ADMINISTRATION OF JUSTICE
CYBER CRIME
EXAM STUDY GUIDE

1. Cyber crime involves three forms of criminal activity involving the use of computers and the Internet using modern technology to accumulate goods and services.
2. Cyber thieves now have the luxury of remaining anonymous, living in any part of the world today.
3. The technology revolution has opened novel methods for cyber theft — ranging from the unlawful distribution of computer software to Internet security fraud — that were previously nonexistent.
4. Many computer crimes are prosecuted under such traditional criminal statutes as larceny (theft) or fraud.

***Theft of information*. The unauthorized obtaining of information from a computer (e.g., hacking), including software copied for profit.**
***The "salami" fraud*. With this type of fraud, the perpetrator carefully skims small sums from the balances of a large number of accounts.**
***Software theft*. The comparative ease of making copies of computer software has led to a huge illegal market, depriving authors of very significant revenues.**
***Manipulation of accounts/banking systems*. Similar to a "salami" fraud, this is committed on a much larger and usually more complex scale.**
***Corporate espionage*. The goal is to increase the rival company's (or a nation's) competitive edge in the global marketplace.**

5. The Internet is an ideal venue for selling and distributing adult material, while the computer is an ideal device for storing and viewing these images.
6. The vast number, websites featuring sexual content, including nude photos, videos, live sex acts, and webcam strip sessions, make it difficult to count accurately.
7. The Internet has also been used for the purposes of prostitution.
8. Cyber prostitutes set up personal websites or put listings on web boards that carry personals, such as Adult Friend Finder. When contacted, they ask to exchange e-mails, chat online, or make voice calls with prospective clients.
9. Some cyber prostitution rings offer customers the opportunity to choose women from their Internet page and then have the women flown in from around the country.
10. A denial-of-service attack is an attempt to extort money from legitimate users of an Internet service by threatening to prevent them from accessing the service.
11. This type of criminal activity include attempts to "flood" a computer network causing the following types of problems: Preventing legitimate network traffic. Attempting to disrupt connections within a computer network, thereby preventing access to a service. Attempting to prevent a particular individual from accessing a service. Attempting to disrupt service to a specific system or person.
12. One national survey found that within the last few years the number of websites that advertise or sell controlled prescription drugs increased 70 percent.
13. Groups of individuals have been working together for the past decade, to illegally obtain software and then "crack" or "rip" its copyright protections.
14. The Computer Fraud and Abuse Act: criminalizes accessing computer systems without authorization to obtain information.
15. The Digital Millennium Copyright Act: makes it a crime to circumvent antipiracy measures built into most commercial software, to manufacture, sell, or distribute code-cracking devices used to illegally copy software.
16. The United States Criminal Code: provides penalties for a first-time offender of five years incarceration and a fine of $250,000.
17. *Market manipulation:* occurs when an individual tries to control the price of stock by interfering with the natural forces of supply and demand.
18. In a pump and dump scheme, erroneous and deceptive information is posted online to get unsuspecting investors to become interested in a stock.
19. The cyber smear is a reverse pump and dump: Negative information is spread online about a stock, driving down its price.

20. This enables people to buy it at an artificially low price before rebuttals by the company's officers re-inflate the price.
21. *Fraudulent offerings of securities*: Some cyber criminals create websites specifically designed to sell securities fraudulently.
22. To make the offerings look more attractive than they are, assets may be inflated, expected returns overstated, and risks understated.
23. In these schemes, investors are promised abnormally high profits on their investments.
24. No investment is actually made and early investors are paid returns with the investment money received from the later investors.
25. The system usually collapses, but the later investors do not receive dividends and lose their initial investment.
26. *Illegal touting:* This crime occurs when individuals make securities recommendations and fail to disclose that they are being paid to disseminate their favorable opinions.
27. Some identity thieves create false e-mails and/or websites that look legitimate but are designed to gain illegal access to a victim's personal information. This is known as phishing (sometimes called c*arding* and *spoofing*).
28. Etailing involve failure to deliver on promised purchases or services, while others involve the substitution of cheaper or used material for higher quality purchases.
29. Cyber vandals are motivated more by malice than greed: Some cyber vandals target computers and networks seeking revenge for some perceived wrong.
30. Some desire to exhibit their technical prowess and superiority.
31. Some wish to highlight the vulnerability of computer security systems.
32. Some desire to spy on other people's private financial and personal information ("computer voyeurism").
33. Some want to destroy computer security because they believe in a philosophy of open access to all systems and programs.
34. A computer virus is one type of malicious software program (also called *malware*) that disrupts or destroys existing programs and networks.
35. Computer worms are similar to viruses but use computer networks or the Internet to self-replicate and "send themselves" to other users.
36. Some hackers may introduce a Trojan horse program in a computer system that looks like a harmless application, but it contains illicit codes that can damage the system operations.
37. Trojan horses do not replicate themselves like viruses, but they can be just as destructive.
38. Web defacement is a type of cyber vandalism that occurs when a computer hacker intrudes on another person's website.
39. Cyber stalking refers to the use of the Internet, e-mail, or other electronic communications devices to stalk another person.
40. A pedophile is an adult who is sexually attracted to a child or children.
41. Cyber bullying is the willful and repeated harm inflicted through the medium of electronic text.
42. Experts define bullying among children as repeated, negative acts committed by one or more children against another.
43. These negative acts may be physical or verbal in nature for example: hitting or kicking, teasing or taunting, they may involve indirect actions such as manipulating friendships, purposely excluding other children from activities, making derogatory or obscene comments about the victim.
44. Because of the creation of cyberspace, physical distance is no longer a barrier to the frequency and depth of harm handed out by a bully to his or her victim.
45. Cyber terrorism has been defined as "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents."
46. One form of attack is cyber espionage.
47. Cyber espionage involves hacking into secure computer networks at the enemy's most sensitive military bases,
48. There are also infrastructure terrorist attacks that are aimed at water treatment plants, electric plants, dams, oil refineries, and nuclear power plants.
49. Some cyber crime goes unreported because it involves low-visibility acts such as copying computer software in violation of copyright laws and is simply never detected.