Ministry of Higher Education and
Scientific Research - Iraq
University of Diyala
College of Artificial Intelligence
Engineering Technology
Department of Cybersecurity Engineering

الملحق 4: وصف المادة الدراسية

MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

Module Information معلومات المادة الدراسية					
Module Title	**Fundamentals of Cybersecurity**			**Module Delivery**	
Module Type	**Core**			☒ **Theory** ☐ **Lecture** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**CSE 106**				
ECTS Credits	**2**				
SWL (hr/sem)	**50**				
Module Level		1	**Semester of Delivery**		2
Administering Department		Cybersecurity Eng.	**College**	College of Artificial Intelligence Engineering Technology	
Module Leader	Hayder Namuq Talib		**e-mail**	haydernamuq@uodiyala.edu.iq	
Module Leader's Acad. Title		Asst. Lect.	**Module Leader's Qualification**		MSc.
Module Tutor	Name (if available)		**e-mail**	E-mail	
Peer Reviewer Name		Ali N. Albu-Rghaif	**e-mail**	ali.alb-Rghaif@uodiyala.edu.iq	
Scientific Committee Approval Date		10/11/2025	**Version Number**	1.0	

Relation with other Modules العلاقة مع المواد الدراسية الأخرى			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Ministry of Higher Education and Scientific Research - Iraq
University of Diyala
College of Artificial Intelligence
Engineering Technology
Department of Cybersecurity Engineering

Module Aims, Learning Outcomes and Indicative Contents أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية	
Module Objectives أهداف المادة الدراسية	1. Introduce students to basic cybersecurity concepts in a simple and practical way. 2. Help students understand common digital threats and how to protect personal devices and accounts. 3. Teach students how to use basic security tools and follow safe online practices. 4. Build awareness of secure behavior when using computers, mobile devices, and the internet. 5. Prepare students for more advanced cybersecurity courses in the future.
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	1. Define cybersecurity and explain its importance in daily life. 2. Identify common threats such as viruses, phishing, and password attacks. 3. Describe basic protection techniques (passwords, firewalls, antivirus). 4. Analyze simple situations and recognize security risks. 5. Use basic tools such as antivirus software and introductory Wireshark/Nmap. 6. Apply basic security settings on operating systems and mobile devices. 7. Practice safe behavior while browsing, downloading, and using online services.
Indicative Contents المحتويات الإرشادية	**Indicative content includes the following.** • Introduction to cybersecurity [2 hrs]. • Basic types of threats (malware, phishing, social engineering) [4 hrs]. • Basic types of hackers [2 hrs]. • Phishing & Social Engineering [2 hrs]. • Account protection (passwords, 2FA, safe login practices) [2 hrs]. • Device protection (antivirus, updates, safe configurations) [2 hrs]. • Network protection & Firewall Basics [4 hrs]. • Introduction to cryptography [2 hrs]. • Safe Internet Practices (Safe browsing, Downloading files, Recognizing suspicious links) [2 hrs]. • Overview of basic cybersecurity tools (Nmap, Wireshark, antivirus) [2 hrs]. • Case Studies (Hacked account scenario, Virus infection scenario, How to respond) [2 hrs].

Learning and Teaching Strategies استراتيجيات التعلم والتعليم	
Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, homework's and examples. Practical examples helps students to understand the course material.

Student Workload (SWL) الحمل الدراسي للطالب محسوب لـ ١٥ اسبوعا			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطالب خلال الفصل	**33**	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	**2.2**
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطالب خلال الفصل	**92**	**Unstructured SWL (h/w)** الحمل الدراسي غير المنتظم للطالب أسبوعيا	**6.1**
Total SWL (h/sem) الحمل الدراسي الكلي للطالب خلال الفصل	**100**		

Module Evaluation تقييم المادة الدراسية					
		Time/Number	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	**2**	**10% (5)**	**7 and 12**	**LO #1 to #4**
	Assignments	**2**	**10% (5)**	**6 and 13**	**LO #1 to #4**
	Participation & Attendance	**1**	**10% (10)**	**Continuous**	**All**
	Case Study Presentation	**1**	**10% (10)**	**Continuous**	**All**
Summative assessment	**Midterm Exam**	**2hr**	**10% (10)**	**8**	**LO #1 to #3**
	Final Exam	**3hr**	**50% (50)**	**16**	**All**
Total assessment			**100% (100 Marks)**		

Ministry of Higher Education and
Scientific Research - Iraq
University of Diyala
College of Artificial Intelligence
Engineering Technology
Department of Cybersecurity Engineering

Delivery Plan (Weekly Syllabus)

المنهاج الاسبوعي النظري

	Material Covered
Week 1	What is Cybersecurity? Basic concepts, CIA Triad, Basic terminology
Week 2	Cyber Threats & Vulnerabilities Types of attacks, Threat actors, Exploits vs vulnerabilities.
Week 3	Basic Threats & Attacks Viruses, worms, Trojans, Simple real-life examples.
Week 4	Types of hackers Black hat, White hat, Gray hat, Blue hat & Red hat hackers
Week 5	Phishing & Social Engineering Online scams, How attackers trick users.
Week 6	Password Security Strong passwords, Two-Factor Authentication.
Week 7	Device Security Antivirus, Importance of software updates.
Week 8	Midterm Review
Week 9	Wi-Fi & Network Security Router basics, WPA2/WPA3, Risks of open networks.
Week 10	Firewall Basics What a firewall does, Windows Firewall simple demo, packet filtering, proxy, and hardware
Week 11	Introduction to Cryptography What encryption means, Why we use it, Simple explanation of Symmetric/asymmetric encryption.
Week 12	Safe Internet Practices Safe browsing, Downloading files, Recognizing suspicious links.
Week 13	Introduction to Cybersecurity Tools Nmap (concept only), Wireshark (interface overview), Antivirus scanning basics
Week 14	Case Studies (Simple) Hacked account scenario, Virus infection scenario, How to respond
Week 15	Course Review
Week 16	**Preparatory week before the final Exam**

Learning and Teaching Resources مصادر التعلم والتدريس		
	Text	**Available in the Library?**
Required Texts	• P.W. Singer & Allan Friedman, "Cybersecurity and Cyberwar: What Everyone Needs to Know". • Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short, "Cybersecurity Essentials"	pdf
Recommended Texts	• William Stallings, "Computer Security: Principles and Practice." • Wenliang Du, "Computer Security: A Hands-on Approach (Simplified sections)"	No
Websites	https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=en-US	

Grading Scheme مخطط الدرجات				
Group	**Grade**	التقدير	**Marks %**	**Definition**
Success Group (50 - 100)	**A** - Excellent	امتياز	90 - 100	Outstanding Performance
	B - Very Good	جيد جدا	80 - 89	Above average with some errors
	C - Good	جيد	70 - 79	Sound work with notable errors
	D - Satisfactory	متوسط	60 - 69	Fair but with major shortcomings
	E - Sufficient	مقبول	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX** – Fail	راسب (قيد المعالجة)	(45-49)	More work required but credit awarded
	F – Fail	راسب	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.