

CyberSecurity Fundamentals

Master of Science in Cybersecurity



Orientation show

عرض توجيهي

Dr. Redhwan Saad

Everyone Smart University

Faculty of IT



Who Am I?

Dr. REDHWAN **MOHAMMED AHMED SAAD**

Head of Cybersecurity Department
Assis. Prof. in Information,
Network Security, and
Cybersecurity



ABOUT ME

I'm senior lecturer at Faculty of Engineering, Ibb University, Yemen.

Currently I'm a postdoctoral research fellow at Computer Engineering Department, Faculty of Engineering, Cairo University, Egypt.

My research interests include Cybersecurity, Internet of Things security, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and IPv6 security.

❖ Assistant Professor in Internet Infrastructure Security

- Ph.D from USM, Malaysia, April. 2016
- Thesis: "ICMPv6 Echo Request DDoS Attack Detection Framework using a Back-propagation Neural Network".
- M.Sc from "LETI", RUSSIA, Sep.2007
- B.Sc from "LETI", RUSSIA, Sep.2004



جامعة القادسية
EVERYONE'S SMART UNIVERSITY



My Contact Information

❖ How to reach me

- By email at redhwan@esu.ac.ae
(please include “Cybersecurity Fundamentals” in subject line)

❖ Office hours

- Discussion Time (Tuesday at 9:00 PM) every week



<https://scholar.google.com.my/citations?user=4CFExCUAAAAJ&hl=en>



<https://www.scopus.com/authid/detail.uri?authorId=56105545600>



<https://orcid.org/0000-0001-7241-9327>



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



The course that will be taught

Cybersecurity Fundamentals



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



Introduction

مقدمة

يُعرّف الأمن السيبراني بأنه عملية حماية الأنظمة، والشبكات، وأجهزة الكمبيوتر، وما تحتويه من برامج من جميع أنواع الهجمات الرقمية والإلكترونية، ومنع الوصول إلى البيانات.

ما أهمية الأمن السيبراني؟

حماية المعلومات الحساسة من السرقة
التصدّي للفيروسات والبرامج الضارة
الحدّ من الجرائم الإلكترونية
منع الخسائر المالية
حصول مواقع الويب على المصادقية

الدفاع عن المعلومات أمام هجمات خرق البيانات
توفير أموال الشركات والمؤسسات



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



Primary Goal of This Course

➤ ***This course aims to:***

Provide students with concepts of

- ❖ Computer security,
- ❖ Cryptography,
- ❖ Secure protocols,
- ❖ Detection and Prevention,
- ❖ and other Security Techniques.



Learning Resources:

➤ **Credit Hours:**

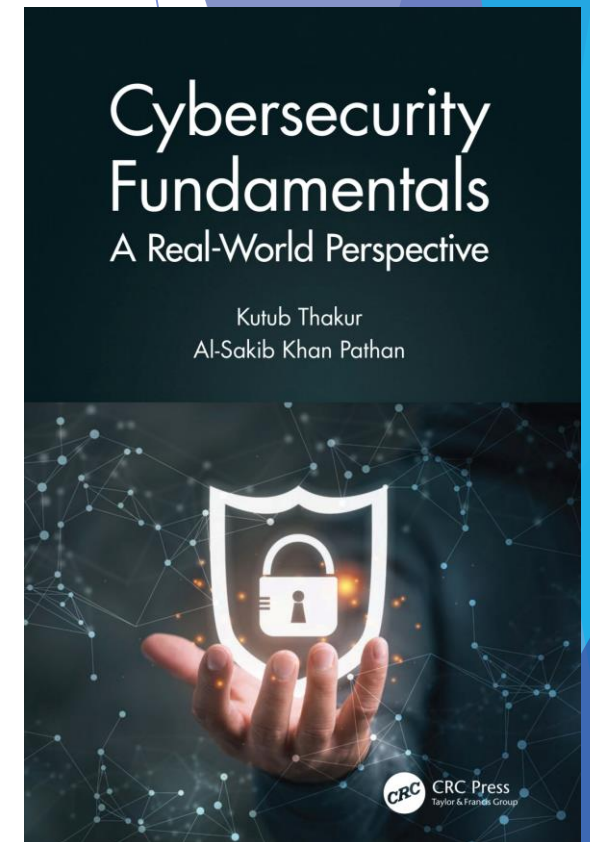
3 credit hours.

➤ **Required Textbook:**

1. ISACA, C. (2015). *Cybersecurity Fundamentals*: ISACA Rolling Meadows.
2. Graham, J., Olson, R., & Howard, R. (Eds.). (2016). *Cyber security essentials*. CRC Press.

➤ **Essential References:**

- Thakur, K., & Pathan, A. S. K. (2020). *Cybersecurity Fundamentals: A Real-World Perspective*. CRC Press.





What This Course is About

- The course will help students to gauge understanding in essential techniques in
 - Protecting information systems,
 - IT infrastructure,
 - Analyzing and monitoring potential threats and attacks,
 - Devising security architecture,
 - and Implementing security solutions.



Units of Course Contents

➤ Lecture Structure:

Module	Course Unit	No.of Weeks	Contact Hours
1	Lecture_1_Introduction to Networks Concepts	1 st	3
2	Lecture_2_Introduction to Cyber Security Concepts	2 nd	3
3	Lecture_3_Hackers and Cyber Crime	3 rd	3
4	Lecture_4_Malware	4 th	3
5	Lecture_5_Attacks Type	5 th	3
6	Lecture_6_Securing Your Computers	6 th	3
7	Lecture_7_Password Management	7 th	3
8	Lecture_8_Prevention from Cyberattacks	8 th	3
9	Lecture_9_Wireless Network Security and Mobile Device Security	9 th	3
10	Lecture_10_Secure Online Shopping and Cybersecurity Standards	10 th	3



Course Information - Evaluation

➤ Assessment Method:

▶ Short Exam

- ▶ 80% marks
 - ▶ Count of short Exam 10 (Weekly)
 - ▶ 8 Marks for each of short Exam.

▶ 20% Final Examination



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



Learning Outcomes

After completion of this course, the students should be able to:

- ▶ Understand, and identify various network technologies and cyber-attacks and its issues.
- ▶ Understand the Cyber Crimes and origin of Malware, and its security.
- ▶ Identify & Evaluate Information security threats and vulnerabilities in information system and apply security measures to real time scenarios
- ▶ Identify and learn of Security Protocols for avoiding basic level threat.
- ▶ Demonstrate the use of standards to enhance information security in the development process and infrastructure protection.
- ▶ Recognize the appropriate steps for information security risk, response, and recovery.
- ▶ Demonstrate the ability to assess and implement access controls

