

4

Lügner und Betrüger im Internet



In diesem Lernmodul erfährst du,

- dass im Internet nicht jeder nett und ehrlich ist,
- dass es verschiedene Typen von Lügner und Betrügern gibt,
- dass du nicht alles glauben solltest, was im Internet behauptet wird und
- was Kettenbriefe sind.

Scanne den QR-Code und bearbeite die Lernthemen so weit, wie du es zeitlich schaffst:

<https://www.internet-abc.de/lm/luegner-und-betrueger-im-internet/einfuehrung/1>



Achtung! Bei der Abfrage: „Möchtest Du das Lernmodul von Beginn an spielen?“ auf NEIN klicken!

Am Ende spielst du dieses Kahoot-Quiz (als Gast):
<https://create.kahoot.it/share/lugner-und-betrueger/af6d1bbc-8eb7-4fa8-aaa5-25d1c7399d1a>



Wenn da was nicht klappt, kannst Du auch das Quiz
zum Lernmodul spielen:
<https://www.internet-abc.de/lm/luegner-und-betrueger-im-internet/abschlussquiz/1>



Station 4: Lügner und Betrüger im Internet - wie kann ich mich schützen?

- Auf einer **sicheren Website** werden Daten verschlüsselt übertragen, sodass sie nicht von Fremden ausgenutzt werden können. Solche Webseiten erkennst du an dem https-Protokoll. Beginnt die Webseiten-URL mit „https://“, wird eine sichere Verbindung garantiert.

- **Spam-Mails** ahmen oft sehr überzeugend richtige E-Mails eines bestimmten Anbieters nach. Allerdings würden dich die meisten großen Internetdienste wie Google, Facebook oder Amazon in einer E-Mail nie nach deinen Account Daten fragen. Daher solltest du nicht auf diese Links klicken und keine Daten preisgeben. Am besten ignorierst du diese Emails und leitest sie auch niemand anderen weiter, sodass andere nicht auf dem Link drauf gehen.

- Ein **Virenschutzprogramm** ist die Grundlage für sicheres Surfen. Halte den Schutz durch regelmäßige Updates aktuell, so schützt du dich vor vielen Gefahren des Internets. Es ist wichtig, beim Surfen stets aufmerksam zu sein: Am besten rufst du nur Webseiten auf, die sicher verschlüsselt sind – das erkennst du an dem kleinen „Schloss“-Icon in der Eingabezeile.

- **Clickbait** ist eine besonders auffällige oder ungewöhnliche Überschrift oder Bilder die Neugier von Nutzern wecken soll. Sie soll dich dazu bringen, das Video anzuklicken.

- Du möchtest vielleicht nicht, dass jeder deine besuchten Webseiten sehen kann. Also **lösche einfach Cache, Cookies und Verlauf**: Im Cache speichert dein Browser besuchte Webseiten zeitweise ab, damit sie später schneller wieder angezeigt werden können. Cookies sind Textdateien mit Nutzerdaten, die Webseiten auf deinem Gerät anlegen. Und im Browserverlauf werden alle besuchten Seiten gezeigt.
(Wie es funktioniert, verraten dir die Medienscouts oder du recherchierst dazu im Netz.)

- Auch **bei Computerspielen** und online Games kommt **Datenklau** vor und es werden **Viren verbreitet** werden. Um das zu verhindern, sollte man nicht auf Anzeigen klicken, die im Spiel angezeigt werden. Diese Anzeigen können aber auch während eines Spieles auftauchen. Man sollte sie also auch da durchlesen und wegklicken, als sie einfach zu akzeptieren.

- Um sich **bei Online-Spielen** zu schützen, sollte man bei der Erstellung eines Benutzernamens nicht seinen richtigen Namen eingeben oder irgendwelche persönlichen Daten, so verhindert ihr, dass eure Daten geklaut werden.

- Sein **Passwort** mit anderen zu teilen, kann dazu führen, dass andere Zugriff auf euren Account bekommen und mit dem Account alles Mögliche anstellen. Um euch zu schützen, solltet ihr also euer Passwort nicht mit anderen teilen.

Bildnachweise:

https://de.freepik.com/vektoren-premium/internet-kriminalitaetskonzept-vektor-illustration_3697864.htm

<https://www.dresden-online.de/files/dresden-online/news/wirtschaft/abzocke-im-internet.jpg>