



„Geben Sie Ihr Passwort ein!“ ... „Passwort vergessen?“
Passwörter umgeben uns, egal wo wir uns aufhalten. Im Supermarkt an der Bankomatkasse, im Internetbanking, beim Abrufen der persönlichen E-Mails, beim Einloggen in den Facebook-Account usw. Die Liste kann man beliebig fortsetzen. Umso wichtiger erscheint eine professionelle Auseinandersetzung mit der Erstellung, Verwendung und Wartung der Passwörter.

Mag.^a
Elvira Mihalits-Hanbauer
BHAK/BHAS Eisenstadt,
Wirtschaftspädagogin
elvira.hanbauer@gmail.com

Software

Internet

Hardware

Ev. PC

Die Schüler/innen lernen

- die Wichtigkeit von Passwörtern verstehen
- „sinnlose“ Passwörter zu vergeben und zu merken.

Hinweise für den Einsatz

In jeder Schulstufe und jedem Gegenstand

1 Einstieg mit einem Brainstorming: Wo gibt es überhaupt Passwörter?

Die Schüler/innen sammeln, wo in ihrem Leben Passwörter vorkommen. Die Schüler/innen schreiben ihre Ideen auf kleine Zettel. Das Ergebnis kann in Form einer Mindmap auf der Tafel dargestellt oder als Brainstorming an der Tafel gesammelt werden. [Tafelbild 1]

2 Diskussion im Plenum: Warum gibt es Passwörter überhaupt?

Diskutiere mit den Schüler/innen im Plenum, warum es sinnvoll ist, Passwörter zu verwenden. Sammle die Meldungen an der Tafel.

Folgende Punkte sollten dabei vorkommen:

- Passwörter schützen wichtige Daten.
- Passwörter garantieren Berechtigten Zugriff.

3 Strukturierung an der Tafel Sind alle Passwörter gleich wichtig?

Strukturiere an der Tafel, welche verschiedenen Arten von Passwörtern es gibt. Versuche die genannten Beispiele aus dem Einstieg gemeinsam mit den Schüler/innen zu ordnen. [Tafelbild 2]

4 Passwörter erstellen

Die Schüler/innen denken sich in Partnerarbeit ein Passwort aus, von dem sie glauben, dass es gut ist.

Anschließend wird auf der Website www.wiesicheristmeinpasswort.de jedes einzelne Passwort auf seine „Stärke“ überprüft.

Am besten erfolgt die Prüfung über den Lehrer/innen-PC mit Beamer, damit alle mitsehen können. Nicht alle Passwörter sind gut!

5 Sichere Passwörter selber erstellen

Die Schüler/innen erhalten von dem/der Lehrenden einen Kurz-Input zu Regeln der Passwortsicherheit: **Welche Passwörter gelten als sicher?**

Sicher sind jene Passwörter, die man auch durch Raten nicht herausfinden kann. Sie bestehen aus einer **beliebigen** Zeichenfolge, ergeben überhaupt **keinen Sinn**, enthalten Klein- und Großbuchstaben, Sonderzeichen und Ziffern in nicht geordneter Reihenfolge. Sie sollten mindestens 8 Zeichen oder noch länger sein und **streng geheim** bleiben.

6 Input: Wie kann ich mir Passwörter merken?

Nun zeigst du den Schüler/innen, wie man sich schwierige und lange Passwörter gut merken kann. Am besten merkt man sich so kryptische Zeichenfolgen nämlich mit einer **Eselsbrücke**. Du kannst zum Beispiel einen Satz aufschreiben und verwendest die Anfangsbuchstaben dieses Satzes als Passwort. [Tafelbild 3]

Jede/r Schüler/in präsentiert danach selbst sein/ihr Beispiel, verrät aber **NICHT** die Eselsbrücke.

7 Abstimmung im Plenum

Mache in der Klasse zum Schluss eine Abstimmung zur Frage: **Kann ich für alle Anwendungen das gleiche Passwort verwenden?**

Die richtige Antwort ist: **Nein**, das solltest du auf gar keinen Fall tun. Gerade bei den sehr wichtigen Passwörtern solltest du darauf achten, dass es **verschiedene Passwörter** sind. Damit kannst du verhindern, dass eine missbräuchliche Verwendung zu mehrmaligem Schaden führt.

8 Video-Zusammenfassung (als Belohnung)

Zum Schluss dürfen die Schüler/innen das Video: *Bit & Byte Show: Passwortschutz* ansehen.

Tafelbild 1

Passwörter verfolgen uns ...



Tafelbild 2

Passwörter sind echt stark ...

Ich fahre jeden Sonntag um 14 Uhr mit
meinen Eltern zu meiner Oma.

IfjSu14UmmEzmO.

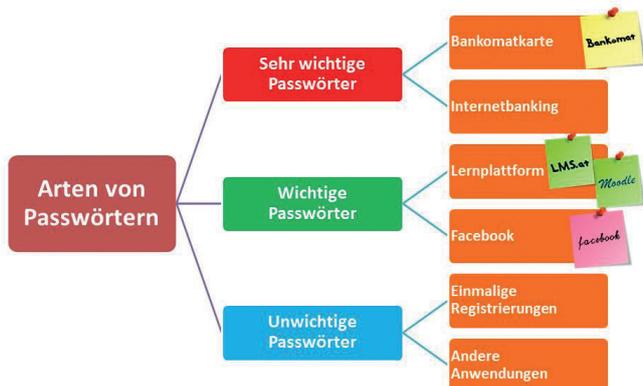


PASSWORT-CHECKER

- Beliebige Zeichenfolge
- kein Sinn
- Kleinbuchstaben
- Großbuchstaben
- Sonderzeichen
- Ziffern
- nicht geordnet

Tafelbild 3

Manche Passwörter sind ...



Infobox:

Es gibt sehr wichtige Passwörter, die man extrem gut schützen muss. Das sind Passwörter für den Einstieg ins Internetbanking, der Bankomatcode, Passwörter für das Login in Computer- oder Lernsysteme. Wenn man diese Passwörter nicht besonders sicher auswählt und gut schützt, kann großer Schaden angerichtet werden.

Weiters gibt es wichtige Passwörter, mit denen man in verschiedene Sites einloggen kann, um an Diskussionen teilzunehmen, etwas zu bestellen, eine Zeitung zu lesen usw. Diese Passwörter sollte man ebenfalls gut schützen.

Schließlich gibt es noch unwichtige Passwörter, mit denen man vielleicht nur eine einmalige Registrierung durchführt und die man später wahrscheinlich nicht mehr braucht. Diese Passwörter sollte man zwar schützen, es entsteht aber kaum Schaden bei missbräuchlicher Verwendung.

Wie lange gilt ein Passwort?

Es gibt Anwendungen, die ihre Nutzer/innen regelmäßig zur Veränderung des Passwortes auffordern. Dabei darf ein Passwort, das schon einmal verwendet wurde, nicht mehr vergeben werden. Bei anderen Anwendungen sollte man selbst daran denken, die Passwörter regelmäßig zu ändern. Vor allem, wenn du den Verdacht hast, dass jemand dein Passwort „geknackt“ hat, solltest du umgehend ein neues Passwort anlegen.

Surftipps:

Wenn dir kein Passwort einfällt, kannst du über die Website www.sicherespasswort.com eines erstellen lassen. Aber Vorsicht: Diese Passwörter sind „echt stark“ und du musst dir eine gute Eselsbrücke dafür einfallen lassen.

Bit & Byte Show:
Passwortschutz