# L1: Network Security: The Attacks P1

This is a lesson for Year 10 students aimed at covering Network Security Attacks. This lesson aims to cover the main topics from 1.4.1 from the OCR specification.
https://www.ocr.org.uk/Images/558027-specification-gcse-computer-science-j277.pdf

Aims:
- Give students an idea of the types of Network Attacks including Malware, Social Engineering, Brute-Force Attacks, The concept of SQL Injection.

| Time | Activity | How will learners be assessed? |
|---|---|---|
| **9:45** | **What is Network Security?**<br>Students write every word they can think of to do with Network Security on a word cloud. | |
| **9:50** | **Malware, Viruses, Worms, Trojan Horses**<br>- Teacher will give a short presentation covering Malware, Viruses, Worms, Trojan Horses<br>- Students will then complete a matching up activity | They will have to write the main features of each Then have to apply that knowledge to work out from scenarios what they are. |
| **10:00** | **Social Engineering & Phishing**<br>- Teacher will give a short presentation on Social Engineering<br>- Students will then be given an email and have to highlight the common signs of social engineering. As an extension they can create their own in the same style. | To create the email they would have to know the common signs of phishing emails |
| **10:10** | **Brute Force**<br>- Teacher will give a short presentation on Brute Force.<br>- Students will try and think of lots of common passwords and use word cloud on menti.com | Students will have to think of common passwords that would be susceptible to Brute Force Attacks. Later we will try and use Brute Force to break into the |
| **10:15** | **DoS & DDoS**<br>- Teacher will deliver a presentation explaining DDoS & Data Interception<br>- Then using the heroku website we will simulate a DoS attack with the whole class with a countdown. The teacher can at the same moment simulate the attack by pressing the DoS button on the Website Controller. This will appear to students as if we've done a DoS attack giving them some real experience. | |
| **10:25** | **Brute Force Exercise**<br>- Students will break into 3 different accounts following hints given to them. | |
| **10:28** | **END Lesson**<br>Survey: Students should complete a google form on the lesson.<br>Homework: Students will be given a set of questions and research to do on Actions of Malware. | This will be checked next lesson through a Kahoot based quiz at the start of the lesson to gauge understanding. |

# L2: Network Security: More Attacks and The Defences

This is a Year 10 students aimed at finishing off Network Threads and covering network defences. This lesson aims to cover the main topics from 1.4.2 from the OCR specification.

| Time | Activity | How will learners be assessed? |
|---|---|---|
| **9:45** | **Intro Kahoot**<br>- Will contains a variety of questions covering the topics from the previous lesson | |
| **9:55** | **Passwords & User Access Levels**<br>- Teacher will give a short presentation covering the main topics.<br>- Students will then complete an activity based on choosing the correct access levels. | By completing the section of the worksheets students will have to understand different network access levels and how different users should have different levels of access to secure information. |
| **10:05** | **Anti-Malware & Firewalls**<br>- Teacher will give a short presentation<br>- Students will have to work out what threats could be protected by Anti-Malware and Firewalls | |
| **10:15** | **Data Interception & Encryption**<br>- Teacher will explain the concepts of Data Interception and how data can be intercepted.<br>- Teacher will then explain how Encryption protects data and keeps it secure.<br>- Students will then complete an exercise on Encryption | |
| **10:33** | **END LESSON**<br>For Homework students will have to translate Ceasar Ciphers | |

# L3: Network Security: Physical Security & Penetration Testing

| Time | Activity | How will learners be assessed? |
|---|---|---|
| **9:45** | **Intro Kahoot**<br>- Will contains a variety of questions covering the topics from the previous lesson | Kahoot Style Quiz Based on Common Misconceptions and Homework/Previous Lesson Content. Some of the questions that students struggled with more last week are repeated here. |
| **10:00** | **Physical Security & Penetration Testing**<br>- Brief sentence on Physical Security. Then getting students to think of Physical Security Aspects in their school, home etc.<br>- Teacher will give a short presentation covering the idea of penetration testing.<br>- Students will then have to research the differences between a White Hat, Grey Hat and Black Hat Hacker. They will then have to work out which one we are in our earlier hacking session and what the Legal Implications are for them. | In the Word Cloud they will have to think of different ideas for security aspects.<br><br>Since they will have to apply their research to discuss what kind of hacker we are they have to evaluate and understand the options. |
| **10:10** | **SQL Injection**<br>- Teacher will give a short presentation explaining the concept of SQL Injection, And What that might mean for users.<br>- Working out how to do it will be part of the Student Activity where they are guided through performing SQL Injection on a Website. | |
| **10:20** | **Password Security Exercise**<br>- Students will have to write a Program that checks various aspects of security<br>- Then they will have to extend it with their own idea of a more complex login checks. e.g. Max Number of Tried, Lockout | |
| **10:33** | **END LESSON**<br>Students will complete a survey before turning in their exercise and the program that they've written. | |