FÜR LEHRKRÄFTE · MEDIEN & INFORMATIK KLASSE 6

Lösungen und Erwartungshorizont

Lösungen zu allen Aufgaben der zwölf Lektionen, die gefüllten Hefteinträge und der Erwartungshorizont zu den Schreibfeldern. Der Test-Abgleich (welche Lektion welche Testfrage trägt) steht in docs/steve-wagner.de/passwort-profi/konzept.md.

1 · Dein digitaler Alltag

Was schützt du mit einem Passwort? (Meinung)

Meinungsaufgabe ohne Lösung. Erwartbar: fünf bis acht Konten mit Passwort; die Zahl kommt in den Hefteintrag.

Deine Vermutung (Schreibfeld)

Offen, keine Musterlösung – Vorwissen. Typisch: „raten“, „zuschauen beim Tippen“, „Passwort weitersagen“; selten Phishing oder die E-Mail-Kette. Wird in Lektion 12 wieder gelesen.

HEFTEINTRAG, GEFÜLLT

Wie kommt jemand an mein Konto – und wie halte ich ihn draußen?

Ich habe **(eigene Zahl)** Konten mit Passwort gezählt.

Meine Vermutung heute: Jemand kommt rein, wenn **(eigene Antwort)**.

2 · Warum Passwörter?

Geheim oder okay? (Sortieren in Fächer)

Okay für Fremde: Dein Spielername im Spiel · Dein öffentlicher Highscore · Dein Lieblingsessen · Deine Lieblingsband

Streng geheim: Deine Wohnadresse · Private Chatnachrichten · Dein Schul-Passwort · Der Code, mit dem du dein Handy entsperrst

Warum will jemand in dein Konto? (Auswahl)

1. Warum könnte jemand Zugang zu deinem Konto haben wollen? → **Spielstände, Skins oder Items stehlen und verkaufen, Mit deinem Konto Geld ausgeben oder einkaufen, In deinem Namen Nachrichten schreiben, Deine Fotos und Chats lesen, Dich ärgern oder bloßstellen** – Hinter einem Konto stecken Wert (Items, Geld), Daten (Fotos, Chats) und dein Name. Alles drei ist für Fremde interessant – helfen will dir dabei niemand.

HEFTEINTRAG, GEFÜLLT

Ein Passwort ist wie der **Schlüssel** zu meiner Haustür.

Hinter der Tür liegen meine Daten: **Wert**, **Daten** und **mein Name**.

Zwei Gründe, warum jemand in mein Konto will: **Items/Guthaben stehlen** und **Geld ausgeben** (auch: in meinem Namen schreiben, Fotos/Chats lesen, ärgern).

3 · Unsichere Passwörter

Sicher oder unsicher? (Sortieren in Fächer)

Unsicher: 123456 · qwertz · passwort · Mueller2012 · bello · geheim123
Sicher: MHBfjM3Ku2W! · BlaueTasseRegen!17 · 7Kekse-fuer-den-Mond

Wahr oder falsch? (Wahr/Falsch)

1. Der Name deines Haustiers ist ein gutes Passwort, weil ihn kaum jemand kennt. → **falsch** – Haustiernamen stehen in Chats, auf Fotos und in Profilen. Freunde und Angreifer raten sie zuerst.
2. „qwertz" ist unsicher, obwohl es kein richtiges Wort ist. → **wahr** – Das ist die erste Buchstabenreihe auf der Tastatur. Solche Muster stehen ganz oben auf jeder Rate-Liste.
3. Ein Passwort auf einem Zettel am Bildschirm ist sicher, solange man niemanden ins Zimmer lässt. → **falsch** – Jeder Besucher, jedes Foto vom Schreibtisch, jedes Video im Zimmer zeigt den Zettel. Der Zettel gehört – wenn überhaupt – in eine Schublade oder in einen Passwortmanager.
4. Wer bei allen Konten dasselbe Passwort nutzt, verliert bei einem Leck alle Konten auf einmal. → **wahr** – Wird ein Dienst gehackt, probieren Angreifer dasselbe Passwort sofort bei E-Mail, Spielen und Shops.
5. Ein Passwort mit Geburtsdatum ist sicher, weil es Zahlen enthält. → **falsch** – Zahlen allein helfen nicht. Das Geburtsdatum steht im Profil, in Glückwünschen und in der Klassenliste.

HEFTEINTRAG, GEFÜLLT

Unsicher sind: Zahlenreihen wie **123456**, Tastaturmuster wie **qwertz** und Wörter aus dem Wörterbuch.

Unsicher ist alles Persönliche: mein **Name**, mein **Haustier** oder mein **Geburtsdatum**.

Ein Zettel am Bildschirm ist **unsicher**, weil jeder ihn **lesen** kann.

4 · Sichere Passwörter bauen

Die Satz-Methode (Lückeneingabe)

1. „Mein Hund Bello frisst jeden Morgen 3 Knochen und 2 Würstchen!" wird zu: **MHBfjM3Ku2W!**
2. „Oma backt sonntags 12 Waffeln mit Sahne!" wird zu: **Obs12WmS!**
3. „Im Sommer schwimme ich 4 Runden im See?" wird zu: **Issi4RiS?**

Welches Passwort ist am sichersten? (Auswahl)

1. Welches dieser Passwörter ist am sichersten? → **RegenAufDemDach!2031** – Ein langer Merksatz mit Zahl und Sonderzeichen hat 20 Zeichen und keine Stelle, die man raten kann. „Katze2009“ ist Tier plus Jahr, „PaSsWoRt“ nur ein bekanntes Wort in Wechselschrift, „abc123xyz“ ein Tastaturmuster.
2. Was macht ein Passwort am meisten sicherer? → **Es ist deutlich länger** – Jedes Zeichen mehr vervielfacht die Möglichkeiten. Ein Großbuchstabe am Anfang oder eine 1 am Ende ist so üblich, dass Rate-Programme es zuerst probieren.
3. Wie viele Zeichen sollte dein Passwort mindestens haben? → **12 oder mehr** – Zwölf Zeichen sind die Untergrenze in dieser Reihe. Kürzere Passwörter probiert ein Rate-Programm in Stunden oder Tagen durch.

HEFTEINTRAG, GEFÜLLT

Regel 1: mindestens **12** Zeichen. Regel 2: **Großbuchstaben**, **Kleinbuchstaben**, **Zahlen** und **Sonderzeichen** mischen.

Satz-Methode: Von jedem Wort den **Anfangsbuchstaben** nehmen. Mein Merksatz: **(eigener Satz)**

Ein Merksatz-Passwort besteht aus mehreren **Wörtern** mit Zahl und Sonderzeichen.

5 · Wie Angreifer raten

Brute-Force – wahr oder falsch? (Wahr/Falsch)

1. Ein Brute-Force-Angriff probiert sehr viele Passwort-Kombinationen nacheinander aus. → **wahr** – „Brute Force“ heißt „rohe Gewalt“: aaaa, aaab, aaac … Ein Programm schafft Millionen Versuche pro Sekunde.
2. Angreifer sitzen am Computer und tippen Passwörter von Hand ein. → **falsch** – Das übernimmt ein Programm. Es hört nicht auf, wird nicht müde und macht keine Tippfehler.
3. Ein Wörterbuch-Angriff probiert zuerst bekannte Wörter, Namen und beliebte Passwörter. → **wahr** – Deshalb sind „passwort“, „bello“ und „Mueller2012“ in Sekunden geknackt – sie stehen auf der Liste.
4. Ein Passwort aus vier Kleinbuchstaben hält einem Rate-Programm mehrere Tage stand. → **falsch** – Vier Kleinbuchstaben sind nur 456 976 Kombinationen. Bei einer Million Versuchen pro Sekunde ist das in unter einer Sekunde durch.
5. Jedes Zeichen mehr macht das Raten um ein Vielfaches länger. → **wahr** – Mit jedem Zeichen vervielfachen sich die Möglichkeiten. Zwölf gemischte Zeichen brauchen viele Millionen Jahre.

Was probiert ein Angreifer zuerst? (Reihenfolge)

1. Die beliebtesten Passwörter der Welt (123456, passwort, qwertz)
2. Wörter aus dem Wörterbuch, Namen und Geburtsjahre
3. Bekannte Passwörter mit angehängter Zahl (bello1, bello123)
4. Alle Kombinationen durchprobieren (Brute-Force)

HEFTEINTRAG, GEFÜLLT

Brute-Force heißt **rohe Gewalt**: Ein Programm probiert **alle** Kombinationen aus – etwa eine **Million** pro Sekunde.

„hund" hat **456 976** Möglichkeiten und ist in **unter einer Sekunde** geknackt.

12 gemischte Zeichen halten **Hunderte Millionen Jahre**.

Ein Wörterbuch-Angriff probiert zuerst **Wörter aus dem Wörterbuch**, **Namen** und beliebte Passwörter.

6 · Phishing erkennen

Echt oder Phishing? (Sortieren in Fächer)

Phishing: Von support@netflx-hilfe.de: „Ihr Konto wird in 24 Stunden gelöscht! Klicken Sie hier und geben Sie Ihr Passwort ein." · Von sicherheit@paypa1.com: „Verdächtige Zahlung! Sofort hier anmelden, sonst Sperre." · SMS von unbekannter Nummer: „Dein Paket wartet. Zahle 1,99 € Zollgebühr unter diesem Link." · Chat von einem fremden Spieler: „Ich gebe dir 1000 Gratis-Coins – schick mir nur kurz dein Login."
Echt: Vom Schulportal, nach deiner eigenen Anfrage: „Du hast das Zurücksetzen deines Passworts angefordert. Falls nicht, ignoriere diese Mail." · Vom Spiele-Anbieter: „Neue Anmeldung auf einem unbekannten Gerät. Warst du das? Wenn nicht, ändere dein Passwort in den Einstellungen."

Woran erkennst du Phishing? (Zuordnung)

Gefälschter Absender → netflx statt netflix, paypa1 statt paypal · **Panikmache** → „Sonst wird Ihr Konto in 24 Stunden gelöscht!" · **Passwort-Abfrage per Link** → „Melden Sie sich hier an" – auf einer fremden Seite · **Zu schönes Angebot** → „1000 Gratis-Coins, nur heute!" · **Unpersönliche Anrede** → „Sehr geehrter Kunde" statt deines Namens

HEFTEINTRAG, GEFÜLLT

Phishing bedeutet: Passwörter **angeln** – mit einer **gefälschten** Nachricht.

Fünf Warnzeichen: **gefälschter Absender**, **Panikmache**, **Link mit Passwort-Abfrage**, **zu schönes Angebot**, **unpersönliche Anrede**.

Bei einer merkwürdigen Mail mit Link: **nicht** klicken, Absender prüfen, im Zweifel **löschen**.

Der Trick in Toms Mail: **netflx** statt netflix.

7 · Warnzeichen und Sperre

Warnzeichen erkennen (Auswahl)

1. Was ist ein typischer Hinweis darauf, dass jemand dein Passwort angreift? → **Viele fehlgeschlagene Anmeldeversuche oder Warn-Mails** – Fehlversuche und Warn-Mails („Neue Anmeldung", „Passwort geändert?") zeigen: Jemand probiert es. Eigene Einkäufe, Lob oder Ladezeit haben mit Angriffen nichts zu tun.
2. Du bekommst eine Mail: „Neue Anmeldung auf einem unbekannten Gerät in einer anderen Stadt." Du warst das nicht. Was bedeutet das? → **Jemand hat sich mit deinem Passwort angemeldet** – Die Mail ist eine echte Warnung: Dein Passwort ist in fremder Hand. Sofort ändern und die Wiederherstellungs-Daten prüfen.
3. Wozu sperrt ein Dienst ein Konto nach zu vielen Fehlversuchen? → **Damit ein Rate-Programm nicht tausende Passwörter probieren kann** – Nach zum Beispiel fünf falschen Versuchen wartet der Dienst oder sperrt. Eine Million Versuche pro Sekunde werden so unmöglich – die Sperre schützt vor vielen Fehlversuchen.

Die Kontosperre – wahr oder falsch? (Wahr/Falsch)

1. Dienste können ein Konto nach zu vielen Fehlversuchen sperren. → **wahr** – Viele Dienste sperren nach fünf bis zehn falschen Passwörtern – für Minuten oder bis du dich per E-Mail meldest.
2. Eine Sperre nach Fehlversuchen schützt vor Brute-Force-Angriffen. → **wahr** – Ein Rate-Programm braucht Millionen Versuche. Wenn nach fünf Schluss ist, läuft es ins Leere.
3. Wenn dein Konto plötzlich gesperrt ist, obwohl du dich nicht angemeldet hast, war es sicher ein Fehler des Dienstes. → **falsch** – Wahrscheinlicher hat jemand dein Passwort geraten. Passwort ändern, Wiederherstellungs-Daten prüfen, Erwachsenen Bescheid sagen.
4. Warn-Mails über eine „neue Anmeldung" kann man immer ignorieren. → **falsch** – Nur wenn du dich gerade selbst neu angemeldet hast. Sonst ist die Mail dein wichtigstes Warnzeichen.

HEFTEINTRAG, GEFÜLLT

Typische Hinweise auf einen Angriff: viele **fehlgeschlagene** Anmeldeversuche und **Warn-Mails**.

Nach **3** Fehlversuchen sperrt der Dienst das Konto für **15 Minuten**.

Die Sperre schützt vor **Rate-Programmen (Brute-Force)**, weil ein Programm dann nicht mehr **Millionen** Versuche machen kann.

8 · Der Hauptschlüssel

Die Kettenreaktion (Reihenfolge)

1. Der Angreifer meldet sich in deinem E-Mail-Postfach an
2. Er klickt bei deinem Spiel auf „Passwort vergessen“
3. Der Link zum Zurücksetzen landet in deinem Postfach – das er jetzt liest
4. Er setzt ein neues Passwort und übernimmt das Spiele-Konto

Wiederherstellung (Auswahl)

1. Wofür braucht man die Wiederherstellungs-E-Mail oder Telefonnummer? → **Um das Konto zurückzubekommen, wenn man das Passwort vergisst** – Vergisst du dein Passwort oder übernimmt jemand dein Konto, schickt der Dienst einen Code an diese zweite Adresse oder Nummer. Ohne sie ist das Konto oft verloren.
2. Welches Konto muss am stärksten geschützt werden? → **Das E-Mail-Postfach** – Fast jedes andere Konto schickt seinen „Passwort vergessen“-Link an die E-Mail. Wer das Postfach hat, hat alles.
3. Wann solltest du Wiederherstellungs-Daten hinterlegen? → **Gleich beim Anlegen des Kontos, bevor etwas passiert** – Im Notfall kommst du nicht mehr in die Einstellungen. Die zweite Adresse oder Nummer muss vorher da sein.

HEFTEINTRAG, GEFÜLLT

Das wichtigste Konto ist mein **E-Mail-Postfach**, weil alle „Passwort vergessen“-Links **dort** landen.

Die Kette: Angreifer im Postfach → klickt „**Passwort vergessen**“ → liest den **Link** → setzt ein neues Passwort.

Die Wiederherstellungs-E-Mail oder Telefonnummer brauche ich, um **das Konto zurückzubekommen, wenn ich das Passwort vergesse oder jemand es geändert hat**.

Hinterlegen muss ich sie **vorher**, nicht erst im Notfall.

9 · 2FA und Passwortmanager

Was gehört zusammen? (Zuordnung)

Passwortmanager → Speichert alle Passwörter in einem Tresor und füllt sie sicher aus · **Zwei-Faktor-Authentifizierung (2FA)** → Zweiter Bestätigungscode, zum Beispiel per Handy-SMS oder App · **Sperre nach zu vielen Fehlversuchen** → Schützt das Konto vor Rate-Programmen mit vielen Versuchen · **Satz-Methode** → Merksatz-Passwort aus den Anfangsbuchstaben eines Satzes · **Wiederherstellungs-E-Mail** → Zweite Adresse, an die der Dienst im Notfall einen Code schickt

Zwei Türen – wahr oder falsch? (Wahr/Falsch)

1. Bei 2FA brauchst du dein Passwort UND einen zweiten Code, zum Beispiel vom Handy. → **wahr** – Erste Tür: etwas, das du weißt (Passwort). Zweite Tür: etwas, das du hast (Handy). Ohne beides kommt niemand rein.
2. 2FA bedeutet, dass du zwei verschiedene Passwörter nacheinander eintippst. → **falsch** – Zwei Passwörter wären zweimal „etwas, das du weißt". Der zweite Faktor ist etwas, das du HAST – ein Gerät.
3. Wer dein Passwort geklaut hat, kommt bei eingeschalteter 2FA trotzdem nicht ohne dein Handy rein. → **wahr** – Genau das ist der Sinn: Das gestohlene Passwort allein nützt nichts.
4. Ein Passwortmanager ist ein Tresor, der sich alle deine Passwörter merkt – du brauchst nur ein starkes Master-Passwort. → **wahr** – Deshalb kann man für jedes Konto ein anderes, langes Passwort haben, ohne sich zwanzig zu merken.
5. Dasselbe Passwort für alle Webseiten zu benutzen erhöht die Sicherheit, weil man es sich gut merkt. → **falsch** – Ein Leck bei einem Dienst öffnet dann alle anderen Konten. Ein Passwort je Konto – der Manager merkt sie sich.

HEFTEINTRAG, GEFÜLLT

2FA bedeutet: Passwort (**wissen**) und Code vom Handy (**haben**).

Wer nur mein Passwort hat, kommt bei 2FA nicht rein, weil ihm **mein Handy (der Code)** fehlt.

Ein Passwortmanager ist ein **Tresor**: Er speichert alle Passwörter und füllt sie sicher aus. Ich merke mir nur das **Master-Passwort**.

Nicht sicherer wird ein Konto durch: **dasselbe Passwort** für alle Seiten oder einen **Zettel** am Bildschirm.

10 · Die drei Schutzziele

Welches Schutzziel ist verletzt? (Auswahl)

1. Jemand hat heimlich deinen Referatstext gelöscht und Quatsch hineingeschrieben. → **Integrität – Daten wurden verändert**
2. Du kannst dich nicht ins Schulportal einloggen, weil der Server abgestürzt ist. → **Verfügbarkeit – Daten sind nicht da**
3. Ein Fremder liest deine privaten Chatnachrichten mit. → **Vertraulichkeit – Daten wurden gelesen**
4. Ein Angreifer macht aus deiner Note 1 eine 6 im Notenprogramm. → **Integrität – Daten wurden verändert**
5. Ein Virus verschlüsselt alle Fotos auf dem Familien-PC, keiner kommt mehr dran. → **Verfügbarkeit – Daten sind nicht da**
6. Jemand fotografiert die Klassenliste mit allen Adressen und schickt sie herum. → **Vertraulichkeit – Daten wurden gelesen**

Die drei Schutzziele erklären (Lückentext)

Vertraulichkeit bedeutet: Nur wer darf, kann die Daten **sehen**. Integrität bedeutet: Die Daten sind nicht heimlich **verändert** worden. Verfügbarkeit bedeutet: Die Daten sind **da**, wenn man sie braucht. Ein Passwort schützt vor allem die **Vertraulichkeit** deiner Daten.

HEFTEINTRAG, GEFÜLLT

Vertraulichkeit bedeutet: Nur wer darf, kann die Daten **sehen**.

Integrität bedeutet: Die Daten sind nicht **verändert** worden.

Verfügbarkeit bedeutet: Die Daten sind **da**, wenn man sie braucht.

Beispiel aus Mias Schule: Klassenliste fotografiert = **Vertraulichkeit**, Note geändert = **Integrität**, Portal abgestürzt = **Verfügbarkeit**.

11 · Teilen und Notfall

Was tust du? (Auswahl)

1. Deine beste Freundin fragt: „Gib mir kurz dein Netflix-Passwort, nur für heute!“ → **Nein – Passwörter gebe ich nicht weiter, auch nicht an Freunde**
2. Ein Klassenkamerad sagt: „Ich habe dein Passwort, ich logge mich mal ein – nur zum Spaß.“ → **Nein sagen, sofort das Passwort ändern und einem Erwachsenen Bescheid sagen**
3. Du hast auf einen Link geklickt und dein Passwort auf einer komischen Seite eingegeben. → **Sofort das Passwort ändern und Eltern oder Lehrkraft Bescheid sagen**
4. Du kommst nicht mehr in dein Konto, und ein Freund sagt, du hättest komische Bilder gepostet. → **Ruhe bewahren, Hilfe holen und die Wiederherstellungs-E-Mail nutzen**

Was sagst du – und was tust du? (Schreibfeld)

Offen. Erwartete Elemente: klares Nein; der Hinweis, dass es verboten ist; sofort Passwort ändern; Eltern oder Lehrkraft informieren. Zwei Punkte (Sagen + Tun), wie im Test.

HEFTEINTRAG, GEFÜLLT

Mein Passwort teile ich mit **niemandem** – auch nicht mit meiner besten Freundin.

Wer sich mit einem fremden Passwort einloggt, begeht eine **Straftat** – auch „nur zum Spaß“.

Notfallplan: 1. **Ruhe** bewahren und Hilfe holen. 2. Sofort das **Passwort** ändern. 3. Die **Wiederherstellung** nutzen. 4. **2FA** einschalten.

Was ich zu Ben sage: **(eigener Satz: Nein – verboten – Passwort ändern – Erwachsenen sagen)**

12 · Der Profi-Test

Die Leitfrage – deine Antwort (Schreibfeld)

Offen. Erwartete Elemente: Wege des Angreifers (raten, angeln/Phishing, Postfach übernehmen) und Schutz (langes gemischtes Passwort, 2FA, nie teilen, Wiederherstellung hinterlegt). Neben die Vermutung aus Lektion 1 legen.

1. Der Profi-Test (Auswahl)

1. Was bedeutet Integrität bei digitalen Daten? → **Die Daten sind nicht verändert worden** – Integrität: nichts wurde heimlich verändert. Geheim = Vertraulichkeit, da sein = Verfügbarkeit.

2. Der Profi-Test (Auswahl)

1. Was ist ein typischer Hinweis auf einen Passwort-Angriff? → **Viele fehlgeschlagene Anmeldeversuche oder Warn-Mails** – Fehlversuche und Warn-Mails („Neue Anmeldung“) zeigen, dass jemand es probiert.

3. Der Profi-Test (Auswahl)

1. Welche Maßnahme erhöht die Sicherheit eines Kontos am meisten? → **Zwei-Faktor-Authentifizierung (2FA) einschalten** – Mit 2FA nützt ein gestohlenes Passwort allein nichts – der zweite Code fehlt.

4. Der Profi-Test (Auswahl)

1. Welches Passwort ist am sichersten? → **Ein langer Merksatz mit Zahlen und Sonderzeichen** – Länge plus Mischung – ein Merksatz wie „RegenAufDemDach!2031“ hat 20 Zeichen und kein ratbares Muster.

5. Der Profi-Test (Auswahl)

1. Wofür braucht man die Wiederherstellungs-E-Mail oder Telefonnummer? → **Um das Konto wiederzubekommen, wenn man das Passwort vergisst** – Der Dienst schickt im Notfall einen Code an diese zweite Adresse oder Nummer.

6. Der Profi-Test (Auswahl)

1. Darfst du dein Passwort mit deiner besten Freundin teilen? → **Nein – Passwörter gibt man nie weiter, auch nicht an Freunde** – Ein geteiltes Passwort ist kein Geheimnis mehr. Streit, Verlust des Handys, ein Screenshot – und es ist unterwegs.

7. Der Profi-Test (Auswahl)

1. Was macht ein Brute-Force-Angriff? → **Er probiert sehr viele Passwort-Kombinationen aus** – „Rohe Gewalt“: ein Programm probiert aaaa, aaab, aaac … millionenfach pro Sekunde.

8. Der Profi-Test (Auswahl)

1. Du bekommst eine merkwürdige E-Mail mit einem Link. Was tust du? → **Nicht klicken, Absender prüfen, im Zweifel löschen** – Kein echter Anbieter fragt per Link nach deinem Passwort. Druck und Panikmache sind das Phishing-Muster.

9. Der Profi-Test (Auswahl)

1. Was können Dienste nach zu vielen Fehlversuchen tun? → **Das Konto vorübergehend sperren** – Die Sperre schützt vor Rate-Programmen: Nach fünf Fehlversuchen ist Schluss – statt einer Million pro Sekunde.

10. Der Profi-Test (Auswahl)

1. Warum will jemand Zugang zu deinem Konto? → **Items stehlen, Geld ausgeben, in deinem Namen schreiben** – Wert, Daten und dein Name – alles drei ist für Fremde interessant.

11. Der Profi-Test (Auswahl)

1. Was bedeutet Vertraulichkeit? → **Nur wer darf, kann die Daten sehen** – Vertraulich = nur für Berechtigte lesbar. Genau das schützt ein Passwort.

12. Der Profi-Test (Auswahl)

1. Was macht ein Passwortmanager? → **Er speichert Passwörter in einem Tresor und füllt sie sicher aus** – Ein Tresor mit einem starken Master-Passwort – so kann jedes Konto ein anderes Passwort haben.

HEFTEINTRAG, GEFÜLLT

Jemand kommt an mein Konto, wenn er mein Passwort **rät**, es mir mit einer falschen Nachricht **abluchst (Phishing)** oder mein **Postfach** übernimmt.

Ich halte ihn draußen mit einem **langen, gemischten** Passwort, mit **2FA** und indem ich mein Passwort **nie** weitergebe.

In Lektion 1 dachte ich: **(eigene Vermutung)**. Heute weiß ich: **(eigene Antwort)**.