**Exercise 1**

|  |  |
| --- | --- |
| **Description** | **Answer**  |
| 1. The act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access. | Hacking |
| 2. This is an act by the criminal, who floods the band width of the victim’s network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide | Denial of Service |
| 3. Malicious software that attaches itself to other software. | Virus Dissemination |
| 4. Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. Retail revenue losses worldwide are ever increasing due to this crime | Software Piracy |
| 5. Chat rooms in which people from anywhere the world can come together and chat with each other Criminals use it for meeting coconspirators | IRC crime |
| 6. Used to steal the amount / defraud the customer, by impersonating the card owner | Credit Card Fraud |
| 7. Copying the company’s confidential data in order to demand said company for huge amount. | Net Extortion |
| 8. It is technique of pulling out confidential information from the bank/financial institutional account holders by deceptive means.. | Phishing |
| 9. Getting one computer on a network to pretend to have the identity of another computer, usually one with special access privileges ,, so as to obtain access to the other computers on the network | Spoofing |
| 10. The Criminal sends emails containing defamatory matters to all concerned of the victim or post the defamatory matters on a website | Cyber Defamation |
| 11. The Criminal follows the victim by sending emails, entering the chat rooms frequently | Cyber Stalking |

Some controls that would help in minimizing the risks include:

* Security Policy
* Regulatory Compliance
* User Awareness programmed
* Access Control
* Security Audit
* Incidence Response
* Firewall, IDS
* Antivirus
* Backup