School: Arison School of Business B.A

Introduction to cyber security

Lecturer:

Dr. David Movshovitz  dmovshovitz@idc.ac.il

Teaching Assistant:

Ms. Aviva Penn  lauren.penn@post.idc.ac.il

Course No.: 2665  Course Type : Lecture  Weekly Hours : 2  Credit: 2

Course Requirements :

Final Paper

Group Code : 202266500

Language:

English

Prerequisites

Prerequisite:

2365 - Introduction to Digital Technology
2370 - Introduction to Programming

Course Description

- Introduction to cyber-attacks (1 lecture)
- Introduction to Information security - terminology (2 lecture)
- Introduction to Information security - concepts (1 lecture)
- Introduction to cryptography (1 lecture)
- Using cryptography to ensure data confidentiality (1 lecture)
- Using cryptography to data integrity (1 lectures)
- Digital identity and Digital certificates (1 lecture)
- Introduction to Authentication (1 lecture)
- Introduction to Authorization (1 lecture)
- Malware taxonomy and categories (2 lecture)
- Cloud and mobile security (1 lectures)

Course Goals

The digital revolution, including the internet, mobile, cloud and social networks, have brought with them many opportunities and challenges, along with legal, ethical, and psychological dilemmas. Cyber attacks are recognized as one of the most serious security challenges faced today by nations, and as an example "Keep America safe in the cyber era" is one of the pillars in the National Security Strategy of USA document published December 2018.

In addition, the level of cyber threats is rising. Thus, organizations must be prepared to defend against threats in cyberspace, and decision-makers must be familiar with the fundamental principles and best practices of cyber security required to protect their enterprises.

The course goal is to provide an introduction to cyber-security. In the course we will discuss the main concepts of cyber-security, how to define and manage an organizational cyber-security policy. In addition, we will review how security is implemented in operating systems, databases, software, networks, the web, the cloud, and mobile devices. Security approaches will be classified into prevention, detection and tolerance, and both the defense and the attacker perspectives will be addressed.

The course will provide the students understanding of:

- The types of cyber-attacks and the risks associated with these attacks
- The technologies, products, policies and procedures that can help mitigating those risks and foster secure, resilient, and reliable operations in the cyber space.
- The process of developing, implementing, and managing an organizational cyber-security program, and how to adjust system protections and responsive actions over time in a changing threat environment.

Grading

Final grade will be composed from:

- final exam grade - 80%
- home assignments grade - 20%
Learning Outcomes

At the end of the course the student should be able to:

- Describe the information security properties of an information system in the cyber era that should be protected
- Describe the various types of cyber-attacks, including attack classification and attacker's motivation
- Describe the information security technologies and products that should be used to mitigate cyber attacks
- Delineate how to defend against the different cyber attacks using the relevant technologies and products

Lecturer Office Hours

Wednesday from 11:30 to 12:30

Reading List

There is no text book for the course as it will cover many different subjects.

The presentations used in the course lectures will be detailed and should be used as a basis for learning the topics learned in the course.

The lectures presentations will be uploaded to the course web site before each lecture.

In addition, I will upload to the course web site additional research papers and other relevant material, and the students are asked to read these papers as preparation to the lectures.