

DAS KANNST DU TUN PERSÖNLICHER DATENSCHUTZ

1. DAS PASSWORT

Wähle eine ausreichende Länge:

- Dein Passwort sollte mind. 12–16 Zeichen lang sein.

Nutze verschiedene Zeichenarten:

- Kombiniere Groß- und Kleinbuchstaben,
- Zahlen und Sonderzeichen (z. B. ? ! & % \$).

Vermeide einfache oder persönliche Wörter:

- Nutze keine leicht zu erratenden Begriffe wie deinen Namen,
- dein Geburtsdatum oder einfache Passwörter wie „Passwort123“.

Mache jedes Passwort einzigartig:

- Verwende für jedes Konto ein eigenes Passwort,
- damit nicht mehrere Accounts gleichzeitig gefährdet sind.



ZUM PASSWORT-



CHECK

2. EINSTELLUNGEN PRÜFEN!

Schau regelmäßig in die Einstellungen deiner Apps und Konten:

- Stelle dein Profil auf privat
- Prüfe, wer deine Inhalte sehen kann
- Deaktiviere unnötige Berechtigungen (z. B. Standort, Kontakte)
- Aktiviere Sicherheitsfunktionen (z. B. Zwei-Faktor-Anmeldung)



DATENSCHUTZ
BEI ANDROID



DATENSCHUTZ
BEI APPLE



APPS MIT ERHÖHTEM DATENSCHUTZ-RISIKO

SOCIAL MEDIA

- TikTok
- Instagram
- Snapchat

Risiken:

- Zugriff auf Kamera, Mikrofon, Standort
- Öffentliche Profile & Fremde können Inhalte sehen
- Daten werden für Werbung genutzt

Wichtig:

- Profil auf privat stellen
- Standort ausschalten
- Kontakte & Kamera nur bei Bedarf erlauben



MESSANGER

- WhatsApp
- Discord
- Telegram

Risiken:

- Zugriff auf Kontakte
- Fremde können Nachrichten senden
- Gruppen & Server können unsicher sein

Wichtig:

- Nur bekannte Kontakte zulassen
- Privatsphäre-Einstellungen prüfen
- Keine sensiblen Daten teilen



VIDEO & STREAMING

- YouTube
- Twitch

Risiken:

- Tracking des Nutzungsverhaltens
- Kommentare & Kontakt mit Fremden

Wichtig:

- Verlauf & Empfehlungen prüfen
- Kommentare einschränken



SPIELE & GAMING-PLATTFORMEN

- Roblox
- Fortnite
- Minecraft

Risiken:

- Chats mit Fremden
- In-Game-Käufe
- Verknüpfung mit anderen Accounts

Wichtig:

- Chat einschränken
- Käufe absichern (z. B. PIN)
- Freundeslisten kontrollieren



WENN DATEN IN FALSCHER HÄNDE GERATEN

WERDE SELBST ZUM DATENSCHUTZ-PROFI!



DATENSCHUTZ

WICHTIGE FAKTEN ZUM DATENSCHUTZ:

Datenschutz bedeutet, dass deine persönlichen Daten geschützt werden. Dazu gehören zum Beispiel dein Name, deine Adresse, Fotos oder Nachrichten.

Wichtig:

Du sollst selbst entscheiden können:

- Wer deine Daten sieht.
- Was mit deinen Daten passiert.

WARUM IST DAS WICHTIG?

Ohne Datenschutz können:

- Fremde deine Daten sehen oder missbrauchen
- Leute herausfinden, wo du bist oder was du machst
- deine Daten für Werbung oder Betrug genutzt werden

WAS SIND PERSONENBEZOGENE DATEN?

Personenbezogene Daten sind alle Informationen, die sich auf eine bestimmte Person beziehen oder sie identifizierbar machen. Dazu gehören zum Beispiel:

- Name (Vor- und Nachname)
- Geburtsdatum
- Adresse / Wohnort
- Telefonnummer
- E-Mail-Adresse
- Geburtsort
- Bankkontonummer / IBAN
- Kreditkartendaten
- Politische Meinungen
- Sexuelle Orientierung

WICHTIGE DATENSCHUTZ-REGELN



inkl. quiz



DARAUF MUSST DU ACHTEN!

Gib nicht zu viele Daten preis

- Gewinnspiele, Apps oder Formulare können deine Daten weitergeben oder verkaufen
 - Folge: Spam, Betrug, Verlust der Kontrolle

Einmal online = schwer zu löschen

- Fotos und Videos können weitergeleitet, gespeichert oder verändert werden
 - Folge: Bloßstellung, Mobbing, Kontrollverlust

Teile deinen Standort vorsichtig

- Andere können sehen, wo du bist oder dich regelmäßig aufhältst
 - Folge: Du wirst leichter auffindbar

Achte auf App-Berechtigungen

- Apps können Kontakte, Daten oder Inhalte nutzen
 - Folge: Deine Daten (und die deiner Freunde) werden weitergegeben

Nutze deinen echten Namen mit Bedacht

- Fremde können dich finden und kontaktieren
 - Folge: Belästigung oder unerwünschte Kontakte

Sei vorsichtig mit persönlichen Daten

- Daten wie Name, Adresse oder Geburtstag können missbraucht werden
 - Folge: Identitätsdiebstahl

Vorsicht bei E-Mail & Werbung

- Deine Daten können weitergegeben werden
 - Folge: Spam und Betrugsnachrichten

Teile nicht zu viele Infos über deinen Alltag

- Schule oder Aufenthaltsorte machen dich auffindbar
 - Folge: Fremde wissen, wo du bist

Deine Bilder können missbraucht werden

- Fotos können für Fake-Profilen genutzt werden
 - Folge: Identitätsmissbrauch

„Private“ Chats sind nicht immer privat

- Nachrichten können weitergeleitet oder gespeichert werden
 - Folge: Inhalte werden öffentlich

Denke nach, bevor du etwas postest

- Infos wie „Ich bin im Urlaub“ zeigen: Niemand ist zuhause
 - Folge: Sicherheitsrisiko (z. B. Einbruch)

Achte auf Logins und Verknüpfungen

- Apps sammeln viele Daten über dich
 - Folge: Dein Verhalten wird analysiert

Vorsicht bei öffentlichem WLAN

- Daten können abgefangen werden
 - Folge: Konten können gehackt werden

ABSCHLIEßENDE CHECKLISTE HAST DU ALLES BERÜCKSICHTIGT?



Überlege, bevor du etwas teilst

- Nicht alles muss ins Internet.



Gib nur notwendige Daten an

- Je weniger, desto besser.



Nutze starke Passwörter

- Und für jedes Konto ein anderes.



Achte auf Einstellungen

- Stelle deine Profile auf privat.



Sei vorsichtig bei Apps & Links

- Nicht alles ist vertrauenswürdig.



Aktiviere Sicherheitsfunktionen

- (z. B. Zwei-Faktor-Anmeldung)

IMMER BEACHTEN!

Wichtige Grundregel

Je mehr eine App über dich weiß, desto vorsichtiger solltest du sein.



Das solltest du immer prüfen:

- Braucht die App wirklich meinen Standort?
- Warum will sie Zugriff auf Kontakte oder Kamera?
- Wer kann meine Inhalte sehen oder speichern?

WO FINDE ICH HILFE?

AUCH ANJA HILFT EUCH!

ANJA PLÄTTNER

Schulsozialarbeiterin am
Gustav-Hertz-Gymnasium

Zimmer X-37
(Gang - hinterm
Sekretariat)

0163- 741 72 98 (SMS, Signal)
sozialarbeit@ghg-leipzig.lernsax.de

