



# Sicheres Passwort!

Mit dem Passwort-Schlüssel-Automaten



## Didaktische Hinweise für Lehrerinnen und Lehrer

URL: [surfen-ohne-risiko.net/passwortschluesel](http://surfen-ohne-risiko.net/passwortschluesel)

## Inhalt

- I Sichere Passwörter im Internet
- II Der Passwort-Schlüssel als aktive Beschäftigung mit Datenschutz
- III Lernziele
- IV Einsatz des Passwort-Schlüssel-Automaten (PS-Automat) im Unterricht
- V Hintergrundinformationen: Privatsphäre lernen

## I Sichere Passwörter im Internet

Auf vielen Internetseiten, z.B. zum Chatten und Mailen benötigen auch Kinder bereits einen eigenen Zugang. Dieser wird in der Regel mit Benutzernamen und Passwort angelegt. Datenschützer raten: Passwörter geheim halten, nirgendwo aufschreiben, regelmäßig ändern und für jede Anwendung ein eigenes Passwort kreieren. Dies führt dazu, dass Kinder und Erwachsene nur leicht merkbare – und damit unsichere – Kombinationen wählen. Um sich das Passwort leicht zu merken, werden oft einfache Wörter verwendet: der eigene Name, der vom Hund oder dem Lieblingsstar. Dazu noch das Geburtsdatum oder das Alter. Aber! Solch ein Passwort kann in weniger als 1 Sekunde geknackt werden. Hacker können dann diesen Zugang nutzen. Ein sicheres Passwort mit dem Passwort-Schlüssel generiert, kann dagegen nicht oder nur sehr schwer geknackt werden. Es ist also wichtig, einen verantwortungsvollen Umgang mit Passwörtern bereits im frühen Alter zu lernen, zumal man im digitalen Zeitalter im Laufe seines Lebens hunderte verschiedene Passwörter benötigt, um sich sicher zu verhalten.

Ein **sicheres Passwort** wird aktuell so definiert:

- Mindestens 10 (thesafeshop) bzw. zwölf (bsi) Zeichen lang
- Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern
- Keine Namen, keine Wörter, die in Wörterbüchern vorkommen
- Keine gängigen Varianten und Wiederholungs- oder Tastaturmuster, also nicht asdfgh oder 1234abcd

Quellen: [bsi.de](http://bsi.de)  
[thesafeshop.de/blog/sicheres-passwort/](http://thesafeshop.de/blog/sicheres-passwort/) > sicheres Passwort

Die Befürchtung, dass ein sicheres Passwort schwer im Kopf zu behalten ist, trifft nicht zu: Schwierige, aber sichere Passwörter haben sich bereits nach wenigen Malen Tippen eingeprägt. Dies gilt auch für jüngere Kinder. Sie können nämlich besonders leicht Kombinationen von Zeichen im Kopf speichern und sind insofern sogar etwas im Vorteil gegenüber Erwachsenen.

## II Der Passwort-Schlüssel als aktive Beschäftigung mit Datenschutz

### Passwort-Schlüssel erzeugen > geheimes Wort ausdenken > geheimes Wort codieren

Mit dem Passwort-Schlüssel kann sich jeder individuelle Code-Zeichen erstellen, die zum Codieren eines ausgedachten Wortes dienen. Jeder Passwort-Schlüssel enthält zwei verschiedene Codefelder.

#### 1. Codefeld: Die 4 Start-Zeichen

Die individuellen 4 Start-Zeichen umfassen alle 4 Zeichentypen. (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen)

Die 4 Start-Zeichen stehen immer zu Beginn eines jeden Passwortes. Der Passwort-Schlüssel-Automat generiert sie extra für jeden Schlüssel mit. Sie werden dann so wie sie sind vor jedem verschlüsselten Wort eingegeben. Damit ist garantiert, dass jedes Passwort alle sicherheitsrelevanten Auflagen erfüllt, egal welches ausgedachte Wort codiert wird.



Denn wählt das Kind z.B. MamaPapa als zu verschlüsselndes Wort, dann sind nur 3 Buchstaben des Alphabetes zu verschlüsseln. Mit dem Beispiel-Passwort-Schlüssel rechts würde 8Z8ZeZ entstehen, also Sonderzeichen fehlen. Die 4 Start-Zeichen machen aber ein sicheres Passwort daraus.

#### 2. Codefeld: Codezeichen zur Verschlüsselung

Jeder Codestelle werden 3 bzw. 4 Buchstaben aus dem Alphabet zugeordnet. Hiermit kann nun ein ausgedachtes geheimes Wort Buchstabe für Buchstabe übersetzt werden.



Das geheime Wort sollte mindestens 8 Buchstaben enthalten. So wird das Passwort ausreichend lang und damit sicher genug.

**Das Passwort besteht dann aus den 4 Start-Zeichen sowie den Zeichen, die sich aus dem individuellen Code und dem ausgedachten Wort ergeben.**

Mit dem **Button „Druckansicht“** erhält man eine PDF-Datei mit fünf automatisch erstellten Druckversionen des vorab individuell generierten Passwort-Schlüssels. Sofern die Möglichkeit zum Ausdrucken besteht, kann der Passwort-Schlüssel dann ausgeschnitten und anschließend in einer ansprechenden Form an Geräten wie Handy, Tablet, Laptop und PC angebracht werden.



Ein weiteres **PDF „Übung und Beispiel“** gibt die Möglichkeit, den Passwort-Schlüssel einmal ganz praktisch und schriftlich auszuprobieren. Achtung: Beim richtigen Passwort-Einsatz im Internet sollte das verwendete Passwort nicht aufgeschrieben werden. Dies ist auch nicht nötig, denn der Passwort-Schlüssel ist die Codierungshilfe für das ausgedachte Wort und kann als Erinnerungshilfe neben dem Gerät liegen.



#### Beispiel

Verschlüsseln  
des Wortes  
**SCHAUKEL**



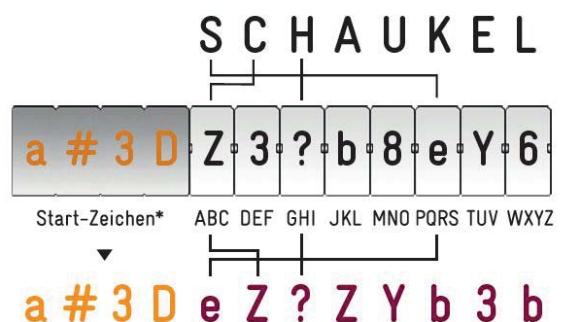
Ausgedachtes Wort



Passwort-Schlüssel



Sicheres Passwort



## Was macht den Passwort-Schlüssel so sicher?

Beide Codefelder auf dem Passwort-Schlüssel werden mit einem Zufallsgenerator erstellt und bestehen aus insgesamt 12 Stellen. Der Einsatz der 4 Start-Zeichen garantiert, dass jedes Passwort die von Experten empfohlene Zeichenvielfalt enthält. Für den Passwort-Schlüssel-Automaten finden Verwendung:

- Alle GROSSBUCHSTABEN ohne Umlaute
- Alle kleinbuchstaben ohne Umlaute
- Zahlen: 1 - 9
- Satz- und Sonderzeichen: ! ? , - . " : #

## Das Besondere:

- Die spielerische Beschäftigung mit dem Thema Sicheres Passwort ist kindgerecht, weil Codieren am „Geheimnis“ ansetzt. Das ist für Kinder besonders spannend, weil sie sich gerne mit Geheimschriften beschäftigen.
- Sofern man den Passwort-Schlüssel ausdruckt, kann ein geeignetes Format am Handy, Tablet, Laptop und PC angebracht werden. So bleibt Datenschutz augenfällig.
- Die Verwendung des Passwort-Schlüssel-Automaten und das Giveaway aus der Broschüre ist nicht nur für Kinder interessant, sondern ebenso für Erwachsene. Es kann also einen besonderen erzieherischen und auch Langzeitwert entwickeln.

## III Lernziele

### Die Schülerinnen und Schüler ...

- sollen sichere Passwörter auf spielerische Weise generieren.
- erkennen, dass einfache Passwörter schnell herausgefunden werden können.
- lernen, dass sie Passwörter geheim halten müssen und auch Freunden nicht weitersagen dürfen.
- ein Verständnis von Datenschutz im Internet erlernen.

## IV Verlaufsplan: Einsatz des Passwort-Schlüssel-Automaten im Unterricht

Phase	Inhalt	Arbeitsform	Medien
Einstieg	Kinder ihre eigene Erfahrung mit Passwörtern / Anmeldungen im Internet erzählen lassen	Plenum	
Einführung	Bedeutung eines sicheren Passwortes erläutern	LehrerIn	
Darstellung	<ul style="list-style-type: none"> <li>- PS-Automaten aufrufen</li> <li>- Einen Beispiel-Passwort-Schlüssel generieren</li> <li>- Code-Zeichen an die Tafel schreiben (einschließlich Start-Zeichen und ABC)</li> </ul>	LehrerIn SchülerIn LehrerIn	<ul style="list-style-type: none"> <li>- PC für URL: <a href="http://surfen-ohne-risiko.net/passwortschluesel">surfen-ohne-risiko.net/passwortschluesel</a></li> <li>- Tafel</li> </ul>
Erarbeitung 1	<p>Arbeitsauftrag:</p> <p>Jedes Kind denkt sich ein geheimes Wort aus und verschlüsselt dieses Wort Buchstabe für Buchstabe durch die passenden Zeichen über dem Alphabet im Beispiel-Passwort-Schlüssel.</p>	Einzelarbeit	<ul style="list-style-type: none"> <li>- Papier</li> <li>- Stift</li> </ul>
Lernkontrolle 1	3 Passwörter unter den Passwort-Schlüssel an die Tafel schreiben (immer mit den 4 Start-Zeichen am Anfang)	3 SchülerInnen	- Tafel
Ergebnis 1	<ul style="list-style-type: none"> <li>- unterschiedliche Passwörter entstehen</li> <li>- mit demselben Schlüssel lassen sich unterschiedliche Passwörter bilden für unterschiedliche Zugänge</li> <li>- die 4 Start-Zeichen garantieren alle benötigten Zeichentypen für ein sicheres Passwort</li> </ul>	Plenum	
Erarbeitung 2	<p>Arbeitsauftrag:</p> <p>Zusätzlich oder alternativ können alle Schülerinnen und Schüler ein von Lehrerin/Lehrer vorgegebenes Wort verschlüsseln. Dies ist am besten ein Wort, dem codiert eines der Zeichentypen fehlt.</p>	Einzelarbeit	<ul style="list-style-type: none"> <li>- Papier</li> <li>- Stift</li> </ul>
Lernkontrolle 2	Dann wird verglichen, ob alle das richtige Passwort gebildet haben.	Plenum	
Ergebnis 2	<p>Der eine hat vielleicht die Start-Zeichen vergessen, der andere nicht gründlich genug geschaut beim Verschlüsseln. So kann man nochmal auf die Spezifika des Passwort-Schlüssels aufmerksam machen:</p> <ul style="list-style-type: none"> <li>- Start-Zeichen dürfen nicht fehlen</li> <li>- ein sicheres Passwort hat mindestens 12 Zeichen</li> <li>- die Buchstaben müssen korrekt codiert sein. Sonst ist das eingegebene Passwort beim nächsten Mal möglicherweise zwar korrekt, aber anders als beim vorherigen Mal eingegeben.</li> </ul>	Plenum	
Hausaufgaben Option 1	Verschlüsseln üben anhand des Beispielwortes <b>SCHULFREI</b> mit dem vorgegebenen Passwort-Schlüssel <b>a#3DZ3?b8eY6</b>	Kind	<ul style="list-style-type: none"> <li>- PDF Üben</li> <li>Ausdruck auf <a href="http://surfen-ohne-risiko.net/passwortschluesel">surfen-ohne-risiko.net/passwortschluesel</a></li> </ul>
Hausaufgaben Option 1	Mithilfe der Eltern einen eigenen Passwort-Schlüssel erzeugen. Sofern erlaubt, PDF Karten/Sticker ausdrucken oder alternativ abschreiben. Karte/Sticker z.B. ausschneiden und einstecken oder an Gerät anbringen. Sonst Schlüssel abschreiben.	Eltern mit Kind	

## V Hintergrundinformationen: Privatsphäre lernen

Wir möchten unsere Kinder lebensstark machen. Sie sollen für sich selbst einen guten Weg finden und fair miteinander umgehen lernen. Nähe und Austausch auf der einen Seite erfordern Abgrenzung und Raum für Eigenes auf der anderen Seite. Im Internet ist diese Balance besonders schwierig zu halten. Denn online ist Privates schnell öffentlich. Wir helfen unseren Kindern, indem wir ihnen den Wert der Privatsphäre vermitteln: was sie von sich preisgeben möchten und was niemanden etwas angeht. Und diese Privatsphäre auch bei anderen zu akzeptieren.

Sobald sich ein Kind im Internet aufhält, sollte es diese Regeln wissen und einhalten:

- Gib keine Infos, Namen, Adressen, Telefonnummern über dich, die Familie und Freunde weiter.
- Passwörter nicht weitersagen. Auch Freunden nicht.
- Wähle einen Nick- oder Benutzernamen, der nichts über dich verrät.
- Dein Profilbild kann jeder sehen. Nimm ein Motiv, auf dem du nicht zu erkennen bist.
- Bilder können von anderen, dir vielleicht sogar fremden, Personen gespeichert und an anderen Stellen ins Internet hochgeladen werden, ohne dass du das merkst.

Diese Webseiten bieten zahlreiche Möglichkeiten, Datenschutz zu lernen:



[youngdata.de](http://youngdata.de)  
Hilfreiche, vielfältige Ideen zum eigenen Schutz



[watchyourweb.de](http://watchyourweb.de)  
Gut gemachte Videos über Datensicherheit, Verbraucherschutz und Onlinerechte



[internet-abc.de/eltern/datenschutz-im-internet.php](http://internet-abc.de/eltern/datenschutz-im-internet.php)  
Aktuelles und Tipps

Diese Webseiten helfen bei allgemeinen Themen zur Sicherheit im Internet:



[jugendschutz.net](http://jugendschutz.net)  
Infos und Materialien zu aktuellen Problemfeldern im Internet



[klicksafe.de](http://klicksafe.de)  
Aktuelles zu Sicherheit und Entwicklungen im Internet



[schau-hin.info](http://schau-hin.info)  
Hilfen zur Medienerziehung



[surfen-ohne-risiko.net](http://surfen-ohne-risiko.net)  
Technische Hilfen, interaktive Spiele

## Impressum und Bestellmöglichkeit

Der Lehrerhandzettel wurde erstellt von jugendschutz.net

- gemeinsames Kompetenzzentrum von Bund und Ländern für Jugendschutz im Internet



Verantwortlich:

Friedemann Schindler

Text und Redaktion:

Andrea Kallweit

Katja Lichtenstein

Idee Passwort-Schlüssel:

Thomas Mühlhoff

Hey!Blau Labs e.K.

[www.heyblau.com](http://www.heyblau.com)

Gefördert vom:

Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ)

11018 Berlin

[www.bmfsfj.de](http://www.bmfsfj.de)



Bundesministerium  
für Familie, Senioren, Frauen  
und Jugend