Module 6: True-or-false questions

1. T/F Cybercrime is a cyber-related behavior that is against the law.
2. T/F According to the sociological definition of cybercrime, the cyber-related behavior does not have to be necessarily illegal but just defined as wrong by society.
3. T/F According to the sociological definition of cybercrime, the cyber-related behavior has to be both wrong and illegal.
4. T/F Cybercriminals tend to have higher IQs than the general population.
5. T/F When caught, cybercriminals rarely go to prison.
6. T/F Cybercrime can be fully prevented with virus protection software.
7. T/F Neutralization theories and self-control theories make a significant contribution in explaining cyber offending and victimization.
8. T/F Neutralization theories and self-control theories are the only branches in criminology interested in explaining cyber offending and victimization.
9. T/F Situational crime prevention focuses on guardianship strategies and has its emphasis on the crime, not the offender.
10. T/F Situational crime prevention focuses on guardianship strategies and has its emphasis on the offender, not the crime.
11. T/F The Criminal Justice and Cybersecurity discipline prefers self-report surveys to study cybercrime because they are accessible and have high validity.
12. T/F The Criminal Justice and Cybersecurity discipline prefers using reports to government agencies to study cybercrime because they address the dark figure of crime.
13. T/F The Criminal Justice and Cybersecurity discipline prefers studying cybercrime through reports to government agencies and self-report surveys as both have their own advantages and disadvantages.
14. T/F Criminal Justice, Sociology and Psychology are among the disciplines that give the foundations of the Digital Forensics discipline.
15. T/F Criminology, Sociology and Physics are the three disciplines that give the foundations of the Digital Forensics discipline.
16. T/F The discipline of Criminal Justice studies appropriate punishments, appropriate prevention strategies, and appropriate policies and laws.
17. T/F The discipline of Criminology studies appropriate punishments, appropriate prevention strategies, and appropriate policies and laws.
18. T/F The regulatory law proscribes monetary and injunctive penalties, viewed as crimes against individuals or organizations.
19. T/F The criminal law proscribes monetary and injunctive penalties, viewed as crimes against individuals or organizations.
20. T/F The civil law proscribes monetary and injunctive penalties, viewed as crimes against individuals or organizations.
21. T/F Hacktivists, script kiddies, empirical hackers and white hat hackers are all types of hackers.
22. T/F Hacktivists, script kiddies, white coat hackers, and empirical hackers are all types of hackers.
23. T/F White hat hackers are researchers and scholars who hack in order to better understand computer vulnerabilities and generate scholarly information about the topic.

24. T/F Companies but not states pay hackers to test vulnerabilities.
25. T/F The term hacktivism combines the words hacking and positivism, as hacktivism is being studied best through positivist theories.
26. T/F Hackers tend to be mostly young white males.
27. T/F Hackers tend to be mostly young white males but when females are perpetrators they usually act alone.
28. T/F Hackers tend to be mostly young white males with at least a bachelor's or even a graduate degree.
29. T/F Ransomware committed for economic reasons is best explained through the Routine Activities Theory.
30. T/F Ransomware committed for economic reasons is best explained through the Social Control Theory.
31. T/F Cyber frauds, unlike other types of cybercrimes, require significant technical knowledge.
32. T/F According to the Routine Activities Theory, crime occurs when three components are present simultaneously: absence of capable guarding, presence of motivated offender and a vulnerable target.
33. T/F According to the Deterrence Theory, crime occurs when three components are present simultaneously: absence of capable guarding, presence of motivated offender and a vulnerable target.
34. T/F Digital Rights Management systems include content identification and encryption but not decryption.
35. T/F Digital Rights Management systems include content identification, encryption and decryption but not licensing.
36. T/F Digital Rights Management systems include content identification, encryption, decryption and licensing.
37. T/F Studies show that girls are more involved in cyber bullying than traditional bullying.
38. T/F Cyber bullies feel less remorse than traditional bullies because they don't see the victim's reactions.
39. T/F It could be concluded about Internet sex crimes that they are also about power.
40. T/F Cyber terrorism is an act or series of acts committed internationally, between states, but not domestically within the same state.
41. T/F The police has only reactive functions – to respond to an incident after being notified.
42. T/F The police has only proactive functions – to actively search for cyber offending.
43. T/F The police has both reactive and proactive functions.
44. T/F Cyber offenders are more likely to plead guilty than go to trial.
45. T/F Cyber offenders are more likely to go to trial than to plead guilty.
46. T/F When convicted, vast majority of the cyber offenders go to jail or prison rather than receiving other type of sentence.
47. T/F Some studies show that cyber fraud victims have low levels of self-control, suggesting they might be more impulsive than non-victims.
48. T/F Some studies show that cyber fraud victims have high levels of self-control, suggesting they might be less impulsive than non-victims.
49. T/F Subcultural explanations suggest that individuals are part of a technology subculture that rewards certain behaviors.