

Digitale Selbstverteidigung Klasse

9/10: Angriffe erkennen

6 Lektionen · ca. 90 Minuten Unterricht · 15 Mitmach-Aufgaben · Stand: 01.11.2026

Fake-Profile, geklonte Stimmen, Betrug in Spielen, Datenschutz im Praktikum und Phishing, mit Praxistest zum Schluss.

So läuft der Kurs

Sie führen den Kurs an der Tafel und entscheiden selbst, wann Sie welche Lektion durchführen. Der Kurs läuft nicht ab. In diesem Kurs ist das Phishing-Training dabei: eine gute Gelegenheit, das Gelernte am eigenen Gerät im eigenen Postfach zu üben. Nur dafür trägt sich die Klasse in der ersten Stunde per QR-Code selbst ein; zum Mitmachen reicht der Vorname. Mitmach-Aufgaben schalten Sie einzeln frei: An der Tafel erscheint dazu ein QR-Code, die Klasse antwortet am Handy, und mit „Auflösen“ erscheint die richtige Antwort gleichzeitig an der Tafel und auf allen Handys. Den Lösungsschlüssel zu allen Quizfragen sehen Sie in Ihrem Cockpit; dieses offene PDF enthält ihn bewusst nicht, damit er nicht vorab bei der Klasse landet. Am Ende schließen Sie den Kurs ab und starten damit das Phishing-Training: drei simulierte Betrugsversuche per E-Mail über die folgenden Wochen. Teilnehmen kann nur, wer das Einverständnis der Eltern hat (Vorlage: Elternbrief) und eine E-Mail-Adresse hinterlegt. Das Zertifikat bescheinigt die erfolgreiche Teilnahme an diesem Training und wird nur bei Teilnahme ausgestellt.

Was Sie brauchen: Beamer oder Display mit Internetzugang, die Klasse mit Smartphones. Wer kein Handy dabei hat, macht mit der Sitznachbarin mit.

Bezug zum Bildungsplan Baden-Württemberg

Klassen 9 und 10 (etwa 14 bis 16 Jahre) · Umfang: zwei Doppelstunden plus Praxistest in den Wochen danach · Stand 03.10.2026

Angriffe erkennen: Fake-Profile und Social Engineering, Fake-Stimmen, Betrug in Spielen, Datenschutz im Praktikum und Phishing. Schließt mit dem Phishing-Praxistest ab, mit Einverständnis der Eltern. Handlungsfelder der Leitperspektive „Leben und Lernen in einer digitalisierten Welt“: Verantwortungsvoll handeln und schützen, Digital kommunizieren, kooperieren, handeln, Informationen sammeln, verstehen, bewerten.



Bereich	Kompetenz (Lesehilfe Informatik und Medienbildung 2026/27 bzw. Bildungsplan 2016)
Digitalität und Partizipation	Akteure und Interessen; Vertrauenswürdigkeit; Desinformation und Deepfakes Lektionen: Fake-Profile, Deepfakes und Fake-Stimmen
Leitperspektive Medienbildung	Jugendmedienschutz, Informationelle Selbstbestimmung und Datenschutz, Kommunikation und Kooperation
Aufbaukurs Informatik, 3.1.4 Informationsgesellschaft und Datensicherheit	(6) Anfall personenbezogener Daten, Nutzen und Risiken

Die Zuordnung ist eine fachliche Einschätzung des Anbieters, keine amtliche Freigabe. Für die Klassen 8 bis 10 gilt bis zum Inkrafttreten des Bildungsplans Informatik und Medienbildung (2027/28) der Bildungsplan 2016.

Überblick über die Lektionen

Lektion	Mitmach-Aufgaben
1. Fake-Profile, Catfishing und Social Engineering Klasse 9/10 · Digitalität und Partizipation Wie Betrüger sich als andere ausgeben und dich manipulieren wollen.	Quiz, Wortwolke, Quiz
2. Deepfakes und Fake-Stimmen: Trau nicht allem, was du siehst und hörst Klasse 9/10 · Digitalität und Partizipation Wie KI täuschend echte Videos und Stimmen fälscht und wie du dich nicht reinlegen lässt.	Quiz, Spiel: faktencheck
3. Gaming: Account-Diebstahl, Scams und wie du dich schützt Ergänzung · Praxis Betrug im Alltag Warum dein Gaming-Account wertvoll ist und wie Betrüger versuchen, ihn zu stehlen.	Wortwolke, Quiz
4. Datenschutz im Beruf: Warum Geheimnisse später Geld wert sind Ergänzung · Praxis Datenschutz (BP 2016, 3.1.4 (6)) Das Datenschutz-Spiel. Spuren in einem Profil finden und die Brücke ins Berufsleben schlagen.	Spiel: datenschutz, Spiel: orion, Quiz, Quiz
5. Phishing erkennen, auch wenn es nach deinem Lieblingsspiel aussieht Ergänzung · Praxis Phishing So erkennst du gefälschte Nachrichten und Links, bevor du draufklickst.	Quiz, Spiel: phishing-duell, Quiz



6.	Zusammenfassung: Dein digitaler Werkzeugkasten Ergänzung · Zusammenfassung Alles Wichtige auf einen Blick und Vorbereitung auf den Praxis-Phishing-Test.	Wortwolke
----	--	-----------

Auf den folgenden Seiten steht jede Lektion vollständig, mit allen Quizfragen und Antwortmöglichkeiten. Die markierten Lösungen finden Sie ausschließlich in Ihrem Cockpit.



1. Fake-Profile, Catfishing und Social Engineering

Wie Betrüger sich als andere ausgeben und dich manipulieren wollen.



Nicht jeder ist, wer er vorgibt zu sein

Du bekommst eine Freundschaftsanfrage von jemandem mit einem netten Profilbild, gemeinsamen Freunden und ähnlichen Interessen. Alles wirkt echt. Aber ist es das auch?





Was ist ein Fake-Profil?

Ein Fake-Profil ist ein Konto, das von jemandem erstellt wurde, der sich als eine andere Person ausgibt. Das passiert auf **allen** Plattformen:

- **Instagram:** Kopierte Profilbilder, erfundene Identitäten
- **Snapchat:** Accounts, die sich als Mitschüler ausgeben
- **Discord:** Fremde, die in Gaming-Servern Vertrauen aufbauen
- **TikTok:** Kommentare von Fake-Accounts, die auf andere Plattformen locken

Catfishing: Wenn jemand eine ganze Identität fälscht

Catfishing bedeutet, dass jemand über einen längeren Zeitraum eine falsche Identität aufbaut, oft mit gestohlenen Fotos, erfundenen Geschichten und viel Geduld. Das Ziel:

- **Persönliche Infos** herausbekommen (Adresse, Schule, Tagesablauf)
- **Vertrauen aufbauen:** um dann Geld oder Bilder zu fordern
- **Manipulation:** dich zu Dingen bringen, die du sonst nie tun würdest

Wichtig

Catfishing ist kein Einzelfall. Laut einer Studie hat jeder dritte Jugendliche bereits mit Fake-Profilen zu tun gehabt. Je jünger die Zielgruppe, desto aggressiver die



Social Engineering: Die Kunst der Manipulation

Social Engineering nennt man es, wenn jemand dich durch psychologische Tricks dazu bringt, etwas zu tun oder preiszugeben. Die häufigsten Hebel:

Trick	Beispiel
Zeitdruck	„Schnell, dein Account wird gleich gesperrt!"
Hilfsbereitschaft	„Kannst du mir kurz dein Passwort geben? Ich teste was."
Autorität	„Ich bin Admin dieses Servers, ich brauche deine Daten."
Neugier	„Schau mal, bist du das auf diesem Video?" + Link
Angst	„Ich habe Screenshots von dir. Bezahle oder ich poste sie."

Wie du dich schützt

- **Kein Fremder braucht dein Passwort.** Niemand. Kein Admin, kein Support, kein Freund
- **Gegencheck machen:** Kennst du die Person wirklich? Frag über einen anderen Kanal nach
- **Bilder prüfen:** Rechtsklick → Bildersuche. Gestohlene Profilbilder tauchen oft mehrfach auf
- **Keine privaten Bilder an Fremde:** auch nicht an „Freunde", die du nur online kennst
- **Blockieren statt diskutieren:** Wenn dir etwas komisch vorkommt, blockiere sofort

Tipp

Ein einfacher Test: Bitte die Person, in einem Videocall ein bestimmtes Wort auf einen Zettel zu schreiben und hochzuhalten. Fake-Profile scheitern daran zuverlässig.



Quiz: Echt oder Fake?

Jemand schreibt dir auf Instagram: „Hey, ich bin neu an deiner Schule und kenne noch niemanden. Magst du mir deine Nummer geben, damit wir uns verabreden können?“

Quizfrage

Was machst du?

Antwortmöglichkeiten

Nummer schicken, klingt nett

Nachfragen: „In welcher Klasse bist du?“ und bei Mitschülern gegenchecken

Ignorieren

Profil prüfen: Seit wann existiert es? Wie viele Posts und Follower hat es?

Wortwolke

Woran merkst du, dass ein Profil gefälscht sein könnte?

Quizfrage

Ein neues Profil schreibt dich an. Was macht dich misstrauisch?

Antwortmöglichkeiten

Wenige Beiträge, aber sehr viele Follower

Es will schnell auf einen anderen Messenger wechseln

Es hat ein Profilbild

Es fragt früh nach persönlichen Details

Alle Fotos sehen aus wie aus einem Katalog



2. Deepfakes und Fake-Stimmen: Trau nicht allem, was du siehst und hörst

Wie KI täuschend echte Videos und Stimmen fälscht und wie du dich nicht reinlegen lässt.



Wenn Augen und Ohren dich täuschen

Früher galt: Ein Video oder eine Sprachnachricht ist ein Beweis. Heute nicht mehr. Künstliche Intelligenz kann Gesichter und Stimmen so gut fälschen, dass man den Unterschied kaum noch sieht oder hört. Das nennt man **Deepfake** (gefälschtes Video/Bild) und **Voice-Cloning** (geklonte Stimme).





Wo dir das begegnet

- **Fake-Promi-Videos:** Ein Star oder Streamer bewirbt angeblich ein „Gratis-Gewinnspiel“ — in Wahrheit ein KI-Fake, der dich auf eine Betrugsseite lockt.
- **Geklonte Stimmen:** Aus ein paar Sekunden einer Sprachnachricht baut KI eine Kopie deiner Stimme. Dann ruft „dein Freund“ an und bittet dringend um Hilfe.
- **„Mama, ich hab ein neues Handy“:** Eine Nachricht oder ein Anruf mit vertrauter Stimme bittet um Geld oder ein Passwort. Ein uralter Trick, jetzt mit KI viel überzeugender.

Wichtig

Eine Stimme oder ein Gesicht ist **kein Beweis** mehr dafür, wer wirklich schreibt oder anruft. Verlass dich nicht darauf, sondern auf den Weg der Nachricht.

Woran du den Trick erkennst

Nicht am Aussehen, das wird immer besser. Sondern am **Ablauf**:

- Es ist plötzlich **super dringend**.
- Du sollst es **geheim halten** („sag es niemandem“).



- Es kommt über einen **ungewöhnlichen Weg**.

So schützt du dich

- **Codewort ausmachen:** Vereinbare mit Familie und Freunden ein geheimes Wort für den Notfall. Wer es nicht kennt, ist nicht echt.
- **Zurückrufen:** Über die Nummer, die du schon kennst, nicht über die aus der Nachricht.
- **Nichts glauben, nur weil es echt aussieht:** Bilder, Videos und Stimmen kann man fälschen.

Quizfrage

Du bekommst eine Sprachnachricht. Die Stimme klingt genau wie dein bester Freund und bittet dich dringend um dein Passwort. Was tust du?

Antwortmöglichkeiten

Passwort schicken, die Stimme stimmt ja

Über die bekannte Nummer zurückrufen oder persönlich nachfragen

Misstrauisch werden, wenn es „dringend“ ist und geheim bleiben soll

Sofort tun, was die Stimme sagt

Lernspiel

Echt oder gefälscht? Schaut euch gemeinsam Beispiele von Bildern, Videos und Nachrichten an und entscheidet, was echt ist und was nicht.



3. Gaming: Account-Diebstahl, Scams und wie du dich schützt

Warum dein Gaming-Account wertvoll ist und wie Betrüger versuchen, ihn zu stehlen.



Dein Account ist bares Geld wert

Du hast hunderte Stunden in dein Spiel investiert. Skins, Ränge, Items, vielleicht sogar seltene Cosmetics. Was du vielleicht nicht weißt: Auf dem Schwarzmarkt haben diese Accounts einen echten Geldwert. Ein Fortnite-Account mit seltenen Skins bringt 50-500 €. Ein CS2-Inventar mit Knife-Skins kann tausende wert sein.

Und genau deshalb sind Gaming-Accounts ein beliebtes Ziel.





Die häufigsten Betrugsmaschen

1. „Kostenlose V-Bucks / Robux / Coins“

Du siehst eine Webseite oder ein YouTube-Video, das kostenlose Spielwährung verspricht. Du musst „nur“ deinen Benutzernamen und dein Passwort eingeben. Was wirklich passiert: Dein Account ist weg.

Wichtig

Es gibt **keine** kostenlosen V-Bucks, Robux oder andere Spielwährung außerhalb der offiziellen Shops. Jede Seite, die das verspricht, ist Betrug.

2. Trading-Scams

„Ich tausche dir mein seltenes Item gegen deins.“ Der Handel wird gestartet, aber im letzten Moment wird das Item ausgetauscht oder der Trade manipuliert. Besonders verbreitet in: Rocket League, CS2, Roblox.

3. Fake-Support

Du bekommst eine Nachricht: „Dein Account wurde wegen Cheating gemeldet. Klicke



hier, um ihn zu verifizieren, sonst wird er gesperrt." Der Link führt auf eine gefälschte Login-Seite.

4. Phishing über Discord

„Hey, ich brauche noch einen für mein Team. Meld dich auf dieser Turnierseite an!“ Der Link sieht aus wie eine echte E-Sport-Plattform, ist aber eine Kopie, die dein Passwort abfängt.

Wie Angreifer an deinen Account kommen

Methode	Wie es funktioniert
Phishing-Link	Fake-Login-Seite, sieht echt aus
Passwort erraten	Weil du überall dasselbe verwendest
Session-Token stehlen	Über manipulierte Browser-Erweiterungen
Social Engineering	„Ich bin Mod, ich brauche deinen Login“

So schützt du dich

- **Zwei-Faktor-Authentifizierung (2FA) einschalten:** bei Steam, Epic, Riot, Blizzard, überall wo es geht
- **Einzigartiges Passwort** für jeden Gaming-Account
- **Niemals Login-Daten in Discord, Teamspeak oder Chat teilen**
- **Offizielle Links nutzen:** nicht über Google suchen, sondern die URL selbst eintippen
- **Browser-Erweiterungen prüfen:** nur installieren, was du wirklich brauchst

Tipp

Schalte 2FA ein. Jetzt. Ernsthaft. Es dauert zwei Minuten und macht deinen Account um ein Vielfaches sicherer. Bei Steam heißt es „Steam Guard“, bei Epic „Zwei-Faktor-Authentifizierung“, bei Riot „Authenticator App“.

Rätsel: Spot the Scam



Du bekommst diese Nachricht auf Discord von jemandem, den du aus einem Gaming-Server kennst:

„Ey, ich hab einen Sponsor für unser Team gefunden! Wir müssen uns nur alle auf dieser Seite registrieren: esport-turniere.net/anmelden. Mach schnell, die Plätze sind begrenzt!“

Wortwolke

Was sind die Warnsignale?

Quizfrage

Eine Seite verspricht dir kostenlose Spielwährung, wenn du dich einloggst. Was stimmt?

Antwortmöglichkeiten

Es ist immer Betrug

Es funktioniert manchmal

Dein Account ist danach weg

Auch die verknüpfte E-Mail-Adresse ist in Gefahr



4. Datenschutz im Beruf: Warum Geheimnisse später Geld wert sind

Das Datenschutz-Spiel. Spuren in einem Profil finden und die Brücke ins Berufsleben schlagen.



Von deinem Profil zum Betriebsgeheimnis

Bisher ging es um dich privat. Jetzt kommt der Teil, der dich später im Beruf einholt.

Wer im Praktikum, in der Ausbildung oder im ersten Job arbeitet, hat plötzlich Zugang zu Dingen, die ihm nicht gehören: Kundendaten, Preise, Konstruktionspläne, Krankenakten, Zugangsdaten. Angreifer nehmen sich dafür fast nie die Technik vor, sie nehmen sich **Menschen** vor. Und sie fangen genau da an, wo wir eben waren: beim öffentlichen Profil.

Wichtig

Die Masche ist immer dieselbe: erst sammeln, was öffentlich ist. Dann eine Nachricht schreiben, die genau dazu passt. Wer angesprochen wird, als würde man ihn kennen, prüft weniger.





Wie ein echter Angriff abläuft

1. Jemand findet heraus, wo du arbeitest, ein Foto im Firmen-Shirt reicht schon
2. Er sieht, wer dein Chef ist, wann Urlaubszeit ist, wie die Mailadressen aufgebaut sind
3. Dann kommt eine Mail: „Kurze Bitte, bin gerade im Zug, brauche das dringend“
4. Und weil alles stimmt. Name, Ton, Zeitpunkt, macht jemand es einfach

Das nennt sich Chef-Masche und kostet deutsche Betriebe jedes Jahr enorme Summen. Angefangen hat es mit öffentlich sichtbaren Informationen.

Das Datenschutz-Spiel

Deine Lehrkraft schaltet jetzt das Spiel frei. Ihr seht das öffentliche Profil einer erfundenen Person. Eure Aufgabe: Findet alles, womit ein Fremder etwas anfangen könnte.

Lernspiel

Freischalten, QR-Code projizieren. An der Tafel läuft mit, wer wie viel gefunden hat und



Ergänzung

Nach dem Spiel lohnt die Frage in die Runde: Welche dieser neun Angaben stehen bei euch selbst öffentlich? Erfahrungsgemäß wird es dann sehr still.

Und jetzt ins Büro: Operation ORION

Das Profil war privat. Jetzt dasselbe an einem Arbeitsplatz. In „Operation ORION“ schleicht ihr durch ein ganz normales Büro und sucht die Stellen, an denen ein Angreifer ansetzt: der Notizzettel am Monitor, das offene Postfach, der USB-Stick vom Messestand, das Meeting, in dem zu laut geredet wird.

Lernspiel

Etwa fünf Minuten pro Durchgang. Am Handy quer halten. An der Tafel sehen Sie, wer

Wichtig

Jede einzelne Fundstelle wirkt harmlos. Gefährlich wird die Summe: Ein Zettel plus ein offener Bildschirm plus ein mitgehörtes Meeting ergeben einen kompletten Zugang.

Was das für später heißt

- **Was dir nicht gehört, teilst du nicht:** auch nicht „nur kurz“ im Freundeskreis
- **Kein Firmenkram in privaten Chats:** keine Screenshots, keine Fotos vom Bildschirm
- **Zugangsdaten sind persönlich.** Wer seinen Login weitergibt, haftet für das, was damit passiert
- **Im Zweifel nachfragen:** über einen anderen Kanal, nicht per Antwort auf die Mail

Quizfrage

Du machst ein Praktikum. Was darfst du öffentlich posten?



Antwortmöglichkeiten

Dass du in einem Betrieb ein Praktikum machst

Ein Foto von deinem Bildschirm mit der Kundenliste

Den Zugangsnamen, den du bekommen hast

Dass dir die Arbeit Spaß macht

Screenshots aus dem internen Chat

Quizfrage

Eine Mail von „deinem Chef“: dringend, kurz, angeblich vom Handy, mit der Bitte um eine Überweisung. Was tust du?

Antwortmöglichkeiten

Sofort erledigen, es ist ja der Chef

Per Antwort auf die Mail nachfragen

Über einen anderen Weg nachfragen, zum Beispiel anrufen

Mit einer Kollegin oder einem Kollegen gegenlesen



5. Phishing erkennen, auch wenn es nach deinem Lieblingsspiel aussieht

So erkennst du gefälschte Nachrichten und Links, bevor du draufklickst.



Was ist Phishing?

Phishing ist, wenn jemand sich als jemand anderes ausgibt, um an deine Daten zu kommen. Meistens per E-Mail, aber auch per SMS, WhatsApp, Discord oder sogar als Nachricht in einem Spiel.

Der Name kommt von „fishing“ (Angeln), der Angreifer wirft einen Köder aus und wartet, bis jemand anbeißt.





So sieht Phishing in deinem Alltag aus

Beispiel 1. Die Steam-Falle:

„Dein Steam-Account wurde wegen verdächtiger Aktivitäten gesperrt. Verifiziere deine Identität innerhalb von 24 Stunden: steamcommunity.com/verify“

Siehst du den Fehler? Es heißt „steamcommunity“ statt „steamcommunity“. Ein Buchstabe Unterschied, aber du landest auf einer komplett gefälschten Seite.

Beispiel 2. Die Instagram-Nachricht:

„Hey, jemand hat ein Video von dir gepostet ☺ schau mal: bit.ly/3xK9mP“

Verkürzte Links verbergen, wohin sie wirklich führen. Und die Nachricht spielt mit Neugier und leichter Panik.

Beispiel 3. Die Spotify-Mail:



„Ihre Zahlungsmethode ist abgelaufen. Aktualisieren Sie Ihre Daten, um Ihren Account nicht zu verlieren.“

Spotify schickt solche Mails tatsächlich, aber die echte Mail verlinkt auf spotify.com, nicht auf spotify-account-update.com.

Die 5-Sekunden-Prüfung

Bevor du auf einen Link klickst, halte fünf Sekunden inne und prüfe:

1. **Wer schickt das?** Kenne ich die Person/Firma wirklich?
2. **Ist Zeitdruck dabei?** „Sofort“, „in 24 Stunden“, „jetzt“, das ist fast immer Manipulation
3. **Wohin führt der Link?** Mit dem Finger draufhalten (nicht tippen!) zeigt die echte URL
4. **Macht das Sinn?** Würde Steam/Instagram/Spotify mich so kontaktieren?
5. **Fragt es nach Zugangsdaten?** Echte Dienste fragen nie per Nachricht nach deinem Passwort

Wichtig

Kein seriöser Dienst schickt dir eine Nachricht mit einem Link, über den du dein Passwort eingeben sollst. Wenn du unsicher bist: Öffne die App oder Webseite direkt, nicht über den Link.

Was tun, wenn du draufgeklickt hast?

Es ist passiert, du hast auf einen Phishing-Link geklickt und vielleicht sogar Daten eingegeben. Kein Grund zur Panik, aber schnelles Handeln ist wichtig:

1. **Passwort sofort ändern:** beim betroffenen Dienst und überall, wo du dasselbe Passwort verwendet hast
2. **2FA einschalten:** wenn noch nicht geschehen
3. **Jemandem Bescheid sagen:** Eltern, Lehrkraft, IT-Verantwortliche. Es ist keine Schande, es ist ein Sicherheitsvorfall



4. **Bank informieren:** falls Zahlungsdaten betroffen sind

Tipp

Du hast nichts falsch gemacht, wenn du Phishing meldest. Du hast etwas falsch gemacht, wenn du es verschweigst. Melden hilft, dir und anderen.

Quiz: Phishing oder echt?

Ordne diese Nachrichten ein. Phishing oder echt?

1. E-Mail von Netflix: „Dein Abo wird morgen gekündigt. Klicke hier, um deine Zahlung zu aktualisieren.“
2. SMS von DHL: „Ihr Paket konnte nicht zugestellt werden. Zollgebühr: 1,99 €. Hier bezahlen.“
3. E-Mail von deiner Schule: „Die neuen AG-Termine sind online. Schau ins Schulportal.“
4. Discord-DM: „Ey, bist du das auf dem Bild??  [Link]“

Quizfrage

Welche dieser Nachrichten sind Phishing?

Antwortmöglichkeiten

- Netflix: Abo wird gekündigt, Zahlung aktualisieren
- DHL-SMS: Zollgebühr 1,99 € über einen Link bezahlen
- Schule: neue AG-Termine im Schulportal
- Discord-DM: „Bist du das auf dem Bild??“ mit Link

Lernspiel

Fünf Nachrichten, jeweils echt oder Fake. Nach dem Spiel die Merkmale an der Tafel durchgehen.

Quizfrage



Woran erkennst du eine Phishing-Nachricht am zuverlässigsten?

Antwortmöglichkeiten

Sie setzt dich unter Zeitdruck

Die Absenderadresse passt nicht zum angeblichen Absender

Sie ist auf Deutsch geschrieben

Sie fragt nach Passwort oder Zahlungsdaten

Sie hat ein Logo



6. Zusammenfassung: Dein digitaler Werkzeugkasten

Alles Wichtige auf einen Blick und Vorbereitung auf den Praxis-Phishing-Test.



Was du in diesem Kurs gelernt hast

Du hast jetzt das Wissen, um dich online deutlich besser zu schützen. Hier die wichtigsten Punkte zusammengefasst:

Deine Daten gehören dir.

- Du entscheidest, wer was sieht
- Öffentlich gepostete Daten lassen sich für Betrug und Manipulation nutzen
- Datenschutz ist ein Recht, kein Luxus

Social Media ist nicht dein Freund, es ist ein Geschäftsmodell.

- Die Apps sammeln mehr Daten, als du denkst
- Profil auf privat, Standort aus, Berechtigungen prüfen
- Nicht alles, was du online siehst, ist echt



Im Gaming steckt echtes Geld und echte Gefahren.

- Kostenlose Spielwährung gibt es nicht
- 2FA einschalten, einzigartige Passwörter nutzen
- Kein Link aus Discord oder Teamspeak ist zu 100 % vertrauenswürdig

Dein Handy verdient Schutz.

- PIN/Biometrie, Updates, App-Berechtigungen
- Offenes WLAN = offenes Buch
- Alte Apps löschen

Ein Passwort, ein Account.

- Passwort-Manager nutzen
- Zwei-Faktor-Authentifizierung überall einschalten
- Passwörter niemals teilen, auch nicht mit Freunden

Phishing erkennen = fünf Sekunden nachdenken.

- Wer schickt das? Wohin führt der Link? Gibt es Zeitdruck?
- Im Zweifel: nicht klicken, sondern die Seite direkt aufrufen
- Melden ist keine Schwäche, sondern schützt alle

Wichtig

Perfekte Sicherheit gibt es nicht. Aber mit dem, was du jetzt weißt, bist du **deutlich schwerer** zu täuschen als vorher. Und das ist der Punkt.





Und jetzt: der Praxis-Test

In den nächsten Tagen bekommst du **drei simulierte Phishing-Mails** an deine Schul-E-Mail-Adresse. Sie sehen echt aus, aber sie sind von uns.

Deine Aufgabe: **Erkenne sie und klicke nicht drauf.**

Dein Ergebnis bekommst du danach als persönlichen Bericht. Und: Es gibt kein „Durchfallen“. Wer auf eine Mail hereinfällt, lernt daraus. Wer keine öffnet, hat den Kurs bestanden.

Tipp

Wende die 5-Sekunden-Prüfung an. Bei jeder verdächtigen Mail. Ab jetzt. Nicht nur bei den Testmails.

Abschluss-Quiz: 10 Fragen, wie viele schaffst du?

1. Wie viele Passwörter solltest du insgesamt verwenden?
2. Was ist 2FA?



3. Was ist Catfishing?
4. Warum ist öffentliches WLAN gefährlich?
5. Was machst du, wenn du auf einen Phishing-Link geklickt hast?
6. Darf jemand ein Foto von dir posten, ohne dich zu fragen?
7. Was bedeutet Social Engineering?
8. Ab welchem Alter bist du in Deutschland strafmündig?
9. Was ist die sicherste Art, ein Passwort zu erstellen?
10. Was ist der wichtigste Tipp gegen Phishing?

Wer mindestens 7 richtig hat, ist gut gerüstet für den Praxis-Test.

Wortwolke

Was nimmst du aus diesem Kurs mit? Ein Wort genügt.

