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? 1/1

1.There may be repeated patterns, for example, if our password is 123 , next month we will change it to 1234 this is so easy to guess what's the password is in the next months . 2. And next we will have password overloads, their management is difficult and all passwords must be saved in somewhere and maintaining them,this is unnecessary!!!!

✓ 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? 1/1

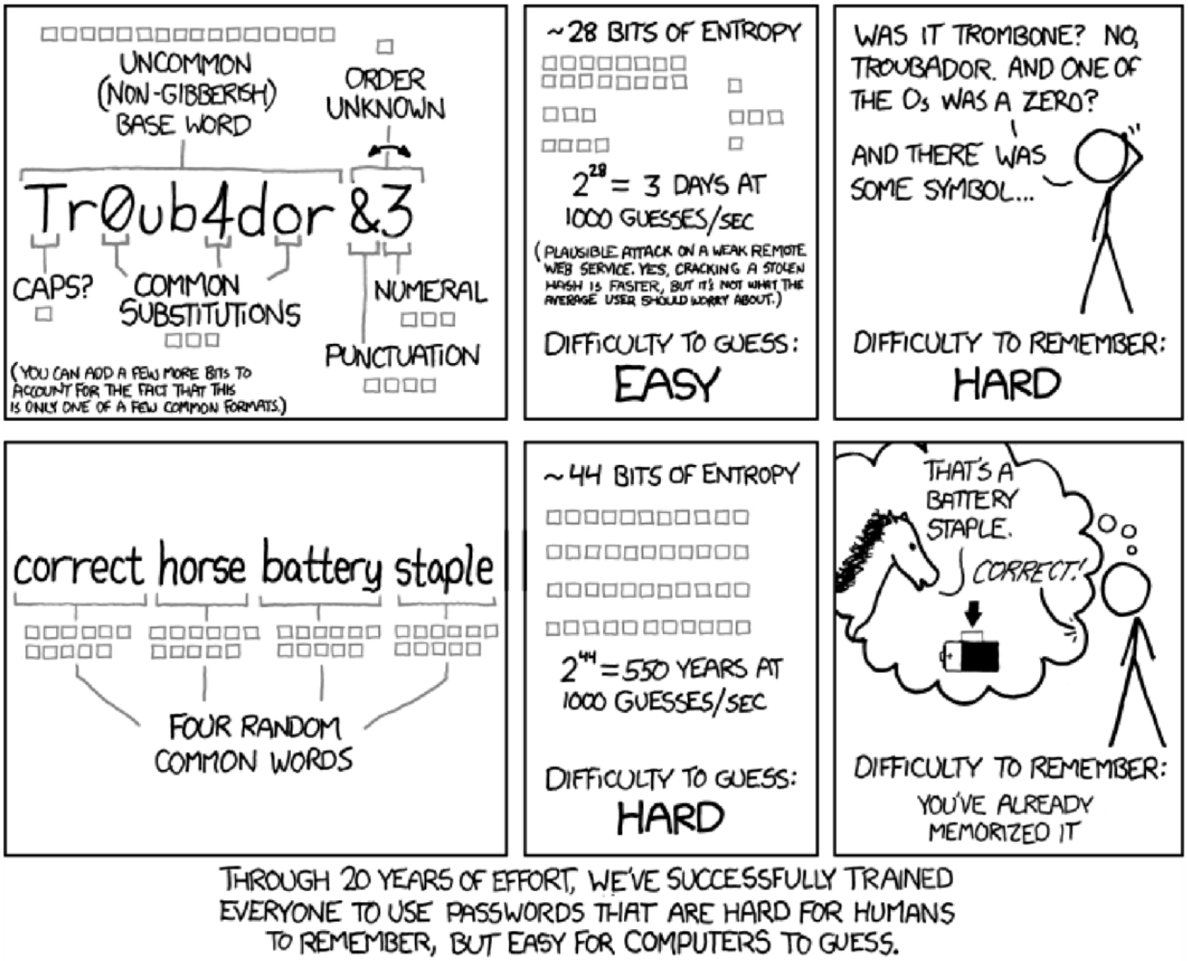
2176782336 ✗

✓ Humor us for a moment, and play The Password Game, trying to get through at least Rule 12. 1/1

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.

If we do this , we will realize that we have so many details and numbers, characters and symbols that are very complex and long , which really cannot memorize so we must be saved and stored somewhere like paper or in the computer. Which can actually be safe forever .but In this situation,we can see there is the issue of security and usability, no matter how hard we try .

Consider the below comic for the next two questions.


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

✗ 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? 0/1

Some passwords are difficult for computer to read and understand like some words, and conversely, passwords full of long numbers, characters, and symbols are difficult for human to remember.

✓ 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? 1/1

Long meaningful sentences are too hard for camputer to boot-force, however too hard for human to remember all the long numbers, letters(uppercase too) and symbols.

✓ What is a "credential stuffing" attack? 1/1

It is an attack that does not require such a system attack, and with the help of pre-hacked data on other websites, accounts, and other platforms, it gains access to the website and others.

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

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.

Password, email address, first pets name ✗

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

Eyeball ,Face recognition ✗

✓ Why are phishing attacks so difficult to prevent? 1/1

Because it's difficult to recognize it and we should always be careful, the SMS related to our favorites or the page of payment portal is seen with the same real payment portal site , in the fact, our interest are being misused.

✗ Suppose that your boss asks you whether the company should require use of password managers for all employees. 0/1

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

Because of the upward rocket attacks, we must definitely reach a security level. One of the things: we can do is to equip the system of all employees and personnel with the password manager, and they will completely prevent attacks.

Feedback

How did you find the difficulty of this assignment? *

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