



Welcome to this session: Cyber Threats

The session will start shortly...

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





What is Safeguarding?

Safeguarding refers to actions and measures aimed at protecting the human rights of adults, particularly vulnerable individuals, from abuse, neglect, and harm.



To report a safeguarding concern reach out to us via email:
safeguarding@hyperiondev.com

Live Lecture Housekeeping:

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly.
- No question is daft or silly - ask them!
- For all non-academic questions, please submit a query:
www.hyperiondev.com/support
- To report a safeguarding concern reach out to us via email:
safeguarding@hyperiondev.com
- If you are hearing impaired, please kindly use your computer's function through Google chrome to enable captions.



Stay Safe Series:

Mastering Online Safety One Week/step at a Time

While the digital world can be a wonderful place to make education and learning accessible to all, it is unfortunately also a space where harmful threats like online radicalisation, extremist propaganda, phishing scams, online blackmail and hackers can flourish.

As a component of this BootCamp the **Stay Safe Series** will/is designed to guide you through essential measures in order to protect yourself & your community from online dangers, whether they target your privacy, personal information or even attempt to manipulate your beliefs.

Don't Take the Bait: How to Spot Phishing Scams

- Check email address.
- Unprofessionalism.
- Avoid attachments from unknown sources.
- Avoid signs of urgency.
- Content should make logical sense.



Cyber Threats



Learning Outcomes

- ❖ Understand the concept of cyber threats and their significance.
- ❖ Identify different types of cyber threats.
- ❖ Learn basic strategies to mitigate cyber threats.



Software Engineering

Have you ever experienced or heard of a cyberattack?



[illegible]

What do you think is the most common type of cyber threat? (Phishing, Malware, Denial of Service, Ransomware)



Cyber Threats

- Harmful activity committed with the intent of destroying, stealing, or disrupting data, critical systems, and digital life.
- Motivation behind cyber attacks:
 - Financial gain
 - Espionage
 - Activism, etc.

Types of Threats

Phishing

- A type of social engineering attack used to steal user data, such as login credentials and banking details.

From: authenticationmail@trust.wiki-media2.com
To: johnsmith@email.com
Subject: **A new login to your Wikipedia account**



WIKIPEDIA
The Free Encyclopedia

Dear user,

There has been a recent login to your Wikipedia account from a new device:

IP address: 192.168.0.1

Location: Newville, Anyland

432 new edits have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

<https://trust.wiki-media2.com/reset-password>

Thank you,

Wikipedia Foundation

Types of Threats

From: authenticationmail@trust.wiki-media2.com
To: johnsmith@email.com
Subject: **A new login to your Wikipedia account**



WIKIPEDIA
The Free Encyclopedia

Dear user,

There has been a recent login to your Wikipedia account from a new device:

IP address: 192.168.0.1

Location: Newville, Anyland

432 new edits have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

<https://trust.wiki-media2.com/reset-password>

Thank you,

Wikipedia Foundation

Types of Threats

Malware

- Malicious software used to disrupt, damage, or gain unauthorized access to a system.
- Types
 - Viruses
 - Worms
 - Trojans
 - Bots



Types of Threats

Denial of Service (DoS) and Distributed Denial of Service (DDoS)

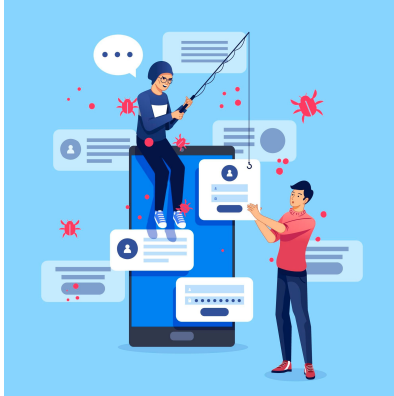
- Attempts to overload a website or network
- Degrades its performance sometimes making it completely inaccessible



Types of Threats

Social Engineering

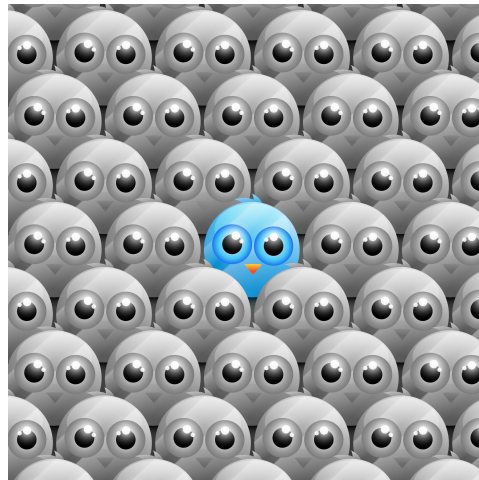
- Uses manipulation tactics to get vulnerable users to provide sensitive information to a malicious actor.
- Phishing is a subset of social engineering.



Types of Threats

Insider Threats

- Threats that exist within the inner working of an organization.
 - Current or former employees
 - Contractors
 - Associates



Threat Mitigation

- Use strong passwords and multi-factor authentication.
- Keep software and systems updated.
- Recognise and avoid suspicious links/emails.
- Backup data regularly.
- Use antivirus software and firewalls.



Polls

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

Which cyber threat do you now feel most confident identifying?

- A. Phishing
- B. Malware
- C. DDoS

Polls

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

What is the primary goal of a phishing attack?

- A. To install hardware on the victim's device
- B. To gain sensitive information like passwords or credit card details
- C. To create fake websites for no purpose
- D. To slow down the victim's computer

Polls

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

What is the best way to protect against ransomware?

- A. Ignoring suspicious emails
- B. Regularly backing up important data
- C. Using public Wi-Fi
- D. Installing ad blockers

Recap

- Harmful activity committed with the intent of destroying, stealing, or disrupting data, critical systems, and digital life.
- We get many different types of threats and it is important to know what each one is doing.
- Use different types of strategies such as strong passwords, 2-factor authentication, data backup, etc. to mitigate the risks of attacks.

Q & A SECTION

**Please use this time to ask
any questions relating to the
topic, should you have any.**

Thank you
for attending



HyperionDev