Welcome to the CoGrammar

Intro to CyberSecurity

The session will start shortly...

Questions? Drop them in the chat. We'll have dedicated moderators answering questions.

Cyber Security Session Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly. **(Fundamental British Values: Mutual Respect and Tolerance)**
- No question is daft or silly - **ask them!**
- There are **Q&A sessions** midway and at the end of the session, should you wish to ask any follow-up questions. Moderators are going to be answering questions as the session progresses as well.
- If you have any questions outside of this lecture, or that are not answered during this lecture, please do submit these for upcoming Academic Sessions. You can submit these questions here: **Questions**

Software Engineering Session Housekeeping cont.

- For all **non-academic questions**, please submit a query: **www.hyperiondev.com/support**
- Report a **safeguarding** incident: **www.hyperiondev.com/safeguardreporting**
- We would love your **feedback** on lectures: **Feedback on Lectures**

Safeguarding & Welfare

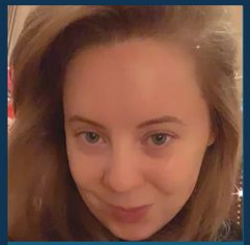
We are committed to all our students and staff feeling safe and happy; we want to make sure there is always someone you can turn to if you are worried about anything.

If you are feeling upset or unsafe, are worried about a friend, student or family member, or you feel like something isn't right, speak to our safeguarding team:

Ian Wyles
Designated Safeguarding Lead

Simone Botes

Rafiq Manan



Charlotte Witcher

Nurhaan Snyman

Ronald Munodawafa

Tevin Pitts

Scan to report a safeguarding concern

or email the Designated Safeguarding Lead:
Ian Wyles
safeguarding@hyperiondev.com

CoGrammar HyperionDev

Learning Objectives & Outcomes

- Explain the importance of cyber security in protecting information.
- Identify types of cyber attacks.
- Recognise the impact of cybercrime.
- Identify types of malware.

CoGrammar


SKILLS FOR LIFE
SKILLS BOOTCAMPS
Department for Education
CoGrammar
CyberSecurity
April 2024

CyberSecurity

Have you ever experienced unexpected or out-of-the-ordinary strange behaviours from your computer?

CyberSecurity

Can you think of some potential reasons you computer exhibited these behaviours?

Polls

Please have a look at the poll notification and select an option.

Have you ever had malware on your computer?

A. Yes
B. Unsure
C. Never

Polls

Please have a look at the poll notification and select an option.

What is malware?

A. Software designed to harm or exploit systems
B. A program that helps clean the computer
C. An operating system for secure computing
D. A hardware component used for internet connections

CyberSecurity

Processes used to protect computers, networks, and programs from unauthorised access or attacks intended to harm an individual or organisation.

- Broad Field.
- Daily activities extended into cyberspace.
- Cybercrime, cyberterrorism, and even cyber warfare.
- Financial loss or data privacy breaches.

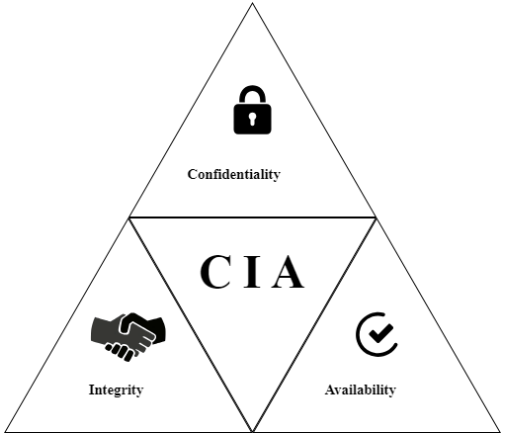
Categories of CyberSecurity

- Systems
  - Includes elements such as firewalls, encryption, and passwords.
- Software and Platform
  - Refers to using the best coding practices to prevent bugs that may lead to vulnerabilities.
- Infrastructure Security.
  - Consists of network and hardware security as well as cyber-physical and physical security.

NO UNAUTHORISED ACCESS

CIA Triad

- Confidentiality, Integrity, and Availability of Information
- Guides defending against threats and detecting problems



Confidentiality

- Protecting against the risk of unauthorised access and leaking of information.
- Includes personal or proprietary information, especially sensitive data related to a person's health or finances.

Integrity

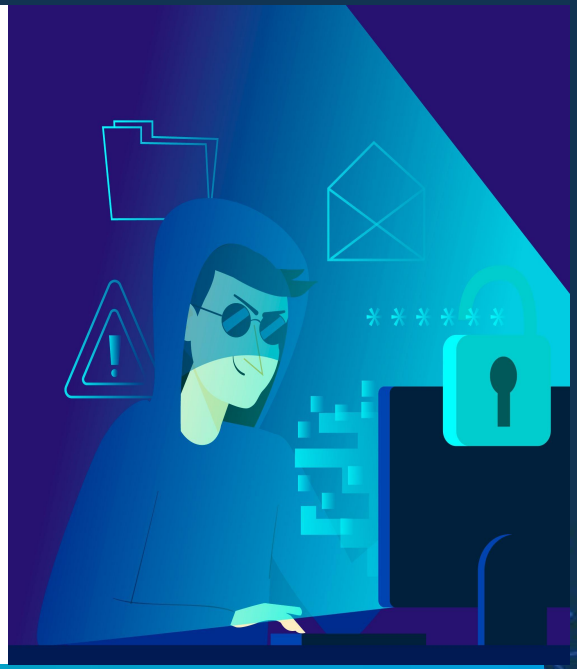
- Protecting information from unauthorised modification.
- Also involves addressing several social-technical issues.

Availability

- Preventing unauthorised access that denies illegitimate users from accessing and modifying information.
- Also refers to creating systems that promote security while maintaining efficiency.

Cyber Attacks

- Has different types of motives.
- Crimes that can be committed easier with the use of technology are referred to as cyber-enabled.
  - Cyberbullying, doxing, advance-fee fraud



Cyber Dependant Attacks

- Email spam
  - Unsolicited bulk emails enticing people to buy fake products.
- Phishing
  - A subset of spam emails.
  - Acts as a legitimate source.
  - Users are persuaded to provide login credentials.
  - "spear" phishing targets a specific individual or organisation.
- Financial malware
  - Records credit card or user credentials when a user visits a website of interest to criminals.

Cyber Dependant Attacks

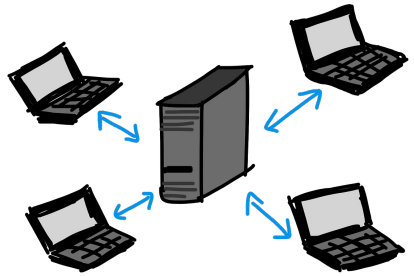
- Click fraud
  - Bots are used to click on web adverts to defraud advertisers.

- Unauthorised cryptocurrency mining
  - Computers are infected with malware to mine cryptocurrency.
  - Webpages can also be infected with scripts that use visitors' computers to mine.

- Ransomware
  - Users' files are encrypted and held for ransom.

Cyber Dependant Attacks

- Denial of service (DoS)
  - Server bandwidth is consumed to slow down or disable a system via the network.
  - Can happen legitimately but it can also be deliberately engineered.
  - Distributed DoS: multiple connected online devices (botnets) flood a target website with traffic.

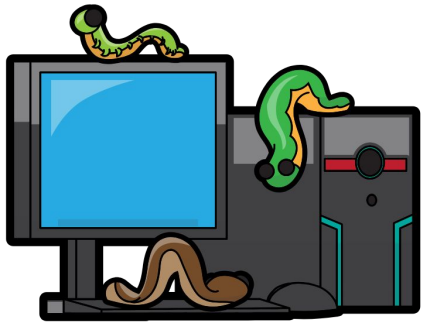


- Man-in-the-middle attack
  - A conversation or data transfer is intercepted.
  - Attacker can access confidential information or insert malware.

Types of Malware

- Standalone or Dependant
  - Worms and botnets are standalone programs that will run once executed.
  - Viruses and Malicious browser plug-ins need a host program.

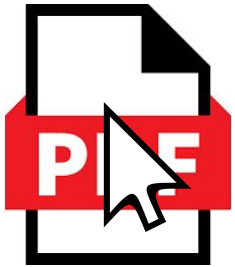
- Persistent or transient
  - Can be embedded in the file system
  - Can also reside in memory.



Types of Malware

- Layer of the System
  - Malware can run at different layers of the system
  - Malware that resides in a deeper layers will be harder to detect.

- Automatic or Activated
  - Malware can install and run itself or require the user to execute it.
  - Malware usually get executed accidentally.



Types of Malware

- Static or Dynamically updated
  - Most traditional malware is static
  - Some software can evade detection by updating via a malware server

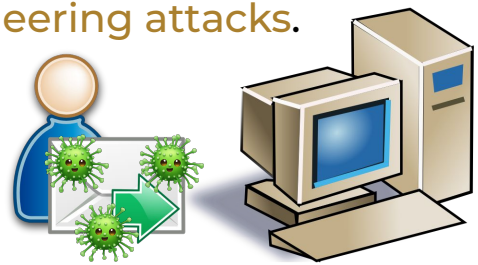
- Individual or Coordinated Network
  - Individual malware is designed to target an individual.
  - Coordinated networks(botnets) are used for DDoS, spam or phishing to a mass audience.

Potentially Unwanted Programs

- PUPs
  - Falls into a grey area between legitimate software and malware.
  - Gets downloaded alongside other software.
  - Has the potential to become malware and is classified as such.

Means of Infection

- Download of infected files via email attachments, websites, or file-sharing sites.
- Clicking on links to malicious websites.
- Visiting a compromised site.
- Inserting infected external hard drives or USB devices.
- Succumbing to social engineering attacks.



Fighting Infection

- Awareness. Be aware of the different methods being used.
- Notice strange behaviour exhibited by your computer.
- Anti-virus software can be used to scan your computer for infections and resolve them.

kaspersky

Avast

Polls

Please have a look at the poll notification and select an option.

What does the term "phishing" refer to in cybersecurity?

A. A type of malware that collects information
B. A fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity
C. The process of encrypting files
D. A method of securing data transfers

Polls

Please have a look at the poll notification and select an option.

What do we call software that could become malware and usually gets downloaded alongside other software?

A. Viruses
B. Worms
C. PUPs (potentially unwanted programs)
D. Infectious

Summary

- CyberSecurity is the processes used to protect computers, networks, and programs from unauthorised access or attacks intended to harm an individual or organisation
- There is a wide range of cyber attacks with everything happening online. Even normal crimes can be committed easier with the use of technology.
- There are different types of malware that work in different ways. Some can be more difficult to detect and remove than others.
- Remember to look for signs of potential attack or signs that your computer has been infected and take appropriate steps.

Questions and Answers

CoGrammar

Thank you for attending

SKILLS FOR LIFE
SKILLS BOOTCAMPS

Department for Education

CoGrammar