

Digitale Selbstverteidigung für Schüler

10 Lektionen · ca. 90 Minuten Unterricht · 18 Mitmach-Aufgaben · Stand: 16.09.2026

Was du über Phishing, Social Media, Gaming und deine Daten wissen musst, damit du online sicher unterwegs bist.

So läuft der Kurs

Sie führen den Kurs an der Tafel und entscheiden selbst, wann Sie welche Lektion durchführen. Der Kurs läuft nicht ab. Die Klasse trägt sich in der ersten Stunde per QR-Code selbst ein; zum Mitmachen reicht der Vorname. Mitmach-Aufgaben schalten Sie einzeln frei, 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 Phishingtraining: Dafür brauchen die Teilnehmenden eine E-Mail-Adresse, nur wer eine hinterlegt hat, bekommt das Training und das Teilnahmezertifikat.

Was Sie brauchen: Beamer oder Display mit Internetzugang, die Klasse mit Smartphones. Wer kein Handy dabei hat, macht mit der Sitznachbarin mit; das Zertifikat können Sie später im Cockpit nachtragen.

Überblick über die Lektionen

Lektion		Mitmach-Aufgaben
1.	Einstieg: Was weiß das Internet über dich? Warum digitale Selbstverteidigung dich betrifft und was in diesem Kurs passiert.	Wortwolke, Quiz
2.	Social Media: Was deine Apps wirklich über dich wissen Instagram, TikTok, Snapchat: wie Plattformen deine Daten sammeln und nutzen.	Quiz
3.	Fake-Profile, Catfishing und Social Engineering Wie Betrüger sich als andere ausgeben und dich manipulieren wollen.	Wortwolke, Quiz

4.	Gaming: Account-Diebstahl, Scams und wie du dich schützt Warum dein Gaming-Account wertvoll ist und wie Betrüger versuchen, ihn zu stehlen.	Quiz
5.	Dein Smartphone absichern: PIN, Apps und Berechtigungen Warum dein Handy dein wichtigstes Gerät ist und wie du es richtig schützt.	Spiel: berechtigungen, Quiz
6.	Passwörter und Accounts: Was gehört dir und was teilst du nie Warum jedes Passwort einzigartig sein muss und was Zwei-Faktor-Authentifizierung bringt.	Spiel: passwort-knacker, Quiz
7.	Datenschutz im Beruf: Warum Geheimnisse später Geld wert sind Das Datenschutz-Spiel. Spuren in einem Profil finden und die Brücke ins Berufsleben schlagen.	Spiel: datenschutz, Spiel: orion, Quiz, Quiz
8.	Phishing erkennen, auch wenn es nach deinem Lieblingsspiel aussieht So erkennst du gefälschte Nachrichten und Links, bevor du draufklickst.	Spiel: phishing-duell, Quiz
9.	Deine Daten, deine Rechte: Was das Gesetz sagt Was Datenschutz mit dir zu tun hat und welche Rechte du hast.	Quiz
10.	Zusammenfassung: Dein digitaler Werkzeugkasten 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. Einstieg: Was weiß das Internet über dich?

Warum digitale Selbstverteidigung dich betrifft und was in diesem Kurs passiert.

Willkommen zur digitalen Selbstverteidigung

Bevor es losgeht, eine ehrliche Frage: Wie viel weiß das Internet eigentlich über dich? Vermutlich mehr, als du denkst und vor allem mehr, als du je bewusst hineingeschrieben hast.

Wortwolke

Was gehört für dich unbedingt privat?

Worum es in diesem Kurs geht

In den nächsten Stunden geht es nicht um Technik, sondern um dich: Wie Fremde an deine Daten kommen, was sie damit anfangen, und wie du das verhinderst. Wir schauen uns Social Media an, Gaming, dein Smartphone, deine Passwörter und ganz am Ende bekommst du unangekündigt ein paar gefälschte Mails, um zu sehen, ob es sitzt.

Wichtig

Alles, was du ins Internet stellst, kann von Fremden gefunden werden. Auch wenn du denkst, dass nur deine Freunde es sehen.

Warum das jetzt schon wichtig ist

Stell dir vor, jemand kennt deinen vollen Namen, deine Schule, dein Lieblingsspiel und den Namen deines Haustiers. Klingt harmlos? Mit diesen Infos kann jemand:

- Dein **Passwort erraten** (viele nutzen den Haustiernamen)
- Dir eine **gefälschte Nachricht** schreiben, die genau zu deinen Interessen passt
- Sich als **dein Freund ausgeben** und andere täuschen

Das ist keine Theorie, das passiert jeden Tag, tausendfach. Und genau deshalb bist du

hier.

Quizfrage

Welche dieser Informationen solltest du niemals öffentlich posten?

Antwortmöglichkeiten
Dein Lieblingslied
Deine Handynummer
Dein Geburtsdatum mit Jahrgang
Dein Lieblingsfilm
Deine Adresse
Der Name deiner Schule und deine Klasse

Tipp

Faustregel: Alles, womit jemand dich finden, kontaktieren oder sich als du ausgeben könnte, gehört nicht ins öffentliche Profil.

2. Social Media: Was deine Apps wirklich über dich wissen

Instagram, TikTok, Snapchat: wie Plattformen deine Daten sammeln und nutzen.

Dein Profil ist nur die Oberfläche

Du postest ein Foto, likest ein Reel, scrollst durch TikTok. Klingt harmlos. Aber hinter jedem Wisch sammeln die Plattformen Daten über dich, viel mehr, als du denkst.

Was Instagram, TikTok & Co. über dich speichern

Was du tust	Was die App speichert
Ein Reel anschauen	Wie lange du schaust, ob du weiterwischst oder nochmal schaust
Ein Foto posten	Standort, Uhrzeit, Gerätetyp, wer es sieht
Jemandem folgen	Dein soziales Netzwerk, wer kennt wen
In der App tippen	Auch nicht abgeschickte Texte werden teilweise erfasst
Dein Handy dabeihaben	Bewegungsprofil über Standortdaten

Wichtig

TikTok zum Beispiel erfasst laut eigener Datenschutzerklärung: Geräte-ID, IP-Adresse, Tastatureingaben, Browserverlauf innerhalb der App, biometrische Daten (Gesichts- und Stimmmerkmale) und Standort. Und das ist nur, was sie offiziell zugeben.

Warum ist das ein Problem?

1. Du bist das Produkt. Die Apps sind kostenlos, weil du mit deinen Daten bezahlst. Je mehr sie über dich wissen, desto gezielter können sie dir Werbung zeigen und desto mehr Geld verdienen sie.

2. Daten können gestohlen werden. Wenn eine Plattform gehackt wird, landen deine Daten im Darknet. Das ist bei TikTok, Facebook, Instagram und Snapchat bereits

passiert, mehrfach, mit Millionen von Accounts.

3. Dein digitaler Fußabdruck bleibt. Was du heute postest, kann in zehn Jahren noch auftauchen, bei einer Bewerbung, einem Stipendium oder einem Streit.

Was du tun kannst

- **Profil auf privat stellen:** bei Instagram, TikTok und Snapchat möglich
- **Standort deaktivieren:** die meisten Apps brauchen deinen Standort nicht wirklich
- **Berechtigungen prüfen:** braucht TikTok wirklich Zugriff auf deine Kontakte?
- **Regelmäßig alte Posts aufräumen:** was vor zwei Jahren lustig war, muss nicht für immer online sein

Tipp

Geh jetzt in die Einstellungen deines Handys → Apps → Berechtigungen. Schau dir an, welche App auf was zugreifen darf. Du wirst überrascht sein.

Rätsel: Daten-Detektiv

Jemand postet auf Instagram:

- Ein Selfie vor der Schule (Schulname auf dem Schild sichtbar)
- Story mit „Endlich 16! 🎉“ am 15. März
- Bio: „Gaming 🎮 | Mainz | @max_gamer auf Discord“

Welche Informationen könnte ein Fremder daraus zusammensetzen?

Quizfrage

Was sammelt eine Social-Media-App typischerweise über dich?

Antwortmöglichkeiten

Deinen Standort

Wie lange du welches Video anschaust

Dein Adressbuch, wenn du es erlaubst

Nur das, was du selbst postest

3. 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 Täter.

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?"

Was machst du?

- ☐ 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

4. 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!“

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

5. Dein Smartphone absichern: PIN, Apps und Berechtigungen

Warum dein Handy dein wichtigstes Gerät ist und wie du es richtig schützt.

Dein Handy ist der Schlüssel zu allem

Dein Smartphone ist nicht nur ein Telefon. Es ist dein Bankkonto, dein Postfach, dein Fotoalbum, dein Navi und dein Ausweis in einem. Wer Zugriff auf dein Handy hat, hat Zugriff auf dein komplettes digitales Leben.

Grundschutz: Sperre und Biometrie

Methode	Sicherheit	Empfehlung
Kein Sperrbildschirm	Keine	Niemals
Wischmuster	Sehr schwach (Fettspuren verraten das Muster)	Nein
4-stellige PIN	Schwach (10.000 Möglichkeiten)	Minimum
6-stellige PIN	Besser (1 Million Möglichkeiten)	Gut
Fingerabdruck	Stark + schnell	Empfohlen
Face ID / Gesichtserkennung	Stark (bei neueren Geräten)	Empfohlen

Wichtig

Die **häufigsten PINs** in Deutschland: 1234, 0000, 1111, 2580 (senkrechte Linie), Geburtsjahr. Wenn deine dabei ist: sofort ändern.

App-Berechtigungen: Wer darf was?

Jede App fragt nach Berechtigungen. Aber nicht jede braucht, was sie verlangt:

- **Kamera:** braucht Instagram, eine Taschenlampen-App aber nicht
- **Mikrofon:** braucht eine Sprach-App, ein Spiel aber nicht
- **Kontakte:** braucht WhatsApp, ein Wetterdienst aber nicht

- **Standort:** braucht Google Maps, ein Taschenrechner aber nicht

WLAN-Sicherheit: Offene Netze sind gefährlich

Kostenloses WLAN in der Bahn, im Café oder am Bahnhof klingt super. Aber in offenen Netzen kann jeder mitlesen, was du tust. Das nennt sich **Man-in-the-Middle-Angriff**: Jemand sitzt zwischen dir und dem Internet und liest mit.

Regeln für öffentliches WLAN:

- Kein Online-Banking, kein Login in wichtige Accounts
- VPN nutzen (es gibt kostenlose Varianten)
- Automatische WLAN-Verbindung deaktivieren

Tipp

Geh in deine WLAN-Einstellungen und lösche alle Netzwerke, die du nicht mehr brauchst. Dein Handy verbindet sich sonst automatisch mit jedem gleichnamigen Netzwerk und ein Angreifer kann ein „Starbucks WiFi“ leicht fälschen.

Updates: Die langweiligste Schutzmaßnahme und die wichtigste

Jedes Update schließt bekannte Sicherheitslücken. Wenn du Updates aufschiebst, lässt du eine Tür offen, von der Angreifer wissen, dass sie existiert.

- **Betriebssystem-Updates** sofort installieren
- **App-Updates** regelmäßig durchführen
- **Apps löschen:** die du nicht mehr nutzt: weniger Apps bedeutet weniger Angriffsfläche

Quiz: Wie sicher ist dein Handy?

Prüfe jetzt auf deinem Gerät:

1. Hast du eine PIN oder Biometrie aktiv? ☐ / ☐
2. Ist dein Betriebssystem auf dem neuesten Stand? ☐ / ☐
3. Hast du Apps installiert, die du seit Monaten nicht benutzt hast? ☐ / ☐
4. Nutzt eine App Berechtigungen, die sie nicht braucht? ☐ / ☐

Für jedes ☐ bei 1–2 und jedes ☐ bei 3–4 gibt es einen Punkt. Wer alle vier Punkte hat, ist gut aufgestellt.

Lernspiel

Sechs Apps, sechs Berechtigungen. Abstimmen lassen, dann an der Tafel vergleichen.

Quizfrage

Welche Berechtigung ist bei einer Taschenlampen-App auf jeden Fall verdächtig?

Antwortmöglichkeiten
Standort
Kontakte
Kamera-Blitz
Mikrofon

6. Passwörter und Accounts: Was gehört dir und was teilst du nie

Warum jedes Passwort einzigartig sein muss und was Zwei-Faktor-Authentifizierung bringt.

Dein Passwort ist dein Hausschlüssel

Stell dir vor, du hast einen Schlüssel, der deine Haustür, dein Schließfach, dein Fahrradschloss und deinen Spind aufschließt. Klingt praktisch, bis du ihn verlierst. Dann ist alles weg.

Genau das passiert, wenn du überall dasselbe Passwort verwendest.

Warum ein Passwort nicht reicht

Wenn eine Webseite gehackt wird (und das passiert ständig), landen die Benutzernamen und Passwörter im Darknet. Angreifer probieren diese Kombinationen dann automatisch auf hunderten anderen Seiten aus. Das nennt sich **Credential Stuffing**.

Wenn du also dasselbe Passwort bei Instagram, deiner E-Mail und deinem Gaming-Account verwendest und Instagram gehackt wird, dann sind **alle drei Accounts** gefährdet.

Wichtig

Die Regel ist einfach: **Ein Account, ein Passwort**. Kein Passwort darf bei zwei Diensten gleichzeitig im Einsatz sein.

Was ein sicheres Passwort ausmacht

Schlecht	Warum	Besser
MaxMustermann2009	Name + Geburtsjahr = erratbar	Korrekt-Pferd-Batterie-Hefter
123456789	Häufigstes Passwort der Welt	Zufällige Wörter kombinieren

Schlecht	Warum	Besser
Sommer2024!	Muster, das Millionen nutzen	Passwort-Manager nutzen

Ein gutes Passwort ist:

- Mindestens 12 Zeichen lang
- Nicht erratbar (kein Name, Geburtsdatum, Haustier)
- Einzigartig für jeden Account

Die einfachste Methode: Nimm vier zufällige Wörter und verbinde sie: „Giraffe-Klavier-Wolke-Sieben“. Lang, einprägsam, sicher.

Passwort-Manager: Dein digitaler Schlüsselbund

Ein Passwort-Manager speichert alle deine Passwörter verschlüsselt. Du merkst dir nur noch **ein** Master-Passwort. Der Manager generiert und füllt alle anderen automatisch aus.

Kostenlose Optionen: Bitwarden, KeePassXC, die Schlüsselbund-Funktion von Apple/Google.

Zwei-Faktor-Authentifizierung (2FA)

2FA bedeutet: Selbst wenn jemand dein Passwort kennt, braucht er zusätzlich einen zweiten Faktor, meistens einen Code auf deinem Handy.

Wo du 2FA sofort einschalten solltest:

1. Deine E-Mail (die ist der Schlüssel zu allen anderen Accounts)
2. Deine Gaming-Accounts (Steam, Epic, Riot)
3. Social Media (Instagram, TikTok, Snapchat)
4. Alles, was mit Geld zu tun hat

Was gehört dir und was teilst du nie

☐ Darfst du teilen	☐ Teilst du nie
Dein Gamertag	Dein Passwort

☐ Darfst du teilen	☐ Teilst du nie
Dein Lieblingsfilm	Dein Geburtstag mit Jahrgang
Dein öffentliches Profil	Deine Adresse
Screenshots (ohne sensible Daten)	Dein Ausweis / Schülerausweis
Dein Discord-Server	Dein E-Mail-Login

Tipp

Auch nicht mit deinem besten Freund. Freundschaften ändern sich. Passwörter, die du geteilt hast, kannst du nicht „zurücknehmen“. Und dein Freund kann unbeabsichtigt gehackt werden, dann hat der Angreifer auch deinen Zugang.

Rätsel: Passwort-Check

Welche dieser Passwörter sind sicher?

1. Fussball2009 → ☐ (Name + Geburtsjahr)
2. kT9\$mP2!xR4# → ☐ (zufällig, aber schwer zu merken)
3. Elefant-Ketchup-Trommel-42 → ☐ (lang, zufällig, merkbar)
4. IchLiebeDich → ☐ (unter den Top 20 der häufigsten Passwörter)
5. qwertz → ☐ (Tastaturmuster)

Lernspiel

Denkt euch ein Passwort aus und seht, wie lange es hält. Übertragen wird nur das Muster,

Quizfrage

Was macht ein Passwort wirklich stark?

Antwortmöglichkeiten

Länge

Ein Ausrufezeichen am Ende

Dass es nur für einen einzigen Dienst benutzt wird

Dass du es dir gut merken kannst, weil es dein Geburtstag ist

Dass es nirgends sonst vorkommt

7. 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

8. 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]“

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

9. Deine Daten, deine Rechte: Was das Gesetz sagt

Was Datenschutz mit dir zu tun hat und welche Rechte du hast.

Datenschutz ist nicht langweilig, er schützt dich

Wenn jemand ein Foto von dir macht und es ohne dein Okay postet, ist das nicht nur unhöflich, es ist in den meisten Fällen **illegal**. Die Datenschutz-Grundverordnung (DSGVO) und das Recht am eigenen Bild geben dir echte Rechte.

Deine wichtigsten Rechte

- 1. Recht auf Information:** Du darfst wissen, welche Daten ein Dienst über dich speichert. Bei Instagram, TikTok und Co. kannst du eine Kopie deiner Daten anfordern und wirst staunen, was da alles drin ist.
- 2. Recht auf Löschung:** Du kannst verlangen, dass deine Daten gelöscht werden. Das gilt auch für Fotos und Videos, die andere von dir gepostet haben.
- 3. Recht am eigenen Bild:** Niemand darf ohne deine Einwilligung Fotos oder Videos von dir veröffentlichen. Das gilt auch in der Schule, auf Partys und im Sportverein.
- 4. Recht auf Vergessenwerden:** Suchmaschinen müssen Links zu veralteten oder irrelevanten Informationen über dich auf Antrag entfernen.

Was andere nicht dürfen

Situation	Erlaubt?
Ein Mitschüler postet ein Foto von dir ohne zu fragen	☐
Jemand leitet deinen privaten Chat weiter	☐
Eine App gibt deine Daten an Werbenetzwerke weiter, ohne dich zu informieren	☐
Deine Eltern gucken auf dein Handy (du bist unter 18)	☐ Grauzone, hängt vom Alter und Kontext ab

Wichtig

„Ich hab doch nichts zu verbergen" ist kein Argument. Datenschutz bedeutet nicht, dass du etwas versteckst. Es bedeutet, dass **du entscheidest**, wer was über dich erfährt.

Was du tun kannst, wenn deine Rechte verletzt werden

1. **Die Person direkt ansprechen:** „Bitte nimm das Foto runter."
2. **Bei der Plattform melden:** Alle großen Dienste haben Melde-Funktionen
3. **Eltern oder Lehrkraft einschalten:** Besonders wenn es um Mobbing geht
4. **Offiziell beschweren:** Bei der Landesdatenschutzbehörde (kostenlos)

Tipp

Mach Screenshots als Beweis, **bevor** du die Löschung verlangst. Einmal gelöscht, lässt sich nichts mehr nachweisen.

Quiz: Deine Rechte

Stimmt das? Diskutiert in der Klasse.

1. „Wenn ich unter 16 bin, brauchen soziale Netzwerke die Zustimmung meiner Eltern."
2. „Was ich einmal im Internet gepostet habe, kann ich nie wieder löschen."
3. „Mein Lehrer darf mich im Unterricht ohne Erlaubnis filmen."
4. „Wenn ein Freund mein Passwort kennt und sich einloggt, ist das kein Hacking."

Quizfrage

Welche Rechte hast du gegenüber einem Anbieter, der Daten über dich gespeichert hat?

Antwortmöglichkeiten

Du darfst erfahren, was gespeichert ist

Du darfst Löschung verlangen
Du darfst falsche Angaben berichtigen lassen
Du musst dafür volljährig sein

10. 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.