



CYBERSECURITY

Semester 2

Maria Ramirez

Threats and Vulnerabilities

- **Cyber Threats**
 - Potential dangers targeting computer systems, networks, or data
 - Aim to steal, disrupt, or damage data and operations
 - *Ex. malware, phishing, ransomware, hacking*
- **Cyber Vulnerabilities**
 - Weaknesses or flaws in systems, software, or networks
 - Exploitable by cyber threats
 - Causes: outdated software, weak passwords, unpatched security gaps, misconfigurations



Importance of Learning Cyber Threats and Vulnerabilities

- Identifies potential risks and weaknesses attackers could exploit
- Enables the creation of effective defenses, including:
 - Secure systems
 - Preventive measures
 - Incident response plans
- Protects sensitive data and ensures network integrity
- Essential for building comprehensive and effective cybersecurity strategies



Some Free and Not Free Resources

Free:

- **TryHackMe**
Offers hands-on cybersecurity training through gamified real-world labs, suitable for beginners
- **SANS Cyber Aces Online**
Provides a free online course teaching core concepts of information security systems
- **Cybrary**
Offers a wide range of free cybersecurity training resources and courses

Have to Pay:

- **Simplilearn Cyber Security Expert Masters Program**
A 4-month program priced at \$2,5992
- **CompTIA Security+ 701**
A 2-month course available for \$1,2002
- **Antisyphon Training**
Offers pay-what-you-can courses, with additional benefits like cyber range access for higher payments