THE DUSTON SCHOOL 4-19

Knowledge Organiser

Computing

Year 9 Term 2: Cyber Security

Enquiry Questions

- What is Cyber Security and what jobs can it lead to?
- What is Phishing?
- What is Cyberwarfare?
- What do cybersecurity personnel do?
- What is the difference between a virus and a worm?
- How can encryption keep your data secure?
- What are some of the dangers of Spyware?
- What do ethical hackers do?
- What is the difference between a grey hat and a black hat hacker?

Terminology

Cyber Security The protection of internet-connected systems, including hardware, software and data, from cyberattacks.	**Malware** Software that can harm devices, which is installed on someone's device without their knowledge or consent.	**Virus** Viruses attach (by copying themselves) to certain files. Users spread them by copying infected files and activate them by opening those files
Worm Worms are like viruses but they self-replicate without any user help, meaning they can spread very quickly.	**Trojan** Trojans are malware disguised as legitimate software. Unlike viruses and worms, Trojans don't replicate themselves – users install them not realising they have a hidden purpose.	**Spyware** Secretly monitors user actions (eg. key presses) and sends info to a hacker
Frequency The frequency of a wave shows its pitch (how high is the note?) Frequency is measured in Hz – cycles per second	**Digital forensics** The process of uncovering and interpreting electronic data for the purpose of reconstructing past events.	**Encryption** The act of protecting data by scrambling it in such a way that only someone with the secret code or key can read it
Decryption The act of unscrambling encrypted data, with a secret code or key, so that it can be read.	**Cipher** An algorithm for performing encryption or decryption.	**Cyber warfare** An Internet-based conflict that involves the penetration of computer systems and networks of other nations.

Online Dangers

Social Engineering

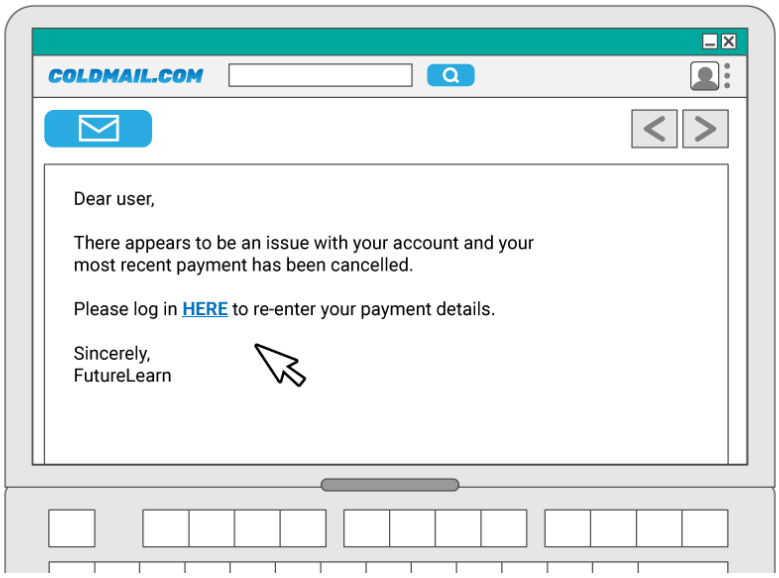
What is social engineering?
Social engineering is the name given to the type of attack that deceives victims into sharing valuable personal data.

There are many different types of social engineering attack. In this step, you will learn about three kinds:

- Phishing attacks
- Pharming attacks
- Name generator attacks

Phishing attacks

A **phishing attack** is an attack in which the victim receives an email disguised to look like it has come from a reputable source, in order to trick them into giving up valuable data.
The email will either ask for the information directly, or provide a link to another website where the information can be inputted. This attack may also come via phone call or text message.



Phishing emails can be recognised in a number of ways. Key indicators to look out for include:

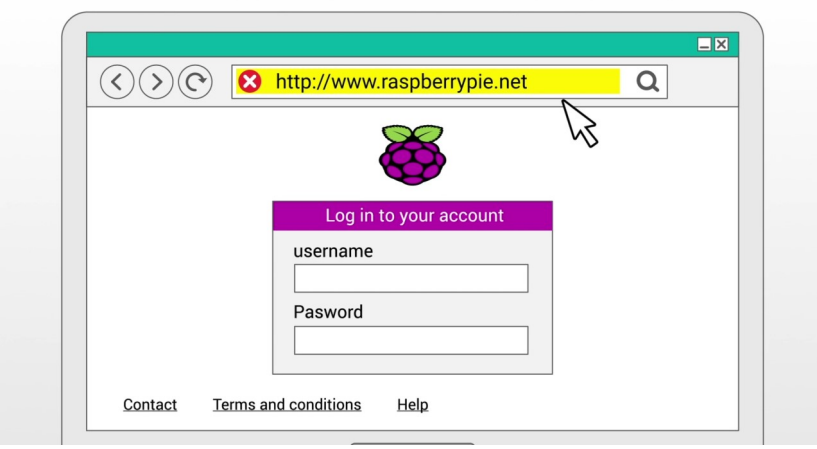
- Any unexpected email with a request for information
- Sender email addresses that contain spelling errors, lots of random numbers and letters, and/or domain names that you don't recognise
- Suspicious hyperlinks:
  - Text that appears to be hyperlinked but does not contain a link
  - Text that is hyperlinked to a web address that contains spelling errors and/or lots of random numbers and letters
  - Text that is hyperlinked to a domain name that you don't recognise and/or isn't connected to the email sender
- Generic emails that don't address you by name or contain any personal information that you would expect the sender to know

Online Dangers

Social Engineering

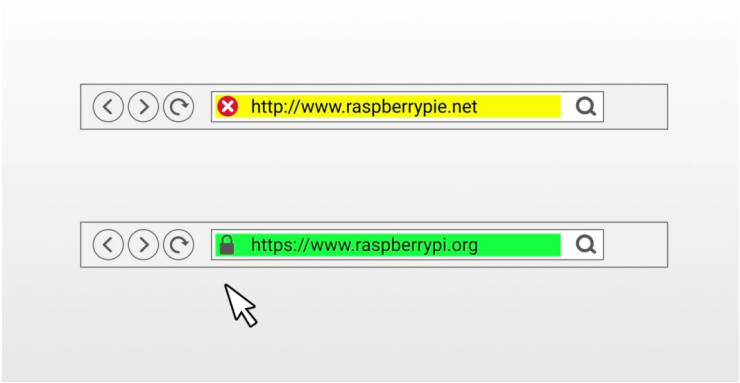
Pharming attacks

A **pharming attack** is an attack in which malware redirects the victim to a malicious version of a website. The malware could infect the victim's computer or the DNS server (the database that allows your browser to find the website you're visiting. Then, when the victim enters a web address into their browser, they visit a website controlled by the attacker, rather than the legitimate website. The attacker can then collect any data that the victim inputs into the website. Links in phishing emails may also redirect victims to pharming websites.



As with phishing attacks, pharming attacks can be identified from aspects of the website that seem out of place or incorrect. For example, any of the following could indicate a pharming attack:

- Spelling errors or incorrect logos
- Broken or missing links
- A notification from your browser warning you that the webpage is insecure
- The lock symbol that your browser uses to confirm that a webpage is secure is missing



If you suspect that a website is malicious, you should close your browser and run up-to-date antivirus software on your computer, then reload the page to see if it has changed.

Online Dangers

Social Engineering

Name generator attacks

A name generator attack is an attack in which the victim is asked in an app or social media post to combine a few pieces of information or complete a short quiz to produce a name.

Attackers do this to find out key pieces of information that can help them to answer the security questions that protect people's accounts.

To protect yourself from name generator attacks, you should avoid providing apps with the following pieces of information or posting this information publicly on social media sites:

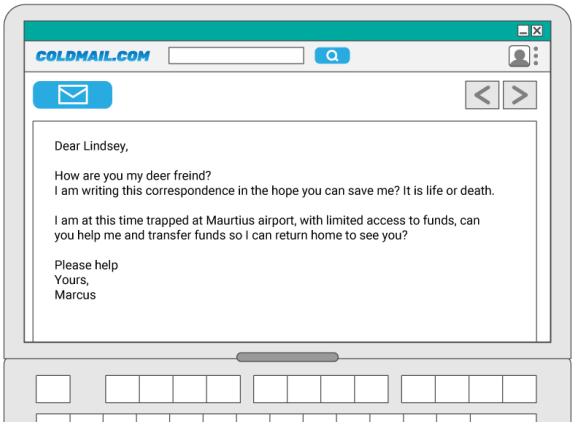
- Your mother's maiden name
- Names of current or previous pets
- Previous or current addresses
- Your age or birthdate
- Your lucky number
- Any of your favourite things (such as your favourite place or author)
- Any information that you know you have used to create a password or set up a security question

Blagging

Blagging (also known as pretexting) is an attack in which the perpetrator invents a scenario in order to convince the victim to give them data or money. This attack often requires the attacker to maintain a conversation with the victim until they are persuaded to give up whatever the attacker has asked for.

Online Dangers

Social Engineering



For example, the victim might receive an email from an attacker pretending to be a friend trapped in a foreign country in desperate need of a money transfer that will be repaid with interest as soon as they are safe.

A particularly common type of blagging attack is an **online dating scam**. In an online dating scam, the attacker might meet the victim through a dating app or chat room and begin an online relationship with them. Then, they might ask the victim for money or gifts, or if they find out that the victim is married, threaten blackmail. Action Fraud estimates that around £27 million was lost to this kind of scam in 2014/15.

Shouldering

Shouldering (also known as shoulder surfing) is an attack designed to steal a victim's password, or other sensitive data. It involves the attacker watching the victim provide sensitive information, for example, over their shoulder. This type of attack might be familiar as it is often used to find out someone's PIN at a cash machine.

Online Dangers

Hacking

How are passwords hacked?
You will learn about three different types of password attack: brute force attacks, theft of individual passwords, and theft of batches of passwords.

Brute force attacks
In a brute force attack, an attacker guesses passwords until they find the correct one. This might involve guessing a combination of characters, or creating a list of passwords beginning with the most common, as in the more specialised dictionary attack. The dictionary that attackers use contains passwords centred around real words and combinations of real words.

Theft of individual passwords
An attacker could steal a victim's password, for example, by using the social engineering techniques discussed previously, or by infecting the victim's device with a form of malware that records their activity, including the letters that they type. You will learn more about malware next week.

How do you make a strong password?

Passwords should be memorable for the individual, but difficult for an attacker to guess. As you have seen, password attacks often rely on victims using common combinations of characters and similar passwords across multiple accounts. Therefore, all of your passwords need to be different and unpredictable.

Avoid using personal details and dictionary words
You should avoid using any personal details, like your pet's name or your favourite sports team, as a basis for your password. To protect yourself from a brute force attack, you should avoid dictionary words altogether, even if you're substituting some letters for numbers or symbols — if "password" is in the attacker's dictionary, so is "p@ssw0rd".

Increase the length and complexity of your password
You should also increase the length of your password and add in more types of character. The more types of character you include and the longer your password is, the more guesses the attacker has to make.

Use a strong password generator
Rather than finding a strong password, it is better to design a strong password generator that you can use to easily create lots of memorable passwords that appear random. Here are three methods of generating passwords:

- Create a phrase from random words — you can still defend against a dictionary attack if you combine words in an unpredictable way. Choosing words at random is the easiest way to do this. For example, this website helps you to choose words at random with dice. Once you have chosen the words, you should add numbers and symbols into the password.
- Use a memorable phrase as the basis of your password, instead of using words. For example, you could turn the phrase 'FutureLearn is the number one online learning platform' into the password 'FLitn1e-lp'. You can tailor this phrase to the purpose of your account to make it more memorable. For example, you could use a phrase about shopping to make a password for an eBay account.
- If you have a visual memory, create a grid of characters (arranged randomly) and choose your password by drawing a pattern. Then, you would just need to learn the pattern, not the actual password.

TYPES OF ATTACKERS

White hat hackers – Ethical hackers who use their programming skills for good, ethical, and legal purposes. Network penetration tests in an attempt to compromise network and systems. Vulnerabilities are reported to developers for them to fix.

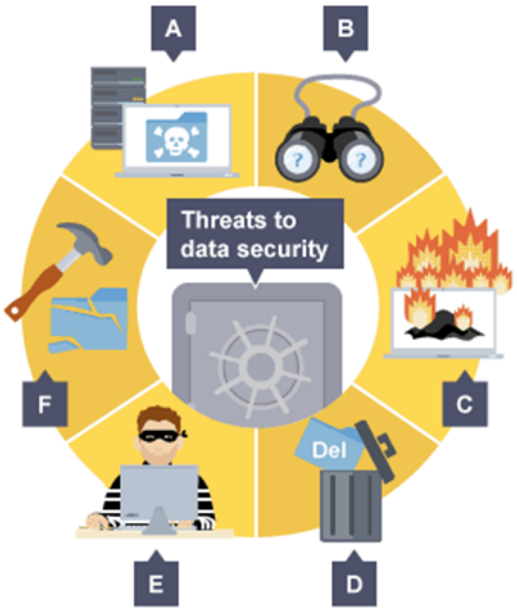
Grey hat hackers – Commit crimes and do unethical things but not for personal gain or to cause damage.

Black hat hackers – Unethical criminals who violate computer and network security for personal gain, or for malicious reasons such as attacking networks.

Knowledge

- **Forms of attack**
  - Passive vs. Active
- **Threats posed to networks (how each is carried out // suitable examples):**
  - Malware
  - Phishing
  - Social engineering (people as the weak point in secure systems)
  - Brute force attacks
  - Denial of service attacks
  - Data interception and theft
  - The concept of SQL injection
  - Poor network policy.

- **Identifying and preventing vulnerabilities:**
  - Penetration testing
  - Network forensics
  - Network policies
  - Anti-malware software
  - Firewalls
  - User access levels
  - Passwords
  - Encryption
    - Symmetric
    - A-Symmetric



Key

A	Corrupted	D	Deleted
B	Lost	E	Hacked
C	Destroyed	F	Damaged

Key

A	Back up files
B	Log off after use
C	Safe file storage
D	Passwords
E	Authorised personnel
F	Antivirus

Online Dangers

Homework

Homework 1 **Due date:**

Miss Cheat is the exams officer at St Failalot's School in Failchester. She is worried because students will be taking their GCSE's soon and she is concerned about data security at St Failalot's.

You have been to the school and had a look around and had a chat with Miss Cheat and have found out the following:

The students take their exams on computer.

During each exam students can come and go as they like but there has been complaints that some students have been copying and changing other students' answers.

When a student finishes each exam they save their data on to a memory stick. The students then hand the memory stick to Miss Cheat who puts each memory stick in a box on a her desk

When Miss Cheat gets the time she copies the contents of each student's memory stick on to the server in her office. Miss cheat is forever accidentally overwriting the contents of the memory sticks meaning that students need to redo the exam.

When she has copied all the finished exam papers on to the server she uploads them to be marked but she suspects someone at St Passalot's over the road is somehow accessing the data because St Failalot's exam results have been dreadful over the last couple of years.

Miss Cheat leaves her office unlocked and often gets angry with the Mr Mop the old cleaner because he comes into her office and knocks over the box of memory sticks and turns off the server because he thinks the "TV" doesn't work because he can't find "ITV".

Last year Miss Cheat nearly lost her job when Mr Mop spilt his cup of tea over the server and it exploded loosing all the students ICT exam papers.

Miss Cheat's office is on the ground floor of the school near the main entrance and she is always moaning about the noise from the traffic on the busy main road just outside her broken window. She is also fed up with the sound of the students celebrating at St Passalot's after their exams.

- **Miss Cheat is also very worried because since she downloaded an illegal copy of "Call of Duty 4" the network has been running a bit slow and sometimes crashes altogether during an exam, resulting in student data being lost.**

Miss Cheat wants you to help by writing a report explaining how you could improve the data security at St Failalot's. She would like you to explain some of the technical jargon that is used in ICT security such as: back-up, anti-virus, write-protection, encryption, hacking etc….

Call your report: St Failalot's School ICT Security Report

Online Dangers

Homework

Homework 2 **Due date:**

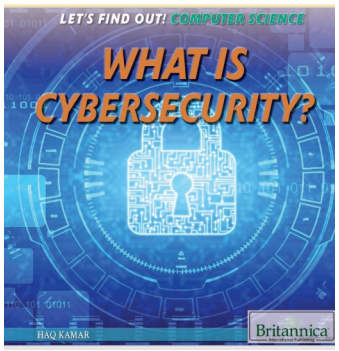
You can use word to complete the tasks and print it or just write it neatly on paper.

1. Everyone stores files on their computer. Write down examples of things on your computer that you want to keep safe.
2. People use the internet for fun, work, shopping etc. What kind of information might they want to keep safe?
3. What could happen if people got access to your computer or your online information?

Wider Reading List

Wider Reading

- OCR Computer Science for GCSE Student Book
- What is cyber security?



https://www.bbc.com/bitesize/guides/zs87sbk/revision/1
https://www.futurelearn.com