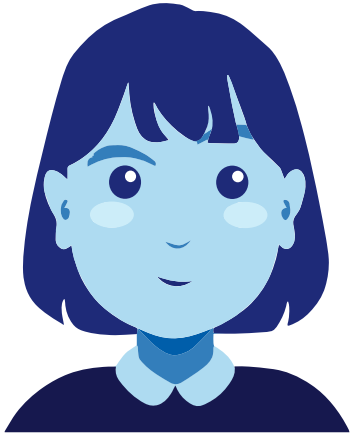
Gefahren im Netz

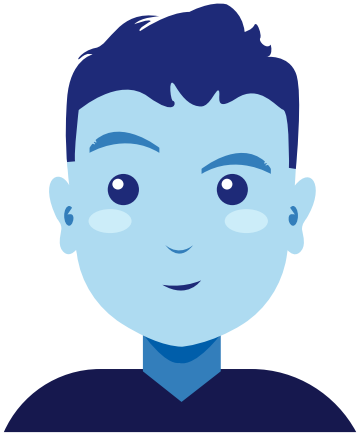
Cyberkriminelle nutzen eine Vielzahl von Methoden



Du bist täglich knapp vier Stunden am Smartphone. Apps wie WhatsApp, Gaming und Social Media verbinden dich – aber 70 Prozent der Jugendlichen hatten letztes Jahr ein Online-Risiko, wie verdächtige Nachrichten oder Verkaufsangebote.

Cyberkriminelle nutzen deine Zeit Online aus, sie stehlen Daten, infizieren Geräte, täuschen dich oder hacken Konten. Motive: Geld (z. B. durch In-Game-Käufe), Erpressung oder Angeberei.

Und deine Daten werden oft im Darknet verkauft – sei kein leichtes Ziel!



Daten und Identitäten stehlen

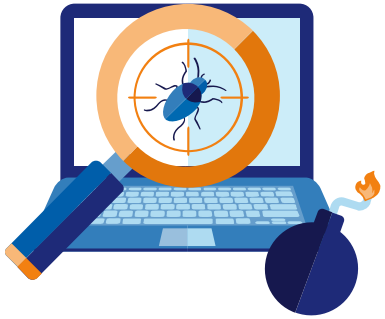
Diebstahl von Namen, Passwörtern, Adressen, Bildern

Über Social Media, Streaming, Grooming oder KI-Deepfakes persönliche Infos erlangen.

Menschen täuschen

Betrug durch gefälschte Inhalte und Angebote

Phishing-Mails, Fake-Gewinnspiele, falsche Profile, Telefon-Anrufe als „Support“ oder Vertrauensbetrug, um Klicks oder Zugangsdaten zu ergaunern.



Geräte infizieren

Installation von Spyware oder Trackern

Durch unbekannte Apps, verseuchte Anhänge/Links, unsichere Downloads oder öffentliches WLAN (ohne VPN).

Konten hacken

Knacken des Zugangs zu Accounts

Über schwache/wiederverwendete Passwörter, „Login mit Social Media“ oder geklaute Codes (z. B. in Spielen, E-Mail, Banking) – oft gefolgt von Erpressung.

So schützt du dich

Die besten Tipps gegen Cyberbedrohungen

Nummer gegen Kummer: 116 111 Reden hilft – für neue Perspektiven bei Mobbing

Bei Problemen
kostenlos und anonym

JUUUPORT.de: Jugendliche beraten Jugendliche

Hilfetelefon Sexueller Missbrauch: 0800 22 55 530

HateAid.org: Melde Hass und schütze Dich mental - Beratung per Telefon (030 25 208 838) oder E-Mail (beratung@hateaid.org)

Cyber-Mobbing Erste-Hilfe App (klicksafe.de)
Videos/Tutorials zu Melden/Blocken auf Plattformen wie Instagram/TikTok

01 | Starke Passwörter und MFA
20-25 Zeichen/Passphrase, einzigartige Passwörter pro Dienst, Passkeys für mehr Sicherheit einsetzen

02 | Geräte schützen
PIN/Biometrie und Auto-Sperre einrichten, Geräte nie unbeaufsichtigt lassen, regelmäßig aktualisieren

03 | Verdächtige Nachrichten meiden
Keine Links/Anhänge aus verdächtigen Nachrichten öffnen – direkt zur bekannten App oder Seite navigieren

04 | Persönliche Daten schützen
Keine Adresse/Schulinfos/Fotos versenden, die nicht öffentlich sein sollen

05 | Apps sorgfältig auswählen
Downloads nur aus offiziellen Stores, Vorsicht vor Fake-Shops, nicht-vertrauenswürdige Quellen vermeiden

06 | Öffentliches WLAN nur in Ausnahmefällen
Idealerweise nur mit VPN-Verbindung nutzen

07 | Gefälschtes erkennen
KI-Antworten hinterfragen, Deepfakes nicht verbreiten

08 | Social Media bewusst nutzen
Hohe Privatsphäre-Einstellungen, nur echte Freunde, keine Standorte teilen – respektiere Meinungen anderer

09 | Sicheres Gaming
Keine Free-Skins-Links, keine privaten Infos in Spielen oder Streams zeigen (via Webcam) oder teilen

10 | Instinkt folgen
Bei Druck/Mobbing: Eltern, andere Vertrauenspersonen oder Helplines einbeziehen, Zugangsdaten zu betroffenen Accounts ändern