G'SCHEIT GEPRÜFT

Powered by LIWEST

Verdächtige Links und Phishing	**Cybersecurity**
Sicheres Verhalten im Internet	**Checkliste für sichere Links**

Teil 1 - Blitzdiskussion: Was fällt dir auf?

Aufgabe: ***Zu Beginn der Einheit diskutierst du gemeinsam mit deiner Klasse verschiedene Nachrichten, die du hier siehst. Deine Lehrperson zeigt die Beispiele über den Beamer und stellt Diskussionsfragen an die Klasse. Zeige auf und sage deine Eindrücke und Meinungen, so zeigst du eine gute Mitarbeit!***

Beispiel 1: Postnachricht

- Was ist dein Eindruck von dieser Nachricht?
- Woran erkennst du die Gefahr?
- Was passiert wenn du klickst?
- Was tust du, wenn du diese Nachricht bekommst?

Beispiel 2: Private Nachricht

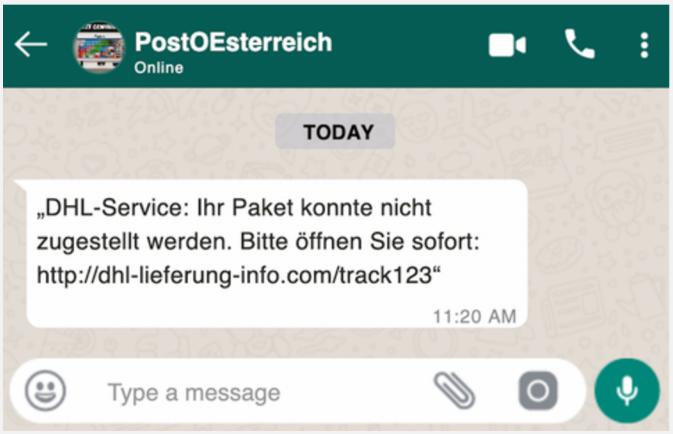
- Was ist dein Eindruck von dieser Nachricht?
- Woran erkennst du die Gefahr?
- Was passiert wenn du klickst?
- Was tust du, wenn du diese Nachricht bekommst?

Aufgabe: ***Lest euch nun gemeinsam als Klasse die Tipps zur Analyse der Beispiele durch. Melde dich zum laut Vorlesen für eine gute Mitarbeit!***

Beispiel 1: Postnachricht

Woran du es merkst:

- Absenderadresse sieht komisch aus (nicht @dhl.com).
- Dringender Ton: „sofort öffnen".
- Domain ist lang/ungewohnt statt der echten Firma.
- Rechtschreib-/Formatfehler möglich.



Was passiert, wenn du klickst:

- Meist führt die Seite zur Eingabe persönlicher Daten (Adresse, Kreditkarte) oder installiert Schadsoftware.

Sicheres Vorgehen:

- Nicht klicken. Öffne die echte DHL-Website oder die App selbst und gib dort die Sendungsnummer ein — oder frage die Eltern/Lehrkraft.

Beispiel 2: Private Nachricht

Woran du es merkst:

- Link ist verkürzt/ungewöhnlich.
- Nachricht kommt unerwartet, obwohl der Freund sonst so nicht schreibt.
- Wenn du den Freund fragst, sagt er, er hat nichts geschickt → Konto gehackt.

Was passiert, wenn du klickst:

- Seite fordert Login für Social Media (Phishing) oder verbreitet sich weiter, indem sie dein Konto nutzt.

Sicheres Vorgehen:

- Nicht klicken. Frag den Freund direkt (per Anruf oder persönlich). Ändere ggf. dein Passwort und aktiviere Zwei-Faktor-Auth, wenn nötig.

Teil 2 - Video: Verdächtige Links und Phishing

Als nächstes schaut ihr euch ein Video an, dass das Thema Phishing und verdächtige Links genauer erklärt. Um das Video für diese Einheit zu sehen und sie interaktiv zu gestalten, scanne den QR-Code und komm' in unser Online-Learning-System! Du kannst die Einheit aber auch ohne Video mit dieser PDF-Datei durchführen.

Teil 3 - Lesen & Verstehen: Übersicht und Merkmale

Aufgabe: ***Im Anschluss zum Video lest ihr euch diesen Text gemeinsam als Klasse mit der Lehrperson laut durch! Melde dich zum laut Lesen, für eine gute Mitarbeit!***

Geprüft – Klick nicht auf alles!

Im Internet gibt es viele Nachrichten, Links oder Postings, die auf den ersten Blick echt wirken, aber in Wirklichkeit eine Falle sind. Das nennt man Phishing. Das Wort kommt von „Fishing" = Angeln. Betrüger*innen werfen eine „Köder-Nachricht" ins Netz und hoffen, dass jemand darauf hereinfällt. Ziel ist fast immer, deine Daten oder dein Geld zu stehlen.

Phishing gibt es in vielen Formen:

- E-Mail-Phishing: Eine Mail sieht so aus, als wäre sie von deiner Bank oder einem Online-Shop. Darin steht oft, dass du sofort auf einen Link klicken musst, weil dein Konto gesperrt ist oder ein Paket nicht zugestellt werden konnte.
- SMS-Phishing (Smishing): Auch über SMS oder WhatsApp können solche Links verschickt werden. Besonders oft geht es um angebliche Lieferungen oder Gewinnspiele.
- Messenger-Phishing: Manchmal kommt eine Nachricht scheinbar von einem Freund, zum Beispiel: „Schau mal, das Video von dir 😂". In Wahrheit wurde das Konto gehackt, und der Link führt zu einer Fake-Seite.
- Phishing über Postings in sozialen Netzwerken: Auch Posts auf Instagram, TikTok oder Facebook können gefährlich sein. Zum Beispiel: „Gewinne ein neues iPhone – klicke hier und melde dich an!" Oft stecken gefälschte Gewinnspiele oder Fake-Umfragen dahinter, die nur deine Daten sammeln wollen.

Warum machen die das?

Die Betrüger*innen wollen damit Geld verdienen. Sie versuchen, deine Passwörter zu klauen, deine Kreditkarte zu belasten oder deine Accounts zu übernehmen. Mit gestohlenen Daten können sie dich oder andere täuschen, Dinge bestellen oder sogar deine Identität missbrauchen.

Was kann passieren?
Die Folgen sind oft unangenehm: Dein Konto könnte gesperrt werden, jemand könnte in deinem Namen Nachrichten verschicken oder deine Freund*innen mit demselben Trick reinlegen. Manche Links laden auch Viren herunter, die dein Handy oder deinen Computer langsamer machen und noch mehr Daten ausspionieren.
Wie kann ich mich schützen?
Die wichtigste Regel ist: Klicke nicht sofort! Nimm dir Zeit und prüfe die Nachricht.

- Absender checken: Kommt die Nachricht wirklich von der Person oder Firma? Oder wirkt die Adresse komisch?
- Sprache ansehen: Viele Fehler oder ein seltsamer Ton sind verdächtig.
- Links prüfen: Zeigt der Link wirklich auf die echte Website oder auf eine komische Adresse?
- Dringlichkeit hinterfragen: Betrüger*innen wollen immer, dass du sofort handelst.
- Bei Gewinnspielen oder Postings: Überlege, ob es wirklich realistisch ist, dass man einfach so etwas Teures gewinnt.

Und wenn du unsicher bist: Anhalten – Nachdenken – Löschen oder Fragen. Rede mit deinen Eltern, Lehrer*innen oder frag direkt bei der echten Firma nach.

Teil 4 - Analyse: Beispiele für unsichere Links

Aufgabe: ***Du wirst nun verschiedene Beispiele sehen für verdächtige Situationen im Internet. Deine Aufgabe ist es, diese Situationen zu analysieren. Die Aufgabe wird in Einzelarbeit gemacht. Halte dich bei deiner Analyse an die Leitfragen, die du schon im Teil 1 der Einheit gelernt hast und an das Beispiel. Fülle deine Antworten direkt in die Felder auf deinem Worksheet, dieses findest du auf der nächsten Seite. Am Ende der Unterrichtseinheit gibts du dein Worksheet bei deiner Lehrperson ab. Wenn du auf einem Blatt arbeitest, gibst du es händisch ab, wenn du digital arbeitest, speicherst du das Worksheet mit deinen Angaben und sendest es per E-Mail an deine Lehrperson! Warte damit aber bis zum Ende des vergleichens der Ergebnisse. Gehe jetzt auf die nächste Seite, um zu starten!***

ANALYSE

Gefährliche Links

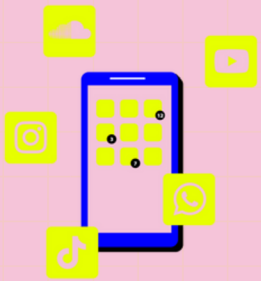
Dein Name:

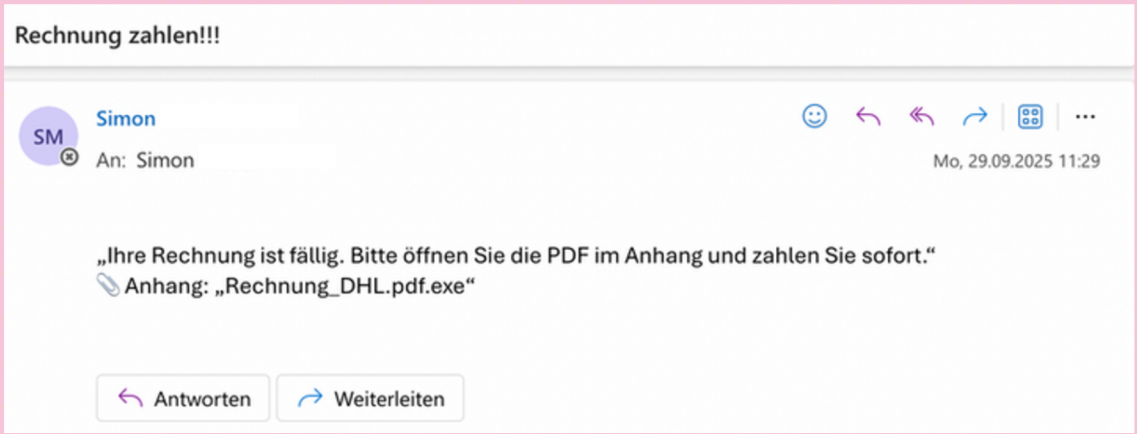
Deine Analyse:

Auf den ersten Blick klingt der Post spannend: Ein neues iPhone gewinnen, nur durch Folgen und Teilen. Doch schnell wird klar, dass etwas nicht stimmt. So teure Preise gibt es nicht ohne Grund, und es fehlen Infos über den echten Veranstalter.

Gefährlich ist vor allem der Link. Er führt auf eine unbekannte Seite, die wahrscheinlich persönliche Daten wie Name, Adresse oder Telefonnummer abfragt. Diese Daten können für Spam oder Betrug genutzt werden. Im schlimmsten Fall wird beim Klick sogar Schadsoftware installiert.

Die richtige Reaktion: nicht klicken, nicht teilen, sofort löschen oder ignorieren. Bei Unsicherheit besser eine erwachsene Person fragen oder auf der offiziellen Seite der Firma nachschauen.





Deine Analyse:

Dein Name:

Deine Analyse:

Deine Analyse:

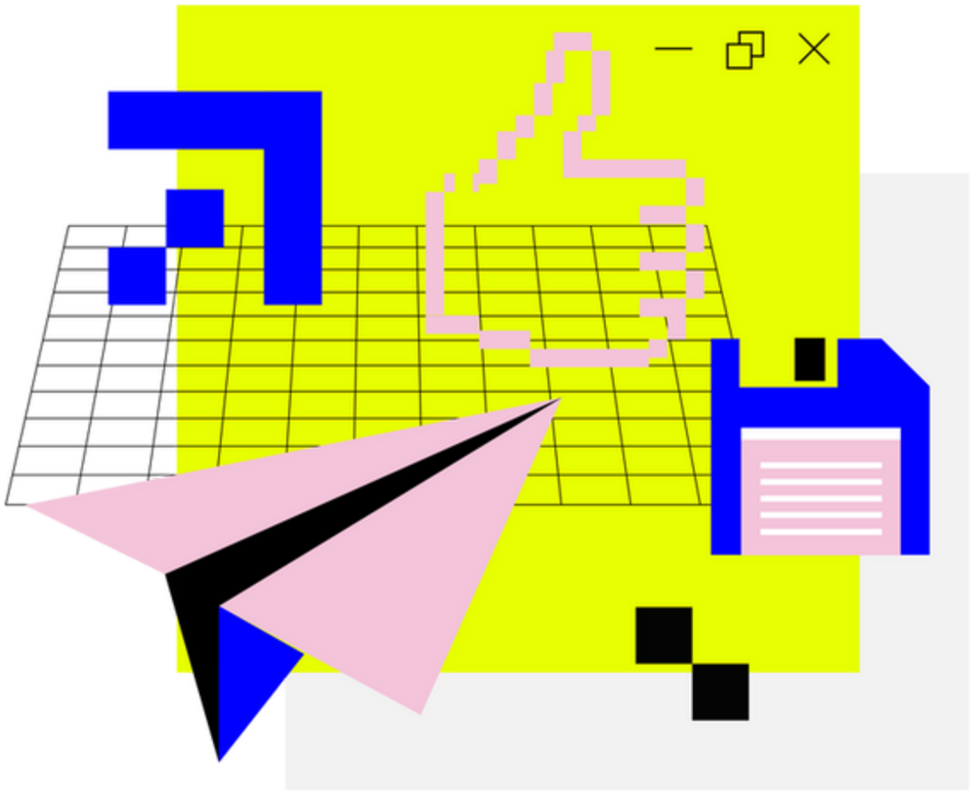
Du hast jetzt gesehen, wie verlockend und gleichzeitig gefährlich Phishing-Postings sein können. Sie wirken oft echt, versprechen aber Dinge, die nicht realistisch sind. Wichtig ist, dass du lernst, solche Nachrichten zu hinterfragen: Wer steckt dahinter? Wohin führt der Link? Macht das überhaupt Sinn? Wenn du unsicher bist, klicke nicht, sondern frage nach oder lösche die Nachricht. So schützt du dich und andere. Merke: Besser geprüft als geklickt!

Teil 5 - Vergleich: Ergebnisse

Aufgabe: ***Wenn alle Schüler*innen ihre Worksheets fertig haben, vergleicht ihr die Ergebnisse. Konzentriere dich dazu auf deine Lehrperson! Ihr werdet jedes Beispiel in der Klasse durchsprechen. Melde dich per Handzeichen, um deine Analysen vorzulesen, oder wenn du zu einer Analyse eines*r Mitschülers*in etwas sagen möchtest. Am Ende des Vergleichs gebt ihr eure Worksheets entweder händisch oder per Mail an eure Lehrperson ab!***

Teil 6 - Gruppenpuzzle: Checkliste für sichere Links

Aufgabe: ***Wenn alle Schüler*innen ihre Worksheets abgegeben haben startet ihr mit dieser Übung. Ihr erstellt gemeinsam als Klasse eine Checkliste für einen sicheren Umgang mit Links. Dazu haben alle Schüler*innen und die Lehrperson die Vorlage auf der nächsten Seite vor sich und ihr diskutiert gemeinsam darüber, welche Regeln ihr aufschreiben wollt. Geht auf die nächste Seite, um zu starten!***



Checkliste für sicheren Umgang mit Links

Regel 1

☐ „Klicke nur auf Links, die du kennst und denen du vertraust – im Zweifel: Anhalten, prüfen, fragen!“

Regel 2

☐

Regel 3

☐

Regel 4

☐

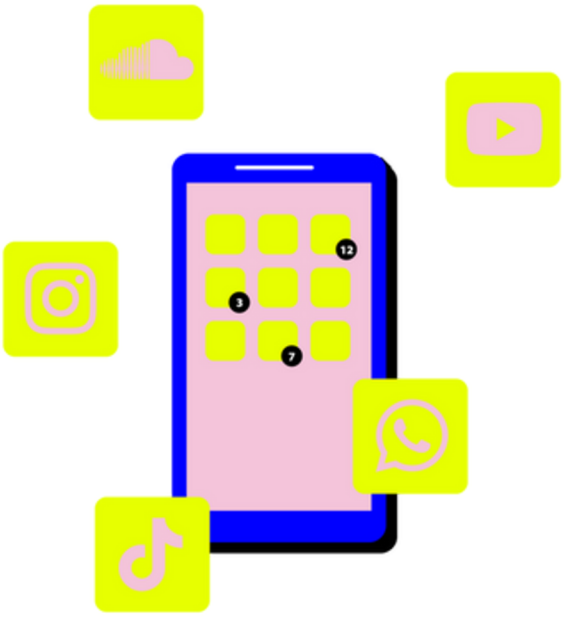
Regel 5

☐

Teil 7 - Abschluss: G’scheit geprüft

Aufgabe: ***Zum Abschluss der Unterrichtseinheit lest ihr gemeinsam diesen Text. Melde dich zum laut Vorlesen!***

Heute hast du gesehen, dass gefährliche Links und Phishing-Nachrichten ganz unterschiedlich aussehen können: als E-Mail von einer angeblichen Bank, als SMS mit einem Paketlink, als Nachricht von einem „Freund“ oder sogar als verlockendes Posting in sozialen Netzwerken. Sie wirken oft echt und bauen Druck auf – zum Beispiel mit Sätzen wie „Sofort klicken“ oder „Gewinne ein iPhone“. Doch dahinter steckt Betrug: Es geht immer darum, deine Daten oder dein Geld zu bekommen.
Wichtig ist, dass du die typischen Merkmale erkennst: ein komischer Absender, viele Fehler, seltsame Links oder unrealistische Versprechen. Wenn du so etwas entdeckst, hilft dir der einfache Notfallplan: Anhalten – Nachdenken – Löschen oder Fragen. So schützt du dich und verhinderst, dass Betrüger*innen Erfolg haben.
Merke dir: Es ist keine Schande, unsicher zu sein – wichtig ist, dass du nicht vorschnell klickst, sondern prüfst und im Zweifel jemanden um Rat fragst. Denn sicher im Netz bist du, wenn du Nachrichten kritisch hinterfragst und bewusst handelst. Besser geprüft als geklickt!



G’SCHEIT GEPRÜFT

Powered by LIWEST