

Learning Launch



Use the chat to enter any cyber security threats you know about





Cyber Security

A level Student Booster

Learning Outcomes

By the end of this 90-minute session, you will:

- Recognise a range social engineering techniques and know prevention strategies.
- Know the characteristics of different types of malware
- Know computer system vulnerabilities and prevention methods
- Understand how and why Symmetric and Asymmetric Encryption is used



Social Engineering

Starter task

You receive an email in school from 'IT Support' asking you to immediately change your password by clicking on a link. They claim there has been suspicious activity on your account.



Comment in the chat



- What concerns should you have?



Social Engineering Techniques

Social engineering is different to other cybercrimes because it involves humans trying to trick or manipulate other humans.

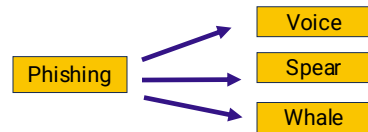
Comment in the chat

- Which techniques do you know?



Social Engineering - Phishing

Variations



You have 1 minute!

Write down the key indicators of a phishing message



Social Engineering – Phishing

Key indicators of a phishing message

Did you get?

- Any unexpected message with a request for information
- Suspicious hyperlinks
- Obvious errors – e.g., spelling errors, fake domain names
- Generic messages that don't address you by name

Also, be aware

- Expected messages – e.g., a parcel due

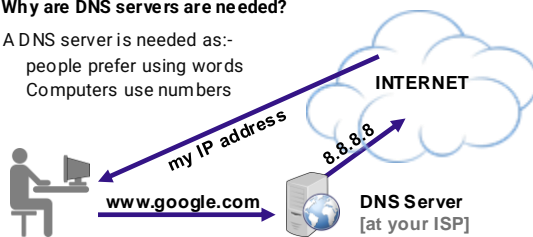


DNS Server

Why are DNS servers are needed?

A DNS server is needed as:-

- people prefer using words
- Computers use numbers



Social Engineering – Pharming

The term pharming is a technical and malicious practice which involves redirecting users to a **fake website** instead of a legitimate one, often without the user's knowledge.



You have
1 minute!

Comment in the chat



- How could you spot a fake website?



Social Engineering – Pharming

Other common indications of a pharming attack

- HTTP used when HTTPS is expected
- The lock symbol that your browser uses to confirm that a webpage is secure is missing
- A notification from your browser warning you that the webpage is insecure
- Broken or missing links



Social Engineering – Pharming

Techniques are used to redirect users

DNS Exploits: Attackers corrupt cache, control servers, and manipulate routers

Man-in-the-Middle Attack: Attackers intercept communication between a user and a website, to redirect to fraudulent sites.

Domain Hijacking: Attackers take control of a domain through exploitation or social engineering.



Malicious software



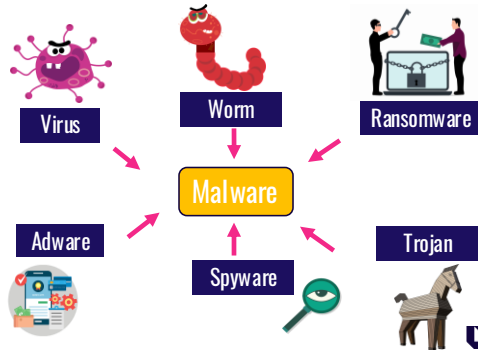
Malicious Software

Malware: Short for "malicious software," refers to programs developed with the intention to damage or exploit devices, networks, or other software.

Malware can cause damage to computer systems, corrupt or change files, steal data, or cause disruption to services.

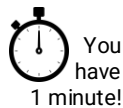


Malicious Software



Vulnerabilities

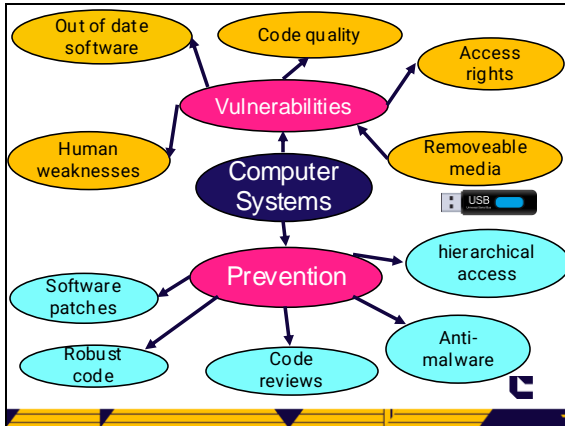
Computer system vulnerabilities refer to weaknesses or flaws that can be exploited by malicious individuals or software to gain unauthorised access or perform unauthorised actions.



Discuss with a partner

Which computer system vulnerabilities can you think of?





Activity – Isaac Questions


Open the Isaac Computer Science topic here and complete the **related questions** at the bottom:

https://isaaccomputerscience.org/concepts/net_sec_viruses?examBoard=all&stage=3_level&topic=malicious_code

Related questions

Booking all seats (A Level - C1)

Defence Against the Dark Arts (A Level - P1)

 You have 2 minutes!

System Recovery

Sometimes, even with the preventative measures that have been discussed, things can go wrong.

This could be the result of **hardware failure**, a **malicious attack**, **fire**, **flood**, **loss of electricity**, or a **natural disaster**.




Image generated by OpenAI's DALL-E



Image generated by OpenAI's DALL-E




Image generated by OpenAI's DALL-E

Comment in the chat 

- Which plans should organisations have to resume operations?

Diagnostic Activity

Please take time to anonymously share your confidence in **malicious software and effective defences**



Confidence Level Form

For the topic of

Please indicate your confidence level for each section
Attempt all multiple choice questions




Network Security



Network Threats– Hackers

The term **malicious hacker** refers to someone who deliberately gains, or attempts to gain, unauthorised access to a computer system with the intent to cause damage or steal data.



Comment in the chat 

- What do you think an **ethical hacker** does?



Ethical hackers

Ethical hackers, also known as a "white-hat" hackers are employed by organisations and work legally to...

- Conducts **penetration testing** on computer systems. ☒ ☐
- Simulate cyberattacks to identify security vulnerabilities.
- Identify and rectify security vulnerabilities.
- Proactively strengthen security measures..



Image generated by OpenAI's DALL-E



Image generated by OpenAI's DALL-E



WHAT IS DDoS?



Denial of Service attacks

A **Denial of Service** (DoS) attack is a cyber attack that aims to make a machine, system, or network resource unavailable to its intended users by overwhelming the target with excessive internet traffic.



Image generated by OpenAI's DALL-E



Image generated by OpenAI's DALL-E

A distributed denial-of-service (**DDoS**) attack comes from a network of distributed computer systems, typically a botnet.



DDoS Activity – Handout 1

Use handout 1 consider the scenarios provided. For each, identify the motivation and reason why.

5 minutes

Scenario	Motivation	Reason
A large tech company faces a DDoS attack, later claimed to highlight their security weaknesses.		
Cybersecurity hobbyists attack gaming websites with DDoS, then compare scores privately.		
Educational platforms are hit by DDoS attacks, with no apparent reason or demand made.		
A sportswear company's website crashes during a sale, indirectly benefiting a competitor.		
A car enthusiast community site crashes after traffic surges, following the ban of some members.		
A government-operated news outlet faces frequent outages during key global events, suggesting deliberate interference.		
A group of hackers targets a website streaming a live, all-weekend concert. The hackers demand a cryptocurrency ransom to stop the attack.		



Handout 1 Answers

Scenario	Motivation	Reason
A large tech company faces a DDoS attack, later claimed to highlight their security weaknesses.	Exposing Vulnerabilities	The attack is positioned as a demonstration of the company's need for better security.
Cybersecurity hobbyists attack gaming websites with DDoS, then compare scores privately.	Skill Testing	These attacks are designed to test abilities without intending serious damage.
Educational platforms are hit by DDoS attacks, with no apparent reason or demand made.	Vandalism	These seem to be purposeless attacks, likely just for causing disruption.
A sportswear company's website crashes during a sale, indirectly benefiting a competitor.	Business Competition	The timing of the crashes suggests a potential strategy to influence customer choices.
A car enthusiast community site crashes after traffic surges, following the ban of some members.	Personal Vendettas	The disruption is likely a response to the bans, suggesting a vengeful motive.
A government-operated news outlet faces frequent outages during key global events, suggesting deliberate interference.	Cyber Warfare	Repeated disruptions align with major political events, indicating potential state-sponsored activities.
A group of hackers targets a website streaming a live, all-weekend concert. The hackers demand a cryptocurrency ransom to stop the attack.	Financial Extortion	It involves a demand for payment in exchange for stopping the attack.



Network Threats– SQL injection

SQL injection is a cybersecurity vulnerability where an attacker can insert malicious SQL code into a query in a database. They exploit poorly secured input fields in a website or application.

SQL injections can:

- Execute commands that can download and install malware
- Extract data such as lists of credit card details
- Bypass sign in systems
- Delete data
- Update data
- Insert data



Image created by OpenAI DALL-E




Activity – Isaac Questions

Open the Isaac Computer Science topic here and complete the **related questions** at the bottom:

https://isaacomputerscience.org/concepts/net_network_security?examBoard=gl&stage=a_level&topic=security

Related questions	
Accepted Passwords (A Level - P1)	Don't do that (A Level - P1)
Legal responsibility (A Level - C1)	Filter them out (A Level - C1)
Limiting devices on a network (A Level - P1)	Password123 (A Level - P1)

 You have 5 minutes!



MAC address filtering

MAC Addresses are used to exchange data packets between devices on a LAN. MAC addresses **don't change**.



Generated by Open AI's DALL-E

MAC addresses are 6 pairs of characters separated by a :
Each pair represents a byte.

EA:16:A7:46:01:6B

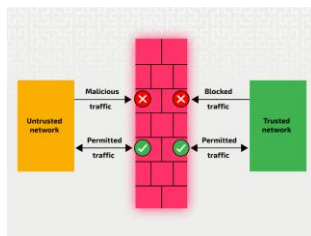
MAC address filtering is a security method which allows or denies network access based on the unique MAC addresses. It's configured through a router or switch typically.



Firewalls

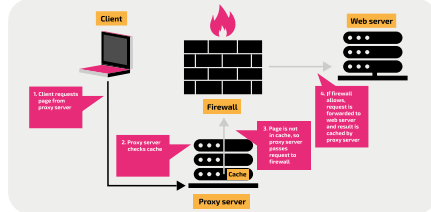
A firewall controls traffic between a trusted network and the internet, blocking malicious incoming and outgoing data.

Firewalls can take the form of both **software** and **hardware**



Proxy servers

A proxy server acts as an intermediary between clients and the internet, anonymising users and caching content to quicken access and lessen network load. It may also log user website visits.



Encryption

Discuss with a partner



Can you think of any everyday examples where encryption is used to protect information



You have 1 minute!

Encryption is a crucial aspect of network security, involving two main types: symmetric and asymmetric encryption.

Symmetric encryption

Symmetric encryption uses **one key** for encryption and decryption. It's faster than asymmetric but distributing the key securely is challenging. If compromised, all encrypted data is at risk.

Symmetric Encryption

Examples of use

- File and Disk Encryption:
- Bluetooth Encryption: pairing and communication use symmetric encryption for securing data exchange.
- Digital TV Broadcasting: The content is encrypted with symmetric keys before being broadcasted and decrypted by the receiver's set-top box.



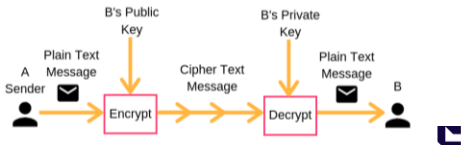
Generated by OpenAI DALL-E

Asymmetric Encryption

Asymmetric encryption

Asymmetric encryption uses a **pair of keys**: a public key for encryption and a private key for decryption.

The **public key**, is widely shared. The **private key** is known only to its owner and must be kept secure.



Asymmetric Encryption

Examples of use

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)



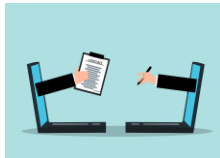
When you visit a website with "https://" in its URL

- Encrypted Messaging Apps: Apps like WhatsApp, Signal, and Telegram use end-to-end encryption based on public-key cryptography



In both examples asymmetric encryption is used to establish the secure connection and exchange a symmetric key. Symmetric encryption is then used for data exchange during the session due to its efficiency in speed

Digital signatures




Digital signatures ensure a document's authenticity using cryptography. A unique signature is created by encrypting a document's **hash** with the signer's private key.

Verification is done by decrypting this with the signer's public key and comparing hashes to confirm the document's integrity.

Diagnostic Activity

Please take time to anonymously share your confidence in network security



Confidence Level Form

For the topic of

Please indicate your confidence level for each section
Attempt all multiple choice questions



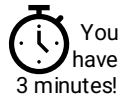
Activity – Isaac Questions

Open the Isaac Computer Science topic here and complete the **related questions** at the bottom:

https://isaaccomputerscience.org/concepts/net_sec_encryption?xamBoard=all&stage=all&topic=security

Related questions

It's a surprise (A Level - P2)	Ordered chaos (A Level - P2)
Don't tell the gamemaster (A Level - P1)	



Isaac Gameboard practice

- If you want more Cyber security practice, then try this gameboard.
- You will need to sign in to **Isaac Computer Science** or register for a free account if not done already.

Cybersecurity for Isaac A-level Booster

0	Accepted Passwords	Isaac	000
0	OSes	Isaac	000
0	Don't tell the gamemaster	Isaac	000
0	Message integrity	Isaac	000
0	It's a surprise	Isaac	000

ncce.io/isc-Acyber



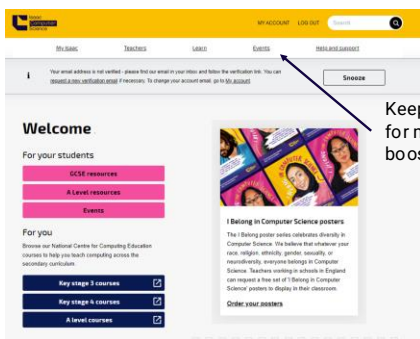
Learning Outcomes

By the end of this 90-minute session, you will:

- Recognise a range of social engineering techniques and know prevention strategies.
- Know the characteristics of different types of malware
- Know computer system vulnerabilities and prevention methods
- Understand how and why Symmetric and Asymmetric Encryption is used



Check for more ISAAC boosters



Keep an eye out
for more student
booster events



**Cybersecurity is a constantly
evolving field where the only
constant is change**



Thank you