

AB: Datenschutz – Welche Daten sollten geschützt werden?

💡 **Merke:** Nicht alle Daten sind für alle bestimmt! Was du im Internet teilst oder akzeptierst, kann gespeichert, weitergegeben oder sogar missbraucht werden. Deshalb ist es wichtig, **bewusst mit deinen Daten umzugehen**.

✗ Welche Daten sollten nicht öffentlich werden?

Aufgabe: Lies die folgende Liste mit verschiedenen Daten. Entscheide, welche Informationen sicher geschützt werden sollten.

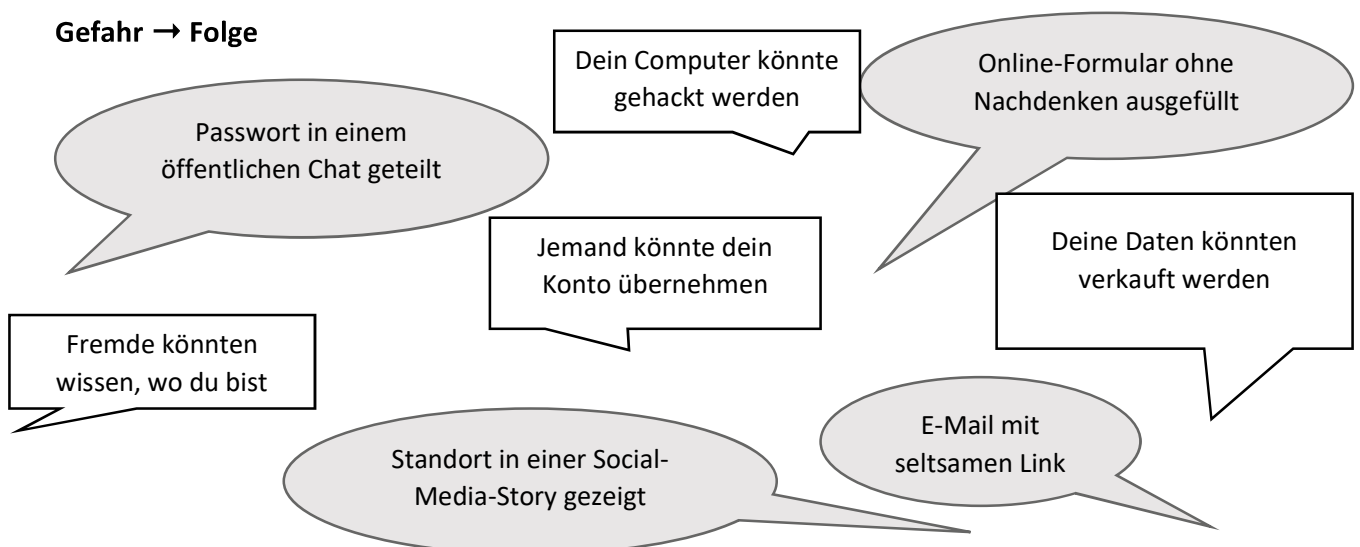
Kreuze an: „Kein Problem“ oder „Privat & schützen“.

Information	Kein Problem	Privat & schützen
Dein Name		
Deine Handynummer		
Dein Wohnort und Adresse		
Dein letztes Urlaubsziel		
Deine Passwörter für soziale Netzwerke		

💡 Gefahren durch ungeschützte Daten

Wenn persönliche Daten in falsche Hände geraten, kann das gefährlich sein. Lies dir die folgenden Gefahren durch und verbinde sie mit den möglichen Folgen.

Gefahr → Folge



Sicherheit im Internet – Webseiten, Cookies & Passwörter

Im Gespräch mit Tom hat Ada erklärt, dass nicht alle Webseiten sicher sind. Hier sind drei wichtige Punkte, die du beachten solltest:

Webseiten:

- Sichere Webseiten nutzen **https://** – das bedeutet, dass deine Daten verschlüsselt übertragen werden.
- **Aber Achtung:** Auch Betrugsseiten können HTTPS haben! Schau dir die Seite genau an, bevor du Daten eingibst, sehr lange Adressen mit vielen Zeichenfolgen können hinweise auf unsichere Webseiten und Emailadressen sein.
- **Online-Shopping:** Überprüfe das **Impressum** – fehlt es oder ist keine Adresse angegeben? Dann lieber Finger weg!

Cookies:

- Cookies speichern Informationen über dich.
- **Technisch notwendige Cookies** helfen, dass eine Webseite funktioniert (z. B. Login speichern).
- **Tracking-Cookies** verfolgen dein Verhalten – oft für Werbung.
- **Tipp:** Wähle in den Einstellungen immer nur die nötigsten Cookies aus!

Passwörter & Verschlüsselung:

- Verwende starke Passwörter: **Eine Mischung aus Buchstaben, Zahlen und Sonderzeichen**, je länger ein Passwort umso sicherer ist es.
(Du kannst einen Satz bilden, den du dir gut Merken kannst und die Anfangsbuchstaben nutzen: Jasmin isst gerne 2 Kugeln Schokoladeneis und 1 Kugel Himbeere! = **Jig2KSu1KH!**)
- Zwei-Faktor-Authentifizierung (2FA) aktivieren. Dabei wird neben dem Passwort ein zweiter Sicherheitsnachweis benötigt, z. B. ein Code auf dem Smartphone.
- Teile deine Passwörter niemals!
- Messenger wie WhatsApp und Signal nutzen Ende-zu-Ende-Verschlüsselung, damit niemand deine Nachrichten mitlesen kann, verwende sichere Messenger, um mit Freunden zu schreiben.



Aufgabe:

Bilde einen Satz und probiere die „Verschlüsselung“ oben für ein Passwort aus.

