



Course Specification

(Bachelor)

Course Title: **Cyber Crimes and Threats**

Course Code: **APIS2207**

Program: **Information Security Diploma**

Department: **Diplomas**

College: **Applied College**

Institution: **Umm Al-Qura university**

Version: **1.0**

Last Revision Date: **13 December 2024**



Table of Contents

A. General information about the course:	3
B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods	4
C. Course Content.....	6
D. Students Assessment Activities	6
E. Learning Resources and Facilities.....	7
F. Assessment of Course Quality	8
G. Specification Approval	8





A. General information about the course:

1. Course Identification

1. Credit hours: (4)

2. Course type

A. ☐ University ☐ College ☒ Department ☐ Track ☐ Others
B. ☒ Required ☐ Elective

3. Level/year at which this course is offered: (Level 2, 1st Year)

4. Course General Description:

This course includes knowledge and skills about threats posed to information security and common attacks associated with those threats. Addition to a broad introduction to crimes and violations in the cyber space. It introduces students to wide range of cybercrimes including but not limited hacking, identity theft, cyber terrorism, and cyber bullying.

5. Pre-requirements for this course (if any):

Introduction to Cyber Security

6. Co-requisites for this course (if any):

None

7. Course Main Objective(s):

- Identify cybercrimes, their motives, how to conduct them.
- Distinguish between the different cybercrimes.
- Understand the legal and technical measures against various cybercrimes.
- To express knowledge of basic information about the threats that may be present in the cyber realm.



2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	60	100%
2	E-learning		
3	Hybrid <ul style="list-style-type: none"> Traditional classroom E-learning 		
4	Distance learning		

3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	60
2.	Laboratory/Studio	
3.	Field	
4.	Tutorial	
5.	Others (specify)	
Total		

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
1.0	Knowledge and understanding			
1.1	Explain and analyze the ways technology is used to commit cybercrimes	K1	Lectures, group activities, use-case scenarios	Assignments , Exams
1.2	Identify different types of cybercrimes and categorize adversary resources, capabilities, techniques, and motivations.	K1	Lectures, group activities, use-case scenarios	Assignments , Exams
1.3	Evaluate the measures used to	K2	Lectures, group activities, use-case scenarios	Assignments , Exams



Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
	counter cyber organized crime			
2.0	Skills			
2.1	Be able to apply basic knowledge of cyber security to defend against cybercrimes	S1	Lecture	Assignments , Evaluations and Exams
2.2	Be able to critically analyze and investigate cybercrime scenarios	S2	Lecture	Assignments , Evaluations and Exams
3.0	Values, autonomy, and responsibility			
3.1	Be able to collaborate effectively in teamwork activities	V4	Lecture	Assignments , Evaluations and Exams

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction to cyber-crimes and their categories	3
2.	Hactivism, Identity theft, fraud, and economic crimes	4
3.	Personal data collection, monitoring, and surveillance	4
4.	Cyber bullying, stalking and harassment, Dark web and digital currencies	4
5.	Cyber warfare and cyber terrorism	4
6.	Models and Types of Cyber Threats	3
7.	Cyber Adversary Model: Resources, Capabilities, Intent, Motivation, Risk Aversion and Access	4
8.	Attack Techniques: Backdoors, Trojans, Viruses, Ransomware, Wireless Attacks, Social Engineering and Covert Channels	4
9.	Password Guessing and Cracking, Data Interception, Spoofing and Session Hijacking	4
10.	Data Disclosure, Alteration and Sabotage Threats, Repudiation Threats	4
11.	Denial of Service Attacks, Distributed Denial of Service Attacks, Bots, MAC Spoofing, Web Application Attacks, Cloud Computing Attacks and Zero-Day Exploits	4
12.	Advanced Persistent Threats (APT), Attack Indication Events and Attack Timing, Attack Surfaces, Attack Vectors and Attack Trees	4
13.	Insider Threats, Threat Information Sources, and Cryptographic Threats	4
14.	Strategies and Tools for Developing Cyber Threat Models	4
15.	Legal Issues of Cyber Threats	3
16.	Cyber Crime Laws: National Laws, International Laws, Treaties.	3
Total		60

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quizzes	Throughout Semester	20
2.	Assignment	Throughout Semester	15
3.	Midterm	8	25
4.	Final Exam	Final Week	40

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.).



E. Learning Resources and Facilities

1. References and Learning Resources

Essential References	<ul style="list-style-type: none"> Kremling, J., & Parker, A. M. S. (2017). Cyberspace, cybersecurity, and cybercrime. Sage Publications. Kolokotronis, N., & Shiaeles, S. (Eds.). (2021). Cyber-Security Threats, Actors, and Dynamic Mitigation.
Supportive References	<ul style="list-style-type: none"> Bryn Caless, Yar M. Cybercrime and Society, Policing: A Journal of Policy and Practice, Volume 8, Issue 3, September 2014, Pages 285–286, https://doi.org/10.1093/police/pau024 Cyberspace, Cybersecurity, and Cybercrime, By Amanda M. Sharp Parker and Janine Kremling, SAGE Publications, Inc; 1st edition, ISBN-13: 9781506347257. Skopik, F. (Ed.). (2017). Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level (1st ed.). Auerbach Publications. https://doi.org/10.4324/9781315397900
Electronic Materials	
Other Learning Materials	

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Traditional Classroom
Technology equipment (projector, smart board, software)	Multimedia Projector
Other equipment (depending on the nature of the specialty)	

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	Survey at the end of the course
Effectiveness of Students assessment	Instructor	Course Report
Quality of learning resources	Instructor	Survey at the end of the course
The extent to which CLOs have been achieved	Instructor	Course Report
Other		

Assessors (Students, Faculty, Program Leaders, Peer Reviewers, Others (specify))

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	Umm Al-Qura University Council
REFERENCE NO.	851141114462/190358
DATE	1446/11/22

