CYBERSECURITY WITH PROF DOUG JACOBSON

TALKING POINTS

KNOWLEDGE

1. What is cybersecurity, and how can it affect you?

2. What makes a strong password?

COMPREHENSION

3. How much information do you post online about yourself? How much control do you have over this information?

4. Is there any information about yourself online that you do not control? For example, from your school or sports club.

APPLICATION

5. What would you do if you found out you had been hacked?

ANALYSIS

6. Why do you think hackers do it?

7. Do you think people are aware of how much information is available online about them? (Hint: Probably more than they think.)

8. What examples of phishing emails have you received? What do they have in common?

SYNTHESIS

9. Use your experience and write up an imaginary phishing email.

EVALUATION

10. How would you judge whether or not a site is trustworthy?

ACTIVITIES YOU CAN DO AT HOME OR IN THE CLASSROOM

ACTIVITY 1. HOW SAFE ARE YOUR PASSWORDS?

Every time we have to log in to our email or social media account, we need a password. One of the best ways to prevent being hacked is to create a strong password that is hard to guess. Passwords like '123456' or 'qwerty' are not strong and will probably be the first ones hackers try if they want to login to your account. Strong passwords need to be long and preferably not actual words, but a random sequence of upper and lowercase letters, numbers and symbols. '67htBhft^kh53£' is much better than 'chocolate123', but how do you remember that?

- Discuss possible strategies to create a strong password. Writing it down on a piece of paper is not a secure option!
- Use an online tool to check the strength of your password. Nordpass, for example, will even tell you how long it will take for hackers to crack your password: https://nordpass.com/secure-password/

A strong password does not guarantee that you will never be hacked. However, following these guidelines will make your password virtually impossible to guess by hackers, and any automated systems they use will take a very long time to get a result.

ACTIVITY 2. USE DIFFERENT PASSWORDS

If you add up all your social media email and online shopping accounts, you probably have quite a few passwords to remember. Even if you have a strong password for your account, using the same one everywhere is a very bad idea. Imagine if you fall victim to a phishing attack, and hackers get hold of your username and password for your email. If you used the same password on other sites, now hackers can login and get your name, home address, phone number, and even connect to your gaming account or delete your photos on Instagram.

- Conduct a simple survey in your class to see how many different passwords your peers use for their accounts.
- Analyse the results to show how many passwords each person uses, and whether they use the same for certain sites, like social media, gaming, etc.
- How could your peers improve their cybersecurity? Try to offer some practical advice based on what you have found out.
- Talk about password keeper programmes that let you security store your password.

MORE RESOURCES

Access some of the materials developed by Prof Doug Jacobson and his team to teach cybersecurity awareness: www.security-literacy.org

Find out more about the Hackerville 'village' that Melissa and Chris worked on: www.hackerville.org

Look into Iowa State University's IT Adventures programme developed for high school students: www.it-adventures.org