Cyber Aware Workers Toolkit

Facilitator Guide

This facilitator guide will assist you in using the Cyber Aware Workers Toolkit in a group setting. No specialist knowledge is required to host a session using the toolkit.

Recommended session length: 45 minutes

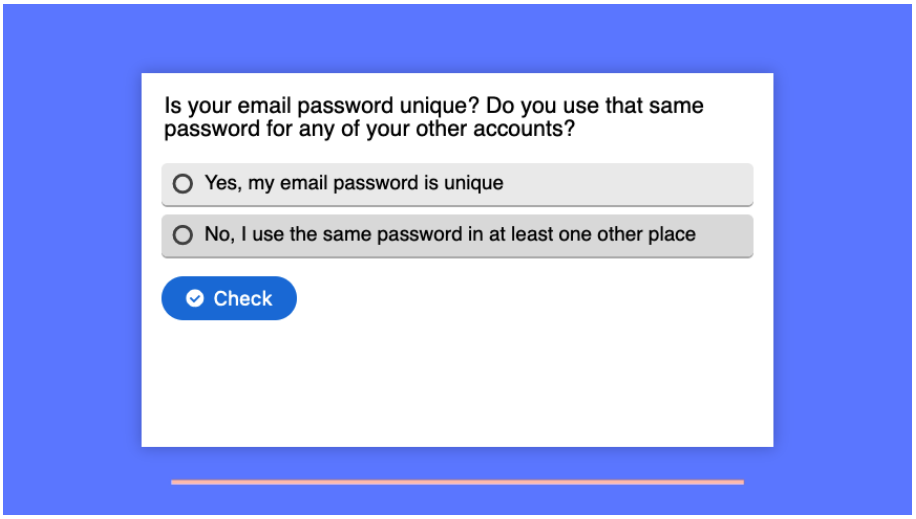
How to use:

1. Play the toolkit on the screen.
2. At the timestamps listed below follow the conversation prompts in this document.

Timestamps are at the same time as multiple choice questions where the video pauses automatically.

The toolkit can be found at:
https://digitalskillseducation.com/cyber-aware-toolkit-preview/

Question: 3:00

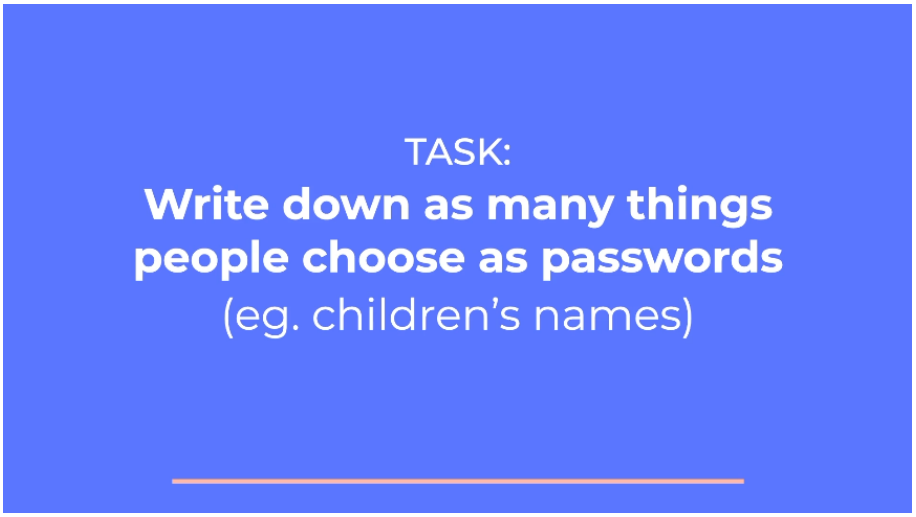


Ask the group: "*Why do you think it's less secure to use the same password over and over again? What might a cyber criminal try to do?*"

Answer: "Cyber criminals will try your email and the known password on lots of different passwords in the hope you reused your password."

The video continues to explain this technique, called *Credential Stuffing*.

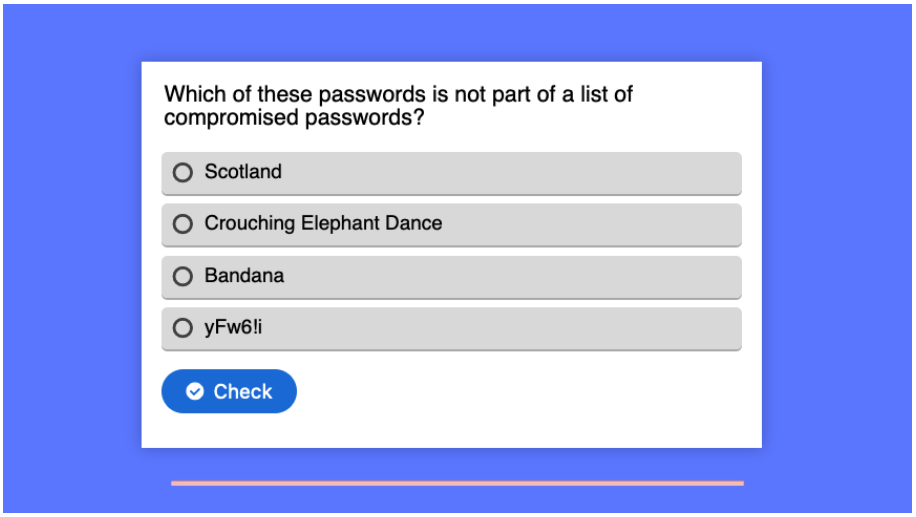
Question: 4:00



Go around the room and get an example of a type of thing people might choose from each person in turn. How long can you go for?

Extension:
What do you think the most popular password was in 2021?
(answer 123456)

Question: 6:20

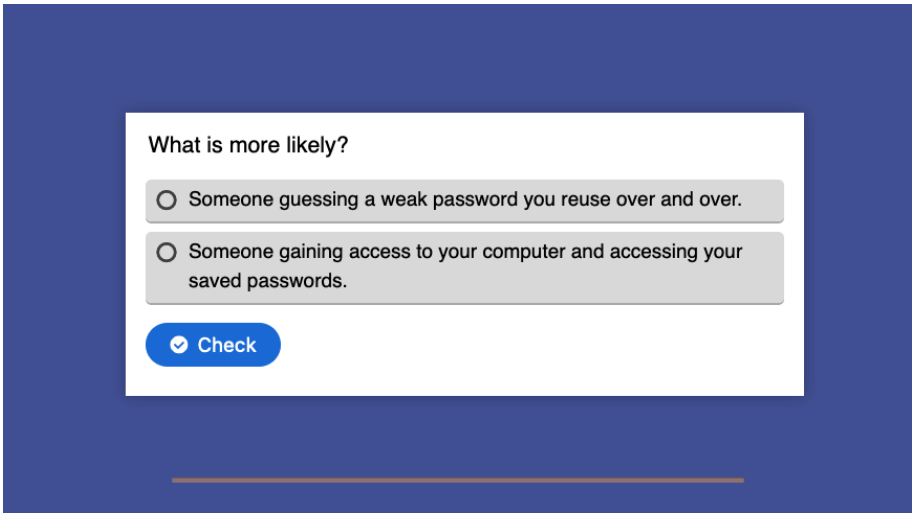


Go around the room. Which password is likely to be the most difficult for a computer to guess? Remember that the thing that makes the biggest difference to the security of a password is its length.

Extension:
If you have time, get the participants to visit:
https://www.security.org/how-secure-is-my-password/ and try out a short password, maybe something they used to use. How long would it take a computer to break it?

Now, get a random word from 3 different people and create a secure passphrase. How long would this take to break?

Question: 9:20

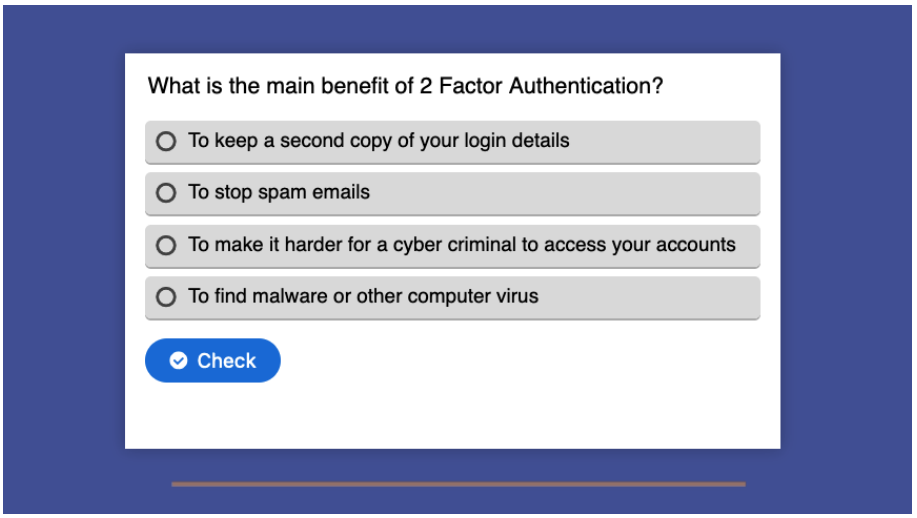


Why not put this one to a poll in your group? Ask participants why they chose their vote.

Extension:
Ask the group how they store their passwords. Do they memorise them all, write them down, save them in their web browser, or use a password manager?

What is the strength or weakness of their approach? Ask everyone for a strength and a weakness.

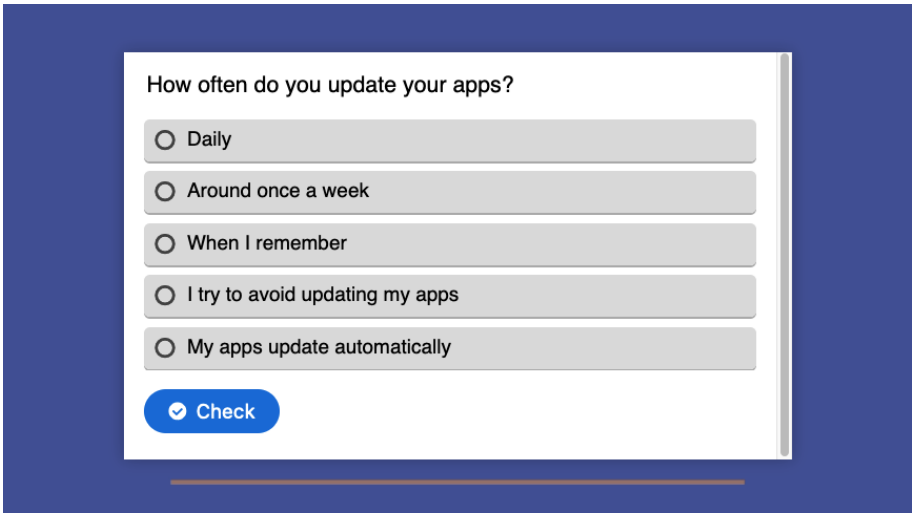
Question 11:20



Answer the question together. The correct answer is “to make it harder for a cyber criminal to access your accounts”.

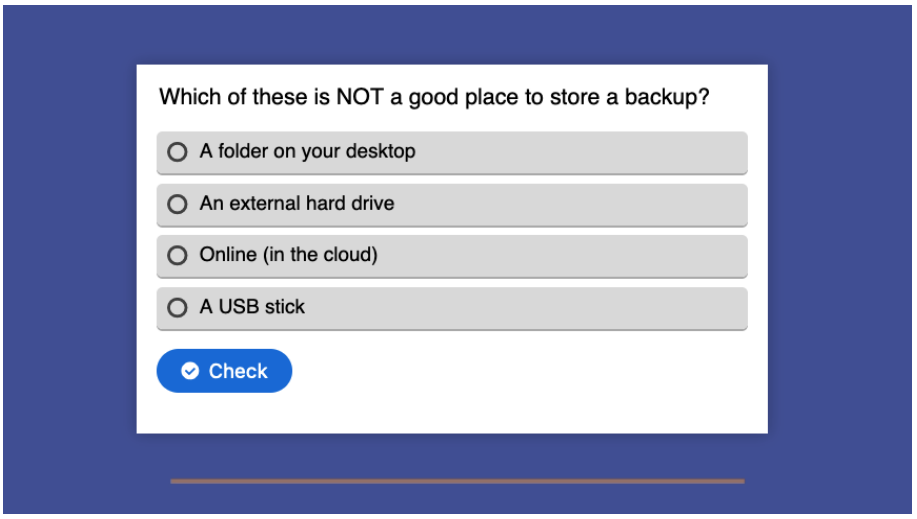
Extension:
Does anyone in your group use 2 Factor Authentication?
What services or accounts have they turned it on for? Is it easy to use?

Question: 12:10



Run this one as a poll. The best way to update apps is automatically, then you never have to remember!

Question 15:40



Answer the question together. Answer is a folder on your desktop, because it is not on a different device to the original files.

Extension:
Where do people in your group make their backups? Do they do it online? To a hard drive? A USB stick?

Has anyone changed their backup strategy after losing data?

At the end of the session:
Please ask your participants to complete the evaluation form. They can find it on the web page under the toolkit, or at this link https://form.jotform.com/220394646702052