Sesam öffne dich (**nicht**)!

Pa$$wOrtTra!n!ng!m$achunterr!cht

123456, 123456789 oder einfach password. Wenn Sie hier Ihr eigenes Passwort entdeckt haben, sollten Sie es schleunigst ändern. Diese sind nicht nur die Top 3 der privat genutzten Passwörter der Deutschen aus dem Jahr 2023, sondern von Dritten auch im Sekundenbruchteil zu knacken. Wie Sie selbst ein geeignetes Passwort zum Schutz Ihrer Daten erstellen und wie Ihre Schüler*innen zu Sicherheitsexpertinnen und -experten werden, wird in diesem Artikel näher beleuchtet.

Foto: Shutterstock/bibiphoto

•• *1 An einem fiktiven Beispiel um den Schutz von Minecraft-bauten erarbeiten sich die Kinder Kriterien für sichere und leicht merkbare Passwörter.*

Von Christian Frenser und Nicola Airo

Didaktischer Hintergrund

In dieser Unterrichtsreihe erlernen die Schüler*innen Fähigkeiten, die für einen verantwortungsbewussten Umgang mit sensiblen Daten und deren Speicherung in einer digital-medial geprägten und gestaltbaren Lebenswelt (Irion 2023) – von Erwachsenen wie auch Kindern – unerlässlich sind. Das übergeordnete Ziel ist dabei, den Kindern die Notwendigkeit der Nutzung sicherer Passwörter zu vermitteln und ihnen entsprechende Werkzeuge zu deren Erstellung an die Hand zu geben. Die Unterrichtseinheit entspricht somit dem im Perspektivrahmen der GDSU (2013) geforderten Ziel, Lernenden die Chancen und Gefahren medialer Verbreitung von persönlichen Daten verständlich zu machen und eine kritische Auseinandersetzung mit diesen zu fördern.

Auch entsprechend des Lehrplans Nordrhein-Westfalen (2021) sollen Schüler*innen zum Ende der Grundschulzeit Kompetenzen im Themenbereich Demokratie und Gesellschaft, speziell hinsichtlich des Zusammenlebens in Klasse, Schule und Gesellschaft erlangt haben, die hier mit einer sicheren Nutzung von Pass wörtern in Bezug gesetzt werden. Zu nennen ist etw die Kompetenz, dass Schüler*innen Möglichkeiten zur Schutz vor Cybermobbing oder -gewalt kennen. Hier an lässt sich eine weitere Kompetenzerwartung zur Ende der Klasse 4 aus dem Bereich Leben in der Med en- und Konsumgesellschaft anknüpfen, welche di Benennung von Kriterien für einen verantwortungs vollen Umgang mit Medien beschreibt. (Lehrplan NRW 2021) Im Besonderen ist hier der verantwortungsvoll Umgang mit eigenen Daten und deren Sicherung i der digitalen Welt hervorzuheben.

Fachlicher Hintergrund

Vor- und Nachname, Geburtstag und -ort, privat Anschrift, Standort-Daten, Urlaubsfotos. Was diese un andere persönliche und personenbezogene Date wohl gemeinsam haben? Man möchte nicht, dass si in die falschen Hände geraten!

Ob in einem orientalischen Märchen als Passphras für eine Höhle oder als Losung in mittelalterliche Geschichten, um in eine Burg eintreten zu dürfen – ei Blick in die (Literatur-)Geschichte zeigt, dass Pass wörter schon seit jeher ein Mittel der Wahl darsteller um das eigene Hab und Gut zu schützen oder une wünschten Personen den Eintritt zu verweigern. Dam nur wir und gewünschte Personen Zugang zu schü zenswerten Informationen erhalten, die in unsere zahlreichen Accounts im Internet verstreut lieger verwenden wir heutzutage – ähnlich wie damals – ge heime Zeichenfolgen.

Während sich früher jedoch Räuber und Bandite Zugang zu fremden Eigentümern verschaffen wollter versuchen dies heute Hacker zu sensiblen Daten. Ihr böse Absicht liegt in der Nutzung dieser Daten, ur Identitäten zu stehlen, finanziell zu schädigen ode auch um Privatsphären zu verletzen, indem sie be spielsweise ihre Opfer im öffentlichen Raum bloß stellen (Stichwort: Cybermobbing). Dafür verwende sie Werkzeuge, die vollautomatisch unterschiedlich Zeichenkombinationen ausprobieren oder etwa ganz Wörterbücher durchgehen und Wörter mit gängige

Wissenswertes

Noch sicherer als die Verwendung eines Passworts ist die Zweifach-Authentifizierung. Hierbei ist zum Einloggen neben dem Passwort ein weiterer Identitätsnachweis wie die Eingabe eines SMS-Codes oder eine biometrische Bestätigung (Fingerabdruck, Facescan etc.) notwendig.

Zahlenkombinationen austesten, um an die Zugangsdaten ihrer Opfer zu gelangen.

Kann man überhaupt Passwörter erstellen, durch die das möglichst verhindert wird? Zum Glück ja. Wichtig ist zunächst einmal die Verwendung eines möglichst langen Passwortes, bestehend aus mindestens acht Zeichen. Darüber hinaus ist eine Mischung aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (!, §, $, %, &, €, @ usw.) sinnvoll. (BSI o.J.) Für ein solch konzipiertes Passwort wird rein rechnerisch nicht mehr nur – wie eben beschrieben – ein Sekundenbruchteil benötigt, um es zu knacken, sondern – beispielsweise bei $@ChVnT€rR1cHt – mehrere Millionen Jahre! (passwortcheck.ch) Doch so ein Passwort ist nicht leicht zu merken. Diese Unterrichtsreihe bietet mit der Verwandlungsmethode eine kreative und altersgerechte Strategie, mit der Grundschüler*innen sichere Passwörter erstellen können, die sie sich zudem auch einfach merken können. Dabei verwandeln die Kinder Buchstaben und Zahlen in Sonderzeichen.

Auf einen Blick

Klasse: 2–4

Zeit: 4–5 Unterrichtsstunden

Kompetenzen:
- Sachkompetenz zu den Eigenschaften sicherer Passwörter
- Medienkompetenz (verantwortungsvoller Umgang mit Passwörtern)
- Methodenkompetenz (Gedächtnistechniken)
- Problemlösefähigkeit

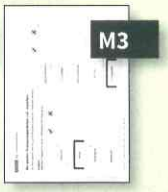
Inhalt:
Passwörter, Passwortsicherheit, Sicherung von Daten

Inklusive/Soziale Aspekte:
Partnerarbeitsphasen als kooperative Lernform zur Förderung der sozialen Kompetenz

Materialseiten:
M1 Yunus und sein Laptop
M2 Was macht ein sicheres Passwort aus?
M3 Wir werden Passwortexpertinnen und -experten!
M4 Tipps und Tricks für dein starkes Passwort – Die Verwandlungsmethode

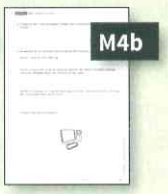
S. 20

online



S.21

S. 22



S. 23

Edi

Materialseiten downloaden oder online bearbeiten!
Infos auf Seite 51

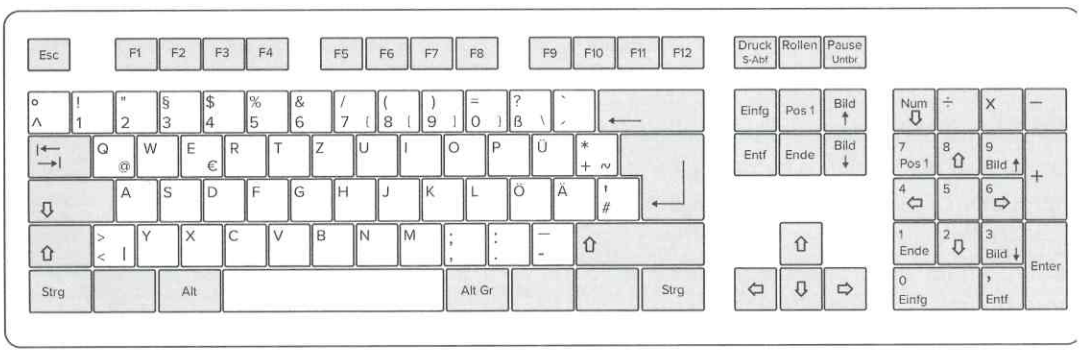
Ergänzende Materialien:
Briefumschlag, Tablets und/oder Tastatur

Einstieg

Um in diese Unterrichtsreihe zur Passwortsicherheit einzusteigen, ist es besonders wichtig, zunächst die Vorstellungen und Erfahrungen der Kinder zur sicheren Verwahrung von wertvollen Dingen oder auch Daten in ihrer Lebenswelt in einem Sitzkreis zu sammeln. Dafür liest die Lehrkraft zu Beginn einer Doppelstunde die kurze Geschichte des Jungen Yunus vor (**M1**). Den Kindern dient sie als Impuls für die Einheit und soll daher nicht ausgeteilt werden.

In dieser Geschichte mit Bezug zur Lebenswelt der Kinder geht es darum, dass Yunus den Speicherstand seines Lieblingsspiels unbedingt vor dem Zugriff seiner Schwester schützen will, die immer wieder ungefragt an seinen Laptop geht. Die Lehrkraft unterbricht die Geschichte an zwei Stellen, um die Schüler*innen nach ihren Ansichten zu fragen. Dadurch erhält jedes Kind die Möglichkeit, entweder sein Vorwissen zu aktivieren oder das Prinzip von Passwörtern – sofern es bislang noch keine Berührungspunkte damit gab – erstmalig kennenzulernen. Im Laufe der Erzählung wird auch ersichtlich, dass besonders komplizierte Passwörter nicht nur Nachteile für diejenigen bringen, die es knacken wollen, sondern auch für die Personen haben kann, die es sich überlegt haben.

Nachdem die Geschichte zu Ende vorgelesen wurde, überlegen sich die Kinder, was sie an Yunus' Stelle getan hätten und welches Passwort sie sich überlegt hätten, um sein Lieblingsspiel vor dem Zugriff der Schwester zu schützen. Jedes Kind schreibt dieses Passwort auf einen Zettel, der zusammengefaltet, mit dem Namen des Kindes versehen und dann in einem Umschlag aufbewahrt wird. So kann kein Kind das Passwort eines anderen sehen. Hierdurch wird den Schüler*innen ein ggf. erstes Gefühl dafür vermittelt, dass man Passwörter für sich behalten und normalerweise nicht mit anderen teilen soll. Daher ist seitens der Lehrkraft wichtig zu betonen, dass sie nur für



Illu: Christian Frenser, Nicola Airo

•• *2 Typische Tastatur mit Sonderzeichen*

diese Stunde in die Rolle einer Passwortmanagerin / eines Passwortmanagers schlüpft und die Passwörter ungesehen verwahrt.

Ziel dieses Einstiegs ist die Sensibilisierung der Schüler*innen für die Wichtigkeit von (guten) Passwörtern und deren Geheimhaltung sowie für die Notwendigkeit der Sicherung von Daten.

Verlauf

Was macht ein gutes Passwort aus?

Als Nächstes bearbeiten die Kinder das Arbeitsblatt **M2**. Dabei setzen sie sich durch das Lesen eines kurzen Textes vertiefend mit den Eigenschaften sicherer Passwörter auseinander und erarbeiten eine Checkliste, die in der gesamten Unterrichtsreihe als Hilfestellung dienen darf. In dieser Checkliste wird auf Basis des Textes notiert, was bei der Erstellung eines Passworts zu beachten ist.

Da auf diesem Arbeitsblatt der Begriff „Sonderzeichen" genannt wird, sollte mit den Kindern gemeinsam erläutert werden, bei welchen Zeichen es sich um Sonderzeichen handelt und wo diese auf der Tastatur zu finden sind. Sofern ausreichend Tablets vorhanden sind, können die Kinder die Sonderzeichen eigenständig entdecken und die Funde gemeinsam besprechen. Alternativ kann auch der Bildschirm eines Tablets an die Wand projiziert und die Tastatur aktiviert werden, sodass alle Kinder diese sehen können (s. Abb. 2). Oder die Lehrkraft bringt eine Tastatur in den Unterricht mit und führt diese den Kindern vor. Im Anschluss gibt sie die Tastatur auch herum, sodass jedes Kind die Sonderzeichen entdecken kann. An dieser Stelle ist es wichtig zu erörtern, wie man diese Sonderzeichen erstellt (häufig in Kombination mit der Umschalttaste „Shift-Taste").

Wir werden Passwortexpertinnen und -experten!

M3 gibt nun den Schüler*innen die Möglichkeit, ihr erlangtes und/oder bereits vorhandenes Wissen zu testen. Hierbei entscheiden die Kinder, welche Passwörter sie als eher sicher oder eher unsicher identifizieren.

Zunächst machen sich die Kinder im Sinne des Prinzips *Think-Pair-Share* eigene Gedanken dazu („think", welche Passwörter auf **M3** sie für sicher befinden und welche nicht. Daran anschließend tauschen sich die Kinder zu zweit über ihre Ergebnisse aus, vergleichen diese miteinander und kommen zu einer gemeinsamen Lösung („pair"). Daraufhin erfolgt der dritte Aspekt des Prinzips („share"), sodass im Plenum die gemeinsamen Lösungen besprochen, möglichst Fehler korrigiert und die richtigen Lösungen erläutert werden.

Foto: Christian Frenser, Nicola Airo

•• *3 Verwandlungsmethode als Tafelbild*

Als Abschluss der Doppelstunde wird der Umschlag mit den Passwörtern der Kinder geöffnet. Die Lehrkraft teilt als Passwortmanager*in die zusammengefalteten Zettel an die Kinder aus. Hier machen sich die Kinder selbstreflexiv noch einmal Gedanken dazu, ob ihr zu Beginn notiertes Passwort den Kriterien eines sicheren Passworts entspricht. Die Doppelstunde kann mit einer kurzen Daumenabfrage zur Zufriedenheit mit dem eigenen Passwort enden.

Abschluss

Die nächste Doppelstunde ist einer Strategie gewidmet, die dabei helfen soll, ein sicheres Passwort zu erstellen, an welches man sich auch erinnern kann: die Verwandlungsmethode (**M4**).

Nachdem die Verwandlungen in Aufgaben 1 und 2 im Plenum oder zu zweit verglichen wurden und bevor die Kinder mit Aufgabe 3 beginnen, ist es ratsam, dass die Lehrkraft einen Beispielsatz an der Tafel bearbeitet und Schritt für Schritt einzelne Buchstaben umwandelt, z. B. „Ein Esel auf der Wiese“ zu „3!n3$3laufd3rW!3$3“ – s. Abb. 3). Es ist wichtig zu erklären, dass nicht unbedingt jeder Buchstabe umgewandelt werden muss.

Die Schüler*innen erhalten die Möglichkeit, sich zum Abschluss dieser Unterrichtseinheit auf Basis ihrer neu erlernten Fähigkeiten nochmals ein Passwort (mit Strategie) an Yunus‘ Stelle zu überlegen und auf einen Zettel zu schreiben. Dieses Mal geht es jedoch nicht darum, dass die Kinder im Anschluss entscheiden, ob ihr Passwort den Anforderungen eines sicheren Passworts genügt, sondern ob sie es sich bis zur nächsten Sachunterrichtsstunde merken können. Dieser Zettel wird wie zu Beginn der Einheit gefaltet, mit dem Namen des Kindes versehen und in einen Umschlag gelegt, sodass auch hier kein anderes Kind und auch nicht die Lehrkraft dieses Passwort sehen können. Die Lehrkraft hat wieder die besondere Verantwortung, die Passwörter als Passwortmanager*in ungesehen bis zur nächsten Sachunterrichtsstunde sicher zu verwahren und den Kindern dann wieder auszuteilen.

Bevor die Zettel in der Abschlussstunde ausgeteilt werden, versuchen sich die Kinder an ihr Passwort zu erinnern und schreiben es auf ein separates Blatt. Nach dem Austeilen der ursprünglichen Passwörter vergleichen sie beide Passwörter. Falls sie nicht identisch sind, werden im Plenum die Gründe reflektiert: Lag es am Ausgangssatz, an den man sich nicht richtig erinnern konnte? Lag es daran, dass vergessen wurde, welche Buchstaben wie verwandelt wurden? Oder weil ein Buchstabe auf unterschiedliche Weise verwandelt wurde (z.B. das „S“ als „$“ und als „5“)?

Weiterführendes

Die in diesem Artikel erwähnte Thematik der personenbezogenen Daten, die in Teilen auch durch Passwörter geschützt werden, können im Anschluss an die Unterrichtsreihe ebenfalls näher beleuchtet werden. Hierzu gehört, dass Unternehmen und Konzerne massenhaft personenbezogene Daten sammeln, auch wenn man diese vermeintlich mit Passwörtern geschützt hat. Hier können Aspekte angesprochen werden, die den Nutzen für die Konzerne verdeutlichen, u. a. verbesserter Kundensupport, personalisiertes Marketing mit angepasster Werbung und daraus resultierendem Wettbewerbsvorteil. Diesen kann man beispielsweise auf globaler Ebene bei Big Playern wie Amazon, Meta und Co. betrachten. Im Zuge der personalisierten Werbung könnte man ebenso das Thema der sozialen Medien wie TikTok, Instagram, Facebook etc. besprechen, deren Feed ebenfalls aus personalisierten Daten gefüttert ist und Kinder als Konsument*innen andressiert. ■

Tipps zur Verwandlungsmethode

- *Je mehr Buchstaben in Sonderzeichen „verwandelt“ werden, desto komplexer wird das Passwort und lässt sich somit schwieriger merken.*
- *Bei der Wahl des Passwortes sollten möglichst die deutschen Umlaute (Ä, Ö, Ü) sowie das Eszett bzw. scharfe S (ß) vermieden werden, da die Eingabe dieser Buchstaben auf Tastaturen außerhalb des deutschsprachigen Raums erschwert ist.*
- *Tastaturen im Smartphone oder Tablet haben noch weitere Sonderzeichen zu bieten. Jedoch sollte man sich im Unterricht auf die gängigsten und zugänglichsten Zeichen beschränken.*

Literatur

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.), Sichere Passwörter erstellen, o.J., www.bsi.bund.de/dok/6596574

Neff, R. / Dr. Wübbeling, M. / Dr. Zickenheiner, F., Whitepaper Passwortsicherheit 2023, Identeco 2023, https://bit.ly/3ysDx9c

Irion, T., Grundlegende Bildung in der Digitalität, in: Schmeinck, D. / Michalik, K. / Goll, T. (Hrsg.), Herausforderungen und Zukunftsperspektiven für den Sachunterricht, Klinkhardt 2023, S. 17–31

Ministerium für Schule und Weiterbildung des Landes Nordrhein-Westfalen, Lehrpläne Primarstufe 2021

Datenschutzbeauftragte des Kantons Zürichs, www.passwortcheck.ch

Die Autoren


Foto: Privat


Foto: Privat

Christian Frenser *und* ***Nicola Airo*** *sind wissenschaftliche Mitarbeiter am Institut für Didaktik des Sachunterrichts an der Universität zu Köln.*

Yunus und sein Laptop

Jeden Tag nach der Schule, wenn Yunus fleißig seine Hausaufgaben erledigt hat, darf er für eine Stunde an seinem Laptop spielen. Am liebsten spielt Yunus Minecraft. Natürlich nur, wenn er dabei nicht wieder von Selma gestört wird. Seine kleine Schwester beschwert sich ständig, dass Yunus sie nicht mitspielen lässt. Doch Yunus möchte nicht. Seit Wochen baut er an einem riesigen Schloss und ist damit noch lange nicht fertig. Tag für Tag baut er neue Türme und gräbt sich immer tiefere Tunnel.

Doch seit einiger Zeit stimmt etwas nicht. Manchmal, wenn Yunus das Spiel öffnet, sieht sein Schloss anders aus als am Vortag. Mal entdeckt er eine Mauer, die er nie gebaut hat, mal fehlt der zuvor gebaute Turm. Das ärgert ihn. Denn es kostet viel Zeit, diese Mauern abzureißen oder die verschwundenen Türme wieder aufzubauen. So wird er nie damit fertig, sein Schloss zu Ende zu bauen.

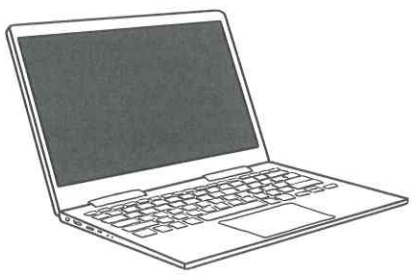
Habt ihr schon eine Idee, wer oder was hinter diesem Problem stecken könnte?

Als Yunus eines Tages früher als sonst nach Hause kommt, sieht er, wie Selma an seinem Laptop Minecraft spielt. Schnell wird ihm klar, dass es seine Schwester ist, die ständig sein Schloss verändert. Verärgert nimmt Yunus ihr den Laptop weg und überlegt sofort, wie er sein Laptop vor seiner Schwester schützen kann.

Habt ihr eine Idee?

Er sucht Rat bei seiner Mutter, die ihm erklärt, dass ein gutes Passwort helfen kann. Yunus weiß: Ein sicheres Passwort ist wie ein gutes Rätsel. Schnell überlegt er sich ein kompliziertes Passwort und richtet es ein. Yunus ist sich sicher, Selma wird nie wieder sein Schloss verändern können.

Als er am nächsten Tag seinen Laptop öffnet, um an seinem Schloss weiterzubauen, wird er nach dem Passwort gefragt. Yunus überlegt und überlegt. Doch er kann sich einfach nicht erinnern ...

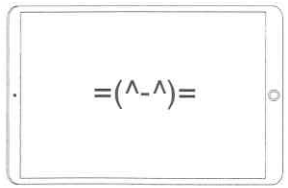


Wir werden Passwortexpertinnen und -experten!

Du hast gelernt, was ein gutes Passwort ausmacht. Teste dein Wissen!

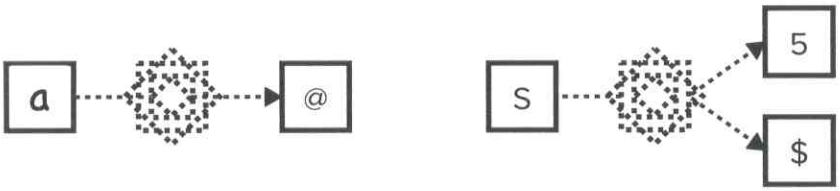
Aufgabe:
Welches Passwort ist sicher? Welches nicht? Kreuze an.

	✓	✗
	☐	☐
	☐	☐
	☐	☐
	☐	☐

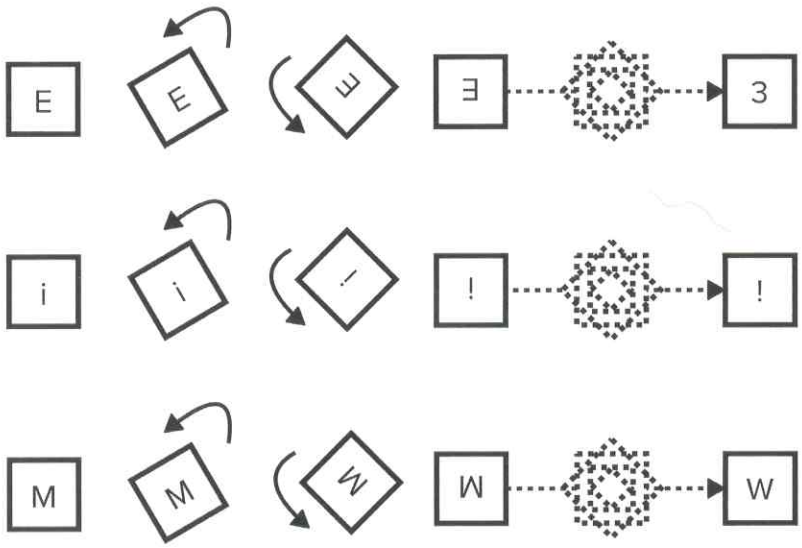
	✓	✗
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐

Tipps und Tricks für dein starkes Passwort – Die Verwandlungsmethode

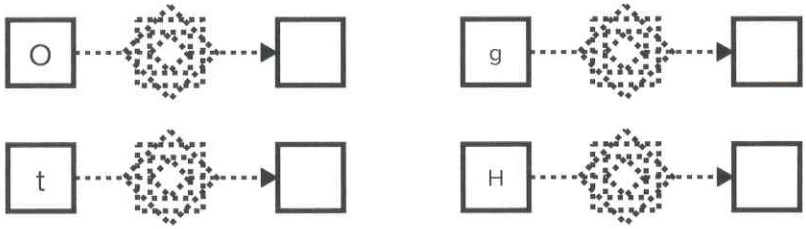
Für diese Methode brauchst du ein bisschen Fantasie. Schau dir noch einmal die Tastatur an. Einige Zahlen oder Sonderzeichen sehen aus wie Buchstaben. Diese kannst du verwandeln:

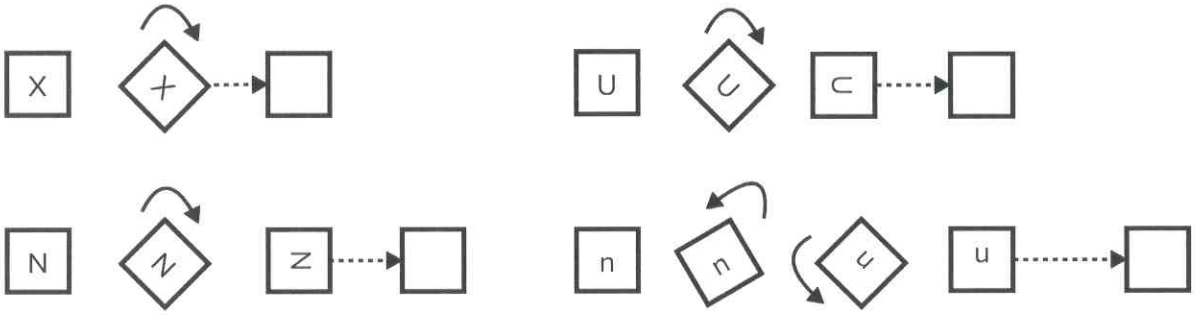


Einige Buchstaben musst du erst einmal drehen, bevor du sie verwandeln kannst:



1. Wie kannst du die folgenden Buchstaben verwandeln?





2. Findest du noch mehr Buchstaben, Zahlen oder Sonderzeichen, die du verwandeln kannst?

3. So wendest du die Verwandlungsmethode für dein Passwort.

Schritt 1: Denk dir einen Satz aus.

Schritt 2: Entscheide, ob du die Abstände zwischen den Wörtern behalten möchtest oder nicht. Schreibe deinen Satz passend auf die Linien.

Schritt 3: Verwandle nun einzelne Buchstaben in Zahlen oder Sonderzeichen. Schreibe den verwandelten Satz auf die Linien.

Fertig ist dein sicheres Passwort!