

Computing

Lesson 3: Automated Cybercrime

KS4 Security

Ben Garside



Task 1 - Ransomware (Wannacry)

Start by watching this short video below:



Wannacry, Source:
:securelist/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/



Task 1 - Ransomware (Wannacry)

In this short video (between 10:40 and 12:51), Computerphile explains why the exploit was successful. Watch the video and answer the following questions:

How did WannaCry spread?	
What type of malware is WannaCry?	
Who can share the blame for the spread of WannaCry?	



Task 2 - Brute force: Passwords

For this activity you will need to use/run and amend the following python program to be able to answer the questions on the following slides:

repl.it/@NCCE/brute-force

Please ask a parent or carer for permission before attempting this task.
Oak National Academy are not responsible for any third party content.



Task 2 - part 1

The program has been set to output how many attempts it took to find the password (set on line 11), as well as how long it took the computer to do it.

Run the program.

Follow the instructions on the next slides and note down the results.



Task 2 - part 2

Instruction	Number of attempts	Time taken (round up to two decimal places)
Run the program with the password 'ab'		
Change the password to 'abc'		
Change the password to 'Abc'		
Change the password to 'Abc1'		



Task 2 - part 4

The program has been set to check only for ASCII letters and digits.

Modify line 15 of the program so that it checks for punctuation and any white space in the password (white space is an empty value in the password, such as a space).

Line 5 should now look like this:

```
15 print(guess_password(password, extended))
```



Task 2 - part 5

Run your program.

Follow the instructions below and note down the results.

Instruction	Number of attempts	Time taken (round up to two decimal places)
Run the program with the password 'abc'		
Change the password to 'Ab1'		
Change the password to 'Abc1?'		
Change the password to 'AB C 1'		



Task 2 - part 6

Thinking about the exercise that you just completed, what simple password rules would you set yourself to reduce the chance of a brute force attack being successful?

What rules do you think a company might place on their login system to reduce the chance of a brute force attack being successful?



Task title

- Info for students to complete the task.
- Images, will be removed from this if printed.
- Optional placeholder for image or text



**Resume the video
now**

