gibt noch mehr Kriterien, die beachtet werden können, um ein Passwort noch sicherer zu machen. Diese Menge an Überprüfungsrastern würde aber eine Unterrichtsstunde weit überschreiten und hätte auch keinen viel größeren Lerneffekt als die Grundlagen, die mit den aufgeführten Kriterien gelegt wurden. Es geht hier speziell nur um ein Grundverständnis eines Systems für das Erkennen und Bewerten von Passwörtern.

Ein Lernfortschritt findet insofern statt, als dass die SuS erkennen, wie sie ihre persönlichen Daten vor Missbrauch schützen. Auch für SuS, die mit digitalen Medien (noch) nicht so vertraut sind bzw. sie noch nicht intensiv nutzen, ist dieses Thema relevant, denn auch sie wollen generell ihre Privatsphäre schützen. Wie das nun konkret im Rahmen von Passwörtern funktioniert, wird in dieser Unterrichtsstunde nachvollziehbar an die SuS herangeführt.

Weiterführende Inhalte der Reihe Sicherheit im Internet werden in den folgenden Stunden thematisiert. Hierzu gehören der Umgang mit personenbezogene Daten im Internet und die Risiken der Veröffentlichung von Fotos und Nachrichten in den sozialen Medien (Facebook etc.).

3. Artikulationsschema

| Dauer (Min.) | Unterrichtsphase | Unterrichtsinhalt | Sozial-/Aktionsform | Materialien/Medien/Werkzeuge | didaktisch-methodischer Kommentar |
|--------------|----------------------------|--|--|---|---|
| 5-10 | Einstieg | <ul style="list-style-type: none"> - Identifizieren mit der Notwendigkeit von Passwortsicherheit - Überlegungen über persönliche Informationen (Spielstände, e-mails etc.), die die SuS für sich behalten wollen | Bearbeitung der Fragestellung im Plenum | Tafel - Liste von Gründen für ein sicheres Passwort | L: Wofür braucht ihr Passwörter? Direkte Anrede → direkter Einbezug ins Thema, Interesse & Motivation wird geweckt |
| 10-15 | 1. Erarbeitung | <ul style="list-style-type: none"> - die SuS überlegen sich einzeln Kriterien für ein sicheres Passwort - die SuS tauschen sich in Partnerarbeit aus | Think-Pair-* | Schülernotizen | L: Wie sieht ein sicheres Passwort aus? Was muss es beinhalten? Was nicht? |
| 10-15 | 1. Auswertung/Präsentation | <ul style="list-style-type: none"> - Kriterien für ein sicheres Passwort werden für alle zusammengetragen - Möglichkeiten für das Merken eines guten Passwortes werden erfragt/vorgetragen → Passwort als Abkürzung eines Satzes | *Share → Plenum Plenumsfrage/Lehervortrag | Tafel - Liste der Kriterien - Merkidée in Form eines verschlüsselten Satzes | Zusammenfassung für alle SuS, danach die Frage an die SuS: L: Wie kann man sich ein solch kompliziertes Passwort merken? Beispiele werden gesammelt |
| 5 | Kleine Pause | | In der Gruppe oder alleine | Schulhof | Kurze Bewegungspause bewirkt verbesserte |

| Dauer (Min.) | Unterrichtsphase | Unterrichtsinhalt | Sozial-/Aktionsform | Materialien/Medien/Werkzeuge | didaktisch-methodischer Kommentar |
|--------------|--------------------------------|--|--|--|--|
| | | | | | Konzentration und Aufnahmefähigkeit der SuS |
| 10 | 2. Erarbeitung | Wiederholung des Tafelbildes, Ausdenken eines persönlichen Passwortes Erstellen einer Überprüfungsliste für sichere Passwörter Basteln eines Passwortprüfautomaten | Plenum/ Input der Lehrperson 2-3 Gruppen | Tafel, Schülernotizen Karton, Stifte zum Beschriften | Kurze Auffrischung der bisherigen Ergebnisse L: Wie kann systematisch ein gutes PW überprüft werden? Hinweis auf Automaten-Funktionsweise → Kriterien werden erfüllt/nicht erfüllt → Ampelfarben zeigen Sicherheit des PW an |
| 15-20 | 2. Auswertung/ Präsentation | Benutzung des Passwortprüfautomaten durch SuS, Überprüfung der Passwörter Überarbeitung der eigenen Passwörter | Plenum/ Schüler als PW-Prüfer im Karton | Karton mit Ein- und Auswurfschlitz, AB: „Die Passwortüberprüfung“, „Passwortprüfautomat“ für den PW-Prüfer | SuS begeben sich in die Rolle des Automaten → SuS verinnerlichen die Grundlagen der Funktionsweise des Prüfvorgangs indem sie ihn selbst durchführen |

| Dauer (Min.) | Unterrichtsphase | Unterrichtsinhalt | Sozial-/Aktionsform | Materialien/Medien/Werkzeuge | didaktisch-methodischer Kommentar |
|--------------|------------------|---|--|--|---|
| 10 | Sicherung | <p>Transfer zur digitalen Erkennung eines sicheren Passwortes → Die Schüler überprüfen ihre selbst gewählten Passwörter auf der Internetseite http://www.browsercheck.pcwelt.de/passwortstarke-messen und www.checkdeinpasswort.de</p> | Plenum/ Input der Lehrperson/ Passwortüberprüfung im Internet, | Laptop AB: „Passwortprüfautomat“ für alle SuS | <p>Zusammenfassung durch Übertragung des Prüfautomaten in die digitale Funktionsweise. Direkte Überprüfung des Passwortes auch online möglich. Lebensweltbezug (s. Einstieg) wird auf diese Weise greifbar.</p> |
| max. 5 | Abschluss | Feedbackmöglichkeit seitens der SuS und der Lehrperson | Plenum | - | Möglichkeit zur Anmerkung von positiven oder negativen Eindrücken |

Literaturverzeichnis

- [MSW08] Ministerium für Schule und Weiterbildung des Landes NRW (Hrsg.): Richtlinien und Lehrpläne für die Grundschule in NRW, Ritterbach Verlag, Frechen, 2008, http://www.schulentwicklung.nrw.de/lehrplaene/upload/lehrplaene_download/grundschule/grs_faecher.pdf, Stand: 28.02.2018.
- [GI16] Gesellschaft für Informatik (GI) e. V. (Hrsg.): Vorlage und Richtlinien für Autoren zur einheitlichen Gestaltung in der LNI-Reihe, <https://www.gi.de/service/publikationen/lni/autorenrichtlinien.html>, Stand: 13.02.2017.
- [GI18] Gesellschaft für Informatik (GI) e. V. (Hrsg.): Kompetenzen für informatische Bildung im Primarbereich, <https://metager.to/qibspdf>, Version: 999, Stand: 28.02.2018.
- [ITMG18] IDG Tech Media GmbH: Passwortstärke messen, <http://www.browsercheck.pcwelt.de/passwortstarke-messen>, Stand: 28.02.2018.
- [BBWF18] Bundesministerium für Bildung, Wissenschaft und Forschung (Hrsg.): digi komp, digitale Kompetenzen Informatische Bildung, <https://community.eeducation.at/course/view.php?id=314>, Stand: 28.02.2018
- [MG18] mecodia GmbH: Wie sicher ist mein Passwort?, www.checkdeinpasswort.de, Stand: 28.02.2018
- Bildnachweis: <https://www.redbubble.com/de/people/motiv-lady/works/21616235-face-funny-thumbs-hand-press-good-best-comic-cartoon-computer-laptop-notebook-pc-write-screen-mobile-tablet?p=sticker>, Stand: 28.02.2018

Anhang

Erwartungshorizont

1.) Einstieg

Warum sind Passwörter wichtig?

- persönliche Informationen sollen nicht alle Menschen einfach einsehen können
- auf meinem Handy, Laptop, Tablet, oder generell im Internet
- Spielstände
- private Nachrichten → E-mails, Chatnachrichten oder Fotos auf Plattformen der sozialen Medien
- Blogbeiträge/Tagebücher/ E-mails
- Sparkassen Account
- etc.

→ so kann ich meine privaten, geheimen Informationen schützen und z.B. Betrügern keine Chance geben meine Accounts zu manipulieren oder Geld von meinem Konto zu stehlen

2.) Erarbeitungsphase

Regeln für ein sicheres Passwort¹

Passwörter, die aus einem Wort (z.B. einem Namen) bestehen, könnte jemand Fremdes erraten, indem er Wörter ausprobiert, die in deinem Leben häufig vorkommen. Ein Name von deinen Eltern, Geschwistern, Haustier o.ä.

Deshalb sollte ein Passwort möglichst kompliziert sein und nicht unserer alltäglichen Sprache entsprechen:

- **mindestens** 8 Zeichen lang
- Groß- und Kleinbuchstaben
- Sonderzeichen wie z.B.: . , - ! < + ? %
- Ziffern
- keine ganzen Wörter, sondern
- Zeichensalat, also alles durcheinander

Denkt euch eigene Passwörter aus, die ihr bisher noch nicht verwendet.

Wie kannst du dir so ein kompliziertes Passwort merken?

Eine Idee:

Bilde einen Satz, den du abkürzen und als Passwort benutzen kannst.

Als ich fünf war, lernte ich schwimmen im Pool.

→ A15w,L1s1P.

Umso länger das Passwort, desto sicherer ist es!

1 Angelehnt an [BBWF18]

Passwortprüfautomat

Überprüfe folgende Kriterien:

1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11.

| | | | | | | | | | | | |
|---|--|--|--|--|--|--|--|--|--|--|--|
| mindestens 8 Zeichen lang | | | | | | | | | | | |
| Groß- und Kleinbuchstaben | | | | | | | | | | | |
| Sonderzeichen wie z.B.: - . ,) ! < + ? % | | | | | | | | | | | |
| Ziffern | | | | | | | | | | | |
| keine ganzen Wörter, sondern | | | | | | | | | | | |
| Zeichensalat, also alles durcheinander | | | | | | | | | | | |

Auswertung mit Ampelprinzip:

6 Punkte: **Grün**

5 Punkte: **Grün/Gelb**

4 Punkte: **Gelb**

3 Punkte: **Gelb/Rot**

2 oder 1 Punkt: **Rot**

Die Passwortüberprüfung

Name: _____

Mein Passwort lautet:

Ergebnisfarbe des Passwortes mit der Nr. ____ : _____

