FÜR LEHRKRÄFTE · MEDIEN & INFORMATIK KLASSE 6 BIS 8

# Lösungen und Erwartungshorizont

Lösungen zu allen Aufgaben der zehn Module und der Erwartungshorizont zu den sieben Schreibfeldern. Die Simulatoren (Angriffszeit, Passwort-Check) rechnen mit einer Million Versuchen pro Sekunde – die Zeiten der Klasse dürfen abweichen, die Größenordnung zählt.

## 1 · Live-Knacken

**Wie lange hält es?** (Zuordnung)

**1234** → unter 1 Sekunde · **hallo** → 12 Sekunden · **Ha7!** → 1 Minute · **Tr7!kelp** → 193 Jahre · **WolkeTanzt7Blau!** → mehr als eine Billion Jahre

**Was hat dich überrascht?** (Schreibfeld)

Offen. Typisch: „hallo123 ist sofort weg“, „ein Wort mit Zahl hält nur Sekunden“, „das lange Passwort hält Jahre, obwohl es keine Sonderzeichen hat“. Ziel: Länge und Mischung der Zeichen sind der Grund – nicht, wie geheim ein Wort klingt.

## 2 · Passwort-Check

**Eine Änderung, die zählt** (Auswahl)

1. Du darfst an deinem Passwort genau EINE Sache ändern. Womit gewinnst du am meisten Zeit? → **Vier Zeichen mehr anhängen.** – Länge zählt am meisten. Jedes zusätzliche Zeichen multipliziert die Möglichkeiten — vier mehr sind kein bisschen mehr Arbeit für dich, aber Millionen Mal mehr Arbeit für den Angreifer. Probier es im nächsten Modul aus.
2. Qwertz12! hat Groß- und Kleinbuchstaben, eine Zahl und ein Sonderzeichen. Warum ist es trotzdem schlecht? → **Weil „qwertz" eine Tastaturreihe ist, die zuerst drankommt.** – Genau. Ein Angreifer probiert nicht bei „aaaa" an — er fängt mit Listen an: Tastaturreihen, bekannte Wörter, geleakte Passwörter. Deshalb hat die Checkliste zwei Regeln, die gar nichts mit Zeichenarten zu tun haben.
3. Was ist eine Passphrase? → **Ein unsinniger Satz aus mehreren Wörtern als Passwort.** – Richtig. Sie ist lang — und Länge ist der stärkste Hebel. Wichtig ist nur, dass der Satz unsinnig ist: „IchLiebeMeineKatze" steht so ähnlich schon auf Leak-Listen.

## 3 · Kombinatorik

**Die Formel verstehen** (Auswahl)

1. Ein Passwort aus 4 Kleinbuchstaben. Wie viele Möglichkeiten gibt es? → **26 · 26 · 26 · 26 = 456.976** – Für jede Stelle gibt es 26 Möglichkeiten, und jede Stelle kommt zu jeder anderen dazu — deshalb wird multipliziert, nicht addiert. Kurz: Vorrat hoch Länge.
2. Du hängst an ein Passwort aus Kleinbuchstaben EIN Zeichen an. Was passiert mit der Anzahl der Möglichkeiten? → **Sie wird 26-mal so groß.** – Ein Zeichen mehr heißt: Alles, was es vorher gab, gibt es jetzt 26-mal. Genau das siehst du am Regler — die Zahl macht bei jedem Schritt einen Sprung, keinen Schritt.
3. Was bringt mehr: aus 8 Zeichen 12 machen, oder zu den Kleinbuchstaben noch Sonderzeichen dazu nehmen? → **Vier Zeichen mehr — mit Abstand.** – Der größere Vorrat multipliziert die Zahl einmal. Vier Zeichen mehr multiplizieren sie vier Mal. Stell es oben ein und vergleiche die beiden Zeiten — der Unterschied ist riesig.

**Länge oder Sonderzeichen?** (Schreibfeld)

Erwartete Elemente: Vier Zeichen mehr bringen mehr als Sonderzeichen dazu – jedes zusätzliche Zeichen vervielfacht die Kombinationen (mal 26 bis mal 94), Sonderzeichen vergrößern nur den Zeichenvorrat. Die abgelesenen Zeiten müssen die Reihenfolge stützen – bei einer Million Versuchen pro Sekunde: nur Kleinbuchstaben 8 Zeichen ≈ 2 Tage, 12 Zeichen ≈ 3 000 Jahre; mit Groß-, Kleinbuchstaben und Ziffern 8 Zeichen ≈ 7 Jahre, 12 Zeichen ≈ 100 Millionen Jahre.

## 4 · Brute-Force sichtbar

**Wie ein Computer wirklich rät** (Wahr/Falsch)

1. Der Computer fängt bei „aaaa" an und zählt stur weiter. → **wahr** – Genau das siehst du in der Zeitlupe. Der Computer überlegt nicht — er zählt.
2. Der Computer errät zuerst die wahrscheinlichsten Wörter und rät dann weiter. → **falsch** – Das ist ein anderer Angriff: der Wörterbuch-Angriff aus Modul „Datenleaks". Brute-Force probiert stur alles der Reihe nach durch.
3. In Wirklichkeit läuft ein solcher Angriff viel schneller als in dieser Zeitlupe. → **wahr** – Rund eine Million Versuche pro Sekunde. Die Zeitlupe ist nur langsam, damit man das Prinzip sieht.
4. Ein Passwort aus vier Kleinbuchstaben hält einem echten Angriff mehrere Minuten stand. → **falsch** – 26 hoch 4 sind knapp 457.000 Möglichkeiten — bei einer Million Versuchen pro Sekunde weniger als eine Sekunde.
5. Gegen stures Durchprobieren hilft vor allem Länge. → **wahr** – Jedes Zeichen mehr multipliziert die Zahl der Möglichkeiten — und damit die Zeit, die der Computer braucht.

## 5 · Passwort-Recycling

**Die Kette in der richtigen Reihenfolge** (Reihenfolge)

1. Eine Spieleplattform wird gehackt.
2. Die erbeuteten E-Mail-Adressen und Passwörter landen in einer Liste.
3. Ein Programm probiert jedes Paar automatisch bei anderen Diensten aus.
4. Bei einem Dienst passt dasselbe Passwort — die Tür geht auf.
5. Über das E-Mail-Postfach lassen sich weitere Konten übernehmen.

**Wie oft benutzt du dasselbe Passwort?** (Schreibfeld)

Offen (Zahl ohne Wertung). Gefährlich ist: Wird ein Dienst gehackt, probiert ein Programm dasselbe Paar aus E-Mail und Passwort automatisch bei allen anderen – ein Leak öffnet dann alle Konten.

## 6 · Datenleaks

**Geleakt — und jetzt?** (Auswahl)

1. Warum probieren Angreifer geleakte Passwörter zuerst? → **Weil sie in Millionen Fällen schon einmal benutzt wurden.** – Genau. Eine Liste mit Millionen echter Passwörter ist viel lohnender als stures Durchzählen — deshalb kommt sie zuerst.
2. Dein Passwort steht in einem Leak. Was ist der erste Schritt? → **Sofort das Passwort dieses Dienstes ändern.** – Richtig. Und danach überall dort, wo dasselbe Passwort noch im Einsatz ist. Eine angehängte Ziffer hilft nicht — auch solche Varianten stehen auf den Listen.
3. Warum ist „Schmetterling" trotz 13 Zeichen kein gutes Passwort? → **Weil es ein normales Wort ist und auf jeder Liste steht.** – Genau. Länge hilft nur gegen stures Durchprobieren. Gegen eine Wortliste hilft sie gar nichts — deshalb besteht eine Passphrase aus mehreren, unsinnig kombinierten Wörtern.

**Deine ersten zwei Schritte** (Schreibfeld)

Erwartete Elemente: 1. Passwort bei dem betroffenen Dienst sofort ändern, 2. überall, wo dasselbe Passwort benutzt wurde, ebenfalls ändern (und 2FA einschalten). Akzeptabel auch: Warn-Mails prüfen, Leak-Check nutzen.

## 7 · Phishing erkennen

**Merkmal und Masche** (Zuordnung)

**„Dein Konto wird in 24 Stunden gesperrt."** → Druck und Drohung · **„Bestätige hier dein Passwort."** → Aufforderung zur Eingabe · **„Du hast 1000 Gratis-Diamanten gewonnen!"** → Zu gut, um wahr zu sein · **Der Link führt zu instagram-login.xyz** → Falscher Absender oder Link

**Woran hast du die Falle erkannt?** (Schreibfeld)

Erwartete Elemente: eines der fünf Merkmale der Seite – gefälschter Absender, Panikmache mit Frist, Link zu einer fremden Adresse, Passwort-Abfrage per Mail, unpersönliche Anrede. Ein echter Dienst fragt nie per Mail nach dem Passwort.

## 8 · URL-Lupe

**Wem gehört diese Adresse?** (Sortieren in Fächer)

**Echt:** https://www.paypal.com/de/webapps/mpp/home · https://www.bbc.co.uk/news · https://accounts.google.com/signin
**Gefälscht:** https://konto.paypa1-sicherheit.com/login · https://sicherheit.paypal.com.login-check.info/ · https://instagram.com.konto-pruefung.ru/anmelden

## 9 · 2FA & Passkeys

**Der zweite Riegel** (Auswahl)

1. Dein Passwort wurde geleakt. Du hast 2FA per App eingeschaltet. Was passiert? → **Der Angreifer kommt nicht hinein — ihm fehlt der Code.** – Genau dafür ist der zweite Faktor da: etwas, das man WEISS (Passwort), plus etwas, das man HAT (Handy).
2. Warum hilft ein Passkey gegen Phishing besser als ein SMS-Code? → **Er ist an die echte Adresse gebunden und passt sonst nicht.** – Einen SMS-Code kann man auf einer gefälschten Seite eintippen. Ein Passkey funktioniert dort technisch nicht — er kennt die echte Adresse.
3. Wo lohnt sich 2FA zuerst? → **Beim E-Mail-Postfach, dem Generalschlüssel zu allem.** – Über die E-Mail lässt sich fast jedes andere Passwort zurücksetzen. Wer das Postfach hat, hat alles.

**Wo würdest du anfangen?** (Schreibfeld)

Erwartet: das E-Mail-Postfach – weil alle „Passwort vergessen"-Links dort landen und wer das Postfach hat, jedes andere Konto zurücksetzen kann. Akzeptabel mit Begründung: Konto mit Zahlungsdaten oder Spiele-Konto mit Guthaben.

## 10 · Sicheres Verhalten

**Passwortsicherheit – Abschluss-Check** (Auswahl)

1. Was schützt ein Konto am wirksamsten vor einem Datenleak bei einem anderen Dienst? → **Für jeden Dienst ein eigenes, einmaliges Passwort verwenden.** – Nur ein eigenes Passwort pro Dienst verhindert, dass ein Leak bei einem Anbieter automatisch auch andere Konten öffnet (siehe Modul „Passwort-Recycling").
2. Warum ist ein Passkey gegen Phishing-Seiten besonders wirksam? → **Er ist an die echte Adresse gebunden und passt auf eine Fälschung nicht.** – Ein Passkey prüft die Internetadresse selbst und verweigert die Anmeldung, wenn sie nicht zur echten Seite passt – anders als ein Passwort, das man versehentlich überall eintippen kann.
3. Eine E-Mail droht mit sofortiger Kontosperrung, wenn du nicht innerhalb von 2 Stunden auf einen Link klickst und dein Passwort bestätigst. Was ist der plausibelste erste Schritt? → **Nicht klicken, sondern die echte Seite selbst aufrufen.** – Zeitdruck und die Aufforderung zur Passwort-Eingabe per Link sind die klassischen Warnzeichen aus Modul „Phishing erkennen".

**Eine Regel ab heute** (Schreibfeld)

Offen. Bewertet wird die Passung von Regel und Änderung („Ich benutze für jeden Dienst ein eigenes Passwort – dafür brauche ich einen Passwortmanager", „Ich schalte 2FA beim Postfach ein – dafür muss ich die App einrichten").