

G'SCHEIT GESPERRT

Powered by LIWEST

Dein Passwort als Festung	Cybersecurity
Starke Passwörter entwickeln	Passwort-Checker

Teil 1 - Video: Was ist Cybersecurity

Zu Beginn der Einheit ist es wichtig zu erfahren, was Cybersecurity genau ist und warum es gut ist dein Passwort zu schützen. Um das Video für diese Einheit zu sehen und sie interaktiv zu gestalten, scanne den QR-Code und komm' in unser Online-Learning-System! Du kannst die Einheit aber auch ohne Video mit dieser PDF-Datei durchführen.



Teil 2 - Lesen & Verstehen: Starke und schwache Passwörter

Aufgabe: Lest euch diesen Text gemeinsam als Klasse mit der Lehrperson laut durch!
Melde dich zum laut Lesen, für eine gute Mitarbeit!

Starke und schwache Passwörter

Ein Passwort ist wie der Schlüssel zu deinem digitalen Leben. Mit diesem Schlüssel sperrst du deine E-Mails, deine Social-Media-Konten oder auch Spiele und Apps ab. Stell dir vor, jemand findet oder errät deinen Schlüssel – dann könnte er in deine Accounts hineingehen, Nachrichten lesen, Fotos sehen oder sogar unter deinem Namen etwas posten. Deshalb ist es so wichtig, starke Passwörter zu verwenden.

Schwache Passwörter sind sehr leicht zu erraten. Dazu gehören Zahlenreihen wie „123456“, Wörter wie „Passwort“ oder „Hallo“ oder auch einfache Kombinationen wie dein Vorname plus Geburtsjahr, zum Beispiel „Lena2009“. Solche Passwörter sind bequem, aber gefährlich, weil Hacker sie in Sekunden knacken können.

Starke Passwörter sehen auf den ersten Blick kompliziert aus, sind aber gar nicht so schwer zu merken. Dafür gibt es verschiedene Methoden:

Die Satzmethode: Du denkst dir einen Satz aus, den du dir gut merken kannst, zum Beispiel: „Meine Oma backt jeden Sonntag Apfelstrudel!“. Dann nimmst du die Anfangsbuchstaben: MObjSA. Damit es sicherer wird, ersetzt du einzelne Buchstaben durch Zahlen oder Zeichen, zum Beispiel: M0bjS@!. Dieses Passwort wirkt zufällig, steckt aber voller Bedeutung, die nur du kennst.

Die Wörter-Methode: Hier suchst du dir drei Wörter, die nichts miteinander zu tun haben, zum Beispiel „Fahrrad – Banane – Kaktus“. Dann fügst du noch Zahlen und Sonderzeichen ein: F@hrrad77Banane*Kaktus. Das Ergebnis ist lang, stark und trotzdem merkbar.

Die Fantasie-Methode: Du erfindest ein ganz neues Wort, das es nicht im Wörterbuch gibt, zum Beispiel „BlupsiZonk94\$“. Durch die Mischung aus Buchstaben, Zahlen und Sonderzeichen entsteht ein Passwort, das extrem schwer zu knacken ist.

Damit du sicher bleibst, solltest du dir drei goldene Regeln merken:

Dein Passwort sollte lang sein – mindestens 12 Zeichen. Es sollte einen Mix enthalten – also Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Es sollte einzigartig sein – also für jeden Account ein eigenes Passwort. Wenn du diese Regeln befolgst und eine Methode wie die Satz- oder Wörter-Methode nutzt, wird dein Passwort zu einer echten Festung. Und dann hast nur du den Schlüssel zu deinem digitalen Leben.

Teil 3 - Webquest: Passwörter ausprobieren

Aufgabe: Du wirst dir nun drei verschiedene Passwörter ausdenken und sie ausprobieren. **Klicke auf den Link, dann kommst du zu einem Passwort-Checker. Dort kannst du dein erfundenes Passwort eingeben und sehen, wie stark oder schwach es ist. Mache dir zu deinen Ergebnissen Notizen!**

Link: checkdeinpasswort.de

Passwort 1:

Wie stark ist es?

Warum ist es stark/schwach?

Passwort 2:

Wie stark ist es?

Warum ist es stark/schwach?

Passwort 3:

Wie stark ist es?

Warum ist es stark/schwach?

Teil 4 - Diskussion: Was ist ein gutes Passwort

Aufgabe: *Du bist mit Teil 3 fertig und schaust nun zu deiner Lehrperson. Ihr diskutiert nun gemeinsam als Klasse. Zeige auf, wenn du eine Wortmeldung oder eine Meinung sagen möchtest. Deine Lehrperson wird euch nun folgende Fragen stellen:*

- Was macht ein Passwort stark?
- Was macht ein Passwort schwach?
- Warum benutzen viele Menschen trotzdem einfache Passwörter, obwohl sie wissen, dass das unsicher ist?
- Was ist wichtiger: Ein Passwort, das man sich leicht merken kann, oder eines, das extrem schwer zu knacken ist?
- Sollten Passwörter regelmäßig geändert werden – oder reicht es, wenn sie einmal stark genug sind?
- Was haltet ihr von Passwort-Managern (Apps, die Passwörter für euch speichern)? Würdet ihr so etwas benutzen?
- Ist ein Passwort wie „BananeKaktus2025!“ besser als „&Xf9!rPz“ – und warum?

Teil 5 - Lesen & Verstehen: Dein Passwort als Festung

Aufgabe: *Im Anschluss zur Diskussion lest ihr euch diesen Text gemeinsam als Klasse mit der Lehrperson laut durch! Melde dich zum laut Lesen, für eine gute Mitarbeit!*

Warum und wie Menschen an deine Passwörter kommen – und was sie damit machen wollen

Menschen mit schlechten Absichten wollen oft an deine Passwörter, weil sie dadurch in deine Konten kommen können: E-Mail, Social Media, Spiele oder sogar Online-Banking. Wenn jemand dein Passwort hat, kann er so tun als wärst du – Nachrichten schreiben, Fotos stehlen, Beiträge posten oder sogar etwas kaufen. Manche wollen nur Ärger machen, andere wollen Geld verdienen oder Informationen sammeln.

Es gibt viele Wege, wie Angreifer an Passwörter kommen. Manche raten einfach: sie probieren häufige Passwörter wie „123456“ oder deinen Namen mit einer Zahl. Andere tricksen dich aus (das nennt man Phishing): sie schicken eine Mail oder eine Nachricht, die echt aussieht, und bitten dich, dein Passwort einzugeben – dann haben sie es. Manche Programme auf fremden Computern können Tastendrücke mitlesen (Keylogger) oder Passwörter ausspähen.

Bei einem Datenleck (wenn eine Webseite gehackt wird) werden viele Passwörter gestohlen und oft im Internet weiterverkauft. Es gibt auch Methoden wie „Shoulder Surfing“ (jemand schaut dir über die Schulter, wenn du dein Passwort eintippst) oder „Credential Stuffing“ – das heißt: Angreifer probieren gestohlene Logins auf vielen Seiten aus, weil viele Leute dasselbe Passwort überall verwenden.

Was machen diese Personen mit gestohlenen Passwörtern?

- Sie loggen sich ein und posten in deinem Namen oder ändern Einstellungen.
- Sie lesen private Nachrichten oder E-Mails.
- Sie stehlen Bilder oder Informationen und verkaufen sie weiter.
- Sie versuchen, Geld zu bekommen – z. B. indem sie Käufe tätigen oder Konten leer räumen.
- Sie verkaufen ganze Passwort-Sammlungen an andere Kriminelle im Internet.
- Manchmal erpressen sie Leute: „Gib Geld, sonst veröffentliche ich deine Daten.“

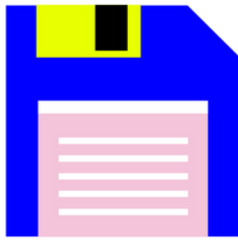
Deshalb ist es wichtig, starke, einzigartige Passwörter zu benutzen, niemals Passwörter in E-Mails oder Nachrichten einzugeben, auf Phishing-Anzeichen zu achten und, wenn möglich, Zwei-Faktor-Authentifizierung zu aktivieren. So machst du es Angreifern deutlich schwerer – und dein digitales Leben bleibt sicherer.

Teil 6 - Gruppenarbeit: Passwörter entwickeln

Aufgabe: Deine Lehrperson teilt die Klasse nun in 3-er Gruppen. Ihr setzt euch im Anschluss in den Gruppen zusammen und entwickelt 4 Passwörter. Versucht dabei alle Regeln für starke Passwörter, die ihr heute gelernt habt, zu beachten! Ihr schreibt eure Passwörter auf und begründet, warum ihr sie so gewählt habt und welche Methode ihr dazu verwendet habt. Im nächsten Schritt zeigt ihr eure Passwörter vor der Klasse über den Beamer und erklärt eure Begründungen und Methoden. Die Passwörter werden dann von der Klasse und der Lehrperson bewertet. Dazu zeigen eure Mitschüler*innen auf und melden sich zu Wort. Zum Abschluss der Präsentation werden die Passwörter mit dem Passwort-Checker kontrolliert. Nachdem alles erledigt ist, sendet ihr euer Dokument an die Lehrperson und es startet die nächste Gruppe.

Du findest deine Vorlage für diese Aufgabe auf der nächsten Seite!

Namen in der Gruppe: _____



Unsere Passwörter

Löst die Aufgabe von Teil 6 auf diesem Blatt. Dieses zeigt ihr dann vor der Klasse!

Passwort 1:

Warum habe ich dieses Passwort gewählt?

Welche Methode habe ich angewandt?

Passwort 2:

Warum habe ich dieses Passwort gewählt?

Welche Methode habe ich angewandt?

Passwort 3:

Warum habe ich dieses Passwort gewählt?

Welche Methode habe ich angewandt?

Passwort 4:

Warum habe ich dieses Passwort gewählt?

Welche Methode habe ich angewandt?

Teil 7 - Reflexion: Was nehme ich mit?

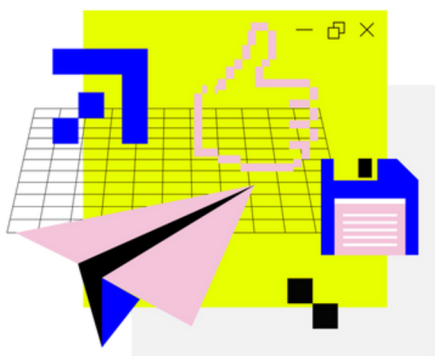
Aufgabe: Wenn alle Gruppen präsentiert haben schaut du nun zu deiner Lehrperson. Ihr reflektiert nun gemeinsam als Klasse über die Einheit und denkt nach, was ihr euch mitnehmen könnt. Deine Lehrperson stellt folgende Fragen:

- Welche neue Erkenntnis über Passwörter war für mich heute am wichtigsten?
- Welche meiner bisherigen Passwörter würde ich jetzt als unsicher einschätzen – und warum?
- Welche Methode (Satzmethode, Wörter-Methode, Fantasie-Methode) gefällt mir am besten, um ein starkes Passwort zu erstellen?
- Was werde ich ab heute bei meinen Passwörtern konkret anders machen?
- Wie kann ich mein Wissen über sichere Passwörter auch in meiner Familie oder bei Freund*innen weitergeben?

Teil 8 - Abschluss: G'scheit gesperrt

Aufgabe: Zum Abschluss der Einheit lest ihr diesen Text gemeinsam als Klasse laut durch. Melde dich per Handzeichen zum Vorlesen!

Heute haben wir gelernt, dass Passwörter wie Schlüssel zu unserem digitalen Leben sind. Schwache Passwörter können leicht erraten oder gestohlen werden, starke Passwörter schützen uns vor Angriffen. Mit Methoden wie der Satz- oder Wörter-Methode lassen sich Passwörter erstellen, die sicher und trotzdem gut merkbar sind. Wichtig sind dabei die drei Goldenen Regeln: lang, gemischt, einzigartig. Wenn wir diese Regeln beachten, wird unser Passwort zu einer echten Festung – und nur wir selbst haben den Schlüssel dazu.



G'SCHEIT GESPERRT

Powered by LIWEST