**Introduction to cyber security
Lesson 1: What is cyber security?**

**Introduction**

In this lesson students learn about cyber security and, through practical application, about ethical hacking. They also learn about the importance of cyber security in the world today, consolidating and extending their prior learning about internet safety.

**Time:** @60 minutes

**Learning objectives**

* to understand about the importance of cyber security in the world today
* to be able to explain what is meant by the term ‘ethical hacking’
* to understand how to recognise potential malware attacks and how to protect data and devices.

**Materials needed:** Lesson plan, lesson guide, whiteboard, ‘malware or made up’ cards printed and cut up, Cyber Security scenarios Slide 7 printed out, ‘Beat the Hacker’ cards printed.

**Lesson summary**

1. What is malware? (10 minutes)
2. What is Cyber Security and why does it matter? (10 minutes)
3. Cyber security risks - a global problem (15 minutes)
4. Cyber security jobs (10 minutes)
5. Beat the hacker (10 minutes)
6. Review and wrap up (5 mins)

**Introduction: What is malware? (10 minutes)**

* Share the learning objectives on **slide 2** if you wish and use **slide 3** to lead a discussion around ‘malware’ and check students’ current understanding.
* Give out mixed-up copies of the **malware or made up cards** to pairs of students and explain you want them to sort the cards into two piles, according to whether they think the name on the card is associated with malware or is made up (**slide 4**).
* Go through the answers using **slide 5** (and see the slide notes if want further information).

**What is Cyber security and why does it matter? (10 minutes)**

* Give students in their pairs a few minutes to think/pair/share the questions on **slide 6** (and to make notes if you wish).
* Lead a class discussion around their ideas, inviting them to share their own examples and using **slide 7** to clarify understanding if needed.

**Cyber security risks: a Global Problem (15 minutes)**

* Explain the role of the National Cyber Security Centre, part of GCHQ (**slide 8**) and follow the link to the website to show students it publishes details of weekly cyber security threats around the world.
* Give students 5-10 mins to research the website, find some interesting stories and feedback as a class.
* Highlight that, as they have seen from their research, Cyber Security is now a global problem that affects many areas of our lives.
* Give students time to think and discuss the questions on **slide 9** before discussing the answers as a class.

**Cyber security jobs (10 minutes)**

* Computer Misuse Act (UK):you can be sent to prison for up to 14 years and / or face a large fine for malicious hacking.
* Watch the video on **slide 10** (or find an alternative if you wish) to highlight a recent story about teenage hackers.
* Use **slides 11 and 12** to explain that hackers can also be employed ‘ethically’, the increase in cyber security risks has led to an increase in the demand for cyber security jobs and people can be employed as ‘white-hat’ (ethical) hackers.
* Students may have stories to share from their own knowledge and understanding and this can be encouraged.

**Beat the hacker (10 minutes)**

* Give out the **beat the hacker worksheets** to pairs or small groups (**slide 13**).
* Ensure they understand what to do and give a suitable amount of time to complete (the suggestions are only some of the possible solutions to the scenarios and they should add in their own ideas). Discuss as a class.
* Ask each pair or team to self-certify as to whether they could be good candidates for cyber-security jobs in the future given their performance on the task.

**Review and wrap up (5 minutes)**

* Review the learning objectives if you wish on **slide 14** and invite students to think/pair/share what they have learnt during this lesson.

**Extension ideas:**

* Student could conduct further research about malware before creating their own blog post or web page and providing top tips to help others avoid the pitfalls. These could be uploaded onto the school website. A good starting point is [BBC Bitesize.](https://www.bbc.com/bitesize/guides/zs87sbk/revision/1)

**Differentiation**

**Support:**

* Students may benefit by being put into mixed ability groupings to aid with discussion and question prompts, particularly in the ‘malware or made up’ and ‘beat the hacker’ activities.
* You could give students only one or two of the scenarios for the ‘beat the hacker’ activity to focus on.

**Stretch & challenge:**

* Students can be asked to provide more of their own ideas in the ‘beat the hacker’ activity, researching possible solutions if appropriate. They could also come up with their own problems for others to try to solve and swop them.
* Students can be encouraged to explore cyber security further and give advice to others (see extension).

**Opportunities for assessment:**

* Informal observation and assessment of students’ during activities and discussion.
* More formal assessment, if wished, of their answers to the ‘beat the hacker’ activity.