

Eure Handys, Computer und digitale Geräte sind kein privater Raum. Inhalte und Daten werden auf verschiedene Weise von Anbietern gesammelt. Seid euch bewusst, dass viele Institutionen, Firmen und Menschen Einblick in euer Verhalten und eure Vorlieben haben!

Hier einige Tipps, wie ihr euch schützen könnt:

Geräte offline schalten, wenn sie nicht mehr gebraucht werden.
So wenig wie möglich private Daten speichern und preisgeben (Sensible Daten und Einstellungen, Fingerabdruck, Stimme, private Photos).
Kamera und Mikrofon bei Nichtgebrauch abdecken oder abstellen.
Dienste verschiedener Anbieter nutzen.
Voreinstellungen der Apps überprüfen und allenfalls einschränken. AGBs lesen und Verhalten danach richten.
Account erstellen:
<ul style="list-style-type: none">• So wenig Angaben wie möglich machen, wenn möglich mit Nickname registrieren.• Für sichere und weniger sichere Accounts verschiedenen Mailadressen und Passwörter verwenden (z.B. Online-Shopping).
Passwortschutz:
<ul style="list-style-type: none">• Ein gutes Passwort sollte mindestens acht Zeichen lang sein.• Du solltest darauf achten, dass dein Passwort Buchstaben, Ziffern und Sonderzeichen enthält. Vermeide Buchstabenfolgen auf der Tastatur.• Das Passwort sollte aber keine Informationen über den Benutzer enthalten (eigene Name, das eigene Geburtsdatum).• Du musst dir das Passwort gut einprägen können, damit du es nicht aufschreiben musst. Mit einer Eselsbrücke aus einem ganzen Satz kannst du dir schwierige Passwortkombinationen leicht einprägen. Jeder kennt Sprichwörter wie „Der Ball ist rund und Das Runde muss ins Eckige“. Daraus kannst Du z. B. das Passwort “Dbir&DRmiE” machen.• Für mehr Sicherheit Passwort-Verschlüsselung verwenden.
Vorsichtiges und überlegtes Handeln im Internet:
<ul style="list-style-type: none">• Guten Ruf bewahren und Rücksicht nehmen
<ul style="list-style-type: none">• Webseiten, die deine Daten sicher und verschlüsselt übertragen, erkennst du am "https" in der Adresszeile des Webbrowsers (Hypertext Transfer Protocol Secure = sicheren Hypertext-Übertragungsprotokoll).
<ul style="list-style-type: none">• Browserdaten immer wieder löschen (Verlauf, Cookies, Cache). Beachte: für das Gerät deiner Schule gelten oft besondere Bestimmungen
<ul style="list-style-type: none">• nur absolut sichere Downloads vornehmen.
<ul style="list-style-type: none">• kostenlose Angebote sehr kritisch prüfen. Dubiose Inhalte nicht öffnen oder weiterleiten, sondern löschen und sperren/melden.
<ul style="list-style-type: none">• Fakten checken, sich informieren:
<ul style="list-style-type: none"><ul style="list-style-type: none">https://correctiv.org/faktencheck/https://www.mimikama.at/https://citizenevidence.amnestyusa.orghttps://hoaxmap.org

- | | |
|---------------------------------------|--|
| • diskrete Suchmaschinen und Browser: | Private Fenster/Modi wählen
https://duckduckgo.com/
https://www.startpage.com/
https://brave.com/ (mit Tor-Integration) |
| • Tracking- und Adblocker: | https://ublock.org/
https://disconnect.me/disconnect
https://adblockplus.org/de/ |