Cyber crime and safety

Presented by – Rajnish Mishra
Manager Systems
SECL HQ

Introduction to Cybercrime

- Cybercrime may be defined as "Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime". Examples include hacking, identity theft, fraud, and cyberstalking.
- As the internet and its associated advantages grew in popularity, so did the notion of cybercrime.
- Cybercrime **targets** can be individuals, businesses, governments, and other organizations. Anyone who uses the internet, computer systems, or other digital devices is vulnerable to cybercrime.
- While anyone can be a target of cybercrime, women and children can be particularly vulnerable.

Major reasons for Cybercrime

- **Financial gain:** through stealing financial information, such as credit card numbers and bank accounts, or through demanding ransom in exchange for stolen data or resources.
- **Espionage:** Some cyber criminals engage in cyber crime to steal confidential or proprietary information for competitive advantage or to *damage the reputation* of an organization.
- **Political or ideological motives:** Some cyber criminals target organizations or individuals for political or ideological reasons, such as to promote a particular cause or to advance a particular agenda.(e.g. ISIS targets military websites, Govt websites for spreading hate and propaganda).
- **Personal motives:** Some cyber criminals engage in cyber crime to harass, defame or harm individuals or organizations.
- **Opportunism:** Some cyber criminals engage in cyber crime simply because they can, taking advantage of security vulnerabilities in technology or in people to steal information or resources.
- **Lack of Awareness:** Many cyber crimes are committed by individuals who are unaware of the consequences of their actions and the legality of their activities.

Types of cyber crime

Social Media Platforms & Financial Frauds

- Cyber Bullying– A form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone, laptop, etc. (impacts mental health, academic performance, social isolation)
- Cyber Stalking- use of electronic communication by a person to follow a person, or attempts to contact a person to foster personal interaction repeatedly despite a clear indication of disinterest by such person
- Cyber Grooming- Cyber Grooming is when a person builds an online relationship with a young person and tricks or pressures him/ her into doing sexual act.
- Sexting- Sexting is an act of sending sexually explicit digital images, videos, text messages, or emails, usually by cell phone.
- SIM Swap SCAM: occurs when fraudsters manage to get a new SIM card issued against a registered mobile number fraudulently through the mobile service provider.
- Spamming: occurs when someone receives an unsolicited commercial messages sent via email, SMS, MMS and any other similar electronic messaging media.
- Credit/Debit Card Fraud:Credit card (or debit card) fraud involves an unauthorized use of another's credit or debit card information for the purpose of purchases or withdrawing funds from it.
- Impersonation and identity theft: It is an act of fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any other person.

HOW DOES IDENTITY THEFT OCCUR?

VISHING

FRAUDSTERS MAY CALL YOU ON THE PHONE, CLAIMING TO BE FROM A BANK OR ASKING FOR MONEY.

PHISHING

SCAMMER MAY SEND DECEPTIVE MALICIOUS E-MAILS TO STEAL YOUR CREDENTIALS

CLONING

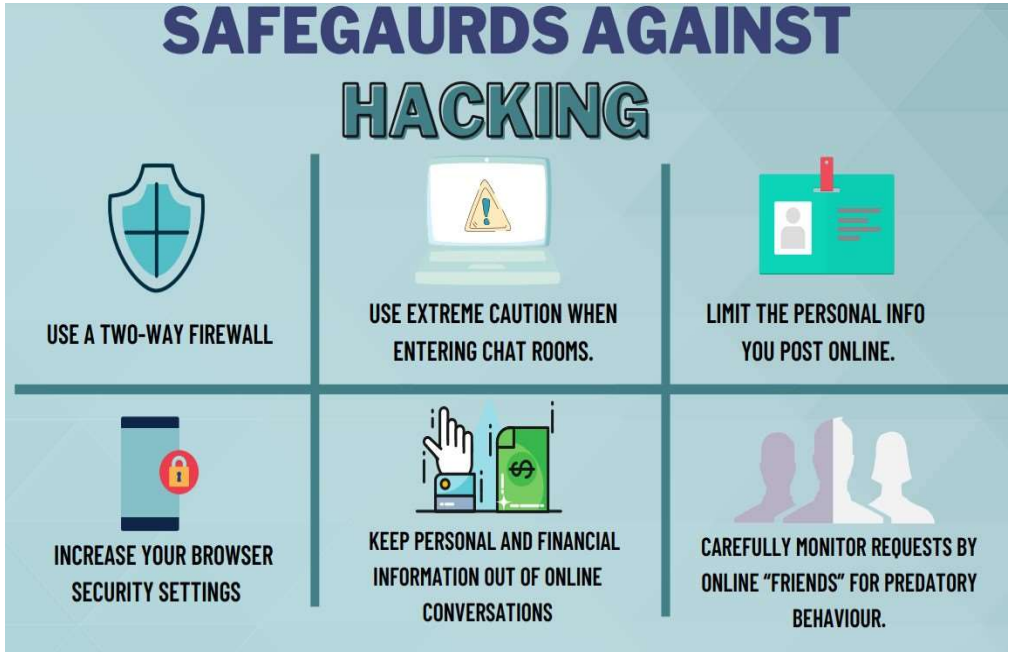
OFFENDERS CAN CLONE YOUR CREDIT/DEBIT CARD INFORMATION

Organisation/Business/Nation targeting cyber crimes

- **Ransomware** is a type of computer malware that encrypts the files, storage media on communication devices like desktops, Laptops, Mobile phones etc., holding data/information as a hostage.
- **Pharming** is cyber-attack aiming to redirect a website's traffic to another, bogus website.
- **Cyber-Squatting** is an act of registering, trafficking in, or using a domain name with an intent to profit from the goodwill of a trademark belonging to someone else.
- **Website Defacement** is an attack intended to change visual appearance of a website and/ or make it dysfunctional. The attacker may post indecent, hostile and obscene images, messages, videos, etc.
- A Distributed Denial of Service **(DDoS) attack** is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
- **Data breaches**: unauthorized access to and theft of sensitive information such as personal and financial data.
- **Salami Slicing Attack** : steal money or resources a tiny bit at a time, so they do not do noticeable difference to the bank account.

Hacking

- This term refers to the crime of unauthorized access to private computers or networks and misuse of it either by shutting it down or tampering with the data stored or other illegal approaches
- Anyone who uses a computer connected to the internet is susceptible to the threats that computer hackers and online predators pose.



Sexting

- Sending sexual photographs of yourself or someone else is illegal. Sending or receiving sexual photographs of anyone is illegal. This is very serious, and you can be charged with crimes related to transmitting pornography.
- It is pertinent to note that the victim can be a male or female and the law punishes anyone who publishes without consent under the information technology Act, 2000 (IT Act)
- Sexting a minor under 18 years of age would also be offence under the Protection of Children from Sexual Offences Act, 2012 (POCSO).

Monetary scams

LOOK OUT FOR THESE SIGNS TO SAFEGUARD YOURSELF FROM MONETARY SCAMS!

BEWARE OF ADS THAT DISPLAY MESSAGES LIKE "LOAN APPROVAL GUARANTEED".

BEWARE OF "NO CREDIT CHECK REQUIRED" MESSAGES. A CREDIBLE FINANCIAL INSTITUTION WILL WANT TO KNOW WHETHER YOU CAN PAY THE LOAN BACK OR NOT.

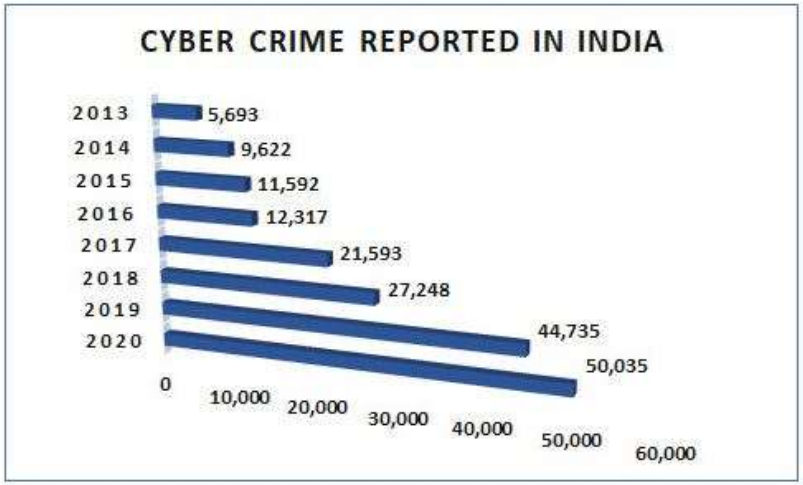
IF THE WEBSITE OF THE LENDER DOESN'T HAVE AN 'S' AFTER THE 'HTTP', THAT'S A RED FLAG. YOU MIGHT BECOME VULNERABLE TO PHISHING.

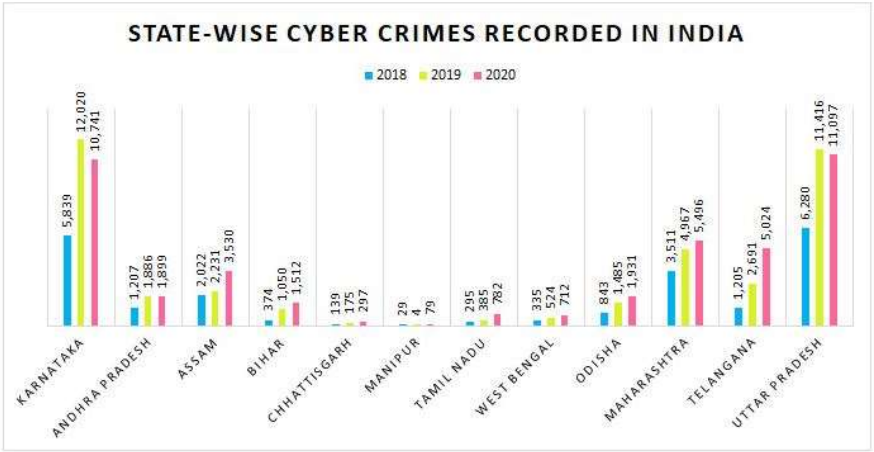
ANY LOAN THAT DEMANDS MONEY BEFOREHAND FOR "INSURANCE" OR "PROCESSING" IS NOT CREDIBLE.

FRAUD LENDERS CALL, SEND MESSAGES AND EMAILS TO PEOPLE IN NEED OF URGENT MONETARY HELP. THESE INTERACTIONS ARE MOST OFTEN, SCAMS.

Warning signs of online loan fraud

Cyber Threat Report of 2020: 69% of Firms Face Serious Cyber Attacks in India!





Recent cyber attacks in India

- Malware(Dtrack) attack on Kudankulam Nuclear Power Plant (KKNPP) 20 oct 2019, by North Korean hacker group- “Lazarus” to get information on thorium-based reactors.
- Cyber-attack on Union Bank of India – july 2017 through a central bank forged email attachment (malware) to get SWIFT codes access and transferred $170 million.
- Facebook database leak data of 419 million users: Insecure database allowed the hackers to access the phone numbers, user‘s name, gender, and location of around 419 million users including the data of many Indian users. Cambridge Analytica scandal (2018)
- Cosmos Cooperative Bank Cyber Attack in Pune (2018):Hackers hacked into the bank‘s ATM server and took details of many visas and rupee debit cardholders and siphoned off Rs. 94.42 crore.
- UIDAI Aadhaar Software Hacked: In 2018, UIDAI revealed that around 210 Indian Government websites had leaked Aadhaar details of people online, a massive data breach of personal records of 1.1 Billion Indians.
- Cyber attack on Indian Healthcare websites: In Dec-2022,**5 AIIMS Servers Hacked, 1.3 TB Data Encrypted in Recent Cyberattack, Govt Tells Rajya Sabha(**records of nearly 3-4 crore patients, including high-profile politicians, were compromised)
- WannaCry ransomware attack (2017) , Equifax data breach (2017) etc

Who are cyber criminals ?

- Cyber crime can be committed by a variety of individuals and organizations, including: Individual hackers , Organized criminal gangs, Nation-states(confidential information, military, election purpose).
- Insider threats: Some cyber crimes are committed by employees, contractors, or other insiders who have authorized access to systems and resources but abuse that access for personal gain or to harm the organization.
- Cyber criminals who hire others: Some cyber criminals may hire others to commit cyber crimes, such as hackers-for-hire, who can carry out cyber attacks on behalf of others.

Modus Operandi of cyber criminals

- Dissemination of Malware through google forms , software downloads etc.
- Social engineering :use of psychological tactics to trick individuals into revealing confidential information .
- Remote Access: exploiting vulnerabilities in software or hardware, IoT devices, tricking a user into providing remote access for tech support.
- SQL Injection: technique used to exploit vulnerabilities in databases to steal or manipulate information.
- Cross-Site Scripting (XSS): type of security vulnerability that allows attackers to inject malicious code into websites.
- Man-in-the-Middle attacks: attacker intercepts and potentially modifies communication between two parties.

Legal remedies for Cyber Crime in India

- IT Act 2000: This act defines and provides punishment for various cyber crimes like hacking, identity theft, cyberstalking, etc.
- Criminal Complaint: A victim can file a complaint with the local police under IPC.
- Civil Suits: A victim can also file a civil suit for damages under the IT Act 2000, or for compensation under the IPC.
- The government has set up a National Cyber Crime Reporting Portal for reporting and registering cyber crime cases.
- Cyber Appellate Tribunal: The IT Act 2000 provides for the establishment of a Cyber Appellate Tribunal to hear appeals against the decisions of the adjudicating officer.

Safety mechanisms to avoid cyber attack

- Antivirus and firewall software: using antivirus and firewall software to protect against malicious software and unauthorized access.
- Regular software updates: keeping all software, including the operating system, up-to-date to ensure the latest security patches are installed.
- Strong passwords: using unique and complex passwords for each online account.
- Multi-factor authentication: using additional methods of authentication such as a security token or biometrics to verify identity.
- Wi-Fi in public places should be disregarded - When utilizing public Wi-Fi, never make online payments, email personal information, or introduce crucial account passwords.
- Unsolicited emails and SMS communications should be avoided - Never click on a link, picture, or video sent to you by an unknown source.
- Check for spelling errors, bad language, unusual phrasing, and urgent requests for money or action to ensure that emails are authentic . Malicious websites may appear to be identical to legal sites, however the URL is frequently misspelt or uses a different domain.
- Protect personal information on social media – Cyber criminals utilize social media to gather personal information that they may subsequently exploit in phishing schemes.
- Don’t use charging/adapter cables from strangers

Safety mechanisms to avoid cyber attack

- Limit physical access to critical information by turning off your computer while you're not using it. To keep private data safe, lock mobile devices and encrypt confidential data. Limit who in your workplace has access to certain network drives.
- Phones and other mobile devices should never be left unattended and visible.
- Awareness and education: staying informed about the latest cyber threats and educating oneself and others about safe online practices.
- Regular backups: regularly backing up important data to minimize the impact of a data breach or ransomware attack.
- Do not amass a collection of computers or digital data- Keep digital data organized and up to date, and delete files on a regular basis.
- Dispose of old or unneeded computer hard drives in a secure manner at your office.

Avoid searching for customer care numbers on google, as they can be misleading

Never believe the gift offers messages or emails circulated which are usually used as bait by cyber fraudsters

Never share your personal details or financial information like login credentials/passwords/cre dit or debit card details

Never click on unknown links or download unauthorized apps or software on your digital device s as it can install malicious software on your device.

Install anti-virus on your digital devices for security and protection.

Only visit authorized/legitimate company/organization website for valid information

Immediately block the number and report against such fake offers

Do not forward fake messages, links, or mails to people as prompted by senders without proper verification or authentication.

Be aware and alert about such attempts of cybercriminals by keeping track of the latest news and updates on the activities of cyber fraudsters.

Secure your digital payments

HOW TO SECURE DIGITAL PAYMENTS?

DON'T USE OPEN PUBLIC WIFI FOR DIGITAL PAYMENTS.

CHANGE THE PIN REGULARLY.

REVIEW ACCOUNT STATEMENTS FREQUENTLY TO CHECK FOR ANY UNAUTHORIZED TRANSACTIONS.

DON'T SHARE YOUR E-WALLET LOGIN DETAILS AND ONE TIME PASSWORD WITH STRANGERS

BE MINDFUL OF WHAT YOU INSTALL ON YOUR PHONE FOR EG. THIRD PARTY APPS

REPORT A LOST OR STOLEN DEVICE IMMEDIATELY

CHOOSE A STRONG PASSWORD I.E. ALPHA NUMERIC COMBINED WITH SPECIAL CHARACTERS TO KEEP YOUR ACCOUNT AND DATA SAFE

MAKE SURE YOU HAVE TWO FACTOR AUTHENTICATION BEFORE A PURCHASE VIA ONLINE MEANS.

Government initiatives to fight against Cybercrime

- Cyber Crime Investigation Cell (CCIC): responsible for investigating cybercrime cases and providing technical support to other law enforcement agencies.
- National Cyber Coordination Centre (NCCC: central hub for coordinating and sharing information related to cyber security between various agencies and organizations.
- National Cyber Security Policy:2013, outlines the government's strategy for protecting the country's critical information infrastructure and securing the cyberspace in India.
- CERT-In: national nodal agency for responding to cyber security threats and incidents in the country. It also provides alerts, advisories, and guidelines for securing IT systems and networks.
- National Critical Information Infrastructure Protection Centre (NCIIPC): responsible for protecting the country's critical information infrastructure, including power grids, financial systems, and government networks, from cyber threats.
- Awareness campaigns: The government regularly conducts awareness campaigns and training programs.

Thank you