Miami Dade College

Course Description

CJE1680 | Introduction to Computer Crimes | 3.00 Credits

This course provides the student with an overview of crimes involving the use of computer technology and the internet. The course will cover computer related crimes, how they are committed and investigated, computer crime scene management, and the legal issues involved in the prosecution of computer crimes and legislation enacted to protect the public.

Course Competencies:

Competency 1: The student will examine and discuss the history of computer crime by:

1. Discussing the development of the internet and its widespread use
2. Exploring how the first worms and viruses shaped the use and protection of the internet
3. Identifying critical computer crime issues
4. Explaining the need for computer crime legislation

Competency 2: The student will demonstrate knowledge of the different types of computer crime by:

1. Distinguishing between hacking and cracking
2. Discussing the impact of illegal interception of computer-based communication
3. Identifying illicit markets, products, and fraudulent software and hardware uses
4. Exploring the impact of theft of data
5. Examining the different types of fraud that can be committed
6. Explaining the impact of stalking and bullying
7. Researching the impact of cyber-terrorism and how technology is used to facilitate terrorism

Competency 3: The student will examine various theoretical frameworks which explain computer crime by:

1. Explaining Routine Activity Theory's influence on cybercriminals
2. Identifying motivated o**f**enders
3. Examining the availability of suitable targets
4. Discussing the role of capable guardians

Competency 4: The student will demonstrate knowledge of the incidence, prevalence, distribution, and impacts of computer crime by:

1. Explaining how the "dark figure" of crime impacts cybercrime
2. Examining how cybercrime data is collected and utilized
3. Discussing the financial impact of computer crime and identifying potential victims
4. Devising ways to effectively apprehend offenders

Competency 5: The student will examine current trends in computer crime by:

1. Identifying commercialization as a big influence on cybercrime
2. Explaining how Integration is used in the commission of cybercrime
3. Discuss how the involvement of juveniles is impacting criminal justice policy and procedures
4. Examining the Cybercriminal organization and the cross-border nature of computer crime
5. Researching how violation of individual privacy by state impacts usage

Competency 6: The student will demonstrate knowledge of the investigation, prosecution, and sentencing of computer crimes by:

1. Examining Search and Seizure requirements and procedures
2. Identifying proper procedures for analyzing and presenting digital evidence
3. Explaining the Jurisdiction and extradition policy and procedure
4. Reviewing Significant cases
5. Evaluating the effectiveness of prosecuting cybercrime

6. Examining Sentencing policies

Competency 7: The student will examine the future of computer crime by:

1. Examining future techniques of prevention
2. Exploring future issues in the control of computer crime
3. Discussing Legislation efforts
4. Explaining International Cooperation

Learning Outcomes:

- Communicate effectively using listening, speaking, reading, and writing skills
- Solve problems using critical and creative thinking and scientific reasoning
- Use computer and emerging technologies effectively