TY B.Tech CSE (CSF) Semester (AY 2023-2024)

Computer Science and Engineering

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

Unit 5: Cyber Law for Cybercrime

Need for Cyber Law, Cyber Jurisprudence at International and Indian Level, Cybercrime and Punishment, Cyber Crimes & Legal Framework Cyber Crimes against Individuals, Institution and State, Hacking, Digital Forgery, Case studies.

Cyber Law

Definition

Cyber law, also known as internet law or digital law, refers to the legal regulations that govern internet usage and electronic communication. It encompasses a wide range of legal issues related to the internet, cyberspace, and digital communications.

Importance

Cyber law is important because it safeguards digital privacy, promotes secure online transactions, prevents cybercrimes, and ensures ethical use of technology, fostering trust, innovation, and a reliable digital environment.

Cyber law and its Need

- **Protect Privacy:** Safeguard personal and sensitive data from unauthorized access and misuse.
- **Prevent Cybercrimes:** Deter and prosecute illegal activities such as hacking, fraud, and identity theft in cyberspace.
- **Ensure Data Security:** Implement regulations for secure storage, transmission, and handling of digital information.
- **Facilitate E-commerce:** Establish legal frameworks for secure online transactions, boosting consumer trust in digital businesses.
- **Protect Intellectual Property:** Enforce copyrights, patents, and trademarks in the digital realm, encouraging innovation and creativity.
- **Regulate Social Media:** Address issues like cyberbullying, defamation, and hate speech, ensuring responsible online behaviour.
- **Define Jurisdiction:** Establish guidelines for legal jurisdiction in cross-border digital disputes and cybercrimes.
- **Promote Ethical Hacking:** Encourage ethical hacking practices to identify vulnerabilities and enhance overall cybersecurity.

Cyber Jurisprudence at International and Indian Level

The term Jurisprudence is derived from Latin word 'Jurisprudentia' which means either "Knowledge of Law". The word "juris" means law and prudentia mean knowledge, science or skill.

Cyber jurisprudence is the legal study that concentrates on the logical structure, the meanings and uses of its concepts, and the formal terms and modes of operation of cyber law.

Cyber jurisprudence refers to the legal principles, rules, and frameworks that govern cyberspace and address the legal issues arising from cyber activities. At the international level, there are several initiatives and frameworks that aim to establish a legal framework for cyberspace. In India, there are specific laws and regulations that govern cyber activities and address cybercrimes.

Cyber Jurisprudence at International and Indian Level

International Level

- United Nations (UN): The UN has been actively engaged in discussions and initiatives related to cybersecurity and cyberspace. The UN General Assembly has adopted several resolutions that emphasize the importance of international cooperation in addressing cyber threats and promoting stability in cyberspace.
- International Telecommunication Union (ITU): The ITU, a specialized agency of the UN, focuses on issues related to information and communication technologies (ICTs), including cybersecurity. It works towards promoting international cooperation, developing technical standards, and addressing legal and policy aspects of cybersecurity.
- Council of Europe (CoE): The CoE has developed the Convention on Cybercrime, also known as the Budapest Convention, which is an international treaty aimed at harmonizing national legislation and facilitating international cooperation in combating cybercrime.
- Regional Initiatives: Various regional organizations and initiatives, such as the European Union's General Data Protection Regulation (GDPR) and the ASEAN Agreement on Transboundary Haze Pollution, address specific aspects of cybersecurity and data protection within their respective regions.

Indian Level

- Information Technology Act, 2000: The Information Technology Act, 2000 (IT Act) is the primary legislation governing cyber activities and addressing cybercrimes in India. It provides legal recognition for electronic transactions, defines cyber offenses, and outlines the penalties for cybercrimes.
- Indian Cyber Crime Coordination Centre (I4C): The I4C is a specialized agency established by the Government of India to coordinate and strengthen the country's efforts in combating cybercrimes. It works towards enhancing cyber infrastructure, capacity building, and cyber law enforcement.
- National Cyber Security Policy: India has formulated a National Cyber Security Policy that outlines the strategic objectives, principles, and actions to be taken to strengthen cybersecurity in the country. The policy focuses on enhancing the security of critical information infrastructure and promoting a secure and resilient cyberspace.
- Data Protection Laws: In addition to the IT Act, India has recently introduced the Personal Data Protection Bill, which aims to regulate the collection, processing, and use of personal data and protect individuals' privacy rights.

These are just some of the key initiatives and laws related to cyber jurisprudence at the international and Indian levels. The field of cybersecurity and cyber jurisprudence is evolving rapidly, as new challenges and technologies emerge, requiring ongoing legal and policy developments to address the complexities of cyberspace.

Cyber Crime and Punishment

Cybercrimes encompass a wide range of illegal activities conducted through computer networks and digital devices. The punishments for cybercrimes vary based on the severity of the offense, jurisdiction, and local laws.

1. **Hacking:**
    1. Unauthorized access to computer systems or networks.
    2. Punishment: Imprisonment, fines, or both, depending on the extent of damage and unauthorized access.
2. **Phishing:**
    1. Fraudulent attempts to obtain sensitive information (such as passwords or credit card details) by posing as a trustworthy entity.
    2. Punishment: Imprisonment, fines, or both, based on the amount of money involved and the victims affected.
3. **Identity Theft:**
    1. Stealing someone's personal information to commit fraud or other crimes.
    2. Punishment: Imprisonment, fines, or both, depending on the scale of the crime and financial losses incurred by the victim.

4. **Distributed Denial of Service (DDoS) Attacks:**
    1. Overwhelming a target's server or network with a flood of traffic, rendering it inaccessible.
    2. Punishment: Imprisonment and substantial fines, especially if the attack causes significant disruption.
5. **Cyberbullying:**
    1. Harassment, threats, or intimidation using digital communication tools.
    2. Punishment: Varies, but can include fines, community service, or even imprisonment for severe cases.
6. **Online Fraud:**
    1. Deceptive practices with the intent to secure financial gain through online transactions or activities.
    2. Punishment: Imprisonment, fines, or both, depending on the extent of the fraud and financial losses incurred.

7. **Child Exploitation and Pornography:**
    1. Producing, distributing, or possessing explicit content involving minors.
    2. Punishment: Severe penalties, including lengthy imprisonment, fines, and mandatory registration as a offender.
8. **Data Breach:**
    1. Unauthorized access, acquisition, or disclosure of sensitive data, often leading to its misuse.
    2. Punishment: Fines, penalties, and potential lawsuits, depending on the data protection laws in place.

Legal Framework Cyber Crimes against Individuals

1. **Identity Theft:**
    1. **Legal Framework:** IT Act, IPC
    2. **Penalties:** Imprisonment, fines

2. **Online Harassment (Cyberbullying):**
    1. **Legal Framework:** Anti-cyberbullying laws, IPC
    2. **Penalties:** Fines, restraining orders, imprisonment
3. **Phishing:**
    1. **Legal Framework:** IT Act, IPC
    2. **Penalties:** Imprisonment, fines

4. **Cyberstalking:**
    1. **Legal Framework:** IT Act, IPC
    2. **Penalties:** Imprisonment, fines

5. **Revenge Porn:**
    1. **Legal Framework:** Specific laws against revenge porn
    2. **Penalties:** Fines, imprisonment

6. **Cyber Extortion:**
    1. **Legal Framework:** Extortion laws
    2. **Penalties:** Imprisonment, fines

7. **Cyber Trespassing:**
    1. **Legal Framework:** IT Act, IPC
    2. **Penalties:** Imprisonment, fines

8. **Financial Fraud and Online Scams:**
    1. **Legal Framework:** Fraud laws
    2. **Penalties:** Vary based on fraud extent

9. **Online Defamation:**
    1. **Legal Framework:** Defamation laws (online specific)
    2. **Penalties:** Fines, imprisonment

10. **Child Online Exploitation:**
    1. **Legal Framework:** Strict laws, international treaties
    2. **Penalties:** Imprisonment, fines, sex offender registration

Institution and State

1.National Cybersecurity Agency:

- **Role:** Coordinates national cybersecurity efforts, develops strategies, and responds to cyber threats.
- **Example:** CERT (Computer Emergency Response Team) in India.

2.Law Enforcement Agencies:

- **Role:** Investigate cyber crimes, apprehend offenders, and ensure legal actions are taken.
- **Example:** Cyber Crime Units in police departments, INTERPOL at the international level.

3.Legislative Framework:

- **Role:** Enacts and updates laws related to cyber crimes, defining offenses and punishments.
- **Example:** Information Technology Act, 2000 in India, and similar acts in other countries.

4.Judicial System:

- **Role:** Adjudicates cyber crime cases, ensuring justice and appropriate punishment for offenders.
- **Example:** Cyber crime cases heard in regular courts, with specialized cyber crime benches in some countries.

5.International Collaboration:

- **Role:** Facilitates cooperation between countries to combat cross-border cyber crimes.
- **Example:** Bilateral agreements, international treaties, and collaboration with organizations like INTERPOL and Europol.

Hacking

Hacking is the unauthorized access, manipulation, or control of computer systems, networks, or digital devices. It involves exploiting security vulnerabilities to gain access to data, disrupt operations, or perform malicious activities.

The unofficial yet interesting full form of HACKER is H-Hide IP, A- Aim Victim, C-Crack Encrypt, K- Kill Firewall, E- Enter System, and R- Return Anonymous.

Types of hackers

Black Hat Hackers: Malicious hackers who exploit systems for personal gain, causing harm or stealing sensitive data. Black hat hackers use their knowledge and skill for their own personal gains probably by hurting others. As the name suggests, these types of hackers try to gain unauthorized access to security systems and data systems with the intent to cause harm. Their objective can be stealing sensitive information (which they can sell illegally), halt the operations process of a firm, damage the system permanently, etc. All of this is an illegal and punishable offense.

- **White Hat Hackers:** Ethical hackers employed to identify and fix security vulnerabilities, enhancing system defenses. It works for defensive purpose. These are the "Ethical Hackers" who attempt to hack into a system for the benefit and security of the system. This type of hacking is legal and is used by individuals, big and small firms, and even the government to test their systems, find any weakness and fix it. White Hat hackers work with the mentality of the malicious hackers but with good intention. They employ different methods to breach the security walls via vulnerability assessments, penetration testing, etc. The system owners often employ these hackers.

- **Grey Hat Hackers:** Hackers who operate between ethical and malicious hacking, sometimes breaking laws but without malicious intent. These are individuals who work both offensively and defensively at various times. Sometimes they use their skills for the common good while in some other times he uses them for their personal gain. These types of hackers are somewhere in the middle of the White Hat and the Black Hat hackers. That is because these hackers exploit the weaknesses of a system without the owner's permission, but it is not done with any malicious intent. These hackers do this for their fun or to learn to hack, but once they are successful, they usually inform the owner about the weak point.

Types of hacking

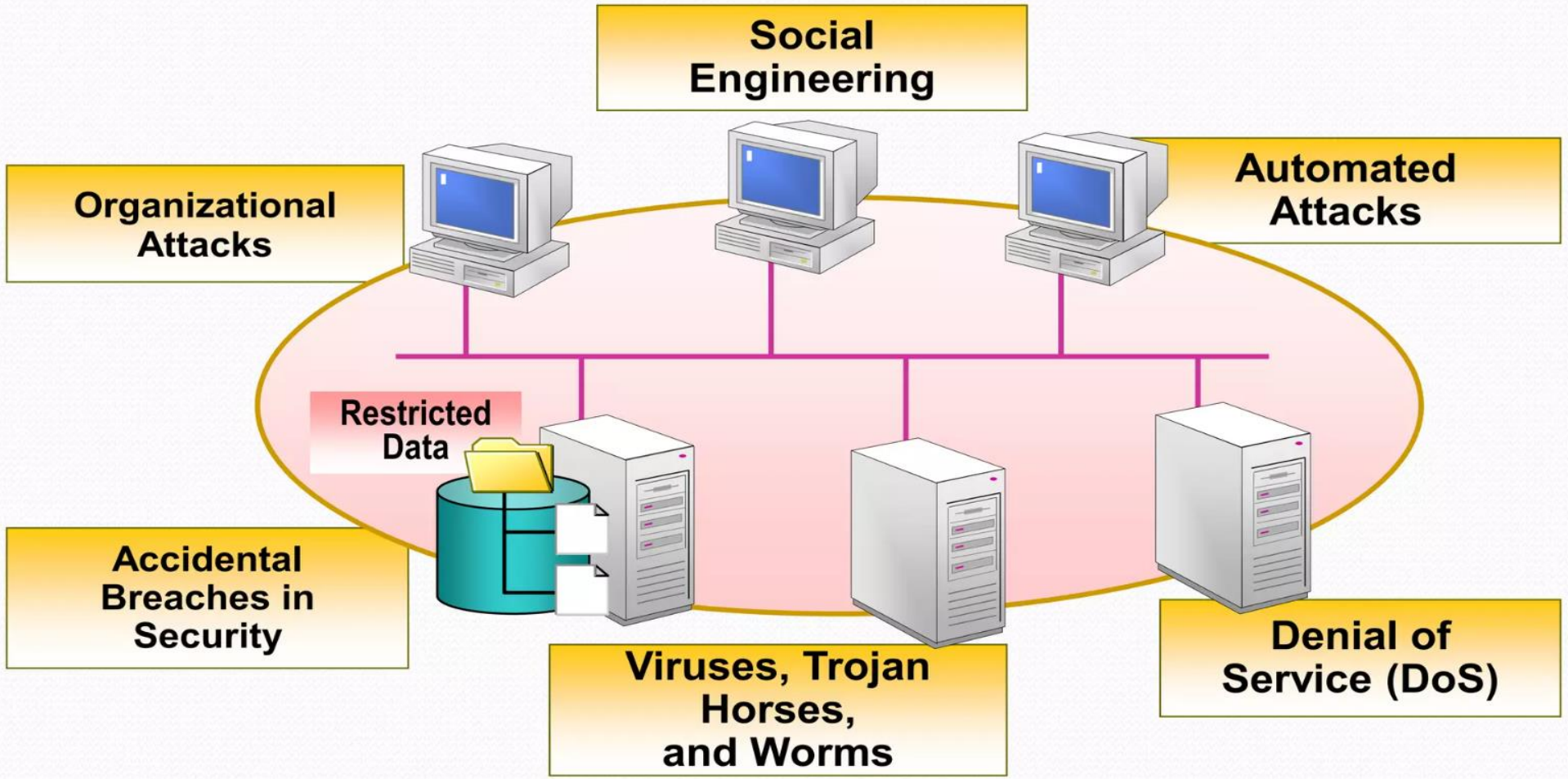
- Website Hacking: Hacking a website means taking control from the website owner to a person who hacks the website.
- Net Hacking: It is generally means gathering information about domain by using tools like telnet, Ns lookup, Ping, Netstat…
- Password Hacking: Password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- Online banking Hacking:
- Ethical Hacking: It is where a person hacks to find weaknesses in a system and then usually patches them.
- Email Hacking: It is illicit access to an email account or email correspondence
- Computer Hacking: It is when files on your computer are viewed, created or edited without your authorization.

Hacking Process

- Foot Printing:
  - Whois lookup: allows you to trace the ownership and tenure of a domain name.
  - NS lookup: nslookup is a network administration command-line tool for querying the Domain Name System to obtain the mapping between domain name and IP address
  - IP lookup
- Scanning
  - Port Scanning
  - Network Scanning
  - Finger Printing:- scanning network traffic and outgoing packets from target systems or launching custom packets toward the target network.
  - Fire Walking:- a technique used to determine which ports are open or closed on a remote host or network.
- Gaining Access
  - Password Attacks
  - Social Engineering
  - Viruses
- Maintaining Access
  - OS backdoors:- Attackers, who choose to remain undetected, remove evidence of their entry and use a backdoor or a Trojan to gain repeat access. They can also install rootkits at the kernel level to gain super user access.
  - Trojans
- Clearing Tracks

Why do you need Ethical hacking

Protection from possible External Attacks



Tools and Techniques Used in Ethical Hacking

Ethical hackers rely on a wide range of tools and techniques to perform effective security assessments. Here are some commonly used tools:

- **Metasploit Framework:** A robust framework for the development, testing, and implementation of exploits.
- **Nessus:** A widely used vulnerability scanner that helps identify weaknesses in systems and networks.
- **Wireshark:** Wireshark is an instrument utilized to intercept and inspect network data, which aids in the comprehension and analysis of network activity.
- **Burp Suite:** A comprehensive web application testing tool for identifying vulnerabilities in web applications.
- **Nmap:** A versatile network scanning tool used to discover hosts and services on a network.
- **John the Ripper:** John the Ripper is a tool employed for password cracking to assess the robustness of passwords.
- **OWASP Zap:** An open-source web application security scanner for finding vulnerabilities.

What Skills and Certifications should an Ethical Hacker obtain?

Some of the common skills that are required to become an ethical hacker include -

- Programming Knowledge that is required while working in the field of network security.
- Scripting knowledge to identify and deal with attacks.
- Network skills, as most malicious hacking attacks are aimed at the network. Proper knowledge of computer networking is required to help find the flaws in the system.
- Basic knowledge of operating systems such as Windows, macOS, Linux, etc.
- Up-to-date knowledge of new hacking methods, tools available, hacking patterns, etc

Ethical Hacking Benefits

Ethical hacking has benefits that help identify and curb any malicious attacks to steal data, cause issues for an individual or a business, bring national security at risk, etc. Some of the most important benefits are -

1. The creation of a secure network is the first step in ensuring low liability. Therefore, ethical hackers also help create a safe network from security breaches.
2. In terms of national security, ethical hacking plays a significant role. Intercepting information regarding digital terrorist attacks, protecting data from malicious hackers, and defending the national systems from security breaches are all some of the common ways in which ethical hacking is beneficial.
3. Ethical hacking reinforces the digital structure of the concerned organization. It discerns and identifies the underlying loopholes and ensures to take necessary measures to avoid compromises in security.

Limitations of Ethical Hacking

Some of the common limitations of ethical hacking include -

1. The process of ethical hacking, if not done carefully, can damage the internal systems and files or even erase data.
2. Even though ethical hackers are often made to sign contracts before they begin working, the information they see during their work may be used for personal gain or malicious use.
3. As ethical hackers will have access to the firm's systems and network, it can raise a question of employee privacy and the privacy of client data.

Ethical Hacking in Action: Real-World Examples

Ethical hacking has played a crucial role in securing organizations and preventing cyber attacks. Let's explore a few notable examples:

- **Bug Bounty Programs**

  Many companies, including tech giants like Google, Facebook, and Microsoft, run bug bounty programs. These programs invite ethical hackers to identify vulnerabilities in their systems and reward them for responsibly disclosing the findings. Bug bounty programs have helped companies identify and fix critical security flaws, ensuring the protection of user data.

- **Penetration Testing for Financial Institutions**

  Financial institutions regularly conduct penetration tests to assess their security posture and ensure compliance with industry regulations. Ethical hackers simulate real-world attacks to identify vulnerabilities in banking systems, payment gateways, and other financial infrastructure, enabling organizations to proactively strengthen their defenses.

- **IoT Security Assessments**

  With the proliferation of Internet of Things (IoT) devices, securing these interconnected systems has become critical. Ethical hackers perform security assessments on IoT devices and systems, uncovering vulnerabilities that could potentially be exploited to gain unauthorized access or disrupt critical infrastructure.

Summary

Ethical hacking is a crucial discipline in the field of cybersecurity. By leveraging ethical hacking methodologies, individuals and organizations can identify and address vulnerabilities, strengthen their defenses, and protect sensitive information from malicious threats. With a proactive approach and a commitment to continuous learning, ethical hackers contribute significantly to the resilience of our digital world. Remember, ethical hacking is not about exploiting vulnerabilities for personal gain but about fortifying our digital infrastructure to ensure a safer and more secure cyberspace.

Digital Forgery

- Forgery is the creation of a document which one knows is not genuine and yet projects the same as if it is genuine. In common parlance, it is used more in terms of affixing somebody else's signature on a document.
- Digital forgery implies making use of digital technology to forge a document, desktop publishing systems, color laser and ink-jet printers, color copiers, and images canners enable crooks to make fakes, with relative ease, of cheques, currency, passports, visas, birth certificates, ID cards, etc.

Digital Forgery

Digital forgery refers to the creation, alteration, or manipulation of digital content, such as images, videos, documents, or audio recordings, with the intent to deceive, mislead, or defraud others.

COMMON TECHNIQUES

- **Photo Manipulation:** Altering images to create false impressions or fake scenarios.
- **Deepfake Technology:** Using artificial intelligence to create realistic fake videos or audio recordings of real people.
- **Document Forgery:** Falsifying digital documents, signatures, or timestamps to create counterfeit records.
- **Metadata Manipulation:** Editing metadata (information about the file) to misrepresent the origin or creation time of digital files.

Indian Law- Section 463- 476

- Section 91 of the IT Act (read with the Second Schedule) amended the provisions of the IPC in relation to **forgery** to include **electronic records** as well. Section 29A has been inserted in the Indian Penal Code to provide for a definition of . The words electronic record will have the same meaning which is assigned to it in section 2(1)(t)2 of the IT Act. Section 464 of the IPC was amended by section 91 of the IT Act to include a false electronic record. Under section 464, a person is said to make a false electronic record:

A) Who dishonestly or fraudulently makes or transmits any electronic record or part of any electronic record, or, affixes any digital signature on any the electronic record, or, makes any mark denoting the authenticity of the digital signature, with the intention of causing it to be believed that such electronic record or part of an electronic record or digital signature was made, executed, transmitted, or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, executed or affixed; or

B) Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters an electronic record in any material part thereof, after it has been made, executed, or affixed with a digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

C) Who dishonestly or fraudulently causes any person to sign, execute or alter an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practiced upon him, he does not know the contents of the electronic record or the nature of the alteration.

- Section 463 of the IPC, after amendment, defines forgery, in relation to electronic records, as the making of any false electronic record or part thereof with intent to cause damage or injury to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed.
- Section 464. Making a false document.
- Section 465. Punishment for forgery :- Whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.
- Section 466 (forgery of record of Court or of Public register, etc.),
- Section 467 (forgery of valuable security, will, etc.),
- section 468 (forgery for purpose of cheating),
- section 469 (forger for purpose of harming reputation),
- section 470 (forged document or electronic record),
- section 471 (using as genuine a forged document),
- section 472. Making or possessing counterfeit seal, etc., with intent to commit forgery punishable under section 467.
- section474 (having possession of the document described in section 466 or 467, knowing it to be forged and intending to use it as genuine) and
- section 476 (counterfeiting device or mark used for authenticating documents other than those described in section 467, or possessing counterfeit marked material) have also been suitably amended to **include electronic records**.

THANK YOU