



Sicher im Netz

Modul: Cyber Security

So geht Geld | Finanzielle Allgemeinbildung im Unterricht

Referent: XXX

Schule: XXX

Die Themen

Die meisten von uns sind täglich online – auf Social Media, in Games, beim Shoppen, Streamen oder beim Online-Banking.

Doch überall lauern Risiken, die ernsthafte Folgen haben können. Umso wichtiger ist es, diese zu kennen – und zu wissen, wie man sich schützt oder im Ernstfall richtig reagiert.



Was tun
Cyberkriminelle



Gerätesicherheit und
Passwörter



KI und Formen
digitaler Gewalt



10 Tipps bei
Cyberbedrohungen

Cyberkriminalität



Daten und Identitäten stehlen

Namen, Adressen, Passwörter, Bilder etc.



Menschen austricksen

Phishing-Mails, Fake-Gewinnspiele, gefälschte Profile



Geräte infizieren

Viren, Apps aus unsicheren Quellen, verseuchte Anhänge



Konten hacken

Spiele-Accounts, Social-Media-Accounts, E-Mail

VORSICHT

Passwörter – Was, wie, warum?

Passwort = euer geheimer Schlüssel

Schützt eure Chats, Games, Mails und Social-Media-Konten vor anderen

Passwörter bleiben geheim

Nie mit Freunden teilen, nicht in Chats oder offen auf Zetteln speichern

Passwortmanager

Speichert viele Passwörter sicher, um euch nicht alle merken zu müssen



KI sicher nutzen

- **Nicht alles glauben:** Antworten und Inhalte kritisch prüfen, mit anderen Quellen abgleichen
- **KI als Hilfe**, nicht als **einzige** Quelle der Wahrheit nutzen
- **Immer hinterfragen:** Ist das, was ich sehe, echt?
- **Keine echten Namen, Adressen, Passwörter** oder privaten Fotos / Videos in KI-Tools eingeben
- **Nichts teilen** oder **generieren**, was ihr z.B. Lehrern oder späteren Arbeitgebern **nicht zeigen würdet**
- Wenn euch ein KI-Bild / Video komisch vorkommt: nicht weiterleiten, sondern einer **erwachsenen Person** oder der **Plattform melden**

VORSCHAU



Quelle: Envato.com/stockasso

Cybermobbing

**Denkt dran, wer auf der anderen Seite sitzt:
Hinter dem Bildschirm sitzt ein echter Mensch!**

Schreibt nichts, was ihr jemandem nicht ins Gesicht sagen würdet.

Netiquette:

Höflich bleiben, keine Beleidigungen,
keine fiesen Witze auf Kosten anderer machen

Die digitale Welt kennt keine echte Anonymität:

Auch online kann man herausfinden, wer etwas
geschrieben hat – selbst wenn der Account auf den
ersten Blick anonym scheint

Worte haben Folgen:

Gemeine Nachrichten können
andere traurig, ängstlich oder krank machen

VORSCHAU



Social Media

Gefahren und wie ihr euch schützt. Was solltet ihr tun?

- **Nur echte Freunde hinzufügen:** Fremde Anfragen ablehnen, Nachrichten von Unbekannten löschen, keine Links / Videos von Fremden öffnen (auch keine merkwürdigen Sprachnachrichten)
- **Influencer und Inhalte hinterfragen:** Nicht alles glauben, keine „Wundermittel“ oder riskante Challenges nachmachen, bei Gewinnspielen und Links in Profilbeschreibungen (Bios) misstrauisch sein
- **Auf Fake-Profile & Betrug achten:** Blockiert und meldet Personen, die nach Geld, Geschenken, privaten Infos oder Bildern fragen
- **Eure Zeit und euer Gefühl im Blick behalten:** Wenn euch Social Media stresst, traurig macht, oder ihr euch ständig vergleicht – macht eine Pause und redet mit jemandem darüber

WARNSCHAU



Online Shopping

Was sind typische Risiken?

- **Fake-Shops:** Sehen echt aus, liefern aber nichts oder stehlen eure Daten / euer Geld
- **Gefälschte Bestell- oder Paket-Mails:** „Deine Bestellung hat ein Problem – bitte hier einloggen“ greift deine Daten ab
- **Gefährliche Links / Pop-ups und Abo-Fallen:** „Gratis“, „Gewinn“, „nur heute“ – Klicks führen zu Malware oder teuren Abos

Was sind Zeichen für Betrug?

- Angebote wirken „zu gut, um wahr zu sein“
- Komische / ungewohnte Web-Adresse, merkwürdige Formulierungen, nur Vorkasse / wenige Bezahloptionen
- Mails mit Links, die euch direkt zum Einloggen oder zur Eingabe von Bankdaten bringen sollen

Wie schützt ihr euch und eure Konten?

- Nur **bekannte Shops / Apps** nutzen, **Web-Adresse** prüfen
- Direkt in der **App / bekannten Website einloggen** statt auf Links zu klicken
- **Keine Konto-** oder **Kartendaten über Links** eingeben, bei Unsicherheit Erwachsene fragen
- Mehr Sicherheit für Passwörter: Überall, wo es geht, **Mehrfaktor-Authentifizierung** (MFA/2FA) einschalten (z. B. TAN-App, SMS-Code) und **Passkeys / Fingerprint / Face-ID** nutzen

HINWEIS

Wir bitten um Rückmeldung
zu deinem Unterrichtsbesuch!

Für die Erfassung deines *So geht Geld*-Workshops bitten wir dich, das Formular über den QR-Code aufzurufen, auszufüllen und mit dem Klick auf „Submit“ abzuschicken.

Vielen Dank!

Dein So geht Geld-Projektteam

