Passwörter

Die Schülerinnen und Schüler lernen, ihre Online-Informationen durch starke Passwörter zu schützen. Außerdem lernen sie die Grundsätze für starke Passwörter und potenzielle Risiken beim Teilen von Passwörtern kennen. Sie erfahren, wie sie ihre Passwörter schützen und welche Schritte sie ergreifen können, um unautorisierten Zugriff auf ihre Konten zu verhindern.

Materialien

- Arbeitsblatt „Informationen über Passwörter“

Grundlagen für Passwörter

Teil 1

Anweisungen an die Schüler

Oft denken wir nicht viel über die Passwörter nach, die wir für Webseiten, Apps und Services verwenden. Wie sicher ein Passwort ist, entscheidet jedoch darüber, wie sicher die in den Konten enthaltenen Informationen sind.

Gruppenarbeit

Sprechen Sie mit den Schülerinnen und Schülern über die folgenden Fragen. Erinnern Sie die Schülerinnen und Schüler daran, dass es wichtig ist, in dieser oder anderen Übungen nicht ihre aktuellen echten Passwörter zu nennen.

Fragen an die Schüler

Wie viele Passwörter habt ihr?

> Verwendet ihr unterschiedliche Passwörter für jedes eurer E-Mail- und Social-Media-Konten?
>
> Unterscheiden sich die Passwörter sehr oder sind sie eine Variante des gleichen Passworts?

Wenn ihr mehr als ein Passwort habt, wie merkt ihr euch, welches Passwort für welches Konto gilt?

Fragen an die Schüler

Wie oft habt ihr schon ein wichtiges Passwort vergessen?

> Was habt ihr getan, wenn ihr ein Passwort vergessen habt?
>
> Was tut ihr, damit ihr euch eure Passwörter leichter merken könnt?

Gibt es ein Passwort, das ihr jeden Tag verwendet?

Was würde geschehen, wenn eine andere Person ohne euer Wissen herausfindet, wie euer Passwort lautet?

> Spielt es eine Rolle, wer diese andere Person ist?

Welche Art von Informationen könnte eine Person über euch erhalten, wenn sie euer Passwort verwendet, um sich bei eurem Konto anzumelden?

Teil 2

Gruppenarbeit

Teilen Sie die Klasse in Zweiergruppen ein.

Anweisungen an die Schüler

Besprecht mit eurem Partner, was passieren könnte, wenn jemand, der Unruhe stiften möchte, das Passwort für eure liebste Social-Media-Plattform erfahren würde.

Gruppenarbeit

Geben Sie den Schülerinnen und Schülern fünf Minuten Zeit, um darüber zu diskutieren. Bitten Sie die Gruppen, ihre Ergebnisse vorzustellen.

Anweisungen an die Schüler

Besprecht nun mit eurem Partner, was passieren könnte, wenn ein Hacker das Passwort für das Online-Banking-Konto eurer Eltern erfahren würde.

Gruppenarbeit

Geben Sie den Schülerinnen und Schülern fünf Minuten Zeit, um darüber zu diskutieren. Bitten Sie die Gruppen anschließend, ihre Ergebnisse vorzustellen.

Teil 3

Anweisungen an die Schüler

Ihr fragt euch vielleicht, wie ein Hacker an ein geheimes Passwort gelangen kann. Dafür gibt es verschiedene Möglichkeiten: Er/Sie könnte Social Engineering nutzen oder jemanden durch einen Trick dazu bringen, das Passwort zu verraten. Der Hacker könnte der Person eine E-Mail senden, die aussieht, als käme sie tatsächlich von der Plattform oder Website, auf der die Person ein Konto hat. In der E-Mail wird die Person gebeten, auf einen Link zu klicken und sich mit ihrem Benutzernamen und ihrem Passwort anzumelden. Wenn sie das tut, werden diese Informationen dem Hacker bekannt.

Manchmal versuchen Hacker auch, Passwörter mithilfe von gängigen Ausdrücken wie „Passwort123“, „Test“ oder dem Vor- oder Nachnamen der Person zu erraten.

Eine weitere Möglichkeit, wie Hacker ein geheimes Passwort erfahren könnten, ist

ein sogenannter Brute-Force-Angriff. Bei einem Brute-Force-Angriff versucht ein Hacker, sich bei einem Konto anzumelden, indem er verschiedene Passwörter ausprobiert. Ein Brute-Force-Angriff kann manuell ausgeführt werden, meist wird jedoch ein Computerprogramm zu Hilfe genommen, das schnell und automatisch eine Vielzahl möglicher Kombinationen von Passwörtern ausprobiert. Es kommt zum Beispiel eine Liste wahrscheinlicher Passwörter oder eine Reihe von Passwörtern aus Kombinationen verschiedener Buchstaben und Zahlen zum Einsatz, wodurch die Wahrscheinlichkeit steigt, das korrekte Passwort zu finden.

Einige Brute-Force-Attacken sind sogar noch raffinierter. Wenn das Passwort auf einer Liste wahrscheinlicher Passwörter wie „Fido123“ oder „Passwort“ zu finden ist, können einige Programme es schneller erraten, indem sie diese Optionen vor unwahrscheinlicheren oder zufällig generierten Passwörtern ausprobieren. Die Attacke wird zudem erleichtert, wenn der Hacker bestimmte Informationen über den Kontoinhaber hat. Wenn der Hacker beispielsweise weiß, dass euer Haustier „Toby“ heißt, wird er „Toby“ mit verschiedenen Zahlenvariationen am Ende ausprobieren (z. B. „Toby629“ oder „Toby3020“).

Grundsätze für starke Passwörter

Teil 1

Fragen an die Schüler

Wer von euch weiß, was es bedeutet, ein „starkes“ oder „stärkeres“ Passwort zu haben? Warum ist das wichtig?

Anweisungen an die Schüler

Ein starkes Passwort trägt zum Schutz eurer Informationen bei. Es garantiert jedoch nicht, dass ein Konto nicht gehackt werden kann. Ein schwaches Passwort macht es anderen allerdings deutlich leichter, auf eure Informationen zuzugreifen.

Übung zu Passwörtern

Fragen an die Schüler

Kennt ihr Beispiele für schwache Passwörter?

1. Mögliche Beispiele: Passwort, 12345, Hallo!, ein Geburtsdatum, ein Spitzname.

Warum sind diese Passwörter schwach?

1. Sie können leicht von einer anderen Person und/oder einem Computer erraten werden, der eine Brute-Force-Attacke ausführt.

Wie kann man ein Passwort stärker machen?

1. Zahlen, Groß- und Kleinbuchstaben oder Symbole verwenden, ein längeres Passwort wählen und für sich stehende gängige Ausdrücke und Wörter vermeiden.

Gruppenarbeit

Nachdem die Schülerinnen und Schüler diese Fragen beantwortet haben, schreiben Sie die folgenden Anweisungen an die Tafel:

> Mindestens eine Zahl verwenden.
>
> Mindestens ein Symbol verwenden.

Mindestens einen Groß- und einen Kleinbuchstaben verwenden.

Die Passwörter sollten mindestens sieben Zeichen umfassen.

Die Passwörter sollten leicht zu merken sein (außer bei Verwendung eines Passwort-Managers).

Ein Passwort-Manager ist eine Website oder eine Anwendung, mit deren Hilfe Nutzer ihre Passwörter speichern und verwalten können.

Passwörter sollten nicht aus einem einzelnen gängigen Wort oder persönlichen Informationen wie Geburtsdatum, Name der Mutter oder dergleichen bestehen.

Passwörter sollten nicht auf verschiedenen Webseiten verwendet werden.

Anweisungen an die Schüler

Es gibt zwei Ansätze für die Erstellung starker Passwörter. Der erste besteht darin, ein „Passwortrezept“ wie das an der Tafel gezeigte zu befolgen. Durch ein solches Rezept werden schwerer zu erratende Elemente in einem Text- oder numerischen Passwort verwendet, sodass auch das Passwort selbst schwerer zu erraten ist. Der Nachteil dieses Ansatzes ist, dass die so erstellten Passwörter nicht leicht zu merken sind.

Starke Passwörter

Anweisungen an die Schüler

Ein anderer Ansatz für die Erstellung starker Passwörter betrifft die Passwortlänge. Die Stärke eines Passworts hängt auch von dessen Länge ab. Eine Abfolge von mindestens vier nicht zusammenhängenden Wörtern ist für Menschen und Brute-Force-Attacken sehr schwer zu erraten. Diese Methode hat zudem den Vorteil, dass die so erstellten Passwörter leichter zu merken sind als bei der Rezeptmethode.

Zudem kann auch eine Kombination beider Methoden zielführend sein, bei der eine Abfolge von mindestens vier nicht zusammenhängenden Wörtern mit Symbolen und Zahlen ergänzt wird.

Beide Methoden verfolgen das gleiche Ziel: Passwörter zu entwickeln, die einzigartig und für andere Personen schwer zu erraten sind.

Anweisungen an die Schüler

Teilen Sie die Schülerinnen und Schüler in Zweiergruppen (Tandems) ein.

Erstellt im Tandem ein starkes Passwort mithilfe der Anweisungen an der Tafel.

Denkt daran, dass ein Passwort, das für einen Computer schwer zu erraten ist, für einen Menschen oder einen Computer mit einer Liste gängiger langer Passwörter dennoch leicht zu erraten sein kann. Das Blatt Papier, auf dem ihr euer Passwort notiert habt, wird nicht am Ende der Aktivität eingesammelt. Ihr solltet dieses Passwort nicht für eines eurer Konten verwenden, da eure Gruppenpartner es kennen.

Geben Sie den Schülerinnen und Schülern fünf Minuten Zeit. Gehen Sie anschließend im Raum herum und fragen Sie die Schülerinnen und Schüler nach ihren Beispielen für starke Passwörter. Bitten Sie die Schülerinnen und Schüler, sich an die erstellten Passwörter zu erinnern, ohne sie abzulesen.

Während einige Webseiten bestimmte Anforderungen an ein Passwort stellen, müssen auf anderen keine bestimmten Kriterien erfüllt werden. Ihr könnt Passwörter auch aus einer Reihe beliebiger allgemeiner Wörter erstellen.

Gruppenarbeit

Lassen Sie die Schülerinnen und Schüler in den gleichen Gruppen neue Passwörter erstellen, die aus Wortfolgen bestehen. Die Passwörter sollten aus mindestens vier Wörtern bestehen, damit sie sicher und leicht zu merken sind. Geben Sie den Schülerinnen und Schülern fünf Minuten Zeit. Gehen Sie anschließend im Raum herum und fragen Sie die Schülerinnen und Schüler nach ihren Beispielen. Erinnern Sie die Schülerinnen und Schüler daran, dass Sie das Arbeitsblatt am Ende der Aktivität nicht einsammeln werden und die Schülerinnen und Schüler die Passwörter nicht für ihre Konten verwenden sollten.

Anweisungen an die Schüler

Einige Webseiten verwenden ein System namens Multi-Faktor- (oder Zwei-Faktor-) Authentifizierung, um die Identität des Nutzers zu bestätigen. Diese Webseiten senden dem Nutzer per Textnachricht, App oder E-Mail einen Code, der zusammen mit dem Passwort eingegeben werden muss.

Durch diese Methode sind die Konten besser geschützt, da eine weitere Sicherheitsebene zum Einsatz kommt, die schwer zu knacken ist. Um sich bei eurem Konto anzumelden, muss eine Person beispielsweise euer Passwort kennen und Zugriff auf die App, das Gerät oder das E-Mail-Postfach haben, die mit dem Konto verknüpft sind.

Passwörter schützen

Teil 1

Anweisungen an die Schüler

Selbst wenn ihr ein Passwort erstellt, das für einen Computer oder eine Person schwer zu knacken ist, kann es in anderer Hinsicht nicht sicher genug sein.

Fragen an die Schüler

Welche weiteren Aspekte gibt es, die ein Passwort unsicher machen?

1. Hier einige Beispiele: Nutzung desselben Passworts für mehrere Konten, Passwörter aus persönlichen Informationen, Nutzung desselben Passworts für mehrere Jahre, Vergessen des Passworts.

Wie oft sollte man ein Passwort ändern?

Anweisungen an die Schüler

Selbst gute Passwörter können geknackt oder gestohlen werden, doch es gibt einige Möglichkeiten, sich zu schützen. Wenn die Sicherheit der Daten einer Website beeinträchtigt ist, auf der ihr ein Konto habt, ändert unbedingt euer Passwort für dieses Konto und andere Konten, für die ihr ähnliche Passwörter verwendet.

Lange und komplizierte Passwörter im Kopf zu behalten, kann schwierig sein.

Fragen an die Schüler

Glaubt ihr, dass es eine gute Idee ist, Passwörter auf einem Blatt Papier oder in einer Datei auf eurem Computer zu notieren? Warum oder warum nicht?

Gruppenarbeit

Nennen Sie verschiedene Möglichkeiten, z. B. dass jemand das Blatt Papier oder die Datei auf dem Computer finden könnte. Erklären Sie, dass die Nutzung eines Passwort-Managers sinnvoll sein kann. Das ist eine Anwendung, in der Benutzer ihre Passwörter speichern und verwalten können.

Teil 2

Anweisungen an die Schüler

Wir nutzen jeden Tag viele verschiedene Konten auf unterschiedlichen Webseiten.

Es kann recht mühsam sein, sich auf jeder Website jedes Mal an- und abzumelden.

Fragen an die Schüler

Habt ihr schon einmal die Funktion „Passwort speichern“ eures Browsers verwendet, um ein Passwort für eine Website zu speichern? Warum oder warum nicht?

Ist euch bewusst, wie eine Website sich an euch erinnert?

1. Bitten Sie die Schülerinnen und Schüler, dies näher zu erläutern. Erklären Sie anschließend, dass Webseiten sich an Nutzer erinnern, indem sie Cookies speichern. Cookies sind kleine Dateien, die auf dem Computer gespeichert werden und einer Website dabei helfen, euch bei künftigen Aufrufen an eurem Computer wiederzuerkennen, sodass ihr euch nicht erneut anmelden müsst. Cookies können jedoch auch verwendet werden, um zu verfolgen, wie ihr von Website zu Website navigiert. Diese Informationen werden zum Beispiel verwendet, um euch gezielt Werbung zu zeigen.

Ist es in Ordnung, ein Passwort auf dem eigenen Computer zu speichern?

Fragen an die Schüler

Ist euer Computer mit einem Anmeldepasswort geschützt?

Wie sieht es aus, wenn ihr den Computer gemeinsam mit anderen verwendet?

1. In diesem Fall können andere Personen, die denselben Computer nutzen, möglicherweise herausfinden, wie euer Passwort lautet – auch wenn das Passwort im Passwort-Feld in Form von schwarzen Punkten oder Sternchen angezeigt wird. Dass das Passwort nicht auf dem Bildschirm angezeigt wird, bedeutet nicht, dass es nicht irgendwo gespeichert ist.

Fragen an die Schüler

Gibt es Situationen, in denen es in Ordnung ist, ein Passwort mit einer anderen Person zu teilen? Wann? Warum wolltet ihr die Informationen nicht preisgeben?

1. Beispiele für solche Situationen könnten sein, wenn Eltern das Passwort ihrer Kinder erfahren möchten oder wenn eine Familie ein gemeinsames Konto bei einem Dienst wie Netflix hat.

Teilt ihr eure Passwörter mit jemand anderem? Wenn ja, mit wem und warum?

Wenn ihr mit jemandem eng befreundet seid, würdet ihr euer Passwort mit dieser

Person teilen, wenn sie sagen würde: „Wenn ich dir wichtig bin ...“? Warum oder warum nicht?

Anweisungen an die Schüler

Vielleicht möchtet ihr euer Passwort mit einer Person teilen, die euch wichtig ist. Doch dass euch jemand wichtig ist, bedeutet nicht, dass ihr dieser Person vollen Zugriff auf eure Online-Konten geben müsst.

Denkt gut über eure Beziehung mit dieser Person nach, bevor ihr ein Passwort mit ihr teilt. Berücksichtigt dabei auch, wie sich die Beziehung im Laufe der Zeit ändern könnte. Ein Passwort mit den Eltern oder Betreuern zu teilen, ist beispielsweise etwas anderes, als es mit dem/der besten Freund/in zu teilen.

Fragen an die Schüler

Was könnte passieren, wenn ihr ein Passwort mit anderen teilt?

1. Jemand könnte auf euer Bankkonto zugreifen, sich online für euch ausgeben oder eure Geheimnisse erfahren.

Wenn ihr ein Passwort für ein Konto mit jemandem teilt, würdet ihr dieses Konto dann anders verwenden?

Fragen an die Schüler

Gibt es Dinge, die ihr nicht auf Netflix ansehen oder in einer E-Mail schreiben würdet, wenn jemand anders dies sehen könnte?

Gruppenarbeit

Die Schülerinnen und Schüler sollen über ihr eigenes Verhalten bei der Nutzung eines gemeinsamen Kontos nachdenken. Dabei sollten sie berücksichtigen, dass ihre Online-Aktivitäten für andere Nutzer des Kontos sichtbar sind.

Fragen an die Schüler

Wenn euer Konto eine virtuelle Darstellung von euch ist, zum Beispiel ein Social-Media-Profil, ist es dann in Ordnung, anderen Menschen die Nutzung eures Kontos zu erlauben?

Gruppenarbeit

Diskutiert über die Möglichkeit, dass jemand sich für euch ausgibt und Nachrichten an eure Freunde sendet.

Fragen an die Schüler

Habt ihr Geräten, die ihr verwendet, erlaubt, eure Passwörter zu speichern? Warum oder warum nicht? Bedeutet das, dass es sicher ist, eure Passwörter auf eurem privaten Telefon oder Computer zu speichern? Was geschieht, wenn ihr euer Telefon oder euren Computer an einen Freund verleiht?

Gibt es Geräte, die ihr mit anderen teilt, zum Beispiel mit Familienmitgliedern oder Freunden? Teilt ihr euch auf diesem Gerät ein gemeinsames Konto, oder hat jede Person ein eigenes Konto?

Habt ihr schon einmal ein „öffentliches“ Gerät genutzt, zum Beispiel in einer Bibliothek, in der Schule oder woanders? Tut ihr auf diesem Gerät die gleichen Dinge wie auf privaten Geräten?

Teil 3

Gruppenarbeit

Teilen Sie die Klasse in Zweiergruppen ein.

Anweisungen an die Schüler

Besprecht in euren Gruppen, ob ihr euch schon einmal in der Schule, in einer Bibliothek oder einer anderen öffentlichen Einrichtung an einem Computer angemeldet und festgestellt habt, dass ein anderer Nutzer noch bei seinem Social-Media- oder E-Mail-Konto angemeldet war. Würdet ihr euch das Konto ansehen oder etwas anderes tun?

Gruppenarbeit

Geben Sie den Schülerinnen und Schülern fünf Minuten Zeit und bitten Sie sie anschließend, ihre Ergebnisse vorzustellen. Diskutieren Sie mit der Gruppe über eine solche nicht autorisierte Nutzung.

Unautorisierter Kontozugriff

Teil 1

Gruppenarbeit

Bitte beachten Sie: Der Inhalt dieser Aktivität wurde teilweise in „Aktivität Nr. 1: Grundlagen für Passwörter“ behandelt. Sie können frei entscheiden, ob Sie diese Thematik noch einmal besprechen oder diesen Teil überspringen möchten.

Anweisungen an die Schüler

Es ist möglich, dass andere Personen auf euer Konto zugreifen können, ohne euer Passwort zu kennen oder es zu erraten. Wenn eine Person genug persönliche Informationen über euch gesammelt hat, ist sie möglicherweise in der Lage, euer Passwort zu erraten. Die Person könnte auch versuchen, einen Mitarbeiter eines Unternehmens zu überzeugen, Informationen über euch preiszugeben. Da für den Zugriff auf euer Konto keine Technologien zum Einsatz kommen, wird diese Art von Angriff als „Social Hacking“ oder „Social Engineering“ bezeichnet.

Fragen an die Schüler

Meldet euch, wenn ihr schon einmal euer Passwort für ein Konto vergessen habt.

Was passiert, wenn ihr auf den Button „Ich habe mein Passwort vergessen“ klickt?

1. Die Website stellt Sicherheitsfragen oder versucht, euch über eine Telefonnummer oder E-Mail-Adresse zu kontaktieren.

Welche Sicherheitsfragen könnte die Website stellen?

1. Einige dieser Fragen könnten von Freunden oder Bekannten beantwortet oder die Antwort erraten werden. Beispiele: der Name des Haustiers der Person, ihr Geburtsort, der Mädchenname ihrer Mutter, der Name ihres Lieblingslehrers, der Name ihres/ihrer besten Freundes/Freundin, ihre Lieblingsmannschaft.

Wer könnte diese Art von Informationen über euch noch kennen?

Wie nimmt eine Website Kontakt mit euch auf, wenn ihr ein Passwort vergessen habt?

Wer könnte auf diese Kontaktmethoden ebenfalls zugreifen?

Fragen an die Schüler

Wie könnte ein Fremder die nötigen persönlichen Informationen erlangen, um eure Sicherheitsfragen zu beantworten?

1. Social-Media-Beiträge, Onlinesuche nach öffentlichen Informationen, mehrmaliges Raten, Kontaktaufnahme mit Freunden usw.

Fallen euch Beispiele für Social-Media-Beiträge mit persönlichen Informationen ein?

1. Beispielsweise ein Instagram-Bild eurer Katze mit ihrem Namen im Bildtext, ein Foto mit einem markierten Standort oder öffentliche Geburtstags-Posts.

Wie kann man über Google mehr über eine Person erfahren und ihr Passwort hacken?

1. Wenn eine Suchmaschine ein Klassenfoto einer Person aus der neunten Klasse in einer Schulzeitung online anzeigt, könnte man den Namen des Lehrers ermitteln.

Teil 2

Anweisungen an die Schüler

Informationen zu posten, die die Antworten auf eure Sicherheitsfragen beinhalten, ist sehr riskant. Wählt unbedingt Sicherheitsfragen aus, deren Antworten tatsächlich nur ihr kennt. Ihr könnt die Antworten auf die Sicherheitsfragen auch frei erfinden, solange ihr sie in einem Passwort-Manager speichert oder ihr sie euch leicht merken könnt.

Webseiten können Nutzer über eine Telefonnummer oder E-Mail-Adresse kontaktieren, die mit dem Benutzerkonto verknüpft ist. Wenn ein Benutzer sein Passwort vergisst, stellen Webseiten oft ein temporäres Passwort oder einen Hyperlink bereit, die der Nutzer verwenden kann, um sein Passwort zurückzusetzen.

Fragen an die Schüler

Ist dies eine sichere Methode, um zu gewährleisten, dass die Person, die das neue Passwort anfordert, tatsächlich der Nutzer ist?

Was geschieht, wenn ihr die mit dem Konto verknüpfte E-Mail-Adresse mit anderen teilt?

1. Ein Link zum Zurücksetzen des Passworts ist meist sicher, doch wenn ihr ein Konto oder ein Passwort mit anderen teilt, besteht immer ein Risiko.

Anweisungen an die Schüler

Social Hacking kann auch erfolgreich sein, wenn euch Personen direkt kontaktieren und versuchen, bestimmte Informationen von euch zu erhalten. Manchmal senden solche Personen euch eine E-Mail und geben vor, jemand anderes zu sein (zum Beispiel ein Freund, ein Familienmitglied oder ein Mitarbeiter eurer Bank). Sie bitten euch, ihnen wichtige Informationen (wie euer Geburtsdatum) zu nennen, um eure Identität zu bestätigen. Diese Anfragen können sehr geschickt sein, beispielsweise indem jemand das Social-Media-Konto eures Freundes hackt, euch (und möglicherweise auch anderen) eine Nachricht schickt und nach eurem Geburtstag oder eurer Heimatstadt fragt. Wenn ihr von einem Freund seltsame Nachrichten erhaltet, könntet ihr euch (außerhalb der jeweiligen Social-Media-Plattform) an euren Freund wenden und nachfragen, ob die Nachricht tatsächlich von ihm stammt.

Angriffe mit echt erscheinenden E-Mails oder Webseiten werden „Phishing“ genannt und können zu Identitätsdiebstahl führen. Bei einem Identitätsdiebstahl kann eine Person beispielsweise in eurem Namen eine Kreditkarte beantragen und verwenden, sodass es für euch schwieriger ist, selbst eine Kreditkarte zu bekommen, wenn ihr älter seid.

Phishing kann es dem Dieb ermöglichen, sich für euch auszugeben und weitere Informationen über euch zu erlangen, sodass er eure E-Mails lesen, in eurem Namen Nachrichten an eure Freunde senden oder euer Geld stehlen kann. Der Dieb könnte euch außerdem von eurem Konto aussperren, indem er ein neues Passwort erstellt, das ihr nicht kennt.

Aufgabenstellung

Arbeitsblatt

Aufgabestellung

Bitten Sie die Schülerinnen und Schüler, die folgenden Fragen zu beantworten und ihre Antworten in Form von Texten oder Bildern im Arbeitsblatt über Passwörter festzuhalten.

1. Welche drei Erkenntnisse aus dieser Sitzung werdet ihr anwenden, wenn ihr das nächste Mal ein Passwort erstellt?

2. In welcher Situation findet ihr es in Ordnung, euer Passwort mit einer anderen Person zu teilen?

3. Welche drei Strategien könnt ihr anwenden, um euer Passwort sicher mit einer anderen Person zu teilen?

4. Nennt drei Beispiele dafür, was schieflaufen kann, wenn ein Passwort in die falschen Hände gerät.