Chapter 3
Cyber security and Cybercrime

Er. Shiva Ram Dam

Assistant Professor

Gandaki University

Content:

1. **Conventional Crime vs. Cybercrime**
2. **Cyber Crimes**
   - ❑ **Phishing, Spamming, Web spoofing, Email spoofing, cyber stalking, pornography, commercial espionage, piracy, illegal betting, financial fraud, identity theft, and other trending cybercrimes**
   - ❑ **Cybercrime prevention measures and cybersecurity**
3. **Case Study in Cybercrime (LOVE-LETTER-FOR-YOU.TXT.vbs, Stuxnet, WannaCry, e.tc.)**

Assignment:

1. Phishing :Bil
2. Spamming: Dhanu
3. Web spoofing: Jerusha
4. Email spoofing: Kripa
5. cyber stalking: Namrata
6. Pornography: Prabesh
7. commercial espionage: Prabesh Subedi
8. Piracy: Prakriti
9. illegal betting: Prakiti subedi
10. financial fraud: Rakshya
11. identity theft: Sabhyata
12. I LOVE YOU.txt.vbs :Shristi Dhakal
13. Stuxnet: shristi LC
14. WannaCry: Swastika

3.1 Conventional Crime vs. Cybercrime

- **Conventional crime**
  - refers to illegal activities that involve physical actions and tangible objects, occurring primarily in the physical world.
  - Such criminal activities are more physical in nature, such as theft, assault, robbery, and murder.
  - These types of crimes can occur in both public and private spaces, and they often involve face-to-face interactions between the perpetrator and victim or the property being targeted.
- **Cybercrime**
  - refers to criminal activities that involve computers, networks, or digital devices.
  - These crimes can target individuals, organizations, or governments and often involve unauthorized access, data breaches, or the use of the internet to commit illegal activities.
  - **Cybercrime** can include various activities, such as hacking, identity theft, phishing, and cyberstalking, among others.
  - The perpetrators of cybercrime often use the anonymity and global reach of the internet to commit their crimes, making it difficult to identify and prosecute them.

Cybercrime vs Conventional crime

Basis	Cybercrime	Conventional crime
Methods used to commit the crime	These crimes basically involve the use of computers, the internet, or other digital devices to commit a crime. Examples of cybercrimes include malware attacks, identity theft, and online fraud.	Conventional crime typically involves physical force or the threat of physical force to commit the crime. Examples of conventional crimes include theft, assault, and burglary.
Duration of detection	Remain undetected for a long period as there is no physical presence and no on-ground evidence.	Get detected immediately because it leaves physical traces of the crime.
Types of victims targeted	Cybercrime targets online interconnected systems, digital assets, and sensitive personal information or health information.	Conventional crime tends to target individuals or physical assets such as offices, relatives, and homes.
Scale of crime	Cybercrimes are committed on a large scale because in such a crime physical proximity to the victim is not required. e.g.- A single computer can hack thousands of bank websites. and loot them at a single instance.	on a limited scale as conventional crime comes in physical proximity to the victim. e.g.- A robber can rob one or two banks in a single day only.
Types of Consequences	Victims of cybercrime experience damage to their digital reputation or loss of sensitive personal information that can be used for identity theft.	Conventional crime can have physical, emotional, and financial consequences for victims.
Examples	Spamming, Phishing, Hacking, Cyberbullying, Cyberstalking, Malware, and many more.	Murder, Extortion, Bullying, and many more.

3.2 Cyber Crimes

- Some of the list of cybercrimes are:
  1. Phishing
  2. Spamming
  3. Web spoofing
  4. Email spoofing
  5. Cyber stalking
  6. Pornography
  7. Commercial espionage
  8. Piracy
  9. Illegal betting
  10. Financial fraud
  11. Identity theft

1. Phishing:

- Phishing involves sending deceptive emails or messages that appear to come from legitimate sources, such as banks or reputable companies, to trick recipients into revealing personal information like passwords, credit card numbers, or other sensitive data.
- **Example**: Receiving an email that looks like it's from your bank, asking you to click a link and enter your account details.

2. Spamming:

- Spamming is the practice of sending unsolicited bulk messages, usually emails, often for advertising purposes. While not always malicious, it can be a vector for malware.
- **Example**: Receiving numerous unsolicited emails promoting a product or service.

3. Web Spoofing:

- **Definition**: Web spoofing involves creating a fake website that looks nearly identical to a legitimate one to deceive users into entering their personal information.
- **Example**: A fraudulent website designed to look like a bank's login page, tricking users into entering their credentials.

4. Email Spoofing:

- **Definition**: Email spoofing is the creation of email messages with a forged sender address. This can make an email appear to come from someone the recipient knows or trusts.
- **Example**: Receiving an email that seems to be from a friend but is actually from a scammer.

5. Cyber Stalking:

- **Definition**: Cyber stalking involves using the internet or other electronic means to stalk or harass an individual, group, or organization.
- **Example**: Repeatedly sending threatening or intimidating emails or messages to someone.

6. Pornography:

- **Definition**: In the context of cybercrime, this often refers to the illegal distribution or possession of child pornography, as well as revenge porn (non-consensual distribution of intimate images).
- **Example**: Sharing explicit images of someone without their consent online.

7. Commercial Espionage:

- **Definition**: Commercial espionage involves using illegal methods to acquire trade secrets or other confidential business information.
- **Example**: Hacking into a competitor’s computer network to steal proprietary information.

8. Piracy:

- **Definition**: Online piracy is the illegal copying and distribution of copyrighted content, such as software, music, movies, and books.
- **Example**: Downloading and distributing movies through torrent sites without authorization.

9. Illegal Betting:

- **Definition**: Illegal betting refers to participating in or running gambling operations that are not authorized or regulated by law.
- **Example**: Operating or placing bets on an unlicensed online betting site.

10. Financial Fraud:

- **Definition**: Financial fraud encompasses a wide range of activities designed to deceive individuals or businesses to gain financial benefits.
- **Example**: Online schemes where scammers trick individuals into sending money or providing banking details.

11. Identity Theft:

- **Definition**: Identity theft occurs when someone unlawfully obtains and uses another person's personal data, typically for financial gain.
- **Example**: Stealing someone’s Social Security number to open credit accounts in their name.

Cybercrime prevention measures

1. **Use Strong Passwords**:
   - Create complex passwords with a mix of letters, numbers, and special characters.
   - Avoid using easily guessable information, such as birthdays or common words.
2. **Enable Two-Factor Authentication (2FA)**:
   - Add an extra layer of security by requiring a second form of verification, such as a code sent to your phone.
3. **Keep Software Updated**:
   - Regularly update your operating system, antivirus software, and other applications to protect against vulnerabilities.
4. **Be Wary of Phishing Scams**:
   - Do not click on links or download attachments from unknown or suspicious emails.
   - Verify the sender's identity before responding to requests for personal information.
5. **Use Antivirus and Anti-Malware Software**:
   - Install and maintain reliable antivirus and anti-malware programs to detect and remove malicious software.
6. **Secure Your Wi-Fi Network**:
   - Use strong passwords for your Wi-Fi network and enable encryption (WPA3 is recommended).
   - Disable remote management and regularly update your router's firmware.

Cybercrime prevention measures and cybersecurity

7. **Backup Data Regularly**:
   - Perform regular backups of important data to external drives or cloud services to recover information in case of an attack.
8. **Educate and Train Employees**:
   - Provide cybersecurity training to employees to recognize and respond to cyber threats effectively.
9. **Implement Firewalls and Intrusion Detection Systems**:
   - Use firewalls to block unauthorized access to your network.
   - Deploy intrusion detection systems (IDS) to monitor and alert on suspicious activities.
10. **Monitor and Limit Access to Sensitive Information**:
    - Restrict access to sensitive data to only those who need it.
    - Implement role-based access controls (RBAC) to manage permissions.
11. **Conduct Regular Security Audits**:
    - Perform regular security audits and assessments to identify and address vulnerabilities in your systems.

Cyber security

1. **Develop a Cybersecurity Policy**:
   - Establish and enforce a comprehensive cybersecurity policy that outlines acceptable use, data protection, and incident response procedures.
2. **Encrypt Sensitive Data**:
   - Use encryption to protect sensitive data in transit and at rest from unauthorized access.
3. **Implement Secure Software Development Practices**:
   - Follow secure coding practices to prevent vulnerabilities in software applications.
   - Conduct regular code reviews and vulnerability assessments.
4. **Establish an Incident Response Plan**:
   - Create a detailed incident response plan to quickly and effectively respond to cyber incidents.
   - Regularly test and update the plan to ensure its effectiveness.
5. **Use Multi-Layered Security**:
   - Adopt a multi-layered security approach, also known as defense in depth, to provide multiple barriers against cyber threats.
6. **Regularly Review and Update Security Policies**:
   - Continuously review and update security policies and procedures to address emerging threats and changes in the cyber landscape.

Assignment: Prepare slides

- Case Study in Cybercrime
  - LOVE-LETTER-FOR-YOU.TXT.vbs,
  - Stuxnet,
  - WannaCry, e.tc.

Useful Video Links for learning:

- Phishing: https://www.youtube.com/watch?v=4TZ9TIrMCCk
- Types of Phishing: https://www.youtube.com/watch?v=rb26NK0jtHM
- I LOVE YOU: https://www.youtube.com/watch?v=NZDiQczOsdc
- Stuxnet: https://www.youtube.com/watch?v=7g0pi4J8auQ
- https://www.youtube.com/watch?v=YGub8195Zus
- https://www.youtube.com/watch?v=yfziAgLOUVk
- Wannacry: https://www.youtube.com/watch?v=jivRCrm4jSw
- https://www.youtube.com/watch?v=RHp44-iqPuw

End of Chapter