Dr. MAHALINGAM MCET COLLEGE OF ENGINEERING AND TECHNOLOGY
Enlightening Technical Minds Estd. 1998
An Autonomous Institution (Since 2011)

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Affiliated to Anna University, Chennai; Approved by AICTE ; Accredited by NAAC with Grade 'A++'
Accredited by NBA - Tier1 (Mech, Auto, Civil, EEE, ECE, E&I and CSE)
Udumalai Road, Pollachi - 642 003. Tel: 04259-236030/40/50 Fax: 04259-236070 www.mcet.in

Department of Information Technology

19ITOC1004-Cyber Law and Information Security

Prepared by

G Keerthika

AP/IT

Objective of the Course

- The cybercrime vulnerabilities and its laws
- The cyber-attacks
- The cybercrime
- The fundamentals concepts of security
- The secure application development

Course Outcomes

At the end of this course, students will be able to:

CO1: Explain the cybercrime vulnerabilities for a networks and its laws

CO2: Describe the cyber-attacks on mobile and wireless devices

CO3: Analyze the cybercrime using tools and methods Analyze

CO4: Explain the fundamentals concepts of information security against cyber-attacks

CO5: Explain the secure application development using information security

Introduction

- Cyber law is a legal framework that governs the use of technology, computers, and the internet.
- It establishes rules and regulations to address legal issues related to cybersecurity, privacy, intellectual property, digital transactions, and online activities.
- The purpose of cyber law is to protect individuals, organizations, and society from cybercrimes and data breaches.

Introduction(contd…)

Information security focuses on protecting sensitive information from unauthorized access, use, disclosure, disruption, or destruction.

GOALS

- Confidentiality
- Integrity
- Availability
- Authentication and Access Control

Applications

- Protection of Personal Privacy
- Cybercrime Prevention and Prosecution
- Data Protection and Compliance
- Intellectual Property Protection
- E-commerce and Digital Transactions
- Cybersecurity and Critical Infrastructure Protection

Unit-1

Introduction to Cybercrime

Classifications of cybercrimes - Cybercrime: legal perspectives - Indian perspectives - Cybercrime and the Indian ITA 2000 - Global perspective on cybercrimes - Cyber offences: Criminals Plan the Attacks - Social engineering, Cyberstalking.

Unit-2

Cybercrime: Mobile and Wireless Devices

Mobile and Wireless Devices - Trend mobility - Authentication Service Security - Attacks on Mobile Phones - Mobile Devices: Security Implications for Organizations – Organizational Measurement for Handling Mobile – Organizational Security Policies and Measures in Mobile Computing Era – Laptops.

Unit-3

Tools and Methods Used in Cybercrime

Introduction - Proxy servers and anonymizes - Phishing, Password cracking - Key loggers and spywares, virus and worms - Trojan Horses and Backdoors – Steganography - DoS and DDoS attacks - Attacks on Wireless Networks.

Unit-4

Information Security

Information Security Concepts - Critical Characteristics of Information - CNSS Security Model -Components of an Information System - Balancing Information Security and Access – The SDLC - The Security SDLC.

Unit-5

Security Investigation

Need for Security - Business Needs - Threats - Secure Software Development – Law and Ethical in Information Security - International Laws and Laws Bodies - Ethics and Information Security

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit I – Introduction to Cybercrime

CO1:Explain the Cybercrime vulnerabilities for a networks and its law

LO1: To learn the classification of cybercrime and its legal perspective

SO1:Discuss about the Classifications of cybercrimes

Prepared by

G. Keerthika

Unit I
Introduction to Cybercrime

Classifications of cybercrimes - Cybercrime: legal perspectives - Indian perspectives - Cybercrime and the Indian ITA 2000 - Global perspective on cybercrimes - Cyber offences: Criminals Plan the Attacks - Social engineering, Cyberstalking.

Cybercrime

- Cybercrime is any criminal activity that involves a computer, networked device or a network.
- While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them.

Classification of Cybercrime

Cyber crimes can be classified in to 4 major categories as the following:

1. Cyber crime against Individual
2. Cyber crime Against Property
3. Cyber crime Against Organization
4. Cyber crime Against Society

Against Individuals

- **Email spoofing :** A spoofed email is one in which the e-mail header is forged so that the mail appears to originate from one source but actually has been sent from another source.
- **Spamming :** Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.
- **Cyber Defamation :** This occurs when defamation takes place with the help of computers and/or the Internet.

  E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.
- **Harassment & Cyber stalking :** Cyber Stalking Means following an individual's activity over internet.

  It can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.

Against Property

1. **Credit Card Fraud** :

•As the name suggests, this is a fraud that happens by the use of a credit card.

•This generally happens if someone gets to know the card number or the card gets stolen.

2. **Intellectual Property crimes :**

- Software piracy: Illegal copying of programs, distribution of copies of software.
- Copyright infringement: Using copyrighted material without proper permission.
- Trademarks violations: Using trademarks and associated rights without permission of the actual holder.
- Theft of computer source code: Stealing, destroying or misusing the source code of a computer.

3. **Internet time theft :** This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.

Against Organizations

(i) Unauthorized Accessing of Computer: Accessing the computer/network without permission from the owner.

- It can be of 2 forms:

  a) Changing/deleting data: Unauthorized changing of data.

  b) Computer voyeur: The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

(ii) Denial Of Service : When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

Against Organizations (contd…)

(iii) Computer contamination / Virus attack :

- A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it.
- Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

(iv) Email Bombing : Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.

(v) Salami Attack :

- When negligible amounts are removed & accumulated in to something larger.
- These attacks are used for the commission of financial crimes.

Against Organizations (contd…)

(vi) Logic Bomb : It is an event dependent program. As soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.

(vii) Trojan Horse : This is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

(viii) Data diddling : This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing completed.

Against Society

(i) Forgery : Currency notes, revenue stamps, mark sheets etc. can be forged using computers and high quality scanners and printers.

(ii) Cyber Terrorism : Use of computer resources to intimidate or coerce people and carry out the activities of terrorism.

(iii) Web Jacking : Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit I – Introduction to Cybercrime

CO1:Explain the Cybercrime vulnerabilities for a networks and its law

LO1:To learn the classification of cybercrime and its legal perspective

SO2:Discuss about Cybercrime: legal perspectives.

Prepared by

G. Keerthika

Unit I
Introduction to Cybercrime

Classifications of cybercrimes - Cybercrime: legal perspectives - Indian perspectives - Cybercrime and the Indian ITA 2000 - Global perspective on cybercrimes - Cyber offences: Criminals Plan the Attacks - Social engineering, Cyberstalking.

The Legal Perspectives Cyber law

- In Simple way we can say that cybercrime is unlawful acts wherein the computer is either a tool or a target or both.
- Cybercrimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code.
- The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

Categories of Cyber crime

- We can categorize Cybercrimes in two ways
- **The Computer as a Target** - using a computer to attack other computers.
- Eg:- Hacking, Virus/ Worm attacks, DOS attack etc.

- **The computer as a weapon** - using a computer to commit real world crimes.
- Eg:- Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cybercrime and Cyber security

- Areas that are related to cyber law include cybercrime and cyber security.
- With the right cyber security, businesses and people can protect themselves from cybercrime.
- Cyber security looks to address weaknesses in computers and networks.
- The International Cyber security Standard is known as ISO 27001.

Cyber security policy

- Cyber security policy is focused on providing guidance to anyone that might be vulnerable to cybercrime.
- This includes businesses, individuals, and even the government.
- Many countries are looking for ways to promote cyber security and prevent cybercrime.
- For instance, the Indian government passed the Information Technology Act in 2000.
- The main goal of this law is to improve transmission of data over the internet while keeping it safe.

Categories of Cyber Crime

Crimes against People:

- While these crimes occur online, they affect the lives of actual people.
- Some of these crimes include cyber harassment and stalking, distribution of child pornography, various types of spoofing, credit card fraud, human trafficking, identity theft, and online related libel or slander.

Crimes against Property.:

- Some online crimes happen against property, such as a computer or server.
- These crimes include DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement, and IPR violations.

Categories of Cyber Crime(contd..)

Crimes against Government:

- When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty and an act of war.
- Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software.

Special Laws and Cybercrimes

Special Laws and Cybercrimes under the IPC include:

- Sending Threating Messages by Email, Indian Penal Code (IPC) Sec. 503.
- Sending Defamatory Messages by Email, Indian Penal Code (IPC) Sec. 499
- Forgery of Electronic Records, Indian Penal Code (IPC) Sec. 463
- Bogus Websites & Cyber Fraud, Indian Penal Code (IPC) Sec. 420
- Email Spoofing, Indian Penal Code (IPC) Sec. 463
- Web-Jacking, Indian Penal Code (IPC) Sec. 383
- Email Abuse, Indian Penal Code (IPC) Sec. 500

Cyber Law and Intellectual Property

- An important part of cyber law is intellectual property.
- Intellectual property can include areas like inventions, literature, music, and businesses. It now includes digital items that are offered over the internet

IP rights related to cyber law generally fall into the following categories:

- **Copyright**.: This is the main form of IP cyber law. Copyrights provide protection to almost any piece of IP you can transmit over the internet. This can include books, music, movies, blogs, and much more.
- Patents: Patents are generally used to protect an invention. These are used on the internet for two main reasons. The first is for new software. The second is for new online business methods.

Cyber Law and Intellectual Property(contd..)

Trademarks/Service Marks.: Trademarks and service marks are used the same online as they are in the real world. Trademarks will be used for websites. Service marks are used for websites that provide services.

Trade Secrets: Trade secret laws are used to protect multiple forms of IP. This includes formulas, patterns, and processes. Online businesses can use trade secret protections for many reasons. However, it does not prevent reverse engineering.

Domain Disputes: This is related to trademarks. Specifically, domain disputes are about who owns a web address. For instance, the person who runs a website may not be the person who owns it. Additionally, because domains are cheap, some people buy multiple domains hoping for a big payday.

Cyber Law and Intellectual Property(contd..)

Contracts: Most people don't think contracts apply online. This is not the case. For example, when you register for a website, you usually have to agree to terms of service.

Privacy: Online businesses are required to protect their customer's privacy. The specific law can depend on your industry. These laws become more important as more and more information is transmitted over the internet.

Employment: Some employee contract terms are linked to cyber law. This is especially true with non-disclosure and non-compete clauses. These two clauses are now often written to include the internet.

It can also include how employees use their company email or other digital resources.

Cyber Law and Intellectual Property(contd..)

Defamation: Slander and libel law has also needed updating because of the internet.

Proving defamation was not altered substantially, but it now includes the internet.

Data Retention: Handling data is a primary concern in the internet age. An area where this has become a big issue is in terms of litigation. In lawsuits, it is now common to request electronic records and physical records.

Jurisdiction: Jurisdiction is a key part of court cases. Cybercrime has complicated this issue.

Cyber Law and Intellectual Property(contd..)

Protecting IP:

- **It** can be difficult over the internet.
- An example of this would be the popularity of pirated movies and music.
- Each business that relies on the internet needs to develop strategies for protecting their IP.
- Governments can also take part in this process. In 1999, India did just this by updating their IP laws.

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit I – Introduction to Cybercrime

CO1:Explain the Cybercrime vulnerabilities for a networks and its law

LO1: To learn the classification of cybercrime and its legal perspective

SO3:Explain Indian perspectives -Cybercrime and the Indian ITA 2000 and global perspectives

Prepared by

G. Keerthika

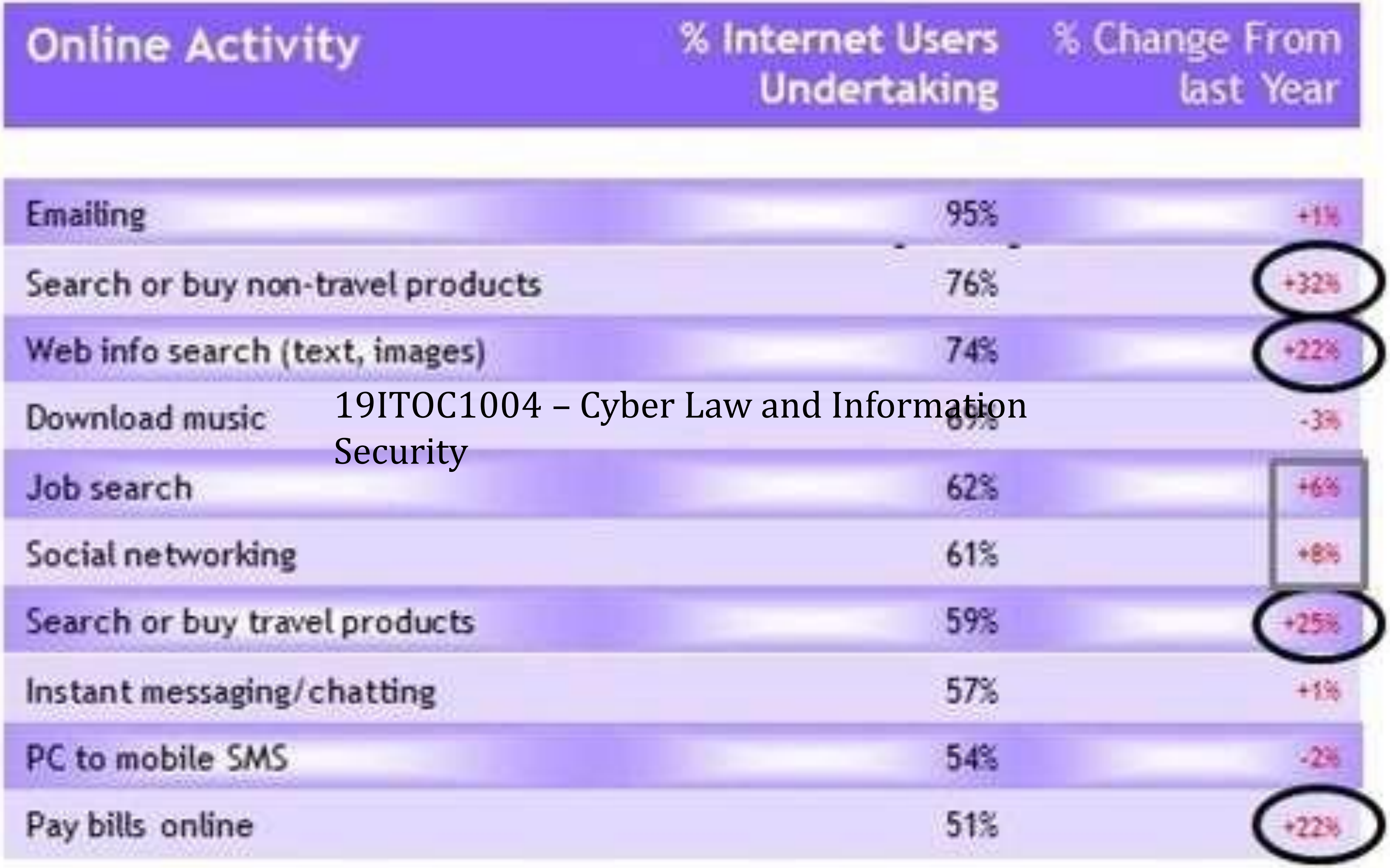
Unit I
Introduction to Cybercrime

Classifications of cybercrimes - Cybercrime: legal perspectives - Indian perspectives - Cybercrime and the Indian ITA 2000 - Global perspective on cybercrimes - Cyber offences: Criminals Plan the Attacks - Social engineering, Cyberstalking.

Interesting Findings of the Indian Online 2011 report

- According to the annual I-Cube Report published by IAMAI (Internet and Mobile Association Of India), India's internet population is expected to grow to 121 million users by December 2011 from 100 million in September this year.
- 28% growth in Internet users (From 51 Mln last year to 65 Mln this year)
- Internet reaches 29 million Indian households
- Over 4 in 5 are 'daily' users. Daily users' base grew faster, at 33%
- 9 out of 10 'home' and 'office' based online Indians log on to the net 'daily'
- Net surfing is among top 3 favorite 'indoor entertainment' for 3 out of 4 of them
- 9 out of 10 of them (86%) use social media sites.

User Activities on Internet



Online Activity	% Internet Users Undertaking	% Change From last Year
Emailing	95%	+1%
Search or buy non-travel products	76%	+32%
Web info search (text, images)	74%	+22%
Download music	69%	-3%
Job search	62%	+6%
Social networking	61%	+8%
Search or buy travel products	59%	+25%
Instant messaging/chatting	57%	+1%
PC to mobile SMS	54%	-2%
Pay bills online	51%	+22%

Most used Websites by Users

Vertical	Top Website	% Use (Among Vertical Users)
Generic Portals (all-purpose websites)	**Yahoo, Google**	84%, 84%
Emailing	**Gmail**	92%
Instant Messaging	**Gtalk/Gmail**	73%
Job Search	**Naukri**	78%
Online News	**Google**	61%
Online Travel Buy	**IRCTC**	81%
Online Buying (Non-Travel)	**Ebay**	49%
Real Estate	**99acre**	64%
Business & Financial News	**Google**	55%
Online Share Trading (Trading)	**Sharekhan**	50%
PC to PC Net Telephony	**Google/Gtalk**	89%
PC to Telephone Net Telephony	**Google/Gtalk**	69%
PC to Mobile Messaging (sms)	**Way2sms**	79%
Net banking	**ICICI Bank**	

49%

Growing Concern

- Computing Technology has turned against us
- Exponential growth in security incidents
- Complex and target oriented software
- Common computing technologies and systems
- Constant probing and mapping of network systems

Why learn about CYBER CRIME ?Because

- Everybody is using COMPUTERS..
- From white collar criminals to terrorist organizations And from Teenagers to Adults
- Conventional crimes like Forgery, extortion, kidnapping etc.. are being committed with the help of computers
- New generation is growing up with computers
- **MOST IMPORTANT - Monetary transactions** are moving on to the INTERNET

WHAT IS COMPUTER CRIME?

- All crimes performed or resorted to by abuse of electronic media or otherwise, with the purpose of influencing the functioning of computer or computer system.

COMPUTER CRIME is any crime where –

1. Computer is a target.
2. Computer is a tool of crime
3. Computer is incidental to crime

Profile of Cyber Criminal

- Discontented employees.
- Teenagers.
- Political Activist.
- Professional Hackers.
- Business Rival.
- Ex-Boy Friend.
- Divorced Husband. etc

Top 5 cyber crime complinats

- Non delivery (paying for the merchandise online, but not receiving it)
- Auction fraud
- Debit/ credit card fraud
- Confidence fraud (advance fee fraud – Nigerian letters)
- Computer fraud

VICTIMS

- Innocent
- Criminals and greedy people
- Unskilled & Inexperienced
- Unlucky people

Types of Cyber Crime

- HACKING
- VIRUS
- DENIAL OF SERVICE
- DISSEMINATION
- SOFTWARE PIRACY
- PORNOGRAPHY
- IRC Crime
- Cyber squatting
- CREDIT CARD FRAUD
- Bot networks
- NET EXTORTION

- PHISHING
- SPOOFING
- CYBER STALKING
- CYBER
- DEFAMATION
- THREATENING
- SALAMI ATTACK
- CROSS SITE SCRIPTING (XSS)
- VISHING

Phishing email

From: *****Bank

[mailto:support@****Bank.com] Sent: 08

June 2004 03:25

To: India

Subject: Official information from *****

Bank Dear valued ***** Bank Customer!

For security purposes your account has been randomly chosen for verification. To verify your account information we are asking you to provide us with all the data we are requesting. Otherwise we will not be able to verify your identity and access to your account will be denied. Please click on the link below to get to the bank secure page and verify your account details. Thank you.

https://infinity.*****bank.co.in/Verify.jsp

****** Bank Limited

Steps to check Cyber crime

- Even when one follows the latest security trends and goes for the best practices to protect the systems and networks, there are still many loopholes left in the network itself that gives into the cyber criminals.

- While IDC (International data Corporation), IPS (Intrusion detection system), Firewalls and Log Analysis are some of the state of the art cyber defenses available, network forensics is an evolving field in the security landscape.

Steps to check Cyber crime

- Data is recorded, stored and reconstructed in order to discover the source of security attacks or other problem incidents.

- This leads us to the unknowns in the security breach and hence to the truth.

- To reach to the truth, the various tools used are archiving the network traffic, sessionizing, and parsing and data extraction.

computer forensics

- computer forensics is the art and science of applying computer science to aid the legal process.

- We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.

Indian Crime Scene

- The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate e-mail traffic.
- Over 86 per cent of all attacks, mostly via 'bots‘ were aimed at lay surfers with Mumbai and Delhi emerging as the top two cities for such vulnerability.
- India has now joined the dubious list of the world's top 15 countries hosting "phishing" sites which aims at stealing confidential information such as passwords and credit card details.
- A 23 year-old person from Tiruchi was arrested by the City Cyber Crime police on Thursday on charges of sending an e- mail threat to the Chief Minister and his family in 2007.

Indian Trends of Incidents

- Computer hackers have also got into the Bhaba Atomic Research Centre (BARC) computer and pulled out important data.
- Some computer professionals who prepared the software for MBBS examination altered the data and gave an upward revision to some students in return for a hefty payment.

Security of Information Assets

- Security of information & information assets is becoming a major area of concern
- With every new application, newer vulnerabilities crop up, posing immense challenges to those who are mandated to protect the IT assets
- Coupled with this host of legal requirements and international business compliance requirements on data protection and privacy place a huge demand on IT/ITES/BPO (IT/IT Enabled Services/ Business Process outsourcing) service organizations
- We need to generate ‘Trust & Confidence’

Cyber Security Strategy – India

- **Security Policy, Compliance and Assurance – Legal Framework**
  - IT Act, 2009
  - IT (Amendment) Bill, 2006 – Data Protection & Computer crimes
  - Best Practice ISO 27001
  - Security Assurance Framework- IT/ITES/BPO Companies

- **Security Incident – Early Warning & Response**
  - CERT-In National Cyber Alert System – Computer Emergency Response Team (Govt of India)
  - Information Exchange with international CERTs

- **Capacity building**
  - Skill & Competence development
  - Training of law enforcement agencies and judicial officials in the collection and analysis of digital evidence
  - Training in the area of implementing information security in collaboration with Specialised
  - Organisations in US

- **Setting up Digital Forensics Centres**
  - Domain Specific training – Cyber Forensics

- **Research and Development**
  - Network Monitoring
  - Biometric Authentication
  - Network Security
- **International Collaboration**

Status of security and quality compliance in India

- Quality and Security
  - Large number of companies in India have aligned their internal process and practices to international standards such as
    - ISO 9000 – Quality maangement
    - CMM – Capital Maturity Model
    - Six Sigma
    - Total Quality Management
  - Some Indian companies have won special recognition for excellence in quality out of 18 Deming Prize winners for Total Quality Management in the last five years, six are Indian companies.

ISO 27001/BS7799 Information Security Management

- Government has mandated implementation of ISO27001 ISMS (Information Security Management system)by all critical sectors
- ISMS 27001 has mainly three components
  - Technology
  - Process
  - Incident reporting and monitoring
- 296 certificates issued in India out of 7735 certificates issued worldwide
- Majority of certificates issued in India belong to IT/ITES/BPO sector

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit I – Introduction to Cybercrime

CO1:Explain the Cybercrime vulnerabilities for a networks and its law

LO1:To learn the classification of cybercrime and its legal perspective

SO3:Explain Indian perspectives -Cybercrime and the Indian ITA 2000 and global perspectives

Prepared by

G. Keerthika

Unit I
Introduction to Cybercrime

Classifications of cybercrimes - Cybercrime: legal perspectives - Indian perspectives - Cybercrime and the Indian ITA 2000 - Global perspective on cybercrimes - Cyber offences: Criminals Plan the Attacks - Social engineering, Cyberstalking.

Information Technology Act, 2000 (India)

- The Information Technology Act, 2000 also Known as an IT Act is an act proposed by the Indian Parliament reported on 17th October 2000.
- This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997.
- It is the most important law in India dealing with Cybercrime and E-Commerce.
- The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes.
- The IT Act has 13 chapters and 90 sections. The last four sections that starts from 'section 91 – section 94', deals with the revisions to the Indian Penal Code 1860.

The IT Act, 2000 has two schedules

- First Schedule – Deals with documents to which the Act shall not apply.
- Second Schedule – Deals with electronic signature or electronic authentication method

The offences and the punishments in IT Act 2000

- The offences and the punishments that falls under the IT Act, 2000 are as follows:
- Tampering with the computer source documents.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Publishing of information which is obscene in electronic form.
- Penalty for breach of confidentiality and privacy & Hacking for malicious purposes.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Penalty for misrepresentation & Confiscation.
- Protected System & Power to investigate offences.
- Penalties for confiscation not to interfere with other punishments.
- Act to apply for offence or contravention committed outside India.
- Publication for fraud purposes.
- Power of Controller to give directions.

Sections and Punishment

Section 43

This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.

Section 43A

This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.

Sections and Punishment(contd..)

Section 43A

This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.

Section 66

Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both.

Section 66 B, C, D

Section 66 B, C, D Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.

Sections and Punishment(contd..)

Section 66 E

This Section is for Violation of privacy by transmitting image or private area is punishable with 3 years imprisonment or 2,00,000 fine or both.

Section 66 F

This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.

Section 66 F

This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.

Section 67

This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine or Rs. 10,00,000 or both.

Amendment

- A major amendment was made in 2008. It introduced Section 66A which penalized sending "offensive messages".
- It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource".
- Additionally, it introduced provisions addressing - pornography, child porn, cyber terrorism and voyeurism.
- The amendment was passed on 22 December 2008 without any debate in Lok Sabha.
- The next day it was passed by the Rajya Sabha. It was signed into law by President Pratibha Patil, on 5 February 2009.

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit I – Introduction to Cybercrime

CO1:Explain the Cybercrime vulnerabilities for a networks and its law

LO1:To learn the classification of cybercrime and its legal perspective

SO3:Explain Indian perspectives -Cybercrime and the Indian ITA 2000 and global perspectives

Prepared by

G. Keerthika

Unit I
Introduction to Cybercrime

Classifications of cybercrimes - Cybercrime: legal perspectives - Indian perspectives - Cybercrime and the Indian ITA 2000 - Global perspective on cybercrimes - Cyber offences: Criminals Plan the Attacks - Social engineering, Cyberstalking.

Cyber-crime: A Global Perspective

International Efforts to Harmonize Cybercrime

- Council of Europe (CoE): Conference on Criminological Aspects of Economic Crime - Strasbourg (1976)
- U.S. Justice Department: Criminal Justice Resource Manual (1979)
- First Interpol Training Seminar for Investigators of Computer Crime - Paris (1981) .
- Organization for Economic Cooperation and Development (OECD): Committee for Information and Communications Policy (ICCP) International Efforts to Harmonize Cybercrime
- Council of Europe (CoE): Conference on Criminological Aspects of Economic Crime - Strasbourg (1976)
- U.S. Justice Department: Criminal Justice Resource Manual (1979)
- First Interpol Training Seminar for Investigators of Computer Crime - Paris (1981)
- Organization for Economic Cooperation and Development (OECD):

Computer Crime

- any illegal act for which knowledge of computer technology is essential for a successful prosecution.
- any illegal, unethical or unauthorized behavior relating to the automatic processing and the transmission of data.”
- updating technical means of prosecuting existing crimes committed using a computer
- new crimes where computer is object of crime
- Internet Jurisdiction

Unauthorized Access

- define a computer system as a protected environment and make control of access to this environment a protected right
- normal operations and exceptions
    - Security Research
    - Quality Assurance
    - Lack of harm or damage
    - Legitimate Use
    - Anti-Competitive Behavior

Cyber crime atacks

- automation of processing and transmission
- complex operation of computer systems
- computer as subject of crime
    - Worms - viruses that self-replicate
    - Trojan Horses - contain hidden malicious code
    - Logic Bombs - activate at specific time
    - Sniffers - network analyzers
- functionality of code lacks specific intent

Convention on Cybercrime

- Illegal Access - infringing security measures, intent of obtaining data
- Illegal Interception - interception, without right, by technical means, of non-public transmission
- Data Interference - damage, deletion, deterioration, alteration, suppression
- System Interference - inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing
- Misuse of Devices - production, sale, procurement for use, import, distribution, making available; designed or adapted primarily for offense
- Computer-Related Forgery - inauthentic data, intent to defraud
- Computer-related Fraud - causing of a loss of property to another person

Guidelines for the Cooperation between Law Enforcement and Internet Service Providers Against Cybercrime - Council of Europe (2008)

- written procedures, information sharing, culture of cooperation, formal partnerships
- protect fundamental rights of citizens - civil, political, & human rights
- enforcing domestic & international data protection & privacy
- procedures, training, technical resources, designated personnel
- standardizing requests, specificity and accuracy requirements
- ISPs encouraged to report offenses and not obligated to monitor
- ensure that customer data and personal information not disclosed

Information Intermediaries

- Hosting Providers
- Internet Service Providers
- Domain Name Registrars
- Financial Intermediaries
- Auction Platforms and eCommerce actors
- Search Engines
- Participative Web Platforms
- Virtual Worlds
- Distributed Computing
- Social Networks

Privacy

- Notice/Disclosure/Collection
- Choice/Consent
- Access
- Security/Integrity
- Enforcement/Redress
    - mandatory disclosure of personal information
    - public-private space distinction
    - content of communications
    - specificity of warrant

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit I – Introduction to Cybercrime

CO1:Explain the Cybercrime vulnerabilities for a networks and its law

LO2: Describe about cyber offenses

SO2: Criminals Plan the Attacks

Prepared by

G. Keerthika

Criminals plan the Attacks

- Criminals plan passive and active attacks.
- Active attacks are usually used to alter the system, whereas passive attacks attempt to gain information about the target.
- Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to breaches of confidentiality.

Phases involved in planning cybercrime

The following phases are involved in planning cybercrime:

- Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
- Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
- Launching an attack (gaining and maintaining the system access).

Reconnaissance

- The literal meaning of "Reconnaissance" is an act of reconnoitering- explore, often with the goal of finding something or somebody (especially to gain information about an enemy or potential enemy).
- In the world of "hacking," reconnaissance phase begins with "Footprinting”.
- Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities.
- The objective of this preparatory phase is to understand the system, its networking ports and services and any other aspects of its security that are needful for launching the attack.
- Thus, an attacker attempts to gather information in two phases: passive and active attacks.

Passive Attacks

- A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge.
- It can be as simple as watching a building to identify what time employees enter the building's premises.
- However, it is usually done using Internet searches or by Googling (i,e., searching the required information with the help of search engine Google) an individual or company to gain information.
- Google or Yahoo search: People search to locate information about employees.
- Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.

Passive Attacks(contd..)

- Organization's website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc.
- These can be used in a social engineering attack to reach the target.
- Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
- Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on its network.

Active Attacks

- An active attack involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack, phase.
- It involves the risk of detection and is also called "Rattling the doorknobs" or "Active reconnaissance."
- Active reconnaissance can provide confirmation to an attacker about security measures in place,, but the process can also increase the chance of being caught or raise suspicion.

Scanning and Scrutinizing Gathered Information

- Scanning is a key step to examine intelligently while gathering information about the target.
- The objectives of scanning are as follows:

Port scanning: Identify open/close ports and services.

Network scanning: Understand IP Addresses and related information about the computer network systems.

Vulnerability scanning: Understand the existing weaknesses in the system.

- The scrutinizing phase is always called "enumeration" in the hacking world.

The objective behind this step is to identify:

1. The valid user accounts or groups
2. Network resources and/or shared resources
3. OS and different applications that are running on the OS.

Gaining and Maintaining the System Access

- After the scanning and enumeration, the attack is launched using the following steps:

  1. Crack the password

  2. Exploit he password

  3. Execute the malicious command/applications;

  4. Hide the files (if required);

  5. Cover the tracks - delete the access logs, so that there is no trail illicit activity.

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit I – Introduction to Cybercrime

CO1:Explain the Cybercrime vulnerabilities for a networks and its law

LO2: Describe about cyber offenses

SO3: Explain Social engineering, Cyberstalking

Prepared by

G. Keerthika

Unit I
Introduction to Cybercrime

Classifications of cybercrimes - Cybercrime: legal perspectives - Indian perspectives - Cybercrime and the Indian ITA 2000 - Global perspective on cybercrimes - Cyber offences: Criminals Plan the Attacks - Social engineering, Cyberstalking.

Social Engineering

- Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.
- social engineers are clever and use manipulative tactics to trick their victims into disclosing private or sensitive information.
- Social engineering is a term that encompasses a broad spectrum of malicious activity.

Attacks

- The five most common attack types that social engineers use to target their victims. These are

  1) Phishing

  2) Vishing and Smishing

  3) Pretexting

  4) Paiting

  5) Quid Pro Quo

  6) Tailgating and Piggybacking

Phishing

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a genuine (legal) organization to ensnare individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
- The information is then used to access important accounts and can result in identity theft and financial loss.
- Phishers frequently use emotions like fear, curiosity, urgency, and greed to force recipients to open attachments or click on links.
- Phishing attacks are designed to appear to come from legitimate (legal) companies and individuals.

Types of Phishing

Spear phishing

- Spear phishing targets specific individuals instead of a wide group of people.
- The attackers can customize their communications and appear more authentic.
- Spear phishing is often the first step used to penetrate a company's defenses and carry out a targeted attack.
- Imagine that an individual regularly posts on social media that she is a member of a particular gym. In that case, the attacker could create a spear phishing email that appears to come from her local gym.
- The victim is more likely to fall for the scam since she recognized her gym as the supposed sender

Whaling

- When attackers go after a "big fish" like a CEO, it's called whaling.
- These attackers often spend considerable time profiling the target to find the opportunity and means to steal login credentials.
- Whaling is of particular concern because high-level executives are able to access a great deal of sensitive company information.

Social media phishing-

- Attackers often research their victims on social media and other sites to collect detailed information, and then plan their attack accordingly.

Vishing and Smishing

- While phishing is used to describe fraudulent email practices, similar manipulative techniques are practiced using other communication methods such as phone calls and text messages.
- Vishing (short for voice phishing) occurs when a fraudster attempts to trick a victim into disclosing sensitive information or giving them access to the victim's computer over the telephone.
- Smishing (short for SMS phishing) is similar to and incorporates the same techniques as email phishing and vishing, but it is done through SMS/text messaging.

Pretexting

- Pretexting is a type of social engineering technique where the attacker creates a scenario where the victim feels compelled to comply under false pretenses.
- Typically, the attacker will impersonate someone in a powerful position to persuade the victim to follow their orders.
- During this type of social engineering attack, a bad actor may impersonate police officers, higher-ups within the company, auditors, investigators or any other persona they believe will help them get the information they seek

Baiting

- Baiting puts something enticing (tempting) or curious in front of the victim to lure (trap) them into the social engineering trap.
- A baiting scheme could offer a free music download or gift card in an attempt to trick the user into providing credentials.
- A social engineer may hand out free USB drives to users at a conference.
- The user may believe they are just getting a free storage device, but the attacker could have loaded it with remote access malware which infects the computer when plugged in.

Tailgating and Piggybacking

- Tailgating is a simplistic social engineering attack used to gain physical access to access to an unauthorized location.
- Tailgating is achieved by closely following an authorized user into the area without being noticed by the authorized user.
- An attacker may tailgate another individual by quickly sticking their foot or another object into the door right before the door is completely shut and locked.

Piggybacking

- Piggybacking is exceptionally similar to tailgating.
- The main difference between the two is that, in a piggybacking scenario, the authorized user is aware and allows the other individual to "piggyback" off their credentials.
- An authorized user may feel compelled by kindness to hold a secure door open for a woman holding what appears to be heavy boxes or for a person claiming to be a new employee who has forgotten his access badge

Quid Pro Quo

- Quid pro quo (Latin for 'something for something') is a type of social engineering tactic in which the attacker attempts a trade of service for information.
- A quid pro quo scenario could involve an attacker calling the main lines of companies pretending to be from the IT department, attempting to reach someone who was having a technical issue.
- Once the attacker finds a user who requires technical assistance, they would say something along the lines of, "I can fix that for you. I'll just need your login credentials to continue."
- This is a simple and unsophisticated way of obtaining a user's credentials

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Affiliated to Anna University, Chennai; Approved by AICTE ; Accredited by NAAC with Grade 'A++'
Accredited by NBA - Tier1 (Mech, Auto, Civil, EEE, ECE, E&I and CSE)
Udumalai Road, Pollachi - 642 003 Tel: 04259-236030/40/50 Fax: 04259-236070 www.mcet.in

Dr. MAHALINGAM MCET COLLEGE OF ENGINEERING AND TECHNOLOGY
Enlightening Technical Minds Estd. 1998
An Autonomous Institution
(Since 2011)

19ITOC1004 – Cyber Law and Information Security

Unit I – Introduction to Cybercrime

CO1:Explain the Cybercrime vulnerabilities for a networks and its law

LO2: Describe about cyber offenses

SO3: Explain Social engineering, Cyberstalking

Prepared by

G. Keerthika

NIA EDUCATIONAL INSTITUTIONS Enlightening Minds

Unit I
Introduction to Cybercrime

Classifications of cybercrimes - Cybercrime: legal perspectives - Indian perspectives - Cybercrime and the Indian ITA 2000 - Global perspective on cybercrimes - Cyber offences: Criminals Plan the Attacks - Social engineering, Cyberstalking.

Cyber Stalking

- Cyberstalking is a crime in which someone harasses or stalks a victim using electronic or digital means, such as social media, email, instant messaging (IM), or messages posted to a discussion group or forum.
- Cyberstalkers take advantage of the anonymity afforded by the internet to stalk or harass their victims, sometimes without being caught, punished or even detected.
- Although cyberstalking is a general term for online harassment, it can take many forms, including slander, defamation, false accusations, trolling and even outright threats.

Cyber Stalking

In many cases, especially when both the harasser and victim are individuals, the motive may be the following

a) monitor the victim's online and in some cases, offline activities

b) track the victim's locations and follow them online or offline

c) intimidate (scare), frighten, control or blackmail the victim

d) reveal private information about the victim, a practice known as doxing or gather more information about the victim to steal their identity or perpetrate other real-world crimes, like theft or harassment

Rejected Cyberstalkers:

- This type of cyberstalker is motivated to pursue their victim in attempt to reverse what they perceive as a wrongful set of circumstances causing a prior divorce, separation or termination of a relationship.
- These offenders either feel misunderstood hoping to reverse the breakup or feel angry and seeking revenge because their attempts at reconciliation with the victim has failed in the past

Resentful Cyberstalkers

- This type of cyberstalker can be dangerous given their perceived motivation for stalking.
- Resentful cyberstalkers are fully aware the victim is cognizant of the stalking but continues to fulfill a distorted (biased or one-sided) vendetta (quarrel) he/she feels is warranted.
- Fear and distress experienced by the victim are the goals of this type of cyberstalker.
- For this type of profile, the cyberstalker believes the victim both deserves and requires being frightened because they have caused them and/or others distress

Intimacy Seekers

- This type of cyberstalker does not have will towards their victim and simply wants to engage in a loving relationship with them.
- Intimacy seekers view their victims as their soulmate destined to be together at all costs. Within their mind, they believe it is their job and purpose to make sure destiny of a loving relationship is fulfilled.
- Intimacy seeking cyberstalkers are often the segment of men or women who harass celebrities and public figures.
- Blinded by their distorted perceptions of a destined love, they lose sight of the distress and fear they are causing the person they cyberstalk.

Incompetent Suitors

- These people who fit this profile are cyberstalkers deeply enamored (loving) with their victim.
- Their interest for the victim at times can reach a state of fixation whereby their entire waking life is focused on the endeavor (try) of one day becoming a couple.
- They tend to lack social, communication or courting skills and may feel entitled that their fantasy of a loving relationship is inevitable (expected).
- Feeling entitled and/or deserving of a relationship with the victim inspires the cyberstalker to gradually increase their frequency of contact.
- Although like the Intimacy Seeker cyberstalker, incompetent suitors are more gradual in their means and methods of contact.

Predatory Cyberstalkers

- ▯ Of the six types, the predatory cyberstalker can be the most dangerous and determined.
- This type of cyberstalker is motivated by a perverted sexual need.
- They do not have feelings of love for their victim nor motivated by a belief of predestination.

Ghost Cyberstalkers

- Ghost Cyber stalkers are online assailants (mask) who their target cannot identify.
- Using Cyberstealth, the ghost cyberstalker repeatedly makes direct or indirect threats of physical harm and inspires fear.
- They can represent an amalgamation (union) of the other five types.
- Ghost cyberstalkers rely upon the veil of secrecy afforded to all online users.

Real Life Examples of Cyber Stalking

- Placing orders for delivery in someone else's name.
- Gathering personal information on the victim.
- Spreading false rumors.
- Encouraging others to join in the harassment.
- Threatening harm through email.
- Creating fear and paranoia(terror / distrust) for someone else.
- Post rude, offensive, or suggestive comments online.
- Follow the target online by joining the same groups and forums.
- Send threatening, controlling, or lewd messages or emails to the target.
- Use technology to threaten or blackmail the target.

To guard against cyberstalking

- update all software to prevent information leaks
- mask your Internet Protocol address with a virtual private network
- strengthen privacy settings on social media
- strengthen all devices with strong passwords or, better, use multifactor authentication
- avoid using public Wi-Fi networks
- send private information via private messages, not by posting on public forums
- safeguard mobile devices by using password protection and never leave devices unattended
- disable geo location settings on devices
- install antivirus software on devices to detect malicious software
- always log out of all accounts at the end of a session and
- beware of installing apps that ask to access your personal information

Prevention of cyberstalked

Block the person

- Don’t hesitate to apply all measures permitted by law, especially those offered by web services.
- If the tools are there, block anyone who you wish to stop hearing from, even if these messages are just annoying and not yet threatening.
- Only you can decide when this boundary has been passed.

Prevention of cyberstalked (contd..)

Report to the platform involved

- If someone is harassing or threatening , should block them immediately and report their behavior to the platform involved.
- Twitter, Facebook, LinkedIn and many other platforms have created easy-to-use buttons to quickly report abusive behavior.
- Law enforcement agencies do not always have the technical ability to protect you from cyberstalking, but platform moderators usually respond quickly and delete attackers' profiles.

Prevention of cyberstalked (contd..)

Call the Police

If you believe their behavior is illegal or you fear for your safety, then we should contact the police and report the cyberstalker.

Even if we don't have enough information or evidence for them to prosecute immediately, the report will go on record and the police can offer advice about what to do if the perpetrator persists.

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You