UNTERRICHTSIMPULS

Thema: Medien
Klassenstufe: 3 bis 6

Deine Daten sind Gold wert!

Persönliche Daten sind das neue Gold – sie machen uns wertvoll, aber auch verletzlich.

Daten in einer digitalen Welt

Besonders für Kinder, die zunehmend das Internet nutzen, ist ein verantwortungsvoller Umgang mit persönlichen Daten von großer Bedeutung.

Kinder nutzen bereits in jungen Jahren das Internet, um Spiele zu spielen, mit Freunden zu kommunizieren, in Online-Shops einzukaufen oder durch soziale Medien zu surfen. Die KIM-Studie 2022 zeigt, dass bereits über 80% der 6- bis 12-Jährigen regelmäßig das Internet nutzen. Sie stoßen dabei auf Werbung, die oft genau auf ihre Interessen zugeschnitten ist, oder auf Influencer*innen, die Produkte bewerben.

Viele Kinder haben bereits Erfahrungen mit In-App-Käufen gemacht oder wurden mit verlockenden Angeboten via SMS oder WhatsApp konfrontiert, die ihre Daten erfordern. Diese frühe Online-Präsenz macht es umso wichtiger, sie frühzeitig über den Wert ihrer Daten und die Risiken im Internet aufzuklären. Kinder interagieren auf Plattformen, die gezielt auf sie zugeschnittene Angebote und Werbung präsentieren, und teilen oft Informationen über soziale Medien, ohne die Tragweite ihrer Handlungen zu erkennen.

Besonders durch die Nutzung sozialer Netzwerke wie TikTok, Instagram oder YouTube, wo sie Inhalte teilen und liken, können sie leicht persönliche Informationen preisgeben, die für Dritte interessant sind. Der bewusste Umgang mit Daten sollte daher gefördert werden.

Bezug zu den Rahmenlehrplänen

Der Unterrichtsimpuls passt in die Themenfelder der Fächer Sachunterricht, Gesellschaftswissenschaften und Medienkompetenz der Klassenstufen 3 bis 6. Die Auseinandersetzung mit dem Thema Datensicherheit wird im Rahmenlehrplan als Bestandteil der Medienbildung und der Förderung der Selbstständigkeit im digitalen Umfeld vorgesehen. Ziel ist es, dass die Schüler*innen die Bedeutung des verantwortungsvollen Umgangs mit persönlichen Daten verstehen und lernen, wie sie sich vor Missbrauch schützen.

Der Unterrichtimpuls

Die Unterrichtsidee umfasst drei Phasen: Zunächst werden die Schüler*innen dafür sensibilisiert, welche persönlichen Daten im Internet preisgegeben werden. Anschließend folgt eine praktische Übung, in der sie typische Phishing-Nachrichten erkennen und darauf reagieren. Abschließend werden die Ergebnisse ausgewertet und Maßnahmen zur Sicherung persönlicher Daten diskutiert.

Unterrichtsverlauf

Phase 1: Sensibilisierung

Starten Sie die Unterrichtseinheit mit einem Brainstorming „Digitale Fußspuren“, indem sie die Schüler*innen fragen: „Welche Informationen sind über euch im Internet zu finden?“ Die Antworten der Kinder werden auf einem Flipchart gesammelt (z. B. Name, Fotos, Spiele, die sie spielen, YouTube-Kanal, Einkäufe in Online-Shops, Posts auf sozialen Medien). Danach wird erklärt, dass diese Informationen wie ein digitaler „Schatz“ sind – wertvoll nicht nur für Unternehmen, sondern auch für Betrüger*innen, die versuchen, an diese Daten zu kommen. Erklären Sie, dass es sich hierbei um personenbezogene Daten handelt. Informationen, wie diese Daten missbraucht werden, finden Sie am Ende.

Sozialform: Plenum | **Material:** Tafel/Flipchart | **Zeit:** 15 Minuten

Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen. Dazu gehören z. B.: Name und Vorname, Privatanschrift, E-Mail-Adresse, Kontonummer, Ausweisnummer, Standortdaten etc.

Phase 2: Erarbeitung

Für die Aufgabe „Phishing-Falle“ werden die Schüler*innen in Kleingruppen aufgeteilt. Jede Gruppe bearbeitet eine typische Phishing-Situation, z. B. eine E-Mail von einem vermeintlichen Spieleentwickler, der nach dem Passwort fragt, ein Angebot aus einem Online-Shop, das nach persönlichen Daten fragt, oder ein Pop-up-Fenster, das verspricht, dass man etwas gewonnen hat, wenn persönliche Informationen angegeben werden. Teilen Sie dazu die Phishing-Situationen (→ Kopiervorlage) an die Gruppen aus.

Teilen Sie zusätzlich das → Arbeitsblatt 1 aus. Die Schüler*innen lesen die jeweilige Situation in ihrer Gruppe und diskutieren, welche Anzeichen darauf hinweisen könnten, dass es sich um Phishing handelt (z. B. unpersönliche Ansprache, ungewöhnliche Aufforderungen). Sie notieren ihre Beobachtungen auf einem Blatt Papier. Anschließend entscheiden die Gruppen gemeinsam, ob sie auf die Nachricht reagieren würden oder nicht und begründen ihre Entscheidung.

Jede Gruppe stellt ihr Szenario der Klasse vor, erklärt die Entscheidung und weist auf die Phishing-Merkmale hin, die sie erkannt haben.

Sozialform: Gruppenarbeit | **Material:** Arbeitsblätter | **Zeit:** 30 Minuten

Phase 3: Auswertung/Sicherung

Diskutieren Sie mit der ganzen Klasse die verschiedenen Phishing-Szenarien und sammeln Sie die häufigsten Anzeichen für Phishing an der Tafel. Dies hilft den Schüler*innen, ein besseres Verständnis für die typischen Gefahren zu entwickeln. Im Plenum wird eine Liste mit Sicherheitstipps erstellt, wie man persönliche Daten schützen kann (z. B. starke Passwörter verwenden, keine Passwörter teilen, bei unbekannten Nachrichten skeptisch sein, keine persönlichen Daten in sozialen Medien teilen, Angebote aus Online-Shops kritisch hinterfragen). Weisen Sie darauf hin, dass hinter vielen dieser Angebote Kostenfallen stecken. Lassen Sie zur Ergebnissicherung Plakate für das Klassenzimmer in Kleingruppen erstellen.

Sozialform: Plenum | **Zeit:** 45 Minuten

Kopiervorlage: Phishing

Gewinnspiel-Nachricht

Herzlichen Glückwunsch! Du hast einen 50 € Gutschein für dein Lieblings-Online-Spiel gewonnen. Klicke hier und gib die Nummer von deinem Bankkonto ein, um den Preis zu erhalten!

Freundschaftsangebot

Hey, ich habe dein Profil gesehen und möchte gerne mehr über dich erfahren. Kannst du mir deine Handynummer geben?

Nachricht Freund

Hey, ich bin es, Tom! Mein Account ist gesperrt und ich brauchen dringend deinen Hilfen. Kannst du mir bitte dein Passwort geben?

Spieleangebot

Exklusiv: Hol dir die neusten Skins für dein Spiel – kostenlos für die ersten 100 Nutzer! Trag einfach deine E-Mail-Adresse und dein Alter ein, damit wir deine Daten prüfen können.

SMS schicken

Schicke eine SMS an diese Nummer, um Superkräfte in deinem Lieblingsspiel freizuschalten! Diese SMS ist kostenlos und du kannst so viele schicken, wie du möchtest.

Sicherheitswarnung

Dein Spielekonto wurde gesperrt. Um es wieder zu aktivieren, klicke auf den Link und gib deine Zugangsdaten ein.

Geheime Spiel-Levels

Um Zugriff auf geheime Spiel-Levels zu bekommen, trage deine Kontodaten ein! Du wirst überrascht sein, wie viel du dadurch freischalten kannst!

Spiele-Angebot

Erhalte 1.000 kostenlose Spielmünzen! Wir brauchen nur kurz deine Login-Daten, um sie deinem Konto gutzuschreiben.

Pop-up

Du hast ein neues Smartphone gewonnen! Gib deine Adresse und Kreditkartendaten ein, damit wir es dir zuschicken können.

Name _____

Klasse _____

Medien

Arbeitsblatt 1: Online-Betrug

1. Lest die Nachricht und markiert die verdächtigen Teile (z. B. Versprechen von Gewinnen, Aufforderung zur Eingabe persönlicher Daten wie Namen, Adresse, Passwort).

2. Notiert drei Maßnahmen, die ihr anwenden könnt, um eure Daten sicher zu halten.

- _____
- _____
- _____

3. Schätzt euch selbst ein: „Was mache ich schon richtig, um meine Daten zu schützen, und was könnte ich verbessern?“

_____

_____

_____

_____

4. Und hier noch ein kleiner Tipp für ein starkes Passwort: Denkt euch einen Satz aus, in dem auch eine Zahl und ein Satzzeichen vorkommt und den ihr euch gut merken könnt. Nehmt jeweils den ersten Buchstaben, die Zahl und das Satzzeichen – fertig ist das Passwort.

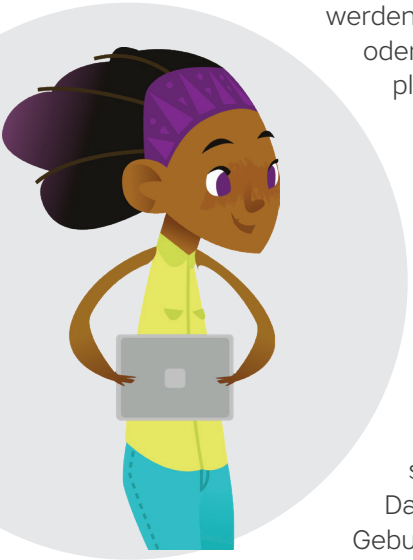
Gut, dass ich 3 Freunde habe!
G,di3Fh!

Missbrauch von Daten

Wer die Wahl hat, hat die Qual – heißt es. Besonders bei der Wahl der richtigen Passwörter tun sich viele Internetnutzer*innen schwer. Wen wundert‘s da, dass schlecht gewählte Passwörter wie „123456“ oder „qwert“ auf der Hitliste besonders häufiger IT-Sicherheitsdefizite ganz weit oben stehen?
(Bundesamt für Sicherheit in der Informationstechnik)

Personalisierte Werbung

Personenbezogene Daten, wie Name, Alter oder Interessen, werden oft für Werbezwecke genutzt, indem Unternehmen damit gezielte Werbung schalten. Sie analysieren unser Verhalten online, um Vorlieben zu erkennen und uns passende Anzeigen zu zeigen. Dies kann auch missbraucht werden, wenn Daten ohne Zustimmung gesammelt oder weiterverkauft werden, um uns zu beeinflussen oder manipulative Werbung zu platzieren, die uns zum Kauf verleiten soll.



Datenbetrug

Personenbezogene Daten können für Betrug eingesetzt werden, indem Betrüger*innen diese Informationen nutzen, um sich als jemand anderes auszugeben. Zum Beispiel können sie gestohlene Daten wie Namen, Adressen, Geburtsdaten oder Bankinformationen verwenden, um Identitätsdiebstahl zu begehen. Das bedeutet, sie können Konten eröffnen, Kredite beantragen oder Käufe im Namen der betroffenen Person tätigen. Auch gezielte Phishing-Angriffe, bei denen Betrüger*innen Opfer zur Preisgabe weiterer sensibler Daten verleiten, basieren oft auf bereits erlangten persönlichen Informationen, um glaubwürdiger zu wirken.

Weitere Beispiele für Datenbetrug sind:

- **SIM-Swapping**: Dabei übernehmen Betrüger*innen die Kontrolle über die Mobiltelefonnummer eines Opfers, indem sie die SIM-Karte auf eine andere Karte umschreiben lassen. Dadurch können sie Zugang zu SMS-basierten Sicherheitscodes erhalten und so auf Bankkonten oder andere gesicherte Dienste zugreifen.
- **Kontoübernahme**: Betrüger*innen nutzen gestohlene Zugangsdaten, um sich in Online-Konten wie E-Mail, soziale Netzwerke oder Online-Shopping-Plattformen einzuloggen. Sie können dadurch persönliche Daten ausspionieren, betrügerische Transaktionen tätigen oder die Identität der betroffenen Person missbrauchen.
- **Fake-Profile** in sozialen Netzwerken: Betrüger*innen erstellen gefälschte Profile, um das Vertrauen von Freunden oder Familienmitgliedern zu gewinnen. Sie nutzen diese Fake-Profile, um Geld zu erbitten oder weitere persönliche Informationen zu sammeln, die sie dann für weitere Betrügereien einsetzen können.

Die Beispiele zeigen, dass man vorsichtig mit der Weitergabe personenbezogener Daten umgehen sollte, besonders online. Misstrauen Sie unerwarteten Anfragen nach persönlichen Informationen, nutzen Sie sichere Passwörter und aktivieren Sie die Zwei-Faktor-Authentifizierung, um sich vor Betrug zu schützen.

Impressum

1. Auflage, Hamburg 2024

Verantwortlich: finlit foundation gGmbH
Steindamm 71, 20099 Hamburg
Telefon: +49 40 2850 2597
info@finlit.foundation
www.finlit.foundation

Konzeption und Umsetzung: Helliwood media & education im fjs e. V., Berlin

Bildnachweis: shutterstock.com – insbesondere Macrovector und drumcheg