Assignment on Securing Accounts for CS50 Cybersecurity

All assignments in CS50 Cybersecurity are out of 10 points. A score of 7 points or better (70%) is required to be considered to have "passed" an assignment in this course. **Please do not resubmit an assignment if you have already obtained a passing score**--we consider that spam, and if detected, the submission will be deleted, meaning you will not receive the score back anyway. You don't receive a final grade at the end of the course, so it will have no bearing on your certificate, and it will only slow down our graders!

Unlike CS50x, assignments in this course are graded on a set schedule, and depending on when you submitted, it may take up to three weeks for your work to be graded. Do be patient! Project scores and assignment status on cs50.me/cybersecurity (e.g. "Your submission has been received...") will likely change over time and are not final until the scores have been released.

* Indicates required question

Email *

doetayvious@proton.me

Name *

Paul Gordon

edX Username *

muslimy

What is your GitHub username? *

If you do not already have a GitHub account, you can sign up for one at https://github.com/join. You can then use this account to log in to cs50.me/cybersecurity to track your progress in the course (your progress will only show up after you have received at least one score release email from CS50 Bot, so do be patient!). Don't worry about seeing a 'No Submissions' message on submit.cs50.io, if you find that. The course collects submissions using Google Forms, and only the gradebook on cs50.me/cybersecurity is important!

- **Be certain the username you provide is correct!** If you provide the wrong username, you will not be able to see your scores.
- **Your GitHub username should not be changed while you are taking this course.** The current gradebook system is not designed to accommodate name changes.
- **Be sure to remove extraneous characters,** such as an @ prefix. Do not input a URL or email address, just your username.

sir-papi

City, State, Country *

philadelphia pa usa

Acknowledgement *

Unlike our course CS50x, grading in this course is not done automatically, and there are human reviewers for each assignment. Grading may, depending on exactly when in our grading cycle you submit, take up to three weeks from the time you submit. Your grade status may change in your gradebook at cs50.me/cs50cy in the interim, but grades are never final until you receive a score release email from CS50 Bot (on this first assignment, in fact, your gradebook may not even become active until that score release email). The staff cannot entertain requests for expedited grading under any circumstance. Your patience is appreciated.

◉ I understand.

This course is graded by human graders, and has a ZERO TOLERANCE plagiarism and collaboration policy. If *any* of your answers are copied and pasted from, or obviously based on (a) an online source, including non-course-sanctioned generative AI tools or (b) another student's work in the course, in *any* of the course's five assignments or the final project, you will be reported to edX and removed from the course immediately. There is no opportunity for appeal. There are no warnings or second chances. *

It is far better, we assure you, to leave an answer blank rather than risk it. This may be an online course, but it is offered by Harvard, and we're going to hold you to that standard. **The full essence of all work you submit to this course should be your own.**

- (●) I understand this policy and agree to its terms; I hereby affirm that I will not plagiarize any answers in this course.

Why might being required to change our passwords regularly actually pose a threat to our security? 1 point

user could make simple adjustments to their pw & would allow a previously known pw to be more easily determined.

If I have a six-character password consisting of uppercase (English) letters and (decimal) digits **only**, how many seconds might it take an adversary to crack, assuming they make one attempt per second? 1 point

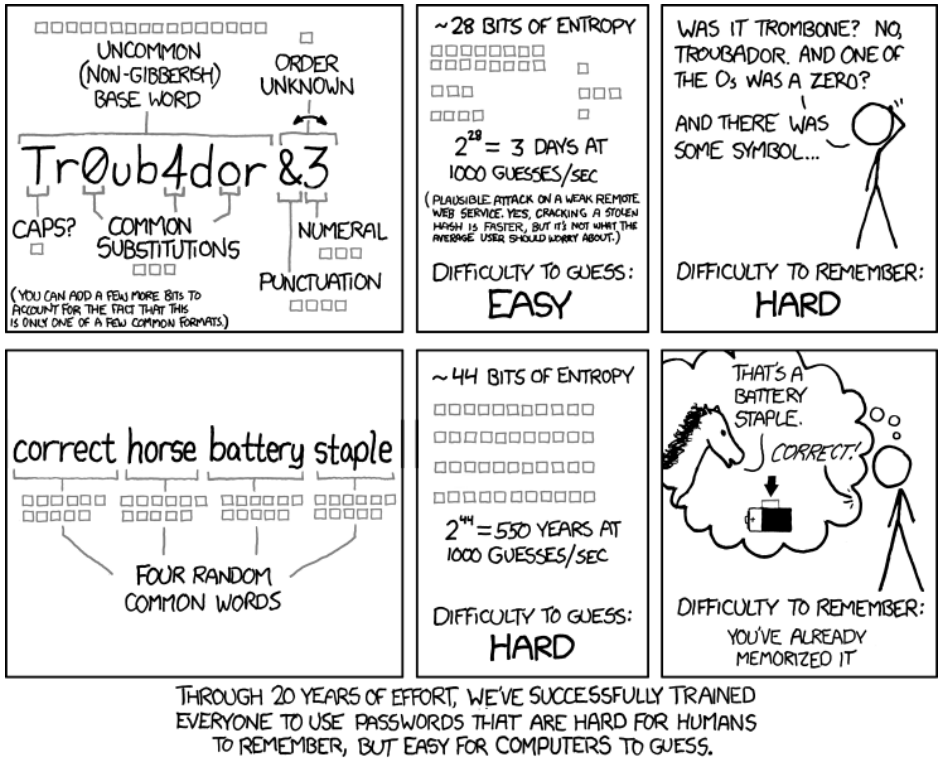
2176782336

Humor us for a moment, and play [The Password Game](), trying to get through at least Rule 12. 1 point

While obviously the game itself is in many ways meant to be humorous, it also critiques the experience many of us have setting up new passwords. Explain how there's a trade-off between usability and security in the context of passwords.

increased security has an adverse affect on usability and vice versa

Consider the below comic for the next two questions.



Consider the top row of the comic above. Why are passwords like those easy (for a computer) to guess but hard (for a human) to remember? 1 point

easy to guess because 28 bits of entropy is a low level of security and attackers with resources wouldn't have a difficult time. hard to remember due to randomness of word, the possible substitutions in characters & numbers, & the order that they appear.

Now consider the bottom row of the comic above. Why are passwords like those hard (for a computer) to guess but easy (for a human) to remember? 1 point

hard for a computer to guess because although its made up of 4 simple words its length creates greater entropy & level of security. its easy because it contains four commonly used words which the user should easily recall

What is a "credential stuffing" attack? 1 point

credential stuffing can result from using the same passwords across multiple platforms and applications so an adversary can brute force many directions with less effort or information.

Provide a specific example of something that would be considered ***a type of knowledge factor*** for authentication purposes. 1 point

Do NOT provide any of your own knowledge factors (or anything resembling them) themselves as an answer to this question. We are looking for you to answer the question in the general sense (a "type of").

If you provide an answer that is, or appears to be, an actual specific knowledge factor, the answer WILL be marked incorrect, without exception, and you should consider that knowledge factor to have been compromised.

the name of your pet or parent

Provide a specific example of something that would be considered ***a type of inherence factor*** for authentication purposes. 1 point

face recognition or fingerprint scan

Why are phishing attacks so difficult to prevent? 1 point

user may be responding to something online that appears to be a legitimate source and looks identical to the authentic trusted source

Suppose that your boss asks you whether the company should require use of password managers for all employees. 1 point

Explain in a short paragraph why you might want everyone in the company to use a password manager.

password managers can prevent employees from needing to: formulate their own passwords; remember them; record them themselves. Because they don't have to remember the pw it can be both computer-generated (and therefore more secure and advanced) and stored and also automatically linked to authentic URLs (and not as vulnerable to phishing attacks.}

Feedback

How did you find the difficulty of this assignment? *

	1	2	3	4	5	
Too easy	○	○	○	◉	○	Too hard

About how many MINUTES would you say you spent on this assignment? *

Just to set expectations for future students.

35

A copy of your responses will be emailed to the address you provided.

Submit Clear form

Never submit passwords through Google Forms.