Classification of Cybercrime

Outline

- Introduction
- Cybercrime against Individuals
- Cybercrime against Property
- Cybercrime against Nation

Introduction

- Cybercrime against individuals: Cyber stalking, trafficking, grooming.
- Cybercrime against property:
  - Stealing a person’s bank details and siphoning off money.
  - Misusing credit cards.
  - Running scams.
  - Using malicious software to gain access or disrupting the systems.
- Cybercrime against nation: Cybercrimes against the government
  - Cyber terrorism.

Cybercrime against Individuals

Internet Grooming

- **Handling**
  - Save screen captures, messages, and conversations.
  - Lodge a complaint if harassment persists.
- **Preventive measures**
  - Install antivirus
  - Use strong passwords.
  - Keep the system malware free.
  - Never upload personal information on social networking sites.
  - If information is stolen, children should seek support from adults.

Cybercrime against Individuals (Cont…)

Case 1 : Internet Grooming		
State : Tamil Nadu	City : Tirupur	Section of Law : Section 67B(c) of Information Technology Act, 2008
A thirteen-year-old girl was enticed, kidnapped, and raped by a twenty one-year-old man in Tamil Nadu. The rapist had befriended the victim on Facebook and sexually assaulted her after having gained her trust online.		

Cybercrime against Individuals (Cont…)

Cyber Stalking

- **Types**
  - *Delusional stalker*
  - *Intimate stalker*
  - *Vengeful stalker*
  - *Erotomanic stalker*
  - *Trolling stalker*
  - *Predatory stalker*
- **Handling**
  - Document in the form of screenshots.
  - Preserve hard copy of the document.
  - Lodge a complaint if harassment persists.

Cybercrime against Individuals (Cont…)

- **Preventive measures**
  - Use primary email account with trusted people.
  - Set up filtering options in email.
  - Never reveal original identity online.
  - Install antispyware software.
  - Turn on security features.

"On the Internet, nobody knows you're a dog."

Case 2 : Cyber Stalking		
State : Haryana	City : Delhi	Section of Law: 509 of the Indian Penal Code (IPC) and Section 66 of Information Technology Amendment Act (ITAA) 2008.

An employee in New Delhi received a series of emails from an offender asking her to either pose in the nude for him or to pay ₹1 lakh. The accused also threatened to put her morphed picture on display on sex websites along with her phone number and address. The accused also hacked her email account and accessed her pictures.

Cybercrime against Individuals (Cont…)

Cyber Harassment

- **Handling**
  - Avoid responding to the attacker.
  - Make a copy of the message, photo, or video, website URL, or a webpage screenshot.
  - Contact website operators by phone, email, or through any contact submission forms.
  - File a case.
- **Preventive measures**
  - Avoid contact with unknown people.
  - Privatize accounts.
  - Use Google Alerts to facilitate email notifications.

Cybercrime against Individuals (Cont…)

Cyber Extortion

- **Handling**
  - Active an incident response plan.
  - Disconnect affected computer, server, or any network equipment.
  - Restore data from backup sources.
  - Vulnerabilities analysis should be done.
- **Preventive measures**
  - Encryption of data can safeguard from being exposed to cybercriminals.
  - Prompt backup can prevent tampering.
  - Risk assessment and mitigation policies can minimize cyber extortion.

Cybercrime against Individuals (Cont…)

Online Paedophilia

- **Handling**
  - ISPs and social media providers should report child pornography incidents to the police.
  - Promotion of civic actions.
  - Promote awareness and education campaigns.
- **Preventive measures**
  - Educate children about online predators.
  - Install parental control software.
  - Limit children's computer usage.
  - Never allow children to have own email account.

Cybercrime against Property

Illegal Access – Hacking and Cracking

- **Handling**
  - Update system regularly.
  - Restrict system and database access.
  - Periodical auditing is essential.
- **Preventive measures**
  - Isolate victim's system.
  - Preserve all logs.
  - Enable counter measures.

Cybercrime against Property (Cont…)

Case 4 : Hacking [Prateek Paranjpe]		
State : Karnataka	City : Bangalore	Section of Law : 66 and 67 of ITA Act 2008
A girl stated that she had been receiving obscene and pornographic materials to her email address and mobile phone from an individual who seemed to know a lot about her and her family and believed that her email account had been hacked.		

Cybercrime against Property (Cont…)

Illegal Data Acquisition – Data Espionage

Phishing

- **Types**
  - Deceptive phishing.
  - Spear phishing attacks.
  - Whaling attacks.
  - Pharming.
  - Clone phishing attacks.
  - Evil twin Wi-fi attack.
  - Voice phishing.
  - SMS phishing.
  - Service specific phishing.

Cybercrime against Property (Cont…)

- **Handling**
  - Isolate the victim's ECD from the network and the Internet.
  - Perform complete scan using antivirus software.
  - Gather information about the source of phishing.
  - Sought assistance from the incident response team and the police.
- **Preventive measures**
  - Educate users.
  - Employ a gateway email filter.

Cybercrime against Property (Cont…)

- Use an email authentication standard.
- Employ a web security gateway.
- Use two-factor authentication (2FA).
- Avoid email links for accessing.
- Avoid sending personal information through email.
- Double check hyperlinks.
- Avoid opening attachments from unknown senders.

Cybercrime against Property (Cont…)

Case 5 : Phishing

A spoofed mail from myuniversity.edu was mass-distributed to many faculty members. The email claimed that the user's password is about to expire. Instructions were given to go to myuniversity.edu/renewal to renew the password within 24 hours. While attempting to renew, the users were redirected to myuniversity.edurenewal.com, a bogus page that appeared exactly like the real renewal page, where they typed both the new and existing passwords. While being redirected, a malicious script was activated in the background to hijack the user's session cookie. Thus, the attacker who monitored the page hijacked the original password to gain privileged access to secured areas of the university network.

Cybercrime against Property (Cont…)

Illegal Interception

Spoofing

- **Handling**
  - Email spoofing
    - Complete scan of the system.
    - Reset password.
  - Call spoofing: Avoid revealing personal and sensitive information.
  - IP spoofing: Turn off network components for few minutes.

Cybercrime against Property (Cont…)

- **Preventive measures**
  - Implement SPF.
  - Search phone number using previous scams.

Case 6 : Spoofing

A branch of the erstwhile Global Trust Bank in India experienced a chaotic situation. Numerous customers decided to withdraw all their money and close their accounts. An investigation revealed that someone had sent out spoofed emails to many of the bank's customers stating that the bank was in very bad shape financially and could close operations any time. The spoofed email appeared to have originated from the bank itself.

Cybercrime against Property (Cont…)

Skimming

- **Handling**
  - Immediate reporting.
  - Change the PIN.
- **Preventive measures**
  - Inspect the ATM and its area before using.
  - Keep track of the account.
  - Shield the number pad with one hand.
  - Ensure transaction accuracy.
  - Change the PIN often.

Cybercrime against Property (Cont…)

Case 7 : Skimming	
State : Karnataka	City :Bengaluru
The accused (a gang of tech-savy thieves) stole at least ₹8.68 lakhs from the HDFC Bank accounts of 17 customers in Bengaluru between 31 July 2017 and 4 August 2017. The customers approached the bank, alleging the transactions happened without their knowledge or authorization. Prima facie, the accused appeared to have skimmed card details and later cloned the cards to withdraw money from ATMs.	

Cybercrime against Property (Cont…)

Data Interference

Worm

- **Types**
  - *Bot worm.*
  - *Instant messaging worms.*
  - *Email worm.*
  - *Ethical worm.*
- **Handling**
  - Isolated the system from the network.
  - Perform a complete scan.
  - Acquire backup of data.

Cybercrime against Property (Cont…)

- **Preventive measures**
  - Avoid clicking on links shared on social media and email.
  - Install a anti-malware protection.
  - Use personal firewall.

Trojan Horse

- **Types**
  - *Trojan-Banker.*
  - *Trojan-DDoS.*
  - *Trojan-Downloader.*
  - *Trojan-Dropper.*
  - *Trojan-FakeAV.*

Cybercrime against Property (Cont…)

- *Trojan-GameThief.*
- *Trojan-IM.*
- *Trojan-Ransom.*
- *Trojan-SMS.*
- *Trojan-Spy.*
- *Trojan-Mailfinder*

- **Handling**
  - Isolate the system from the network.
  - Perform a complete scan.
  - Acquire a backup of data.

Cybercrime against Property (Cont…)

- **Preventive measures**
  - Never open emails and attachments from unknown source.
  - Install antivirus software.
  - Avoid autorun.
  - Backup data regularly.

Logic Bomb

- **Handling**
  - Change the system date before activation.

Cybercrime against Property (Cont…)

- **Preventive measures**
  - Avoid downloading pirated software.
  - Be careful while installing shareware and freeware applications.
  - Be cautious when handling emails and attachments.
  - Update antivirus routinely.
  - Install latest OS patches.

Cybercrime against Property (Cont…)

Virus

- **Types**
  - *File system or cluster viruses.*
  - *Stealth virus.*
  - *Polymorphic virus.*
  - *Fast infectors.*
  - *Slow infector.*
  - *Sparse infector.*
  - *Companion virus.*
  - *Armored virus.*
  - *Macro virus.*

Cybercrime against Property (Cont…)

- **Handling**
  - Isolate the system from the network.
  - Perform complete scan of the system.
  - Acquire backup of data.
- **Preventive measures**
  - Never open unknown email attachments.
  - Perform virus scan after opening an email attachment.
  - Download files only from trusted sites.
  - Perform virus scan after a peripheral is connected to the system.
  - Antivirus software should be kept up-to-date.

Cybercrime against Property (Cont…)

Case 9 : Virus [Prateek Paranjpe]

The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate. In May 2000, this deadly virus became the world's most prevalent virus. Losses incurred during this virus attack were pegged at US $10 billion. VBS_LOVELETTER utilized the addresses in Microsoft Outlook and emailed itself to those addresses. The email which was sent out had "ILOVEYOU" in its subject line. The attachment file was named "LOVELETTER-FOR-YOU.TXT.vbs". People wary of opening email attachments were influenced by the subject line and those who had some knowledge of viruses did not notice the tiny .vbs extension and believed the file to be a text file. The message in the email was "Kindly check the attached LOVELETTER coming from me".

Cybercrime against Property (Cont…)

Malware

- **Types**
  - *Adware.*
  - *Spyware.*
  - *Browser hijacking software.*
- **Handling**
  - Isolate the system from the network.
  - Perform complete scan of the system.
- **Preventive measures**
  - Use antivirus and anti-malware software.
  - Never open email attachments from unknown sources.

Cybercrime against Property (Cont…)

Rootkit

- Enables administrator-level access when installed.
- **Examples**
  - *NTRootkit.*
  - *HackerDefender.*
  - *Machiawaeli.*
  - *Creek Wiretrapping.*
  - *Zeus.*
  - *Flame.*
- **Handling**
  - Isolate the system from the network.
  - Perform complete scan of the system.
- **Preventive measures**
  - Keep the system patched.
  - Update antivirus software.
  - Never open email attachments from unknown sources.

Cybercrime against Property (Cont…)

System Interference – Computer Threats

DoS Attack and DDoS Attack

- **Types**
  - Bandwidth attacks.
  - Application attacks.
- **Handling**
  - Wipe and reinstall the OS.
  - Turn off the network components.
- **Preventive measures**
  - DDoS mitigation applications.
  - Configure server applications.
  - Monitor network with technology.
  - Update firewalls and network security programs.
  - Configure routers.
  - Use IDS with firewalls.

Cybercrime against Property (Cont…)

Case 10 : DDoS Attack

On 21 October 2016, the DDoS attack that disrupted internet was the largest of its kind in history. The cause of the outage was a distributed denial of service (DDoS) attack, in which a network of computers infected with special malware, known as a 'botnet', was coordinated into bombarding a server with traffic until it collapses under the strain. Dyn, a company that controls much of the internet's domain name system (DNS) infrastructure was the victim of the denial of service attack that was orchestrated using a weapon called the Mirai botnet [Symantec] as the primary source of malicious attack. Unlike other botnets, which are typically made up of computers, the Mirai botnet is largely made up of so-called 'Internet of Things' (IoT) devices such as digital cameras and DVR.

Cybercrime against Property (Cont…)

Email Bombing

- **Types**
  - Mass mailing.
  - List linking.
  - ZIP bombing.
- **Handling**
  - Similar to viruses and worms.
- **Preventive measures**
  - Use antivirus software.
  - Install firewall.
  - Use email filter applications.
  - Configure proxy server with rules.
  - Use SMTP.

Cybercrime against Property (Cont…)

Case 11 : Email Bombing [Prateek Paranjpe]

A foreigner who had been residing in Shimla (India) for almost 30 years wanted to avail of a scheme introduced by the Shimla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take revenge. Consequently, he sent thousands of emails to the Shimla Housing Board and repeatedly kept sending emails till their servers crashed.

Cybercrime against Property (Cont…)

Email Spamming

- **Handling**
  - Delete spam email.
  - Employ multilevel authentication.
  - Reset passwords.
  - Report spamming incident.
- **Preventive measures**
  - Set multiple email addresses.
  - Never respond to spam.
  - Never click unsubscribe link from unknown sources.
  - Update browsers.
  - Use anti-spam filters.

Cybercrime against Property (Cont…)

Malvertising

- **Handling**
  - Isolate system from the network.
  - Use security software.
  - Enable ad-blocking browser plugins.
  - Install antivirus software.
- **Preventive measures**
  - Keep web browsers and plugins up-to-date.
  - Avoid pop-up ads.

Cybercrime against Property (Cont…)

Botnet

- **Handling**
  - Use appropriate measures discussed earlier.
- **Preventive measures**
  - Avoid clicking on suspicious links.
  - Avoid relying on online ads.
  - Download software from reputable source.
  - Turn on firewall.

Cybercrime against Property (Cont…)

Potentially Unwanted Programs (PUP)

- **Handling**
  - Perform complete scan of the system.
  - Report sources of PUP.
- **Preventive measures**
  - Download software from reputable source.
  - Check pre-set and unwanted options while downloading software.
  - Prefer user-defined or advanced options while installing software.

Cybercrime against Property (Cont…)

Rogue Security Software

- **Handling**
  - Isolate system from the network.
  - Perform complete scan of the system.
- **Preventive measures**
  - Download security tools from official source.
  - Install legitimate security programs.
  - Avoid clicking on scary ads.
  - Be aware of common phishing attacks.

Cybercrime against Property (Cont…)

Spyware

- **Types**
  - *Adware.*
  - *Pornware.*
  - *Porn-Dialer.*
  - *Porn-Downloader.*
  - *Porn-Tool.*
  - *Riskware.*
- **Handling**
  - Isolate system from the network.
  - Install utilities such as Ad-ware, Spybot, etc.
- **Preventive measures**
  - Install anti-spyware software.
  - Update OS and all the installed software.
  - Employ firewalls.

Cybercrime against Property (Cont…)

Copyright- and Trademark-related Offences

Software Piracy

- **Types**
  - *Softlifting.*
  - *Client-server overuse.*
  - *Hard-disk loading.*
  - *Counterfeiting.*
  - *Online piracy.*

Case 12 : Software Piracy [Prateek Paranipe]		
State : Karnataka	City : Bengaluru	Section of Law : 65 and 66 of the Information Technology Amendment Act 2008
A software company stated that some of the former employees of the company had accessed the IT system of the company and tampered with the source code of the software under development.		

Cybercrime against Property (Cont…)

Data Piracy

Case 13 : Data Piracy [Prateek Paranjpe]		
State : Haryana	City : Delhi	Section of Law : 420 / 408 / 120B IPC R/W 66 ITA ACT 2008

The complainant filed a case of fraud and cheating, alleging theft and sale of proprietary data. The complainant had a subsidiary company in the United States which did business with its US partner. The US partner provided mortgage loans to US residents for residential premises. The business of the complainant was providing leads to their US partner. The data included the details of loan seekers along with their telephone numbers. The complainant generated leads through arrangements with call centres in India who called from their database and shortlisted home owners who were interested in availing re-finance facility on their existing mortgage loans. The complainant realised that there was a sudden drop in the productivity of the call centres and therefore the production of leads, although the inputs meant to be given to various call centres by the employees of the company had remained the same as before. The concerned officials of the company got alarmed and made an in house enquiry. On careful and meticulous scrutiny it was revealed that one of the employees of the complainant (company), in connivance with some other officers, had been deceiving and causing wrongful loss to the company by selling the data purchased by the company and in effect wrongful gain for themselves.

Cybercrime against Property (Cont…)

Audio and Video Piracy

Case 14 : Audio Piracy
State : Tamil Nadu City : Chennai
Maestro Illayaraj served a legal notice on playback singer S. P. Balasubramanyam for rendering his songs in a concert in the US in August 2016 without his consent.

Case 15 : Video Piracy [Manish Raji (2016)]
State : Tamil Nadu City : Chennai
The Central Crime Branch (CCB), Egmore, Chennai, received a tip-off that a man was making pirated copies of recently released Tamil and English movies.

Cybercrime against Property (Cont…)

Computer-related Offences

Impersonation

- **Handling**
  - Reset credentials subjected to impersonation.
- **Preventive measures**
  - Avoid revealing passwords and sensitive information to anyone.
  - Secure the premises physically.

Cybercrime against Property (Cont…)

Data Diddling

Case 16 : Data Diddling [Prateek Paranjpe]

The New Delhi Municipal Council (NDMC) Electricity Billing Fraud Case took place in 1996. The computer network was used for receipt and accounting of electricity bills by the NDMC. Collection of money, Computerized Accounting, Record Maintenance and Remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

Cybercrime against Property (Cont…)

Identity Theft

- **Types**
  - *Financial identity theft.*
  - *Child identity theft.*
  - *Medical identity theft*
- **Handling**
  - Report identity theft.
  - Reset user credentials.
  - Block or close associated account.
- **Preventive measures**
  - Dispose sensitive information safely.
  - Examine bank account statements.
  - Set difficult passwords.
  - Protect computers with antivirus.
  - Monitor credits.

Cybercrime against Property (Cont…)

Case 17 : Identity Theft [Prateek Paranjpe]		
State : Maharashtra	City : Pune	Section of Law : 467, 468, 471, 379, 419, 420, 34 of IPC and 66 of ITA ACT 2008
The accused in the case was working in a BPO which was handling the business of a multinational bank. During the course of the work, the accused had obtained the personal identification number (PIN) and other confidential information of the bank's customers. Using this information, the accused and his accomplices transferred huge sum of money from the accounts of different customers to fake accounts through different cyber cafes.		

Cybercrime against Property (Cont…)

Salami Slicing Attack

- **Handling**
  - Report the incident.
  - Reset user credentials.
  - Block or close associated account.
- **Preventive measures**
  - Bank have to update security policies.

Case 18 : Salami Slicing Attack

In 2008, a man was arrested for fraudulently creating 58,000 accounts which he used to collect money through verification of deposits from online brokerage firms, a few cents at a time. While opening the accounts and retaining the funds may not have been illegal by themselves, the authorities charged that the individual opened the account using false names (cartoon characters), addresses and Social Security Numbers, thus violating the laws against mail fraud, wire fraud, and bank fraud.

Cybercrime against Property (Cont…)

Pharming

- **Handling**
  - Isolate system from the network.
  - Perform complete scan.
  - Opt for a more reliable ISP.
- **Preventive measures**
  - Use trustworthy ISP.
  - Ensure HTTPS is active while enabling payment option.

Case 19 : Pharming
In 2004, a German teenager hijacked the country's eBay domain name leaving thousands of users redirected to a bogus site. In 2005, the domain name for Panix, a New York-based ISP was redirected to a bogus site in Australia. In the same year, a secured email service was attacked by redirecting users to a defaced website.

Cybercrime against Nation

Cyber Terrorism

- **Types**
  - *Privacy violation*
  - *Data theft*
  - *Demolition of government database*
  - *DoS attack*
  - *Damage and disruption of networks*
  - *Packet sniffing*
- **Handling**
  - Follow handling measures for viruses and worms.
- **Preventive measures**
  - Install IDS.
  - Keep all patched programs up-to-date.
  - Preserve logs of activity.
  - Use strong passwords and effective firewalls.
  - Test defence mechanisms regularly.

Cybercrime against Nation (Cont…)

Case 20 : Cyber Terrorism

In the year 2011, Indian Parliament was attacked with the help of Information Technology. Accused forged an official gate pass with the logo of Ministry of Home Affairs and other information along with the layout of Indian Parliament. Police found out a laptop from the main accused, Md. Afzal and S. Hussein Guru and also found out that they did it through a Pakistani Internet Service Provider. They controlled the identity and email system of Indian Army.

On 1 September 2011, the attack on World Trade Center (WTC) can also be pictured under Cyber Terrorism. Terrorist's unauthorized access over the network of one airline and hijacking two airlines resulted in crashing of those airlines into WTC twin towers and Pentagon.

Cybercrime against Nation (Cont…)

Cyber Warfare

- **Handling**
  - Ascertain cause and nature of attack.
- **Preventive measures**
  - Government should form an agency that solely focuses on cyberspace and cyber attacks.
  - Frame proper security framework and policies.
  - Risk management towards critical assets should be available.
  - Observe changes in the network or network device.

Case 21 : Cyber Warfare [Maragaret Rouse]

The earliest instance of a nation waging cyber war was the Stuxnet worm which was used to attack Iran's nuclear program in 2010. The malware targeted SCADA (Supervisory Control and Data Acquisition) systems and spread through infected USB devices. While the United States and Israel both had been linked to the development of Stuxnet, neither has formally acknowledged its role.

Cybercrime against Nation (Cont…)

Case 23 : Email Spamming

Stephanie, a university student living in Cairns, received an email from an airline saying that she has won a $999 credit towards her next holiday. To redeem the credits, the email requested Stephanie to respond within the next 12 hours with her credit card details. She responded straight away, including her full name and credit card details. The next day, Stephanie notices that $1000 has been taken from her bank account.