Programme: Bachelor of Commerce

Subject: Computer Science (GE)

Paper Code: CSG106

Paper Title: Computer Application

Unit: Unit III – Emerging Threats in Cyber Space

Module Name: Cyber Crime- Identity Theft, Email Spoofing, E-mail bombing, Online gambling, Sale of illegal articles, Cyber Defamation, Salami attack, Phishing, Pharming, Data Diddling, logic bombs, Web jacking, Theft of computer system, physically damaging a computer system, Cyber warfare, Cyber terrorism.

Module No: 08

Name of the Presenter: Ms. Vinita V. Korgaonkar

Assistant Professor

SSA Government College of Arts & Commerce,

Pernem- Goa

Glossary

Cyber Crime:

Computer crime which is also variously referred to as cyber-crime, e - crime, high-tech crime, and electronic crime can include many different types of offenses. If a computer or a network is the source, target, tool or place of the crime, it is considered a type of computer crime. Other crimes that can be facilitated by a computer crime are fraud, theft, blackmail, forgery and embezzlement.

Types of Cyber Crime:

1. **Identity Theft**

   Identity theft is the crime of obtaining the personal or financial information of another person or a small business for the purpose of assuming that person's or business' name or identity to make transactions or purchases, according to Investopedia. Identity theft occurs in many ways through the use of a computer

and is among the fastest growing crimes in the United States, according to the Department of Justice.

2. **Email Spoofing**

A spoofed email is one that appears to originate from one source but has actually emerged from another source. Falsifying the name and / or email address of the originator of the email usually does email spoofing, usually to send an email the sender has to enter the following information:

- email address of the receiver of the email
- email address(es) of the person(s) who will receive a copy of the email (referred to as CC for carbon copy)
- email address(es) of the person(s) who will receive a copy of the email (referred to as CC for carbon copy, but whose identities will not be known to the other recipients of the e-mail (known as BCC for blind carbon copy)
- Subject of the message (a short title / description of the message)
- Message

3. **E-mail bombing**

Email bombing refers to sending a large amount of emails to the victim resulting in the victim's email account (in case of an individual) or servers (in case of a company or an email service provider) crashing. A simple way of achieving this would be to subscribe the victim's email address to a large number of mailing lists. Mailing lists are special interest groups that share and exchange information on a common topic of interest with one another via email. Mailing lists are very popular and can generate a lot of daily email traffic - depending upon the mailing list.

4. **Online gambling**

Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

5. **Sale of illegal articles**

Internet is being used now to sell articles which otherwise are not permitted to be sold under the law of a country. One can find articles like drugs, guns, pirated software or music, illegal collection and distribution of data to private persons and organizations etc. being offered for sale on the Internet which are not permitted under the law to be sold.

6. **Cyber Defamation**

It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

7. **Salami attack**

This kind of crime is normally prevalent in the financial institutions or for the purpose of com-mitting financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed.

8. **Phishing**

Phishing is the name given to the technique of stealing personal information from Internet users. The information phishers want is usernames, passwords, account numbers, credit card numbers and social security numbers. They this information to commit identity theft or fraud... in other words, to either withdraw or spend your money or to use your identity to set up loan accounts and credit cards to spend money in your name. Often, these fraudulent purchases are put up for resale and the personal data can also be sold on to others.

9. **Pharming**

Pharming is similar to phishing in that they are both attempts to capture information from unsuspecting users on fraudulent Web sites. However, pharming is different in that it does not require victims to click on fraudulent links in emails. Pharming is much harder to detect, since it is very difficult for a victim of pharming to detect that an attack has been attempted. Pharming also allows an attacker to reach a large number of victims at once.

10. **Data Diddling**

This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed. The electricity board faced similar problem of data diddling while the department was being computerised.

11. **Logic bombs**

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date.

12. **Web jacking**

This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling

political objectives or for money. E.g. recently site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein. Further the site of Bombay crime branch was also web jacked. Another case of web jacking is that of the gold fish case. In this case the site was hacked and the information pertaining to gold fish was changed. Further a ransom of US $ 1 million was demanded a ransom. Thus web jacking is a process whereby control over the site of another is made backed by some consideration for it.

13. Cyber warfare

It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.

14. Cyber terrorism

Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.