

Prifysgol Wreccsam Wrexham University

Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: [Module directory](#)

Module Code	COM398
Module Title	Foundations of Cyber Security
Level	3
Credit value	20
Faculty	FACE
HECoS Code	100376
Cost Code	GACP
Pre-requisite module	N/A

Programmes in which module to be offered

Programme title	Core/Optional/Standalone
STEM Foundation Year	Optional
Standalone module aligned with STEM FY for QA purpose	Standalone

Breakdown of module hours

Learning and teaching hours	40 hrs
Placement tutor support hours	0 hrs
Supervised learning hours e.g. practical classes, workshops	0 hrs
Project supervision hours	0 hrs
Active learning and teaching hours total	40 hrs
Placement hours	0 hrs
Guided independent study hours	160 hrs
Module duration (Total hours)	200 hrs

Module aims

In this module, students will develop an understanding of essential concepts in computer security, including common cyber threats, detection methods, and defence strategies. Through case studies and practical experiments, students will explore core security principles, terminology, and foundational skills necessary for cybersecurity professionals.

Module Learning Outcomes

At the end of this module, students will be able to:

1	Identify and describe common cyber threats, such as malware, phishing, and social engineering, demonstrating understanding of their impact on computer systems and networks.
2	Apply core security concepts and terminology to analyse and evaluate real-world case studies, demonstrating an understanding of how security principles are implemented in practice.
3	Develop and implement basic defence strategies to mitigate cyber threats, utilising appropriate security measures and best practices to protect against potential attacks

Assessment

Indicative Assessment Tasks:

This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

Assessment 1:

The assessment strategy for the Foundations of Cyber Security module encompasses a multifaceted approach designed to comprehensively evaluate students' grasp of essential concepts in cybersecurity. Throughout the module, students will engage in various tasks aimed at constructing a portfolio that demonstrates their proficiency in both theoretical understanding and practical application. These tasks include small written assignments probing theoretical concepts, detailed write-ups of hands-on exercises, dynamic presentations on selected topics, and periodic in-class tests assessing comprehension and problem-solving skills. Each component of the assessment is carefully structured to provide students with opportunities to showcase their knowledge, critical thinking abilities, and communication skills. By embracing diverse assessment methods, this strategy not only ensures a thorough examination of student learning but also cultivates a holistic understanding of cybersecurity principles essential for navigating real-world challenges in the field.

Assessment number	Learning Outcomes to be met	Type of assessment	Duration/Word Count	Weighting (%)	Alternative assessment, if applicable
1	1,2, 3	Portfolio	1	1,2, 3	Portfolio

Derogations

None

Learning and Teaching Strategies

Aligned with the principles of the Active Learning Framework (ALF), the module will incorporate a blended digital approach utilising a Virtual Learning Environment (VLE). These resources may include a range of content such as first and third-party tutorials, instructional videos, supplementary files, online activities, and other relevant materials to enhance their learning experience.

The learning methodology for this module adopts a blended approach, integrating both theoretical and practical components. Students will engage in a series of workshops and practical sessions, which combine theory-based lectures with hands-on activities. These activities will involve students working on simulated problems and developing solutions

Welsh Elements

Elements of the Welsh language and culture will be embedded throughout the module.

Indicative Syllabus Outline

- Introduction to Cybersecurity Concepts
- Introduction to Linux
- Understanding the Cyber Threat Landscape
- Attacks and Threats
- Tools and Techniques
- Cyber Kill Chain
- Case Study
- Legal and Ethical Considerations
- Emerging Trends and Technologies

Indicative Bibliography

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads:

N/A

Other indicative reading:

Conklin, W. A., White, G., Cothren, C., Davis, R., & Williams, D. (2021), *Principles of Computer Security: CompTIA Security+ and Beyond*, 6th Ed. McGraw-Hill Education.

Administrative Information

For office use only	
Initial approval date	Sept 2024
With effect from date	Sept 2024
Date and details of revision	July 2025: Reapproved as part of IFY revalidation Sept 26: template update
Version number	3