NCA Cyber Choices Lesson Plan

This lesson plan is available for teachers across the UK to help to educate pupils about what Cyber Crime is, the effects it has and to introduce the Computer Misuse Act

We passionately believe that the teacher is the best person to decide on the suitability and specifics of activities in their classroom or other learning environment, therefore this lesson plan is deliberately designed to be flexible and we encourage adaptation to suit the individual needs of your classes

National Crime Agency

http://www.nationalcrimeagency.gov.uk/

Lesson Plan written by Jason Stanton, Cyber Security Challenge UK

https://cybersecuritychallenge.org.uk/

Ongoing support provided by Computing at School network

http://www.computingatschool.org.uk/

Learning Objectives:

- Increase pupils' cybersecurity vocabulary
- Providing pupils with information on what is considered to be a cyber crime
- Raise pupils' awareness of the consequences of criminal behaviour online through the Computer Misuse Act

	TEACHER ACTIVITY	PUPIL ACTIVITY
STARTER ACTIVITY (5-10 MINS) [INDIVIDUAL/PAIRED OR GROUP]	- Read accompanying NCA information. - Cut out the terms from the Key Terms Starter Sheet and place on each table of pupils - Display correct answers and initiate discussion on answers given by pupils	- Pupils have to match up the correct term with the correct definition - Discussion around correct and incorrect answers
MAIN ACTIVITY ONE (15 MINS) [GROUP ACTIVITY]	- Gather pupils into a position to see the main screen and show the NCA Choices video and video of former LulzSec Hacker Ryan Ackroyd reflect on his experiences - Lead a discussion on the impact of Cybercrime on victims, cybercriminals, families, and on society as a whole - List down as a many types or examples of cybercrime that the class can come up with - Helpful page here http://www.thewindowsclub.com/types-cybercrime - Construct a 'class-agreed' hierarchy of crimes from 'not at all serious' to 'very serious' on the board and initiate discussion on answers given by pupils (could use a lead learner for this activity)	- Pupils watch NCA Choices video - Discussion about the video and what they feel are the consequences of cybercrime - The pupils, in groups, need come up with as many different types and examples of cybercrime they can think of in 5 minutes - Class discussion leads to a class agreement on a hierarchy of seriousness of the cyber crimes
MINI-PLENARY (5-10 MINS)	- Assess learning against the learning objectives - This is an open activity whereby the teacher will decide on the best approach to do this based on the pedagogical approach your school takes on assessment.	- Possible assessment options include but are not limited to: - 5 minute timed writing exercise on what has been learned so far - Write a blog post/wiki post - Discussion - Directed questions
MAIN ACTIVITY TWO (15 MINS) [INDIVIDUAL]	- Direct pupils to the Cyber Crimes Game on the CSC website teaching them about the Computer Misuse Act - Monitor progress of pupils on the game and help out where pupils might have questions (although game should be fairly self-explanatory)	- Pupils play the game and make judgements based on what they are learning about the CMA - Able to improve their scores if necessary, depends on teacher decision on pace of lesson
PLENARY (5-10 MINS)	- Assess learning against the learning objectives - This is an open activity whereby the teacher will decide on the best approach to do this based on the pedagogical approach your school takes on assessment.	- Possible assessment options include but are not limited to: - 5 minute timed writing exercise on what has been learned so far - Write a blog post/wiki post - Discussion - Directed questions
HOMEWORK (OPTIONAL)	- Teacher choice based on homework policy of school. - Recommend pupils registering for the Play On Demand system of games on CyberSecurity which can be found at: - www.cybersecuritychallenge.org.uk	Pupils to create an aide memoir in whatever format suits the age group. Poster, revision cards, page on a school VLE, wiki-page, podcast, etc.

Key Terms Starter Sheet

Cybercrime	Any illegal activity that uses a computer as its primary means of commission
Spamming	Sending the same message indiscriminately to a large numbers of Internet users
Identity Theft	The fraudulent practice of using another person's name and personal information in order to obtain credit, loans, etc.
Hacking	Gaining unauthorised access to data in a system or computer
Phishing	The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information online
Botnet	A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.
Denial of Service (DOS) Attack	An attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet
Firewall	A security barrier designed to keep unwanted intruders "outside" a computer system or network while allowing safe communication between systems and users on the "inside".
Virus	A malicious program or code that attaches itself to another program file and can replicate itself and thereby infect other systems