Wie kann ich meine Daten schützen?

Es gibt **keinen einzelnen Ansatz**, mit dem Du Deine Daten umfassend schützen kannst. Du musst und kannst auf verschiedene Schutzmechanismen zurückgreifen:

- einige sind **technische** Lösungen,
- einige beruhen auf Deinem **Wissen** und Deinem **Verhalten**.

Dein **Wissen** und die **Selbstkontrolle Deines Verhaltens** sind die wichtigsten und wirksamsten Möglichkeiten für Dich, anderen in Netz keine ungewollten Einblicke in Dein Privatleben zu geben.

AUFGABEN

1. Lies die folgenden Tipps durch und besprich den Inhalt mit einem Partner.
2. Überlegt gemeinsam, welche Punkte Ihr persönliche umsetzen könntet und notiert Euch diese Beispiele.
3. Führt diese Schritte möglichst direkt durch (z.B. durch Umstellung der Privatsphäreeinstellungen in Profilen etc.)

Geräte sicher einrichten

- Sichere Einrichtung Ihres Computers, Tablets und Smartphones

Datensparsamkeit

Informationen, die Du NICHT online postest, können nicht missbraucht oder gegen Dich verwendet werden. Dieses bewusste Zurückhalten von Daten nennt man »Datensparsamkeit«. Letztlich geht es darum sich zu fragen, ob eine bestimmte Information, Statusmeldung, ein bestimmtes Foto oder ein Kommentar nun wirklich gepostet werden »müssen« oder ob man es nicht einfach auch für sich behalten könnte.

Bewusste (Nicht)-Verwendung von Diensten

In eine ähnliche Richtung geht die Vermeidung von bestimmten Angeboten und Diensten. Oftmals registriert man sich vielleicht ohne lange nachzudenken bei einem neuen Service, weil man ihn ausprobieren möchte oder weil Freunde auch schon dort sind. Auch hier kann es sinnvoll sein, kurz innezuhalten und sich zu fragen, ob man diesen Dienst WIRKLICH braucht und nutzen möchte oder ob man nicht auch ohne ganz gut auskommt.

Falsche Angaben

Manche Dienste sind sehr »neugierig« und erlauben es unter Umständen nicht, dass man Informationsfelder leer lässt. Man kann also eventuell gar nicht »datensparsam« sein, wenn man einen solchen Dienst nutzen möchte.

Gerade als Jugendlicher kann es dann sinnvoll sein, falsche Angaben zu machen, um sich selbst zu schützen. Wenn ein Dienst zum Beispiel eine Postadresse fordert und es nicht ersichtlich ist, warum diese nötig ist, kann man einfach eine Phantasieadresse eingeben.

Verschiedene Benutzernamen und E-Mail-Adressen

Viele Dienste identifizieren Dich anhand von Benutzernamen oder E-Mail-Adressen. Es empfiehlt sich daher, verschiedene Benutzernamen und/oder E-Mail-Adressen zu benutzen. Auf diese Art ist nicht sofort ersichtlich wer sich hinter einem Account verbirgt. Drei oder vier verschiedene E-Mail-Adressen sind sicherlich ein guter Anfang und noch gut zu handhaben (neben einer »guten« Hauptemailadresse, die nur vertrauenswürdige Leute kennen und zu der alle anderen Mail-Konten weiterleiten.

Ein Beispiel für die Bedeutung von Benutzernamen: In dem Artikel Datenschutz-Fallrückzieher sind ganz am Ende »Recherchetipps« aufgelistet. Es stellt sich heraus, dass die Redakteure über gleiche Benutzernamen (Nicknames) eine Menge Informationen über die freiwillige Testperson erfahren konnten.

Privatsphäreeinstellungen

Natürlich solltest Du genau wissen, welche Informationen Du mit welchem Personenkreis teilst.

Die Privatsphäreeinstellungen in den einzelnen Netzwerken ändern sich praktisch ständig. Daher macht es hier wenig Sinn, einzelne Einstellungen zu erklären. Eine gute Anlaufstelle mit entsprechenden Tipps ist zum Beispiel klicksafe.de. Auch netzdurchblick.de hat einige gute Tipps.

Browsereinstellungen

Dein Browser (das Programm, mit dem Du im internet surfst, z.B. Internet Explorer, Mozilla Firefox, Google Chrome oder Safari) hat verschiedene Einstellungsmöglichkeiten, um Deine Daten online zu schützen. Informiere Dich darüber zum Beispiel hier:

- Wie kann ich meine Daten im Internet schützen?
- Browser-Sicherheitsmaßnahmen

Alte Accounts löschen

Wenn Du einen Account nicht mehr benutzt, solltest Du ihn löschen. Auf diese Art besteht zumindest eine gute Chance, dass Deine Daten damit auch gelöscht sind (obwohl einige Anbieter wie zum Beispiel Facebook zunächst den Account nur deaktivieren und Deine Daten behalten – oft muss man lange suchen, bis man das »richtige« Löschen durchführen kann). Es gilt auch hier wieder: Daten, die nicht (mehr) online sind, können auch nicht missbraucht werden.

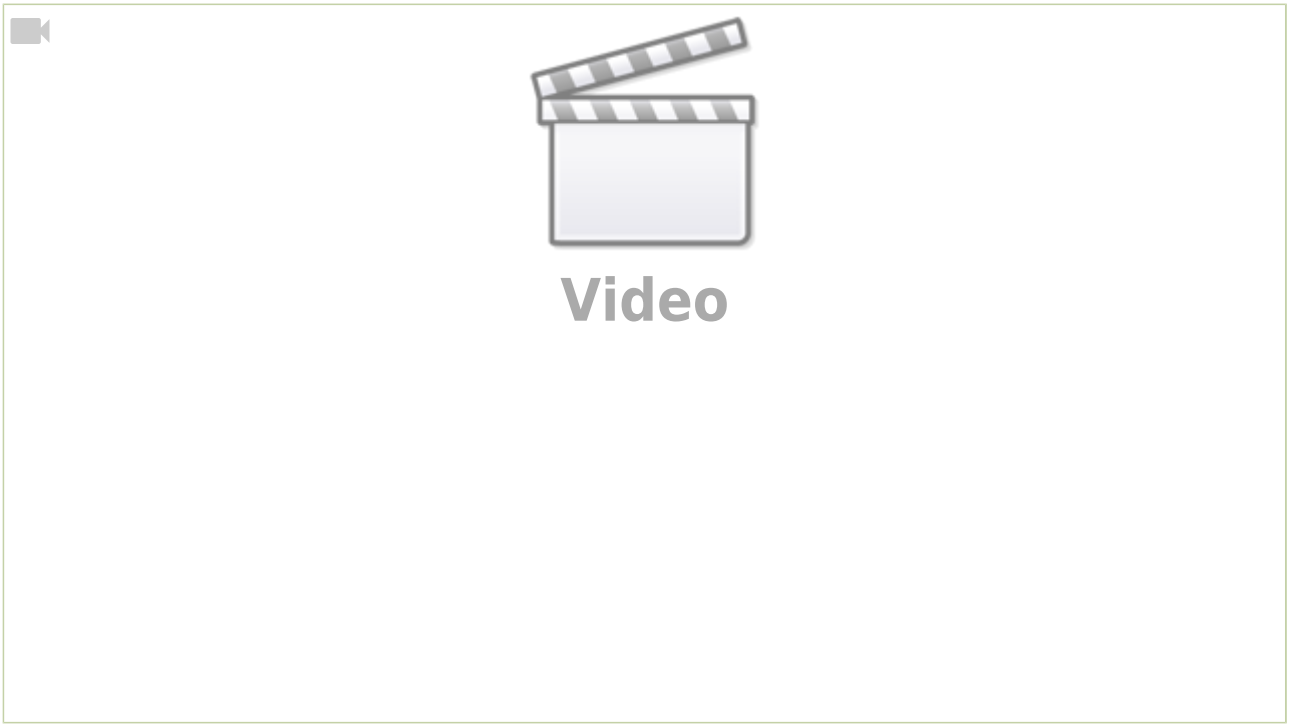
Passwörter

Passwörter sind extrem wichtig, wenn Du Dich gegen Missbrauch Deiner Daten schützen möchtest. Du solltest immer gute, das heißt: ausreichend lange, Passwörter verwenden und diese niemandem anderen mitteilen. Idealerweise verwendet man für jeden Dienst ein eigenes Passwort (dann braucht man in der Regel ein Programm zur Verwaltung der Passwörter, siehe unten). Man kann aber auch ein Grundpasswort variieren, z.B.

Grundpasswort	`24Autohausen_Hauptstreet!`
Passwort für web.de	`24Autohausen_Hauptstreet!_web`
Passwort für YouTube.com	`24Autohausen_Hauptstreet!_youtube`

Diese Passwörter scheinen Dir vielleicht unglaublich lang, da sie aber weitgehend aus leicht zu schreibenden Wörtern bestehen (die aber nicht genauso in einem Wörterbuch stehen), lassen sie sich schnell tippen.

Tipps für **gute und dennoch leicht zu merkende** Passwörter gibt es in diesem Video:



Passwortmanager verwenden

Natürlich ist es nicht einfach, sich verschiedene Passwörter zu merken. Dafür gibt es Programme, in denen man seine Passwörter speichern kann.

- Ein kostenloses ist KeePass.
- Evtl. kann es sich auch lohnen, ein Programm wie 1Password zu verwenden, vielleicht sogar mit der ganzen Familie. Für einige Euro pro Monat kann so die ganze Familie sichere Passwörter verwenden und verwalten und für gemeinsame Accounts auch Passwörter untereinander teilen.

privatsphaere, reflexion, medien, datenschutz