


Thema: Passwörter und Sicherheit in Netzwerken

1. Passwörter im Internet:



Um es potentiellen Passwort-Dieben möglichst schwer zu machen, solltest du folgende Tipps für das Erstellen von sicheren Passwörtern beherzigen:

- Kein Standardpasswort für "Alles" verwenden. Falls zum Beispiel dein SchülerVZ-Passwort gehackt wird, hat der Hacker auch gleich Zugriff auf deinen E-Mail-Account.
- Benutzername und Passwort sollten unterschiedlich sein, weil der Benutzername vielen bekannt ist
- Das Passwort sollte nicht zu kurz sein und aus mindestens 8 Zeichen bestehen
- Personennamen, insbesondere der eigene oder aus dem nahen Bekanntenkreis, sind keine guten Passwörter, da diese zu leicht zu erraten sind
- Das Passwort sollte aus einem Mix von Zahlen und Buchstaben (Groß- und Kleinschreibung) bestehen
- Keine Umlaute "ä", "ö", "ü" und kein "ß" verwenden
- Zusätzliche Sonderzeichen wie "_" können die Sicherheit erhöhen, aber manche Sonderzeichen wie zum Beispiel "/" sollten vermieden werden, da diese zu technischen Problemen führen könnten
- Passwörter sollten nicht auf dem Computer gespeichert werden
- Passwörter in regelmäßigen Abständen ändern

Quelle: www.netzdurchblick.de

Aufgabe:

Teste mindestens zwei verschiedene Passwörter, die Du zur Zeit benutzt auf folgender Seite: <http://www.passwordmeter.com/>

The Password Meter

Home
Feed

Test Your Password		Minimum Requirements
Password:	<input type="password" value="••••••••"/>	<ul style="list-style-type: none"> • Minimum 8 characters in length • Contains 3/4 of the following items: <ul style="list-style-type: none"> - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	<input checked="" type="checkbox"/>	
Score:	100%	
Complexity:	Very Strong	

Weitere Informationen zu Passwörtern findest Du beispielsweise hier: <http://netzdurchblick.de/passwort.html>

2. Was gilt es zu beachten, wenn ich Inhalte im Internet veröffentliche?

- Überlege genau, wann und wie Du persönliche Daten veröffentlichst
- Wenn Inhalte online veröffentlicht wurden, ist es nahezu unmöglich, sie wieder zu entfernen, da Daten sehr einfach und schnell verbreitet und kopiert werden können

Aufgabe:

Schaut unter <http://netzdurchblick.de/meinprofil.html> und schaut Euch die vier Bildergeschichten „Fake Profil“, "Cyber-Grooming", "Cyber-Mobbing" und "Dos and Don'ts" an. Im weiteren Informatikunterricht werden wir eine Internetseite (ein Blog) selbst erstellen. Setzt Euch zu viert zusammen und notiert Euch, worauf ihr achten wollt, wenn ihr Euren Blog erstellt.

Dos
Don'ts

Ihr habt jetzt einiges über die Sicherheit im Internet erfahren. Hier könnt ihr jetzt auf einen Blick erkennen, was ihr im Internet veröffentlichen könnt und was ihr bei Problemen tun solltet:

- Veröffentlich persönliche Angaben in sozialen Netzwerken und Communities nur eingeschränkt (zum Beispiel nur sichtbar für deine Freunde)
- Lade nur Videos oder Fotos hoch, bei denen du sicher bist, dass sie keiner gegen dich verwenden kann
- Schließe neue Bekanntschaften im Internet nur mit Vorsicht (du weißt nie, wer hinter dem anderen Bildschirm sitzt)
- Wenn du Opfer einer Mobbingattacke wirst, wende dich umgehend an eine Bezugsperson (Eltern, Lehrer, Geschwister, Freunde)
- Wenn du das Gefühl hast, belästigt zu werden, blockiere oder melde diese Person




Quelle: www.netzdurchblick.de

Dos
Don'ts

Hier könnt ihr noch einmal nachlesen, was ihr lieber nicht im Internet veröffentlichen solltet und wie ihr euch richtig verhaltet:

- Lade keine freizügigen Fotos oder Videos von dir und deinen Freunden hoch! Das Internet vergisst nie! Auch nach Jahren können deine Fotos gefunden werden
- Achte beim Chatten darauf, dass du nicht zuviel von deiner Privatsphäre preisgibst (Adresse, Handynummer, Kontonummer etc.)
- Vertraue keiner Internetbekanntschaft, du weißt nie, wer sich dahinter verbirgt
- Schließe dich keinen Mobbing-Gruppen an! Nach dem Prinzip: "Was du nicht willst, das man dir tut, das füge auch keinem anderen zu."



Quelle: www.netzdurchblick.de