CYBERCRIMES AND CYBER HYGIENE

Awareness for netizens

AMIT DUA   AKASH JYOTI SAHOO   NISHEETH DIXIT

©Cybercrimes & Cyber hygiene
Amit Dua, Akash Jyoti Sahoo & Nisheeth Dixit
1st Edition
All rights reserved
Publication Date: April 2022
Price: 520 $ 6.82
ISBN: *978-93-91374-01-3*
Published by:
Adhyyan Books
Office No. 125,
Opposite Vivanta by Taj,
DDA SFS. Pocket-1, Dwarka,
Sec-22, New Delhi-110077
Website: http://adhyyanbooks.com
E-mail: contact@adhyyanbooks.com

Every effort has been made to avoid errors or omissions in this publication. In spite of this, errors may creep in. Any mistake, error or discrepancy noted may be brought to our notice which shall be taken care of in the next edition. It is notified that neither the publisher nor the author or seller will be taken responsible for any damage or loss of action to any one, of any kind, in any manner, therefrom. It is suggested that to avoid any doubt the reader should cross-check all the facts, law and contents of the publication with original Government publication or notifications.

For binding mistake, misprints or for missing pages, etc., the publisher's liability is limited to replacement within one month of purchase by similar edition. All expenses in this connection are to be borne by the purchaser. All disputes are subject to Delhi jurisdiction only.

Printed at: Repro Printers, Delhi

Disclaimer

Nothing contained in this book is to be considered as rendering of legal and or technical opinion(s) and readers are responsible for obtaining such advice from their own legal / technical experts. The book and the material enclosed within are intended for educational and informational purposes only and are based on media reports. Before relying on the materials of the book, one should verify the same with other available resources and the authors are in no way responsible for any sort of damage.

Any information or discussion that resembles anyone is pure coincidence and is not meant to replicate the same for any unlawful purpose.

Contents

About the Book

What should I do if I get hacked? What are the different types of scams I can face online? What should I do to prevent myself from getting scammed? This book answers all the questions one might have with regard to cybercrime and presents them in an easy to read fashion. The book educates the readers about the psychology of criminals and the general mindset of potential victims of cybercrimes. The major portion of the book covers the discussion about different types of cybercrime cases and the steps one can take to prevent further loss from the crime. By the end of the book, the reader will have a proper understanding of the different types of cybercrimes and cybercrime laws and will be equipped with methods and techniques to safeguard their presence online.

About the Author

Dr. Amit Dua is an Assistant Professor in the Computer Science department at Birla Institute of Technology and Science Pilani (Pilani Campus). Amit has over 10 years of research and teaching experience and has taught cyber forensics and incident handling to the masters' students of BITS Pilani. He has worked actively in solving the practical problems for e-waste management, smart grid, health care, security and transportation systems using technology. He is the co-founder and CEO of Yushu Excellence Technologies Pvt. Limited. He has published over 50 International Journal and Conference publications and has filed an Indian patent to enhance cyber security.

Akash Jyoti Sahoo is a Computer Science student pursuing his Bachelor’s of Engineering degree from Birla

Institute of Technology and Science Pilani (Pilani Campus). He has worked on projects involving the creation of secure crypto wallets and other mobile applications. He is passionate about cybersecurity and Blockchain technology and is actively trying to solve real-life problems using them.

Nisheeth Dixit is a renowned practicing Advocate since 2001, handling constitutional, civil and criminal matters, specialized in Cyber Laws, Information Security and Cyber Forensics. He is also founder of NDCyberLaw (ndcyberlaw.com). He has represented multiple corporate clients including Aviation,Telecom, Real - estate, Banking and other IT companies. He also provides training on cybercrimes, cyber laws and admissibility of electronic evidence to judicial, prosecution and police officers at various Judicial, Police academies and cyber cells throughout the country.

Foreword

As the digital revolution is transforming the lives of people, cyber-attacks are getting more sophisticated and undetected. With almost everyone having access to the internet, ensuring cyber safety and security has become a great challenge unless people are informed how to protect themselves. This book closes that knowledge gap by informing readers on technological and security aspects of cyber risks with practical examples and also providing tools to safeguard against cybercrimes. I congratulate Dr. Amit Dua, Sh. Akash Jyoti Sahoo and Sh. Nisheeth Dixit for their effort towards increasing cyber literacy.

Keshni Anand Arora
IAS (Retd), Ex Chief Secretary, Haryana

Introduction

"For every lock, there is someone out there trying to pick it or break it"

- David Berstein

India is the second largest country in the world in terms of internet users right after China with over 600 million internet users. With the ongoing research and rapid development in the field of internet technology, the speed of internet and the internet bandwidth has increased incredibly, but at the same time the price of technology has been lowered immensely. Thus, making technology more affordable and available to more people in the world.

Today's world is powered by the internet and technology. The Indian economy is also marching towards the E-way.

Indians are using the internet now for everything - shopping, banking, gaming and a lot more. Even during the COVID-19 pandemic where all the people were forced to live inside their houses, learning and teaching continued through online classes. We have become entirely dependent on the internet for our daily needs. What originally started as a means to communicate with people has now turned into a necessity in everyone's day to day lives.

In India, the internet boom began with the introduction to smartphones and cheap 4G internet services. This has enabled internet connectivity to reach different parts of the country. Thus, the internet has reached a big user base and is still increasing its user base everyday. Along with the speed with which the internet is growing, cybercrimes are also growing in proportion to the usage. Cyber attacks have increased exponentially over the last decade, exposing sensitive personal and business information, disrupting all critical operations and imposing high costs on the economy. Hence, there is a growing need to invest in the cyber infrastructure of the country.

Given the security problems, there is an increased emphasis on investment in the security of the cyber infrastructure. Core internet protocols are insecure, and an explosion in the number of mobile devices based on the same insecure systems adds up to the problem because the users are vulnerable. This is adding up to the increased usage of the internet in more vulnerable cyberspaces.

When we talk of cyberspace, we refer to the space that comprises the IT network, computer resources, and all the fixed mobile devices connected to the global internet. A nation's cyberspace is part of the global cyberspace. It cannot be isolated to define its political boundaries, since cyberspace is borderless. This is what makes cyberspace a unique space, and this is also what makes it very difficult and challenging to regulate in this medium. Unlike the physical world which is limited by geographical boundaries like land boundaries, sea boundaries, rivers, water, etc, cyberspace cannot be defined in boundaries. It continues to expand. Increased internet penetration is leading to growth in cyberspace, since its size is proportional to the activities that are being carried out in cyberspace. Therefore, nations are investing heavily in their ICT infrastructure with a view to provide higher bandwidth, integrate national economies with the global market and to enable citizens to access more and more E-services.

Inspite of all of this, there are a few challenges that technologies face in cybersecurity.

1. Supply chain interconnection: The supply chains are increasingly interconnected. Companies are urging vendors and customers to join their networks. This makes the company's security wall very thin.

2. Hacking: Hacking means to penetrate into someone's system in an unauthorized way to steal or destroy data. The availability of information online makes it easy for even non technological people to do hacking. There are a lot of tools and softwares available nowadays with the help of which even a layman can hack into systems with ease.

3. Phishing: This is one of the easiest and most common threats performed by people and has very low effort involved. It is the act of sending out fake emails. Even with all the knowledge and information, it is still common to find cyber specialists failing to differentiate between a genuine mail and a mail sent by a cybercriminal.

A lot of popular phishing cases involve income tax returns. People generally do not understand the intricacies of income tax and fall for any mail that has to do with income tax. The attackers here send a link to the refund page and steal the personal information of the victim.

4. Lack of uniformity in devices used for internet access: Not everyone can afford to have an expensive phone which comes with high security norms. In India, most of the internet users use cheap phones which compromises on a lot of security features. This widening gap between the security features of the high end phones and the cheap phones make it almost impossible for legal and technical standards to be set for data protection, especially by the regulators.

5. Lack of awareness: This is the most important challenge to cybersecurity. At the end user level people need to be aware. The government may improve its security standards and national level architecture, companies and organizations may run many awareness campaigns, but if the end user is reckless and careless, unaware of the different scams, then nobody can save them.

The challenges associated with the devices and security will get fixed with time as the government invests in cyber infrastructure and manufacturers make devices which are both affordable to the general public and which does not compromise on user safety. However, the problem of cybercrime still persists. People need a way to safeguard themselves while the different challenges get sorted out. This is why there is a big need to bring about awareness among the people. Awareness is the main key to prevent a person from becoming cyber victimized.

No person on the internet is completely safe and there is no guarantee that a person will never get scammed. If a cyber specialist in Bangalore with all the technological prowess and information can get scammed, anyone can get scammed. What we can do is, we can aim to reduce the number of cyber victims by being aware and by having knowledge of the different tactics employed by cyber criminals to dupe their targets.

This book aims to provide awareness to the reader by providing knowledge about cybercrime and its types, the steps that can be employed to prevent cybercrime and the possible legal actions that one can take. The reader will also be able to understand general human psychology and the reasons why a layman makes mistakes and falls for cybercrime. The book will also touch upon some case studies of popular cybercrimes which have occurred in India. This should help the reader understand the different tactics cybercriminals use to operate and the different ways that could have been used to prevent them. Just like people engage in personal hygiene to maintain their good health, there is also a need to engage in steps routinely to maintain our cyber health. This practice is called cyber hygiene and the book will provide multiple opportunities for the readers to learn about cyber hygiene and the things that he / she should do. Finally there are some example questions at the end of the book which are meant for the reader's practice. These questions will help the readers be aware of their online presence and will serve as a reminder for changing their habits.

We shall now learn about cybercrime and the different cases involved by following the story of Rahul, a 17 year old boy who has just lost all his money in a fake Tata game scam.

Rahul received a whatsapp forward with a link to a lucky draw game. The link was made to celebrate Tata's 100th year anniversary and it mentioned that lucky people would get a chance to win a smartphone. When he opened the link, he was greeted with a page with multiple boxes and instructions on how to play the game. Rahul complied with all the instructions given. The user had to select three boxes and after each time they selected a box, a message would appear on the screen stating if they had won the prize or not. Rahul did not win the prize in the first or second attempt. However at the third attempt, he won the prize and was very excited. The next step to claim the prize was to share the link to atleast 5 whatsapp groups or to 20 contacts. Rahul spammed the link to as many people he knew and told them about the lucky draw as well. Once he had shared the link and satisfied the criteria, he was redirected to a new page where he had to put in his personal details like name, address of delivery, card number etc. Rahul happily filled in the details and was glad with himself. After a few hours, he was notified that a huge transaction had been made from his account. It was empty now.

What happened here?

The link was actually a phishing link. It's main purpose was to trap the users into believing that they would receive a product by playing a simple game. This game was designed in such a way that every user who plays this game would win the lucky prize at the third attempt. When Rahul shared the link to multiple whatsapp groups, he was in fact bringing in a larger number of people to play this game and thus, get trapped as well. What he did not realize is that after getting redirected to the details page, an app was installed into the device which tracked all his keyboard movements. These details were then sent to the perpetrator who used the data to steal his money.

What could he have done here to prevent the crime?

Rahul could have realized that Tata Steel was 181 years old and that it was impossible for the organization to celebrate their 100th anniversary at this time. He should have checked the domain name of the website and realized that it was a fake site. Any website which asks you to do a favour in return for a gift is a scam and people should not fall for these offers. A lot of users are gullible and fall for such whatsapp forwards and hoaxes without thinking.

Cybercrime and its types

“Every case involving cybercrime that I’ve been involved in, I’ve never found a master criminal sitting somewhere in any country. It always ends up that somebody at the company did something they weren’t supposed to do. They read an email, went to a website they weren’t supposed to.“

- Frank Abagnale

Definition of cybercrime

Rahul: “Hi, I got scammed online recently and I heard from my friends that it falls under the category of cybercrime. Can you explain what cybercrime exactly is?”

Me: I am really sorry to hear about that Rahul. Let me explain to you what cybercrime actually is. Cybercrime is basically a criminal activity where the attacker targets a computer or uses the computer as a tool to attack other people, hence stealing their data, money, personal details and other secrets.

Imagine this way: you are currently using your mobile phones and computers to communicate with people all over the world. The medium through which you all are communicating is a virtual one and it is called **cyberspace**. So basically all people in the world have their presence in cyberspace with the help of their mobile phones or computers. Now, there is a section of people in this cyberspace who have malicious goals and they try to harm other people by attacking them online through their profiles, or by stealing their passwords and personal information. These people are called cybercriminals and the act that they are performing is called cybercrime.

Types of Cybercrime

Rahul: "The way I got scammed was through an online "lucky draw" scam. Are there some other ways through which one can get scammed or victimized?"

Me: We have understood what cybercrime means. It is similar to the conventional crimes which are carried out in the physical world, except in this case the medium has changed to cyberspace. Scammers and cybercriminals have multiple ways through which they steal your personal information and money. Some of the ways are:

1. Phishing: In this method, the cybercriminal attempts to trick the user into giving his personal details like bank details, credit card information and other sensitive information through an email. This is the most common form of cyber attack and is also the easiest one to be carried out. To carry out the attack, the criminal fakes an organization's identity and sends out emails to a lot of people. The email usually contains a malicious link which is disguised to be important to the user stating that he/she would need to update his/her credentials or else their account would be blocked. Or basically anything that conveys a sense of emergency to the end user. The user generally fails to understand the difference between a fake and a real email and complies to what is written in the mail. Once the user clicks on the link, he is sent to a fake website where he enters his details, and then gets redirected to the original website. This way the person is unaware that he has been scammed while on the other hand, the cybercriminal gains all your personal information and steals your money with that information.

2. Hacking: The word 'hacker' was earlier used in a positive sense and was meant to refer to people of great technical calibre, people who loved working with gadgets and knew how to solve problems in computers. In the current context this word has gained negativity and is used to refer to cybercriminals who gain unauthorized access into computer systems without the owner/ organization’s permission, thus stealing their personal information and other data.

These people may modify your data and insert malware into the computer through virus infected files, thus corrupting their computers.A lot of tools and resources are available online which makes it easy for even beginners to perform hacking.

3. Smishing: This word is derived from two words : sms and phishing, which indicates what the term might mean. It is similar to phishing, the only difference being that the medium through which the crime is undertaken is different. Phishing was done through emails. Smishing is done through messages sent to your mobile phones. People receive a lot of spam messages in their cell phones with lucrative offers and malicious links. Most of these messages offer to give the user a large amount of money for charity work, or they may be disguised to show money transactions made into your account with a link. These links are often tempting to the end user and hence, they get tricked into opening such links, thus compromising their personal information and bank details to the attacker.

4. Vishing: These are the types of cybercrime which involve phishing using voice calls. The impostors call the customers through telephone calls and pretend that they are bankers or insurance agents and ask the customer details about their secure credentials by telling them their name, age, address, etc to gain their confidence.

In a lot of cases, the impostors trick the customers by telling them that their account is in danger and that they need to urgently tell their details so that the account can be blocked to prevent any further unauthorized transactions. The customers, after hearing this, panic and tell out their details and the impostors gain control of the person’s account and empty it.

You should always remember that banks never ask customers for their details and it is always a fraud call if someone asks you to reveal your personal credentials or your PIN number.

5. Identity theft: Identity theft means to steal a person's personal information to commit fraud. The criminal steals your personal information and then uses that identity to do transactions around the world. So at the time of investigation, your name comes up instead of the criminal. Cyber criminals usually sell this information on the dark web and people pay to get other people’s identity to commit such crimes. Apart from this, a person may fake another person's identity on social media and spread hateful messages and propaganda which are not aligned with the original person's ideals. When a person fakes another person's identity online, he/she is still committing identity theft and can be punished in court.

6. Cyber stalking: Whenever we upload a picture or express ourselves online, we don't really take into account the number of people there are online who can see what we have posted. Initially it may begin with a few people but when your post gets more attention, it reaches more people and it opens up to a whole new audience, who may not really be your friends. Celebrities get trolled online and get a lot of negative and hate comments, but this is not cyberstalking.

Sometimes a person might stalk the another person on every platform - his/her email groups, chats, comment sections in social media like Facebook and Instagram, sending frightening messages and death threats. These people keep sending multiple messages in a day, and terrorize the victim. Sometimes the criminal can have multiple accounts to send messages to the victim. These people may be motivated by anger, revenge or even lust.

The criminal can also monitor the person and blackmail him/her. He might be stalking the person online so that he/she can steal the person's identity at a later point of time.

7. Ransomware attacks: This method is employed by the cybercriminal to gain financial benefit. Ransomwares are malicious softwares which lock the computer system and encrypts all the files in the computer and displays a message demanding a fee which the victim has to pay to get his system running again. This fee is usually in some sort of cryptocurrency. The cybercriminal can also blackmail the victim by stating that his personal information would be exposed to the public or that all the files will be deleted if he fails to comply with the message.The cybercriminal might also try to sell the victim's personal information to another person in the dark web, thus the identity of the person would be stolen by another person.

This type of software is usually downloaded by the user from deceptive mails or malicious links. The person is unaware that he is downloading software from a malicious link, hence compromising his computer system.

8. Through malware: Malware is a dangerous software which aims to damage the computer and the files present in it. The three main types of malware are viruses, worms and trojan horses. Viruses are spread through malicious files which enter the victim's computer usually because the person has opened a malicious link or through external sources like USB drives. When the person opens the malicious file, the virus becomes active and starts damaging all the important files present in the computer. Worms are similar to viruses, the only difference is that they don't need the user to open any file. As soon as the worms enter the computer, it starts damaging and corrupting important files. Trojans are disguised to be important files while in reality they act just like viruses. These malware affect the computer files and send back details to the propagator of the malware through an email.

9. VOIP: Voice over Internet Protocol is basically a technology that allows you to talk over internet. A lot of cybercriminals use this technology in E-commerce and Banking sites. There may be instances when you order a particular product online, the scammer will call you with a robotic voice telling you that the product is a fraud one and that you will need to call to a number to report the product, When the person calls to the number given it gets transferred to fake call centers who then direct you in such a way that you agree to their terms. Finally they steal your money from your accounts when you have complied with their instructions. This is similar to bank scams where people call you informing that your bank account has a problem and that they have to sort it out. They ask for your pin number and other details. Since the person is worried about his account, he immediately complies with the person's instructions and thus, loses money.

10. Deepfake: This form of cybercrime involves morphing a person's face into a video to make it look like the person is talking. Cybercriminals create morphed videos of a victim's relatives and ask them for financial help. The victim believes the video and rushes to help the person without confirming from the relatives itself if the video is genuine or not.

Deepfakes are created using machine learning algorithms. The person trains a neural network to replicate another person's face from multiple different angles to give an idea about how the person looks. Once the neural network has been trained, it is run over the person which it should replace, thus producing a video which actually never existed. A lot of websites are now available which offer to produce deepfake videos for you for a price. Deepfakes are also used by cybercriminals for revenge porn over women.

11. Web Jacking: In this form of cybercrime, the criminal illegally gets control over a website by taking its domain name. The criminal first creates a fake page of the original website it wants to target. Then the person sends the link of the fake website to the user. When the user visits the website, he is greeted with a message saying "The website abc.com has moved to the following url, click on this button to navigate to the site." The user being unaware that this is a trap, follows the link and then gets redirected to a fake page, where the attacker might ask for sensitive information like name, email, password, card number etc. The user readily gives in without thinking and loses his personal information.

12. Data diddling: Data diddling is a type of cybercrime in which the criminal alters the computer data manually or through some malware or computer virus. This is usually done to get some fraudulent benefit. Once the benefit is obtained, the data is then returned back to the original state so that people are unaware of the changes that have taken place.

The worst thing about this crime is that you do not have to be a well trained IT professional to perform data diddling. It can be performed even by data entry clerks or any random person. For example, tapes and receipts can be altered to obtain some monetary benefits. Once the criminal gets the money, he then restores it to the original state so that the victim is unaware that his data has been manipulated. Another example is where the accounts executive manipulates the data of the employee before entering into the payroll application. Forgery, counterfeiting documents, etc all come under data diddling.

13. Denial of services (DoS): A denial of service attack is a type of cybercrime in which the criminal intentionally tries to shut down a computer network or computer system, making it inaccessible to the authorized users. To carry out DoS attacks, the cybercriminal may flood the network with traffic thus, crashing the victim's computer and rendering it useless. Some other ways by which criminals perform DoS attacks are by exploiting vulnerabilities in the computer system which causes the computer to crash. When the perpetrator targets online websites or other services, then it is known as a Distributed Denial of Services attack (**DDoS attack**).

In 2016, Dyn, a major domain name service provider was hit with a massive DDoS attack which caused major companies and services to temporarily halt their operations, such as AirBnB, CNN, Netflix, PayPal, Spotify, Amazon, Reddit, Github and many more.

14. Drive by download attack: This refers to the types of attacks in which the user downloads a file from the internet without understanding the consequences of the downloads. In these types of downloads, a malware or a spyware also gets downloaded along with the file without the user's consent and compromises the user's computer security features and makes it vulnerable to further attacks.

These types of attacks happen when the user enters an infected site. The hacker exploits the website so that whenever any user enters the site, malware will get installed into the computer of the user. This will then be used to spy on the user or to slow down the user's computer or to share personal information to an email id. A lot of time links are sent to users and are masked to look like they have been sent by close friends and family, but when they are opened, the malware script runs and downloads the malware into the computers.

15. Watering hole attack: In a watering hole attack, the hackers exploit sites which they know are commonly visited by a user, a group of users or even an organization. The hacker guesses by the nature of the organization and their activities, which sites they will visit or which sites they are a regular customer to. They understand that people who frequently visit a site will often have their guards down and may have security flaws. These hackers exploit the site and install malware which will then get downloaded into the user's computer through a drive-by download attack or through a script that automatically installs malware into the computer's system whenever it visits the site. The hacker will then be able to use the user's computer to further his goals by gathering information about the victim.

16. Tailgating: This is a technique which enables unauthorized people to access highly secure and restricted areas in a company or an organization. How this technique works is the attacker follows an authorized person and manipulates him/ her to let the person into the room. For example, an attacker might disguise himself as a delivery agent to the company, with a lot of packages and may ask an authorized person to hold the door while he unloads the packages. This way, the unauthorized person has entered into the compound without any electrical identification or security number.

17. Juice Jacking: This is a type of cybercrime in which the attackers use charging stations as a mode of stealing data from your mobile phones and laptops. Usually people think that phishing mails, malicious websites and hacking are the only ways to get into your computer, and this ignorance is exploited by cybercriminals. The criminals “jack” the USB ports of such stations so that when they get plugged into your device, they steal the data from your device.

The criminals hijack your power supply (the juice) and then install malware into the devices. This could be a tracking software or a virus that records your passwords and PIN codes and then sends them to an email address while the device is charging.

While such cases are rare, it’s better to avoid charging your device in such booths by using a power bank of your own or keep your device charged beforehand while travelling.

18. Business Email Communication scams: This is a type of scam in which an impostor uses an email id which is similar to that of a company which it tries to disguise as. Then the person uses this email address to fool people into believing that the mail address is legitimate and will thus get manipulated into fulfilling the impostor’s agenda.

An attacker hacks into the company’s email account and then impersonates the owner of the real account to defraud it’s company’s staff and members into revealing their passwords and secure credentials and sending money to the attacker’s account. This is a classic example where the victims were fooled into believing that they had received an email from the boss while in reality they had received an email from a hacker.

19. Whaling attack: A whaling attack is a method used by cybercriminals to pretend as a senior member at an organization (possibly the CEO) and then directly targets seniors or other important individuals at an organization, with the aim of stealing money or sensitive information or gaining access to their computer systems for criminal purposes. Whaling is similar to phishing in that it uses methods such as email and website spoofing to trick a target into performing specific actions, such as revealing sensitive data or transferring money.

20. Using Digital voice assistants: Digital voice assistants are really good listeners. In recent times, we have seen cases where cyber criminals have tapped into these devices and listened to what the people at the house are saying. This may be done through a script which converts the audio into text and saves it in the hacker's computer. This way, the hacker will be able to extract sensitive information that has been discussed at the victim's house and then later use it to blackmail the victim or use his audio in a different context to exploit another person.

Your best bet to save yourselves is to turn off your Voice Assistants when you have to discuss something sensitive so that it will not be able to capture your discussions.

Psychology

"Threat is a mirror of security gaps. Cyber-threat is mainly a reflection of our weakness. An accurate vision of digital and behavioral gaps is crucial for consistent cyber-resilience."

- Stephane Nappo

Rahul: Alright! I finally understand the different types of cybercrime. What are the personality traits of a cyber criminal?

Me: We had an interview with Dr Archana, a psychologist to understand why people indulge in cybercrime.

According to Ma'am, the people who are involved in cybercrime usually belong to the **B cluster** of personality spectrum. The people who are associated with this cluster are usually antisocial and risk takers. They often do not have empathy towards other people and have no regrets for their behaviors. People who steal, tell lies, hurt animals, etc., all fall in this cluster. These traits may also change over time if the environment around them supports the change, but the basic nature of the person still remains. Let's say a child belonging to cluster B grows up in a hostile and negative environment where people are always violent and hurting each other, then these types of people start behaving violently by the time they turn 18-19 years and indulge in criminal activities. They are no longer empathetic towards others and do not care if the other person feels any pain.

There may also be other factors because of which a person might resort to cybercrime - like financial issues or because they did not find any other way to resolve their debt and hence, they fell into this path. These type of people may feel guilty and do not necessarily have the antisocial traits that were discussed above, but they were forced into this field because of their circumstances. These are the type of people who fall into anxiety and depression after committing the crime, as opposed to the antisocial type who do not feel any regret after committing the crime.

You may be able to identify such people in your society and get a hunch about the types of activities they are involved in.

Rahul: Why do the cybercriminals partake in such activities?

Me: The cybercriminals are able to indulge in such activities because they are anonymous online. They are able to mask themselves and their IP addresses which makes it difficult to trace them. Besides, cyberspace is borderless and hence, it is difficult to apply laws in case of international attacks.

Along with cybercriminals, the people who fall for them are also to be blamed for their lack of awareness and are a major reason why cybercriminals are successful in being able to dupe people.

Rahul: If we are already aware of the different ways to prevent ourselves from cybercrime, then why do we still fall for them?

Me: The cyber criminals understand general human psychology and take advantage of people's emotions. The criminals know that the people act in a certain manner given a particular situation and take advantage of them.

People need to understand that cybercrime is a two step process. It consists of the cyber criminal and the user. The cyber criminal sends a malicious link through email or through social media with the expectation that the receiver will open the link. Unless the user opens the link, the cybercriminal will not be able to get the access, hence denying him from carrying out the cybercrime. After gaining access to the user's computer after he has opened the link, the cyber criminal can find out security loopholes and steal his/her personal information. This would not have been possible if the user had not clicked on the link in the first place. This shows that the criminal depends more on the user's action to steal the information. Thus, the role of the user is very important. If the person is careful online, then he is safe from cybercrime victimization. If he is careless online and clicks any link which is visible to his eyes, then he is bound to get victimized. The moment the user clicks on the link, his system gets compromised and the criminal gains access to his personal information.

From this, we understand that the main problem lies in our human attitude. Unless we make an effort to change our behaviour, we will continue to fall for their tricks and continue to be victims of cybercrime. People are generally careless when it comes to the internet. When they are working in their offices, they are in a restricted space and are careful, but when they are at home, they tend to feel comfortable and act carelessly. For instance, people have multiple accounts online, however they do not remember the number of accounts that they signed up for in their device. Many people use the same passwords for multiple sites. If the hacker is able to crack the password for even a single site, then all his accounts get compromised because the user was careless in using the same password everywhere. Hackers are aware of this mentality of the user and are hence able to exploit them.

It may be possible that the person was careless in the past, but has recently started using secure passwords for his new accounts. The hacker can easily hack websites which are 5-6 years old and then can easily obtain your passwords because they were weak. They get your personal information from such sites and sell them off to other people on the dark web. It is therefore important to maintain a list of the websites that you have signed into so that you can update your accounts or delete them at a later point of time instead of just forgetting them.

Many kids and teenagers are on multiple social media platforms, and are highly active on these sites. A lot of these kids are not able to go outside and talk to their friends, or they may not be very close with their family. Hence they try to seek comfort from social media. They blindly accept friend requests from unknown people and start chatting with them. Accepting friend requests is fine, but we should remember that not everyone is a friend online. A lot of people have a hidden agenda and will be looking for that one step where they will be able to exploit you. Many teens make the mistake of sharing all their personal information online with anyone and everyone. This teen then gets contacted by cybercriminals who act nice in order to lure them into fulfilling their vicious desires.

Cybercriminals take advantage of human emotions and target them in a particular situation. Let us try to understand this with the context of the COVID pandemic.

The COVID pandemic has seen a huge rise in the number of cyberattack related cases. The pandemic has brought about a huge change in the workstyle. A lot of people have started working from home while some have lost their jobs. Meetings and conferences were all held online. This pandemic has seen reduced human interaction, thus taking a toll on mental health and making them easy targets for cyber attack. Such people are not in the state of mind to think carefully and they work based on their impulses. Depending on the emotion the person is facing, the attacker sends emails related to the problem, thus making the person click the malicious link immediately.

Consider a person who has just lost his job in the pandemic. He is looking for financial assistance. Then he comes across an email which says that he can get a lot of money by just participating in a survey. The person does not think carefully because he is in dire need of money and feels that the offer is the best way to get out of his misery. This person falls into temptation after seeing the lucrative offer and wonders ”what if the offer is actually true?”. He complies with the instructions given in the email. He fills in the survey and the hacker gains access to the person’s information.

Since people were not allowed to get out of their houses, a lot of people used E-commerce to get their goods. This gave cybercriminals a massive opportunity to exploit the people using E-commerce services. Cybercriminals disguised themselves as call centre workers and contacted people stating that their offers were hoax and that they should fill a cancellation form to cancel the order. Some people fell into this and lost a lot of money when they filled in their details. Sometimes instead of a human voice, the people received a robotic voice. The people thought that the robotic voice could not be false and concluded that the message shared was genuine and complied with the instructions. This was also a way by which the people were scammed because of their gullibility.

A lot of bogus websites were also made in the pandemic which disguised themselves as E-commerce websites. They seemed legitimate but they did not actually sell any product. The products were on display and the people were able to select the product to purchase. When they clicked on the purchase option, they had to enter the pin number. A keylogger software was enabled which monitored the user's keystrokes at the time of purchase and thus, the criminal was able to obtain the pin number of the user. Not only did the person not receive the product, but also lost all his money in the bank.

A trend that has been seen in this pandemic is that of charity. Cyber attackers understand that the people were interested in donating to charity, and hence they came up with charity hoaxes and scam websites. These websites were designed to look like the official page of a charity organization, but in reality, they were scams. Similar advertisements were spammed through emails and some people fell for it as well. A lot of these websites appeared as pop up advertisements in multiple websites and youtube videos with catchy phrases which made the user want to learn more about them. These websites were in fact scams and were designed to attract the user to their sites. A person who is genuinely concerned about people might fall into this trap and donate to a scam website instead of an official charity organization. The root problem of all of this is that people are always in a hurry and want to get done with the different steps involved quickly. Hence, they do not take the time to do proper research and understand the organization that they are donating to and the reviews that the organization currently receives.

A lot of people were concerned about their relative's health in the pandemic. Some cyber attackers deep faked a relative into a covid patient and made the video in such a way that it genuinely seemed that the relative had actually contracted covid and that he had to contact them to get more information. These people sent a contact number to call as a message. When the person clicked on the contact number, it was actually a link which downloaded malware in the phone, thus accessing the person's personal information to the criminals.

Another trend that has been observed is that people open covid urls regularly to check the status of the virus. They are curious to know when they will be able to go out again and how many days they will have to stay at home further. Cybercriminals understand this and make covid websites similar to the original websites which display covid statistics. The only difference is that when you open the website, malware will be downloaded to your computer without your knowledge. Similar to this, people download covid apps to check the status. A lot of these apps are trojans and are built with the purpose to install a virus into the mobile phones of the end users.

There are a lot of other factors which contribute to this carelessness of human beings when it comes to cyber activities. As we have seen from the above examples, cyber attackers take advantage of the situation that a person is in and cater their attacks so that it fits the situation. Bottomline is that the hackers target such individuals who do not think carefully and make decisions impulsively. They try to understand the person they want to hack - what they are interested in, what they frequently search and then at the right opportunity, they strike.

Cybercrime against Adults

"If you think you know-it-all about cybersecurity, this discipline was probably ill-explained to you."
- Stephane Nappo

Q: I've been hearing a lot of cases against adults lately. What can be done to prevent the different types of crimes that we are witnessing and what are the redressal methods for each crime?

A: As discussed earlier, cyberspace is an area a lot of people are not familiar with and hence the chances of getting scammed online is very high. Cybercriminals exploit the naivety of people and are able to get away with their crimes easily because these people do not know what to do after they have been duped. Hence there is a necessity to be aware of the different crimes that are happening daily in cyberspace. A lot of women have been victims to crimes like sexual assault and stalking. With the advent of digital devices, these crimes have taken to another dimension in the form of cyber stalking and sextortion. There have also been cases where men have been duped into thinking that they are chatting with the opposite sex online and then are lured into paying money or exposing themselves online, which is then used by cybercriminals to blackmail them. A lot of cases involve women who do not give in to a person's desire, then the person may indulge in some sort of cybercrime to harm the victim's image and take revenge against them. We shall be looking at a couple of cybercrime cases where people take advantage of the other gender to try to gain material benefit or money.

It has been observed that a lot of women do not report cybercrime cases to the police station because they are afraid that their identity will get revealed and they will have a bad image. There are some special laws and redressal measures for women so as to not disclose their identity while filing a complaint or lodging an FIR. If you are a woman and have become a victim to a cybercrime, then you can file a complaint anonymously on the website

cybercrime.gov.in and then your complaint will be immediately sent to the concerned police station in your area to tackle your case.

Let us look at some of the most popular types of cybercrimes that adults face and their redressal methods:

Debit card cloning :

Online mode is not the only area where people get frauded. A lot of people have faced cases of credit card and debit card cloning and these cases are rapidly increasing everyday causing huge losses to the victims of such crimes.

So what is debit card cloning?

Debit card cloning is the crime of stealing the data from your debit or credit card with the help of a skimmer or a shimming device. This device is usually placed in the area where the user inserts the debit card and then it records the data on the card with the help of hidden cameras, thus compromising his/her security pin to the scamster. The scamster can later make a card with your details and then use it to empty your bank account. ATMs are not the only places where your debit card can get cloned. Shops, malls, and even hotels have been found to have skimming devices. Any device which can be used to swipe your card in can have a skimmer installed in it to scan your card details.

A lot of cases have been reported by people who are currently in a relationship. These people gave away their debit card / ATM card to their significant other with whom they had become comfortable with. They took advantage of the victim by skimming the card details and then breaking up with them. The cloned card is then used to empty the victim's bank account.

Some cases involve people peeking at your card while you are making a transaction in an ATM. This is known as shoulder surfing and is a very common crime performed in crowded areas. Be wary of the people behind you trying to figure out the PIN number that you are entering for withdrawing money. These people will later steal your card and then use the PIN number that they memorized and empty your bank account.

Many other cases involved skimmer devices being installed in the card swiping device in popular malls and hotels. For example, recently the Mumbai police had cracked a case where four people were arrested for cloning the debit cards of several people checking into a hotel in Andheri. People would check into the hotel with their debit cards and the skimmer device in the card slot would scan the card details and save it. A keylogger was also installed into the keyboard to save the pin number entered by the user. The pin number and the card details were saved for later use. This practice continued for over six months, and the criminals would empty the bank accounts of the victims.

So how do we prevent ourselves from becoming the next victim to debit card cloning?

Here’s what you can do.

- Make sure you never give your ATM card and pin number to anyone, no matter how close they are to you. Not even your closest relatives and family members.
- Check for extra layering in the area where you insert your card for skimmers.
- Also cover the keyboard while entering the pin because there may be suspicious cameras lying around tracking the keys you enter.
- Never share your card details, CVV number and OTP number with anyone over call or in person.
- If you ever receive an OTP for any transaction which you did not initiate, then you should immediately get your credit card and debit card blocked as it is possible that someone has made an attempt to steal your money.

Alright, so you have become a victim in a debit cloning case. What can you do next?

If you have become a victim of skimming, then you should lodge an FIR before the concerned Police Station immediately. Once you have got duped by a fraud online, call the helpline number **1930**, and make a complaint. This number reaches the police and they will immediately instruct the bank to block your account to stop any further transactions.

Also report to the concerned bank branch in your localities immediately within 72 hours.

On 6th July 2017, RBI put out a notification that it will pay the money that the user has lost through cybercrime given the following situations.

1. If a third party was involved and took your money without your knowledge, then the bank is liable to pay you the exact amount that you have lost. If some sort of skimmer device was installed into the ATM because of which your card got cloned without your knowledge, then it is not your liability and the bank has to pay back your amount.

2. If you lost your money due to some security flaw of the bank, or if your account got hacked, then the bank will have to pay the amount that you have lost.

3. Finally if the user has lost his money from his account because of a mistake on his part (shared his OTP or passwords with another person) then the bank will not pay back the amount because it was entirely the person's fault.

There are also laws that protect you in such a crime and you can seek legal action under the following sections:

IT Act Section 66 for Computer Related offences,
IT Act Section 66C for punishment for identity theft.
IT Act Section 66D for punishment for cheating by personation using a computer resource.
IPC Section 419 for punishment for cheating by personation.
IPC Section 420 for cheating.
IPC Section 468 for forgery.

Keylogger:

Keyloggers are malicious programs installed on the victim's computer for recording user keystrokes to steal passwords and other sensitive information. The criminal is able to collect login details and other important details saved in the computer which is then mailed to an email address which the criminal can access. These keyloggers may be in the form of a hardware that can be attached to a computer system or ATM keypad or it can also be a software implanted into the computer system.

Keylogger cases are very popular in work places like offices and ATM kiosks or any store where you have to enter your pin number.

Keyloggers can be installed by people who know your daily routines and habits. These may be people who work with you in the same office. For example, let's say that you are an employee in an XYZ company and are eyeing for a promotion. You have a rival in your company who is eyeing the same promotion and is very competitive. On the day of the results, the boss chooses you for the promotion and you are very happy and celebrating. Meanwhile, your rival, out of jealousy, is planning a way to defame you and spoil your image. He observes that you leave your computer open without saving a password. He notes your daily movements and then strikes at the moment he finds you go away from your computer. He installs a keylogger software on your computer when you go out to have coffee because he knows your routine. While you are out for coffee, your rival has installed the keylogger software into your computer and acts like nothing has happened. The next day, you find that everyone in the office has crowded around the board looking at your intimate photos and private chats. This is a classic case of keylogger softwares being used for defamation.

Another example of keylogger softwares being used are in public places like libraries and cyber cafes. When you log into your email accounts and enter your bank details, the keylogger software will track the keys that you enter and will save them and send them to the email address of the scamster. The scamster will then be able to use these details for their personal benefit and will be able to blackmail you at a later point of time or use those details for extortion purposes.

So what was common in all the cases here?

The crime always involved the victim entering his personal information into a device which had a keylogger installed.

How do we prevent ourselves from getting victimized?

- You can always make sure that you lock your computer with a password so that strangers cannot access your computer. If someone is able to access your computer, make sure to change your password immediately.
- Also make sure to have antivirus software installed so that it can detect any trojan files or suspicious softwares and alert you if some suspicious activity is going on in your computer.

- Make sure that your computer is updated and you install licensed software instead of pirated copies, since pirated copies often come with viruses.
- Keep your operating system updated to the latest version.
- Use a virtual keyboard when you have to enter sensitive information like your bank details.

What can you do if you have become a victim to key loggers?

First of all, report to the police station and lodge an FIR.

You can take legal action by consulting the following laws :

Keylogger installation will fall under IT Act Section 66 and Section 43.

Punishment for Identity theft will fall under IT Act Section 66C.

IT Act Section 66D for cheating by impersonation using computer resources.

SMS Spoofing and Email spoofing:

SMS Spoofing is a cybercrime technique through which people are able to send messages which appear to come from an original mobile phone number, but the messages are sent by a different person. The scamster does this to lure potential people into believing that the messages are authentic and coming from a legitimate number. A lot of websites and apps are available on the internet that allow a fraud to send spoofed SMSs to cheat and defame someone.

In email spoofing cases, the attacker pretends to be another person while sending an email. Let's say that you were to pay some amount to a party for selling their product to you. You receive an email which contains their bank account details. However what you did not realize was that you did not receive the mail from the organization that sold you the product. Instead you received the mail from a hacker who knew that you had bought a product. The hacker changes the email header by replacing a few letters in the name and sends you a mail. Generally human beings do not read email headers, but rather read the content of the mail only. Hackers know that humans act in this way and are hence able to trick people into paying amounts to the wrong bank accounts.

Let's say that you are a shopaholic and you enjoy purchasing items whenever there is a sale or a discount. A person who is your friend knows your craze about shopping and decides to take advantage of this situation. He uses a spoofing software to personate a popular shopping site, say Amazon and sends you a phishing link which would offer you a huge discount if you open it. You, being the shopaholic that you are, immediately fall for the trap and do not want to miss the opportunity to get the huge discount. Without verifying the source, you open the link and purchase the product by entering your user credentials and bank details. Unknown to you, you entered a fake website and submitted your details to a person who was trying to trap you. You have made the online transaction and now wait for the product delivery. After a few months have passed, you try reaching out to the web store by calling their helpline number and then realize that the link you had clicked on was fake.

Another popular case is that in times of financial crisis or health problems, a relative may send a message asking for money. You, being emotional, without thinking decide to send the amount that they have asked for. It turns out that the person was not actually your relative, but it was a person who was impersonating your relative to get financial gain from you. You were taken advantage of. Now in this situation, what you could have done is: you could have called the person to verify about the problem and understand whether they actually needed the money or not.

How do you prevent yourself from getting fooled by SMS or email spoofs?

- The best way to prevent yourself from getting spoofed is by being aware and knowledgeable. Know that massive discounts and free offers are rarely given and always have a hidden agenda behind them.

- Always go for a traditional mode of payment transfer instead of opening suspicious links.
- Always verify from the person if they actually need the money incase you get a message for sending money.
- Unfortunately SMS spoofs are challenging to trace, so the best way to prevent them is by staying aware.
- Cultivate a habit of reading email headers and verifying if the mail you received is genuine and from the right person.

What can you do if you have become a victim to sms or email spoofing?

Kindly preserve the primary electronic evidence, through screenshots, or saving the emails so that they can be brought up in court later.

Since the criminal has committed an act of hoax and tried to trick you through a device of communication, you can consult the following laws:

IPC Section 465 - for making a false document (forgery).

IPC Section 419 - for cheating by personation.

IT Act Section 66D - for cheating by personation by using a computer resource.

Call spoofing:

Call spoofing is also similar to SMS spoofing. This cybercrime technique happens through phone calls. The scamster / hacker uses your phone number to call people and scam them for their own personal benefit. Call spoofing apps are also easily available online and the skill required to pull this off is really low. These apps can easily manipulate the criminal’s voice to that of a female or a small kid to make it appear like they are innocent and do not have any criminal intention. You psychologically believe that the person must be telling the truth by hearing the voice of a female or a kid or even a robotic voice. Hackers may also clone your phone and sim card details and use them for spoofing.

The hackers may use VOIP (Voice over internet protocol) to spoof. These VOIP calls are difficult to track and hence more and more cases of cybercrime are being recorded that use this technique for duping the victims.

Let's take an example of a woman who made friends with another guy online. They became close enough to share contact information with each other. The guy kept the woman’s number and shared a wrong contact number with her. After a few days, the guy contacted her father and impersonated her. He asked the father for 1 lakh rupees for an emergency. The father, believing that her daughter had called him and needed the money, sent the amount without thinking. The guy ran away with the money and could not be traced back because he did not use his own number to call the person.

There may also be cases where a person might pose to be an employee to a company that you always wanted to work for. After applying for the job, you get a phone call from the company stating that you have been shortlisted and need to come to a hotel to give an interview. The caller is not actually from the company, but has used the company's identity for his gain to get physical with the woman who believed that she was going to get a job.

It is almost impossible to differentiate in these situations if the caller is real or fake. So what can be done to prevent ourselves from getting manipulated?

- To stay protected in these situations, don't place all your trust on the caller ID information that is being displayed to you, since these can be altered using any third party apps.
- Use an authenticated app to identify where the call is coming from to get some assistance in whether to believe the person or not.

What should you do if you have become a victim of spoofing?

Reach out to police forces and file for a case. You can also take help of legal measures. There are laws that protect you in this regard , such as:

IPC Section 465 - for making a false document (Forgery).
IPC Section 419 - for cheating by personation.
IPC Section 468 - Forgery for the purpose of cheating.
IT Act Section 66C - for punishment for identity theft
IT Act Section 66D - for cheating by personation by using a computer resource.

Cyber stalking:

Cyberstalking is a very serious crime and refers to the use of the internet or other electronic means to stalk or harass another person by misusing information uploaded by the victim on social networking sites.

Cyberstalking cases are on a rise in India and there is a need for people (specially women) to be aware of it and to take the necessary steps to prevent cyberstalking and know what to do if they have become a victim to cyberstalking.

You know how people use social media to upload their pictures and videos. This seems harmless and innocent at first, but it turns creepy when you realise that a lot of people are stalking you online and keeping notes on your whereabouts and eyeing for a potential chance to victimize you.

Such a case happened in India, when a woman received anonymous mails from a person. He blackmailed her to pay him one lakh rupees otherwise he would leak her morphed pictures online and spread it all over the internet, along with her telephone and home address. It turns out that the girl had stored her images in her mail and the guy hacked it and accessed the images. Initially she ignored the mails, but the stalker continued to threaten her by sending letters through post and threatening her to leak the pictures in her neighbourhood. The stalker sent the woman's photos to her and continued to threaten her. It was at this point that the woman was terrified and seeked police intervention. The police were finally able to trace the stalker and found out that he was the woman's neighbour and knew her daily routine and whereabouts.

This goes to show that stalkers can also be your close ones and it is important to know about the people that are around you and to trust less.

A woman was a victim to cyberstalking. She uploaded a lot of pictures and videos on Instagram and always mentioned her whereabouts through those pictures. Once, she put up a story telling where she would be going and a stalker who was active in her profile noted it down. He reached the same beach that she was going to and when she was finally alone, he tried to molest her. The girl luckily escaped, but she was traumatised by the experience.

These cases are really scary, but what can you do to prevent them?

- First of all, maintain a low profile and low social media presence, because everyone watches you on the internet.
- Keep all your personal information private on the internet.
- Be careful about allowing physical access to your computer and other web-enabled devices like smartphones.
- Always log out your devices when you step away from them and use a screensaver with a password so that people do not access your computer.

- Make sure you always use two-factor authentication on your devices.

If you have become a victim of cyberstalking, what measures can you take?

As you have read in the case study given above, always report such cases to the police and seek their intervention. These people are dangerous and should be caught at all costs. If you do not want to disclose your identity for fear of bad image and publicity, you can file a complaint anonymously on **cybercrime.gov.in**. You will receive a mail which will refer you to the concerned police station and you can move further with your case in that police station.

There are laws in the legislature that protect a person if they have been the victim of cyberstalking. You can consult IPC Section 354D for cases that involve cyber stalkers.

Picture morphing:

Replacing body parts of the image of a person with the image of the victim is called picture morphing. A lot of tools are available online to cut and paste images into other images, making it child's play.

In picture morphing, an unauthorised user downloads images of a person online and then edits it and makes it hard to recognise that it has been altered. These are then reuploaded and used for vicious purposes like defamation and monetary gain. Cybercriminals generally use this to blackmail women by morphing their faces into images of naked women, which are then made viral on the internet, thus causing a lot of embarrassment to the victim and the family. A lot of morphing cases are a result of hate and are used as a tool of revenge between the two parties involved in the case.

Another case has been reported where a cyber criminal morphed a doctor's image over video call. The person was disguised as a patient and was seeking video consultation with the doctor. Two hours after the call, the doctor received a message from an unknown number stating that she had to pay the person Fifty Thousand rupees otherwise her morphed pictures would be leaked online. She was also sent all the morphed pictures that they had made of her to threaten her that they were serious and would post the pictures on Facebook and make them viral. The woman immediately went to the local police station and reported the matter. The police began an investigation and found out that two people in a nearby city were responsible for the picture morphing incident. These people had been involved in many picture morphing cases earlier and were not caught until now. The criminal had taken a screenshot during his video call with the doctor and had sent the image to his partner in crime. The other person morphed the images into nude pictures which they found online. They did not like the doctor because of some personal history between them and they wanted to take revenge on her by leaking her pictures online.

Some more cases involved a man who liked a girl and proposed to her. The girl, creeped out by the guy's attempt, rejects him and continues to move on. Angry by the incident, the guy decides to take revenge against the girl by morphing her pictures online. He downloads her images from her social media handle and then morphs them into bodies which he finds online and shares them among his friend circle which made the images viral within the college that they went together in. The girl, when she found out, reported it to the police and they eventually caught the culprit, but they could not prevent the images from spreading in the first place.

We saw a lot of cases about picture morphing. How can you prevent yourself from becoming the next victim?

- A lot of these cases involve downloading pictures from the internet. So to prevent the person from getting your images in the first place, maintain a low profile online and do not upload your photos.

- Do not accept friend requests from people whom you do not know because you never know with what intentions they asked to be your friend in the first place.

- Also keep your accounts secure to prevent people from hacking them.

What can I do if I have become the victim of picture morphing?

- Please report the case to the police immediately when you get a message or a picture of yourself. The extortion will continue if you do not take any steps.

- Immediately make your accounts secure and remove your images which you had online to prevent any more cases of picture morphing.

- There are laws that protect the citizens if they have become a victim of picture morphing. You can consult the following laws:

1. IPC Section 465 - for morphing photographs and making a false electronic record
2. IPC Section 469 - for making false electronic documents for causing defamation.

3. IPC Section 507 - for criminal intimidation by anonymous communication.
4. IPC Section 509 - for words, gestures or acts intended to insult the modesty of a woman.
5. IT Act Section 67 - punishment for publishing or transmitting obscene material in electronic form.
6. IT Act Section 67A - punishment for publishing or transmitting of material containing sexually explicit acts in electronic form.
7. IT Act Section 66C - punishment for Identity Theft

Profile hacking:

Profile hacking happens when your email or social media profile is accessed by a probable stalker who then compromises it to upload posts, images and videos which you would have never posted for the stalker's personal agenda or for monetary gain.

A very common trend that has been found is that people forget to log out of their devices in public areas like libraries. A lot of people use the same computer everyday and you never know when a cyber criminal will use the computer for hacking into the previous user's profile. A similar case was reported in NCR when a hacker got into a woman's account in a public library and changed her account passwords so that she could not access them anymore. After changing the account password, he put up vulgar and obscene posts and images on the woman's profile which she would never have done, and sent videos to her friends online. The criminal sent posts with the woman's number stating that they should call her to have a good time with her. The woman got defamed online and suffered embarrassment and trauma from this incident.

Phishing links are also a popular way by which people give their account details to hackers. A woman once saw a message for a discount sale on make-up products on the facebook store. The link asked her to log into her facebook account, however she was unaware that the link she opened did not redirect her to the actual facebook website, but instead redirected her to a clone of the website created with the intention of stealing account information. After she entered her account details, nothing happened. She did not enter the site she wanted to enter, instead she got an email stating that she had reset her password. A hacker got access to her account. She could have recovered her account if she knew about facebook security measures, but she was unaware about them. She had no other choice but to report the matter to the police. However, by the time she reported to the police, the damage was already done. The hacker used her account to send vulgar messages to her family members on facebook and posted morphed images on her account.

How do you prevent yourself from becoming a victim of profile hacking?

- Again this goes without saying, ensure that your social media accounts are secure and private. If you got hacked, it means that you were lacking in security and needed to tweak some settings to get yourself secured.
- Please do not share your account details with anyone, not even your family and friends because

you never know when your friend can turn into your foe.

- Use 2-factor authentication so that even if the hacker is able to access your account, he would not be able to log into the account until he enters the code, which would be sent to your mobile device.
- Avoid clicking on any links that appear in your messages or spam folder in your mail account. A lot of these are phishing links with the intention to steal your account information.
- Use virtual keyboards so that your account information is not tracked by keyloggers which might be attached to the computer.

What steps should I take if my profile has been hacked?

- First off all, report the case to. The police and do not panic.
- You can take this experience as a learning example to make all your accounts secure by enabling 2-factor authentication and enabling private mode in your social media handles.

If the damages are serious, make sure to seek legal action by consulting the following laws;

1. IT Act Section 66 - for computer related offences
2. IT Act Section 66C - punishment for identity theft.

Deepfakes:

Deepfakes are recent technologies that are used to combine and superimpose new images onto source videos which are already available. You must have already seen a lot of harmless deepfakes through youtube or some other platform. However deepfakes are very powerful in the sense that it is almost impossible to differentiate between a good deepfake and an original clip. Deepfakes are created by training machine learning models to superimpose images onto clips. While not everyone knows how machine learning works and might not possess the skill to write the code to make a deepfake, a lot of ready made tools and apps are already available online that do the work with the press of a single button.

This is extremely dangerous when used for vicious purposes like defamation and extortion as the people who view the deepfakes will not be able to differentiate and will consider the deepfake as truth. Considering the ease with which one can produce a deepfake, the possibilities for cybercriminals to victimize a person are endless.

One such example of the dangerous use of deepfake was reported in Maharashtra recently. A woman rejected a guy's proposal to be together. Out of anger, the guy threatened to post her videos online if she did not get with him. The woman ignored the man, and the man downloaded all the photos that he had of her and used an AI tool available on the internet to make a deepfake of her on a porn video. He posted the video online in multiple porn websites and even sent the video to her family members and friends. The woman was so embarassed and traumatized by this incident that she committed suicide.

What can you do as a viewer on social media platforms ?

Please do not trust any information that has been shared on the internet. A lot of them are fake and are made with the purpose of tarnishing the image of the person in the video. Trust less and make sure that you verify the source of the video from where it originated.

The size of the deepfaked video and the original video are different and could be used to differentiate between the original and the fake. A lot of information is also stored in the metadata of the video and you can use that to verify if the video sent is original or fake.

What can you do to prevent yourself from getting deepfaked?

Please do not upload clear pictures of yourself online. A lot of people are eyeing for that one chance to defame you and you have just given them a weapon to do so. Keep a private life online and ensure that you have enabled security for your social media platforms.

What can you do if you have been a target of a deepfake?

Report to the police forces immediately and take legal action against the cybercriminal.

Consult the following laws that the legislature provides for deepfake related cases.

1. IT Act Section 66C - Punishment for identity theft.
2. IT Act Section 66D - Punishment for cheating by personation using a computer resource.
3. IT Act Section 67 - Punishment for publishing or transmitting obscene material in electronic form.
4. IT Act Section 67A - Punishment for publishing or transmitting obscene material which are sexually explicit in electronic form.

5. IPC Section 419 - punishment for cheating by personation.
6. IPC Section 420 - Cheating
7. IPC Section 354A - Sexual harassment and punishment for sexual harassment.
8. IPC Section 465 - for making a false document.
9. IPC Section 469 - for making false electronic documents for causing defamation.
10. IPC Section 507 - for criminal intimidation by anonymous communication.
11. SEC 509 - for insulting the modesty of women.

Ponzi scheme

A fraudulent investing scam promising high rates of return with little risk to investors is called a Ponzi scheme. These schemes are made to look like they will profit the investors, but there is a catch. For the investors to get a commission, they will have to invite more people into this scheme. The amount that the new person invests goes as commission to people who are at the level of the first person. This cycle continues and people keep getting the money from the arrival of new investors. However, there is a problem. As the network increases and the people involved become large, the people who started the scam disappear, leaving the next investors in a horrible situation because they have to pay back the money that was stolen by the scamsters to the new investors. This scam causes huge losses to the people involved and are hence not recommended to get themselves involved in it. A lot of times, these victims will be reached out by hackers with malicious intent who will promise them that they will recover their money, but they would have to pay a certain amount for it and they fall prey to their promises of recovery of their losses.

Both educated and uneducated people fall prey to such schemes. The greed to make a fortune out of nothing is always there in people's heads. We always try to look for a way to make more money out of little effort. The scamsters are aware that people with this mentality exist and thus, their model of scamming always works.

Many cases of people from middle class families have been recorded where they have been victims to Ponzi schemes. A woman from a middle class family always wanted to go to foreign tours and own luxurious vehicles. She once saw an article online that said that she could get all of these only for Rs 10000. She was immediately mind blown with the offer and went ahead with the enrollment.

She then gets two more people on board as well. She receives a commission of Rs 500 for enrolling them in, As the number of people enrolling reduced, she got less commission and hence invested more for self enrollment. After a few days, she noticed that the site was non-functional and had disappeared. The people whom she was reporting to had disappeared and all the people that she had convinced to join are now asking her for their money. She found herself in a trap and suffered a lot of losses because of this scheme.

How to identify such schemes?

- You should have enough awareness and knowledge to know that no one provides anything for a discount without a reason. There is always some hidden agenda involved and you should not enroll in such programs because they are likely to be scams.

- Study the entire project and research before investing your money into any program or scheme.

- Do not trust agents who promote these schemes. The only reason they are promoting such schemes is because they receive a commission.

What can you do if you have been trapped in a Ponzi Scheme?

- The law has sections which can be applied in this scenario such as:

1. Sections 3, 4, 5, 6 of Prize Chits and Money circulation schemes (Banning) act,1978.
2. Different states have laws that can be used for Ponzi scams.
3. IPC Section 120-B : Punishment for criminal conspiracy.
4. IPC Section 406 - Punishment for criminal breach of trust.
5. IPC Section 420 - Cheating
6. R/W IPC Section 34 - Acts done by several persons in furtherance of Common intention.
7. Relevant IT Act Sections

Sextortion:

These types of frauds can take place both against males and females, but the current trend shows that females are most affected by this cybercrime. In such crimes the culprit usually manipulates the victims into showing their private or nude photographs or videos over phone, which are then saved and stored by the criminal for future extortion. Since this offence consists of sexual acts and extortion, the crime is known as sextortion. This cybercrime is really dangerous as a lot of victims have committed suicide because they are extremely embarrassed and are no longer able to show themselves in society.

In a lot of cases which have been reported, the people came in contact with the culprit through dating apps or even in matrimonial sites. The profiles that the victim connects to are mostly fake. Most of the time, behind the profile is a cybercriminal with the intention to gain monetary benefit through sextortion. These fake profiles are made in such a way that they appear very attractive to the viewers and they are usually approached for connection. After having a long chat over a few days, the person behind the profile asks for a video call where they display their private parts or asks for nude pictures. Once the criminal has access to the pictures and has taken a screen recording of the video, he extorts the victim by blackmailing her that the images and videos would be circulated all over the internet and made viral. Out of embarrassment and fear of bad image, she considers paying the amount in exchange for the pictures to get deleted. The victim gets tricked into believing that the images would be deleted once she pays the amount specified by the blackmailer. However, the blackmailer does not delete the media files and continues to blackmail her after a few days for more money.

Another popular case is when a couple splits after a relationship. The husband or boyfriend has some videos and pictures of their intimate moments together and threatens to make them viral over the internet. The woman, out of fear, pays money to the blackmailer and this cycle continues in the future.

How do you prevent sextortion?

- Please remember that anything you post online will always stay online in one form or another. Once a post is shared, it gets spread around quickly and it gets difficult to remove every photo or video that has been posted about you. Therefore, never allow anyone to take a recording or a picture of you that can be used later for blackmail.

- If the other person in an online chat is rushing and trying to develop intimacy quickly, or is asking for nudes quickly, then understand that this is an attempt at sextortion and you should immediately block the contact.

What should you do if you have become a victim to sextortion?

If you have become a victim of sextortion, you should immediately tell your close ones whom you trust and take immediate action to the police.

- File a formal report to the nearby police station cybercrime cell, or if you are afraid that your identity will be exposed, then you can file a complaint anonymously on the website **cybercrime.gov.in**, and they will send an email with details about the police station to refer to and the next plan of action to be taken.

You can also seek legal action under the following sections:

- IT Act Section 66C for Identity Theft (dishonestly or fraudulently using a unique identification feature)
- IT Act Section 66D for cheating by personation by using computer resource
- "IT Act Section 66E for punishment for violation of privacy"
- IT Act Section 67 for publishing or transmitting obscene material in electronic form
- IT Act Section 67A for publishing or transmitting of material containing sexually explicit act etc., in electronic form
- IPC Section 354C for voyeurism
- IPC Section 419 for cheating by personation

- IPC Section 354A for sexual harassment
- IPC Section 509 for words, gestures or acts intended to insult modesty of a woman
- IPC Section 384- Extortion

Cybercrime against Children

"Social media can be a useful and fun way to interact with others and to share content, but use it carefully. Remember that there is nothing totally private on the internet and once online it is hard to control."

- Amanda-Jane-Turner

Kids these days have access to the internet and are able to browse youtube and other streaming services without any effort. Technology has paved the way for even 5 year olds to download apps from the play store and use them without assistance. Kids play a lot of mobile games online like Pubg, Call of Duty. These games are multiplayer and enable you to interact with a lot of people, however not all people online are of the good type and a lot of them send offensive messages and bully the kids.

Children lack the maturity to tackle the internet and can be swayed easily by people's opinion online which might make them act in ways which are totally different to their usual selves. It is the role of the parent to monitor the child's activity online and to ensure that he/she is not being attacked by some bully online or he/she is not accessing a site or opening a link which is dangerous for the child. Recently a minor child had committed suicide because he was getting bullied a lot while playing online games. This just goes to show that cybercrime against children is a very serious matter and there needs to be awareness about this. We will learn about the different types of cybercrimes that criminals do against children and what you can do as a parent if your child has become a victim to some of the crimes mentioned below:

Cyberbullying:

Cyberbullying is bullying that takes place through digital devices like cell phones, laptops and tablets. It can take place on social media, messaging platforms, gaming platforms and mobile phones. A lot of bullying that takes place online is done through tormenting posts, hate messages, blackmails and emails. Sometimes kids share embarrassing photos of each other online which the other person might not feel comfortable about. Sometimes lies are spread about a person which makes a bad image for the kid and this traumatizes the kid and does not want to talk to anyone anymore. Sometimes kids may impersonate other kids and say things on their behalf which they would have never done. All of these instances take a toll on the child's mental state and affect his daily life activities. Such a child may go into depression and anxiety, and may often indulge in self harm and in the worst case, suicide.

It's pretty evident that cyberbullying is a very serious issue and needs to be tackled immediately by the parent since children are immature and often do not tell their parents about the things they face online. Parents need to keep a watch on their child and know what they are going through and make an environment at home which makes the child feel open to share his feelings.

What can you do as a parent to protect your child against cyberbullying?

- First of all, make your child feel safe at home and feel like he/she can share anything and be open with you. If the environment at home feels threatening or scary to the child, he/she might refrain from talking or sharing about the things he/she faces online because they are worried that you will be angry with them.

- It is advisable to not provide mobiles and tablets to young kids and keep a cap on their daily internet usage. Let them spend most of their time outdoors doing physical activities and enjoying themselves with other kids of their age instead of the grown ups who they might meet through games and social media.

- You can enable safe browsing feature on your internet browser so that the child cannot access dangerous sites.

- If your child does play games online, make sure they are games which are not too violent and which are marked safe for kids.

Cyber roasting:

Roasting culture has become very popular through media and youtube videos and kids are the active audiences of such videos. These kids start practising it in their friend groups by willingly posting their images and videos online in social media and video sharing platforms, inviting other people to post insults about them.

These kids have been manipulated into believing that roasting is a fun activity and since everyone is doing it, they fall into peer pressure and participate in it as well. However the goals of roasting sessions are to bombard the person’s feed with abusive online comments, images and videos until the person cannot take it any longer.

A lot of these roasts target the student’s physical features and their personal characteristics. Children are usually not mature enough to deal with these roasts and get mentally affected by the roasts that happen online, to such an extent that they get depressed and have low self esteem. In the worst case scenario, the kids may indulge in self harm and suicide.

What can you do as a parent?

- Efforts should be made to sit down as a family and understand what your child is going through online on a daily basis.

- Block channels and websites which are harmful to your children until they have become mature enough to understand how the internet works and the dependency between children and social media.

- Teach them about social media privacy and make a clear line between personal life and online life.

- Monitor their online activities in order to stay aware.

- Engage them in other physical and household activities.

Cyber grooming :

This is usually done by pedophiles online. When a child is unaware of the goods and bads of the internet, pedophiles take advantage of the child’s naivety and talk to them nicely and try to form an emotional bond with them. The criminal poses as a good guy with no malintent and manipulates the child into forming a good bond with him.

Once the child has gotten used to the criminal and has gotten comfortable with him, the pedophile (groomer) makes attempts to reach out to him online or tries to find out his address or contact details to take advantage of the poor kid. This method of preparing a child and the environment for sexual abuse and exploitation and ideological manipulation is called cyber grooming. The groomer "grooms" the child to make him ready to face torture and sexual abuse.

A lot of cyber grooming cases have been reported in India lately. Recently, a man was caught for raping a young 13 year old girl. What makes the case even more frightening is the fact that the man had befriended the girl on facebook and used to message nicely with her to finally gain her trust. After gaining her trust and getting her contact details, the man met her and sexually assaulted her.

Another similar case was reported where a man met a child on a gaming platform and played games with him regularly. After that, they continued their friendship through social media and would regularly discuss game strategies and ways to play better. The man bought him free recharges and in-game currencies which were used to buy skins in games, all to gain the child's trust. Once the child trusted the man, he got the child involved in pornographic activities and then later used this to blackmail the child. The child was naive at first and did not realise that he was being manipulated and controlled by the guy.

What can you do as a parent to prevent your child from getting cyber groomed?

- First of all, make sure that your child feels comfortable enough to share details that happen in his daily life with you.

- Keep a cap on their daily internet time and the amount of time he/she spends on online games.

- If possible, please do not let them have a social media account until they are 18 or mature enough to understand that not all people are good on the internet.

- Educate your child to not talk to strangers or give into their demands.

Child Pornography:

Any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities, or the representation of sexual parts of a child, the dominant characteristics of which is depiction for a sexual purpose, is called child pornography.

Even viewing and surfing the internet for child pornography is an offence, let alone storing, posting, sharing, forwarding and creating child porn.

In the recent years, child pornography has increased a lot due to the easy access of internet and easily available videos on the internet. Child pornography is the most heinous crime which occurs and has led to various other crimes such as sex tourism, sexual abuse of the child, etc.

During a regular surveillance of the dark web, a police officer and his cybercrime team based in South India found a disturbing visual of a minor girl doing objectionable things with her uncle. The uncle enticed the kid into doing the objectionable things using dolls and toys. These kids are immature and do not know what they are doing and manipulating them to do sexual activities is really condemnable. People pay a lot on the dark web to watch illicit videos like child porn and because of this people engage in creating them. The police were able to trace the video after three months of surveillance of the IP address using special tools.

Another case was reported where a parent uploaded a video of their minor children naked and painting each other. The intention was not pedophilia, however it does not change the fact that the content was obscene. This would have been fine if it was confined within the house itself, however this video was indecent and shared publicly which was then shared by other people and so on.

For parents, it is important to remember to never upload any content of their children which may be indecent or obscene.

Child laws:

There are laws which protect children if they have been a victim of sexual offences or child pornography. Let us look at some of them and understand what they are and what punishment is given to the offenders.

POCSO Act 2012: This stands for "Protection of Children from sexual offences" Act. It provides sections which describe different scenarios in which children may be exploited and the punishments for the offences that have been conducted.

Section 13. This section talks about the use of children for pornographic purposes.

If a person uses a child in any form of media for the purpose of sexual gratification, which includes representation of the sexual organs of a child, the usage of a child engaged in sexual acts (with or without penetration) or the indecent representation of a child, then the person shall be guilty of the offence of using children for pornographic purposes.

Section 14: This section talks about the punishment for using a child for pornographic purposes.

If a person uses a child or children for pornographic purposes, then they shall be punished with imprisonment for a term which shall not be less than five years and shall also be liable to fine, and in the event that the person gets convicted again for the same crime, then they will receive imprisonment for a term which shall be more than seven years and the person shall also be liable to a fine.

Section 15: This section talks about the punishments for a person possessing child pornographic material.

(1) If a person, who stores or possesses pornographic material in any form involving a child, but fails to delete or destroy or report the same to the designated authority, with an intention to share or transmit child pornography, shall be liable to fine not less than five thousand rupees, and in the event of second or subsequent offence, with fine which shall not be less than ten thousand rupees.

(2) Any person, who stores or possesses pornographic material in any form involving a child for transmitting or propagating or displaying or distributing in any manner at any time except for the purpose of reporting, as may be prescribed, or for use as evidence in court, shall be

punished with imprisonment of either description which may extend to three years, or with fine, or with both.

(3) Any person, who stores or possesses pornographic material in any form involving a child for commercial purpose shall be punished on the first conviction with imprisonment of either description which shall not be less than three years which may extend to five years, or with fine, or with both, and in the event of second or subsequent conviction, with imprisonment of either description which shall not be less than five years which may extend to seven years and shall also be liable to fine.

To avoid getting charged under these sections, make sure that you send any content that you find related to Children Pornography or Child sexual abuse to the concerned social media website. You can also report the incident to the National cybercrime portal: **cybercrime.gov.in** or you can report the case to the nearby local police station and file an FIR which will be forwarded to the nearby cybercrime cells.

Prevention of Cybercrime

"Rather than fearing or ignoring cyber attacks, do ensure your cyber resilience to them."

- Stephane Nappo

Rahul: Alright. I learnt that cybercrime is a two person system - it involves the attacker and the victim. Unless the victim complies with the attacker's agenda, he shouldn't be able to get victimized. But how do I know what I should do to prevent myself from getting cyber victimized?

Me: It's good that you are interested in finding out ways to prevent yourself from getting cyber victimized. See, that's the first step in fighting cybercrime - to be aware of the different methods to fight against cybercrime. As you already know that cybercrime is a two person activity involving the cybercriminal and the cyber victim. Until the victim complies to what the hacker wants: such as clicking a malicious link, providing bank details to a fake website, the hacker cannot do anything.

Some ways by which you can safeguard yourself against cybercriminals and hackers are:

1. Two-factor authentication: This is the most basic way to safeguard your account in various apps and social media platforms. Through 2-factor authentication, you add an extra layer of security in case your password has been stolen. All you have to do is enable 2-factor authentication. This means that when you log into your social media account, you will receive a passcode in your registered mobile number which you have to enter to access the site. This just makes the work of hackers tougher because now along with your account credentials, they need to find your mobile details to access your account. This is a very simple, yet effective way through which you can secure your accounts.

2. Keep a record of all your accounts: This is the most important step yet very few people actually do this. A person has multiple accounts on a device - his social media accounts, his bank details, etc. It is possible that a hacker might hack a very old website with low security features, which by chance you had also logged into. Now since your account was available on that website, the hacker is able to crack into it and steal your personal details. Maintain a record of all your websites that you have used in your device and logged into. This way, you will not forget the accounts that you have logged into and you will be able to update your account settings or delete your account if needed so that a hacker will not be able to access them at a later point of time.

3. Update passwords: Along with keeping a record of your accounts, it is important that you change your password often so that it makes the job of the hacker much tougher than usual. Just changing passwords is not enough though. You need to make sure that your password is not just a simple word that can be easily cracked by a dictionary attack. Your password should be a mixture of numbers, characters and special characters so that it becomes difficult to crack for a hacker. Random password generators can also be used to create your passwords.

4. Keep a low profile online: It is important to be aware of what we present to the outer world online. Try to analyse what pops up when your name is typed online and understand what people see when they open your profile. You should be careful not to post too many details which can attract unwanted attention and cyber attackers.

5. Update software regularly: Older software lack certain features and are buggy. Updates are usually meant to improve on these security features and fix the bugs in the previous insecure version of the software. Update your software regularly so that the hackers are not able to exploit that particular loophole in the older version of your software and thus, gain access to your system

Make sure to use licensed software and apps so that updates can take place regularly. Pirated software cannot be updated and hackers are able to easily exploit any vulnerability present in the software.

6. Check for fishy websites: A secure website always has a lock symbol on the left of the address bar. Check to see if the lock symbol is available when you open a website.

Apart from that, also check if the website opens with a “https" protocol. The ‘s’ at the end of https stands for secure and thus, if you open any website starting with https, it is probably safe.

You should also check if the domain name is correctly spelled. Sometimes hackers swap two letters of the word to create a fake website. A lot of visitors to the website do not notice this mistake and believe that they have entered the correct website.

7. Avoid clicking malicious links and emails: Cybercriminals use emails to share malicious links with the hope that the user will click on them and get navigated to a bogus website, give them credentials and thus access to the computer systems. People should avoid clicking spam links and pop up advertisements which appear in multiple websites with offers which are too good to be true. The person should act practically and consider the risk involved in clicking such malicious links.

Clear your spam mail as it gets cluttered and avoid clicking on any of them. Some spam mails are programmed to download malware into your computer and get executed when you click on that mail.

One should avoid downloading any files from fishy websites. These websites may pretend to be delivering the software that you want but in reality, they may be delivering malware to your computer instead. Download software only from the official websites.

Alternatively, you could use some websites and apps to check if a link is clean or not. An example of such a website is VirusTotal. All you have to do is copy the url link of the suspected malicious website and paste it on this website. The website tells you if the suspected website has been flagged before by security vendors for phishing, web jacking or other types of cybercrime.

8. Delete unnecessary apps: Delete unnecessary apps so that you have an easy to manage device and so that you are able to track each app for any unusual activity.

9. Examine content of messages: People may get a lot of spam messages and blindly follow the instructions that are written in them and then get scammed. People should pause and analyze what they are reading and decide whether the message is actually genuine or spam. Be skeptical of each and every message you read.

10. Avoid sharing passwords and any other information: Do not trust anyone to share your passwords with them since you never know who your contacts may encounter somewhere. The same is for meetings and conferences. Do not share your zoom passwords in whatsapp groups or other social groups. Instead share them through emails to the registered users so that only they can enter the meeting and also the confidential information discussed remains preserved.

Question yourself why someone would ask your information in the first place and then take a decision if you have to share your information or not.

11. Encryption of files: If your device gets hacked by a person, you lose access to your confidential information that you have saved in your computer devices. You can save your folders from being accessed by an outside party by enabling encryption. If you have an operating system which matches any of these: Ultimate and Enterprise editions of Windows Vista and Windows 7, Pro and Enterprise editions of Windows 8 and 8.1, Pro, Enterprise, and Education editions of Windows 10, then you can enable BitLocker to encrypt your files and folders. To do this, go to your start menu and type in BitLocker. Select the option "Manage Bit Locker" that pops up and enable it for the drives and folders that you want to be encrypted. Save the recovery key somewhere so that you can use it in case of an emergency later.

12. Change in behavior or attitude: This is the single most important step that you can take to prevent cybercrime victimization. Stay careful and start taking precautions from the start instead of waiting to get victimized. People need to develop some reflexes when they come across a mail or an sms. Pause and think before making a decision. Always be doubtful of the messages that are being shared to you and confirm them from official sources. Do not trust robotic calls as they can be easily manipulated to tell you things that you would like to hear. Do not panic in any situation and think with a cool mind, and finally research well about anything and everything.

Inform your family members and friends about different preventive measures and help them save themselves as well. Unless you change your attitude towards cybercrime, you are always at a high risk of getting scammed and victimized.

Law Enforcement

"As the world is increasingly connected, everyone shares the responsibility of securing cyberspace" ***- Newton Lee***

Rahul: My neighbour got hacked last week. All his important documents have been stolen and his personal information has been compromised. He got an email demanding a ransom otherwise all his files would be deleted. He does not know the correct course of action to be taken. Can you suggest any legal procedure that is to be taken?

Me: I'm really sorry to hear that Rahul. Your neighbour should immediately seek legal action against the cybercriminals. He should be able to receive compensation under the IT Act through criminal and civil remedies. He can seek help from the Honourable IT secretary and IT adjudicator of the state by filing a complaint under the IT Act.

Also do tell your neighbour to check out the website **cybercrime.gov.in** . Through this website, you can file a complaint against any form of cybercrime and also learn about the different forms of cybercrime and their legal remedies.

Rahul: Thank you very much for the information. Can you explain the different sections that the Indian legislation has for cybercrime?

Me: Sure Rahul, I will explain the Indian legislation and the different sections briefly so that you can understand which sections to look for when you face a cybercrime. Ignorance of law is not excusable and it is important that people behave well on the internet so that they cannot be prosecuted.

The IT Act, 2000

The Indian legislature contains laws which are meant to penalize cyber offenders. The Information Technology Act (ITA, 2000) was passed to help promote the IT sector in India and to promote E-commerce in the country. This act has been divided into 90 sections and 13 chapters. IT Act was amended in 2008. Any person facing cybercrimes can refer to the corresponding sections in the IT act. Section 43 and Section 66 of the IT act greatly focus on cybercrime and we shall look into it in great detail.

The IT Act consists of two parts, the civil remedies and the criminal remedies. The Sections 43 (a-j) and Section 43A are called cyber contraventions, and if any person does any act referred in sec 43(a-j) with dishonest or fraudulent intention then it becomes faces cyber offences (Sec 66), then they can go before IT secretary (IT adjudicator) of the state and file a complaint case. The person will be able to seek compensation for upto 5 crore rupees and more than 5 crore from Civil Courts.

Section 43 (Cyber contraventions) deals with the civil remedy aspect of the IT Act. It talks about the compensation that a person can receive for damage to computers, computer systems or computer networks. The word damage here means to destroy the device/data, to alter, modify or even rearrange the data in the device.

If a person faces a cyber contravention which falls under any of the sections below, he can file a case for remedy for the losses that he has faced to the IT secretary of the state.

43-a: If a person tries to access or secure access to a computer, computer system or a computer network, computer resource without the permission of the owner or the person in charge of the computer. This person may try to physically or remotely access the computer system by hacking the computer network.

43-b: If a person without the owner's permission downloads, copies or extracts data, computer database, or information from such a computer, computer system or computer network including information or data held stored in any removable storage medium.

43-c: If a person without authority introduces any computer contaminant or computer virus into any computer, computer system or computer network. This could be done through email links, ransomware links or through external drives and pen drives. Here, "computer contaminant" refers to any set of computer instructions that are designed to disrupt the normal operation or which are designed to modify, destroy, record, transmit data residing within a computer, computer system or computer network.

43-d: If a person damages any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network without the knowledge of the owner or authorized person in charge of the system. The person involved may corrupt the files.

43-e: If the person disrupts or causes disruption of any computer, computer system or computer network. This section will be used if someone tries to temporarily shut your computer system.

43-f: If the person denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means. This could be through hacking the computer system or by encrypting the files of the computer, or could also be done through a DoS attack (Denial of services attack).

43-g: If the person provides any assistance to any unauthorized person to facilitate access to a computer, computer system or computer network without the permission of the owner/manager of the computer network or system. For example, if a person gives access rights to an outgoing employee, who can then spy from another company and steal the data for his company's profit.

43-h: If a person charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network. For example, if someone uses your internet connection without your permission, and alters any information then you can refer to this section.

43-i: If a person destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means. This is mainly done through data diddling.

43-j: If a person steals, conceals, destroys or alters or causes any other person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

If a person has faced a cyber contravention belonging to any one of the above categories, then he can file for compensation upto Rs 5 crore through this section to the IT secretary (IT Adjudicator).

The IT act also provides another section 43A. Under this section, if a corporate body or a firm handling personal data or sensitive information does not follow proper security protocols ((**The Information Technology – Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**) and as a result of which, loses the data to another person, then the firm is liable to pay for the damages in the form of compensation to the person affected.

Section 66 talks about the criminal remedy of the IT Act. Now, if any person performs one of the acts under section 43 with dishonest or fraudulent intentions, then he/she is liable to the following punishments provided in section 66 of the IT act. The person involved shall be punished with imprisonment for a term which may extend to three years and he/she may have to bear a fine of upto five lakh rupees or with both.

66A: This section describes the punishment that a person shall receive if he/she sends offensive messages through a computer or through any communication device. The message sent may be -

a) Any information that is grossly offensive or has a menacing nature

b) Any information that is known to be false and yet spread to cause annoyance, inconvenience and hatred.

c) Any information spread for the purpose of deceiving or misleading the recipient of the message.

The person shall be punishable with imprisonment for a term which may extend to three years and with fine. This section has been declared unconstitutional by the honourable Supreme court in Shreya Singhal vs Union of India (2015).

66B: This section describes the punishment for a person who has dishonestly received or retains a stolen computer device or communication device.

If a person dishonestly receives and retains stolen computer resources or a communication device, then he shall be punished with imprisonment for a term which shall extend upto three years and he may have to bear a fine of upto rupees one lakh or both.

66C: This section describes the punishment for identity theft.

If a person fraudulently or dishonestly makes use of another person's electronic signature, password or any other unique identification feature i.e., performs identity theft, then he shall be punished with imprisonment for upto three years with a fine upto rupees one lakh.

66D: This section describes the punishment for a person who tries to cheat by impersonation.

If a person, by means of a computer resource or a communication device, cheats by personating another person with an intention to deceive, then he shall be punishable with imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66E: This section describes the punishment for violation of privacy.

If any person intentionally captures, publishes or transmits the image of a private area of a person without his/her consent, then he shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees or both.

66F: This section describes the punishment for cyber terrorism.

If any person -

a) With the intention to threaten the integrity, security and sovereignty of the country or tries to strike terror in people or any section of the people by when

- someone denies or causes the denial of access to any person authorised to access computer resource; or
- attempts to penetrate or access a computer resource without authorisation or exceeding authorised access; or
- introduces or causes to introduce any computer contaminant.

b) Knowingly penetrates into a computer resource without permission or exceeding authorised access, and as a result gains access to confidential information which is restricted for national security and foreign relations.

If a person comes under any of the two categories above, then he shall be punished with life imprisonment.

Section 67 talks about the punishment for publishing or transmitting obscene material in electronic form. If a person publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees

We will talk about two sections 67A and 67B under this section.

Section 67A: It talks about the punishment for publishing or transmitting material containing sexually explicit acts, etc., in electronic form. -Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67B: This section deals with the punishment for publishing indecent, obscene or sexually explicit acts involving children (a person who is not yet 18 years old).

The Indian Penal Code (IPC)

We have just seen the important sections under the IT Act. Apart from the IT Act, the Indian legislation also has the Indian Penal Code (IPC), which contains laws that a person can avail to if he has been subjected to other forms of cybercrime.

Some of the important sections which come under IPC are:

Section 153A: This section deals with activities which promote enmity or cause disturbance in the harmony between different groups on the ground of religion, race, place of birth, residence, language, caste or community. People who are involved in this offence shall be punishable with imprisonment for upto 3 years or with fine or both.

Section 292: This section deals with the possession or sale of obscene material involving sexually explicit acts The punishment for this crime is imprisonment and fine upto 2 years and Rs 2000. If the person commits the same crime again, then he shall be imprisoned for 5 years with a fine upto Rs 5000.

Section 295 A: Deliberate and malicious acts intended to outrage religious feelings of any class by insulting its religion or religious beliefs. People who are involved in this offence shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

Section 354C: This section deals with the punishment for crimes involving the capturing or publication of pictures of a private act involving women without their consent. This section is similar to Section 66E of the IT act where both males and females are liable. The punishment for such a crime involves imprisonment for 1 to 3 years and 3 to 7 years if the crime is repeated again.

Section 354D: This section deals with the punishment for stalking in both physical and cyber form. The punishment for this crime is imprisonment for upto 3 years for the first time and 5 years for the second time along with a fine.

Section 379: If a mobile phone or a computer is stolen, then the person shall be punished with 3 years of imprisonment and fine.

Section 411: This is a continuation of the crime performed in section 379. If a person receives a stolen mobile phone or computer, then he shall be punished under this section. The punishment shall be imprisonment for upto 3 years with a fine.

Section 419: This section deals with the punishment for cheating by personation. Any person who cheats by personation shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

Section 420: This section deals with cases involving cheating and dishonestly which induces the delivery of a property. If a person cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Section 465: This section deals with cases of forgery. Punishable offenses under this section involve preparation of false documents and email spoofing. Criminals who are dealt with under this section shall face imprisonment for upto 2 years or with a fine or with both.

Section 468: This is basically an extension of the above section. If the cases of forgery are committed with the purpose of committing serious crimes, then the criminal shall be punished for imprisonment for upto 7 years with a fine.

Section 469: This section again deals with forgery. If the forgery is committed with the purpose of harming the reputation of the other person involved, either through online documents or other electronic forms, then the person shall be punished with imprisonment for upto 3 years and shall also be liable to fine.

Section 500: This section deals with defamation cases. If a person sends any defamatory content or abusive messages through email or other electronic form, then he will be tried under this section. The punishment for this crime is 2 years or with imprisonment or fine or with both.

Section 504: If a person intentionally insults with the intent to provoke breach of peace with another person through mail or any other electronic means, then he shall be tried under this section. The punishment for this section is upto 2 years imprisonment or with fine or with both.

Section 505: This section deals with cases of public mischief. If a person makes a statement or circulates a rumour with the intention to cause or which can likely cause alarm to the public, then he can be charged under this section. Some examples of offences that can get you charged are circulating rumours related to COVID or vaccination in India. People who fall in this category shall be punished with imprisonment which may extend to three years, or with a fine, or with both.

Section 506: If a person tries to criminally intimidate another person with respect to the life of a person, property destruction or the chastity of a woman, then it will attract this section. The punishment for this crime is a maximum of 7 years of imprisonment or fine or both.

Section 507: This section deals with criminal intimidation through anonymous communication. If a person commits a cybercrime anonymously or conceals his/her name or the place from where the cybercrime originates, they shall be punished with imprisonment for a term which may extend to 2 years, in addition to the punishment provided for the offence in the previous section.

Case Studies

"As cyber threats evolve, we need to evolve as well"

- Christopher A Wray

Rahul: I have now somewhat got a sense of what cybercrime is all about. Can you provide some real life examples to solidify my understanding?

Me: Sure Rahul, case studies are the best ways to understand cybercrime and the possible mistakes that one can make. Let us look at some prominent examples and case studies.

Nigerian Scams

Nigerian scams are also known as advance fee frauds because of the nature in which the criminal operates. In this form of cybercrime, the attacker tends to send emails promising the victim a large amount of money in return for a small payment (advance fee) which would be required to obtain the huge amount of money.

Modus operandi:

The attacker here targets the naivety of the victims. The criminal aims to fool the victim into believing that he/she is going to get a huge reward at the end and hence he/she should continue paying the small amount required to receive the huge sum of money. This scam can go on for months and the attacker may try to find new ways of making the victim believe that the mail is genuine and that the victim has to continue paying.

The medium through which the criminal communicates with the victim need not necessarily be through emails. The person can contact the victim through social media, by sending a friend request on facebook or by sending an anonymous direct message through instagram.

Other variants of the nigerian scam involve employment scams, lottery scams and romance scams. The interest of the victim is targeted and then used to gain monetary benefit.

Case study:

In a country like India where employment is a huge issue, Nigerian scammers found a valuable topic to target on. In January 2020, a gang of people in Mumbai pretended to be a job consultation agency. They charged huge amounts of money on the pretext that the person would get a guaranteed job.

In one particular case, a woman was offered the job of a nurse at a Hospital situated in in the US. The job consultation agency also offered to help her with the visa proceedings and help her relocate to the US along with her family. The criminal convinced the victim to deposit 13 lakh rupees as instalment for the help being offered. The victim complied with the instructions of the agency. However, the victim was suspicious of the agency as they kept asking for money before any step was taken and hence filed a complaint against the agency to Mumbai police.

Upon investigation, it was found that the bank accounts into which the woman had deposited money belonged to different branches all over the country, but the mail sent to her originated from Maharashtra. On further investigation, it was found that withdrawals were made through several

ATMs in Mumbai. Thus, a team of police officers from Mumbai traced the accused and took him into custody. The members of the gang consisted of both Nigerian citizens and Indian citizens. The police confiscated SIM cards, credit cards, debit cards, laptops and bank passbooks, from which they were able to obtain more information on the other members of the gang.

Why do people fall for these scams?

The reasons why people fall for these scams are because they are very tempting. These scams play on the person's greed. The person is promised huge financial profit without effort which seems like a lost opportunity if not taken. People don't want to miss out on an opportunity which could make them rich and hence fall for these traps.

How do you save yourself?

The best way to save yourselves from these scams is to be aware of them. No person offers money freely without a reason. If such offers come up in your email or personal messages, always ignore them. Always avoid making any sort of transaction with a stranger.

ONGC Identity Theft

Case study:

ONGC is an Indian public sector multinational crude oil and gas company. In 2015, ONGC had agreed to deliver 36000 tonnes of naphtha to a middle-east based oil company. In return, the company had to pay Rs 193 crore as a part of the deal. The delivery was facilitated on behalf of ONGC from the email address "patel_dv@ongc.co.in". After multiple email communications, the deal was closed and the oil company claimed that they had paid the full amount. ONGC denied this claim stating that they didn't receive any payment. The oil company claimed that they deposited the amount in ONGC's Bangkok based bank account, whereas ONGC claimed that the deposit was to be made in the Indian bank account. Now here's the catch: There were two email accounts with similar names: "patel_dv@ongc.co.in" and "patel_dv@ognc.co.in".

Modus Operandi:

The fraudster behind the Identity theft either hacked the accounts of ONGC or the oil company and was able to read the email conversation between both companies, and waited for the right time to perform this act. The fraudster created a similar domain to that of ONGC i.e ognc.co.in, and created a similar username patel_dv. The fraudster performed identity theft on ONGC and got away with a huge amount of money just by swapping two letters.

How was the company not able to notice the difference between the two email accounts?

It is a general human tendency to read only the username and to ignore the domain name. The oil company made the same mistake and focused only on the first part of the email i.e “patel_dv” and could not differentiate between the two emails as the contents were similar.

How could this have been avoided?

We can save the email accounts that we communicate frequently with in the contacts option in most email websites. The company could have similarly saved the original email account with an alias/nickname, so that if the next mail did not come with the alias, The client would have realised that they were communicating with the wrong email account. Apart from this, 2-factor authentication should have been used in the emails,

This was a classic case where a simple mistake led to one of the biggest cyber frauds in India.

Liberty Reserve Cybercrime

Liberty Reserve was a Costa Rica based financial services company founded in 2006. It allowed people to send and receive their payments without revealing their account numbers or real identities. The currency used in this bank was LR, which could further be converted into dollars or euros. The company stopped operating in May 2013 since it was a hub for multiple money laundering cases.

Case study:

In January 2013, two youths targeted a B.Com student with the intention to kidnap him and then demand a ransom from his family members. To carry out their plan, they first befriended the person on facebook and started communicating with him. They got to know that he was studying for an examination and they offered question papers to him. To get the question papers, they called the boy to a remote location at night. The boy listened to them and went to the remote location. The two youths kidnapped the boy and killed him brutally. Then they sent a ransom message to the parents of the kid and demanded that 16000 LR be deposited in the Liberty Reserve account number that they specified. The kidnappers sent the message through their mobile phones which was traced within 3 days and they got caught, however the kid did not survive.

Modus operandi:

The two youths here used the modus operandi of kidnapping and then demanding a ransom. However this was not a conventional method adopted. If they manually tried collecting the ransom, then they would get caught. Hence they used Liberty Reserve's anonymous feature and demanded that the ransom be deposited in their account. Since Liberty Reserve does not disclose any of the personal information, they would be protected from being traced through their accounts.

Major takeaway:

The young boy accepted the friend requests of the two people even though he did not know them personally. The major takeaway from this case study is to avoid talking to strangers online and to always be skeptical if you are being called to a remote location by a stranger. It would still have been fine if he was being called to a public place or if he had been called in the daytime where there would still have been a lot of people around.

QR Code Scam

A QR code scam involves a cybercriminal pretending to be interested in buying a particular product from a person. The criminal then shares a QR code with the victim asking him/her to scan it so that the amount would be paid to the victim for the product.

The criminal usually targets the people who are vulnerable and who follow instructions without questioning.

Case study:

In February 2021, a young woman put up a sofa on sale on the popular e-commerce platform, OLX. She was approached by a man who was interested in making the purchase. To check if the account details shared by her were correct, he initially transferred a small amount of money into her account. Subsequently, the man sent a QR code to the seller and asked her to scan it so that the amount fixed under the deal could be transferred to her account. To do this, she had to enter her UPI pin after scanning the QR code. However, after she did this, Rs 20000 got deducted from her account.

When she enquired about it, the man said that he had sent the wrong QR code by mistake and sent another link to her, asking her to follow the same procedure. After she followed the instructions again, another amount of Rs 14000 got deducted from her account.

What went wrong here?

The girl here was naive and followed the instructions without second thought. She could have stopped the second time and understood that the man was a fraud after he got 20000 from the first QR code scan, but she continued and hence lost an extra 14000 rupees. She was also unaware of the common scam techniques that cybercriminals employ in such platforms.

How could she have prevented the mistake?

The girl could have prevented the mistake if she was aware that QR codes can never be used to debit an amount to a person's account. It can only be used to receive an amount which is specified. The best way to deal with this situation is to stay calm and composed. A UPI pin is not necessary while receiving a payment, it is only necessary while making a payment. So when the buyer asked her to scan the QR and it showed the option to enter her PIN, she should have immediately cancelled the transaction.

Robocall Scam

In January 2021, an Indian national from Ahmedabad, Gujarat was caught in an identity theft and for being in connection with a robocall scam which defrauded thousands of people in the US, and led to a loss of 8 million dollars.

Case study:

A 39 year old man operated in a call center in Ahmedabad, Gujarat that placed automated robocalls to victims in the US. The victims were mainly elderly people who could easily be duped. After establishing contact with the victims through these robocalls, the criminal and his other colleagues at the call center would trick the victims into sending huge amounts of cash through physical deliveries or through online money transfer.

To convince the victims, the criminals used a variety of methods including using the identity of law enforcement officers, DEA officers and representatives of other government agencies such as the Social Security Administration to threaten the victims with legal and financial consequences.

The gang then hired a network of money mules (a person who transfers money obtained illegally through some courier service or electronically) and gave them fake identification documents so that they could transfer money without any hassle. This money was then deposited into multiple accounts which ultimately reached the criminal.

Why did the people listen to the criminal at all?

People generally tend to believe robocalls as they sound more professional and legit. Above that, the victims here were mainly elderly people who are generally weak when it comes to technical knowledge and hence they were vulnerable to the calls and followed what was told to them.

How could they avoid being defrauded?

Again, the most important way to avoid getting defrauded is by being aware. The elderly people trusted the robocalls and complied with its instructions. Always stay skeptical of any phone calls from random phone numbers and make an informed decision. Another way to avoid getting continuous phone calls is to block numbers that are not stored in the mobile phone.

Business Email Compromises:

Business email compromise attacks are cybercrime techniques which are employed by criminals to dupe commercial or government organizations by using email fraud. The hacker may employ phishing techniques or invoice scams to gather data for other criminal activities which the hacker might attempt in the future.

Case study:

In a middle sized company in Bangalore, a hacker once sent a phishing mail to the accounts person in the company stating that her mail account was deactivated and that she needed to click on the link to activate it again.

The woman clicked on the link and she was prompted to enter her email address and her password. She entered her details into it and the window then closed off. After an hour, she received a phone call from one of the banks where the company deposits money asking her if she had sent them a mail to transfer 10 lakhs rupees to a bank account. She was shocked and denied immediately. She got worried and immediately called another bank which the company also deposits money to and asked them if they had made any transfers. The bank agreed and said that they had received an email to send 10 lakhs to a bank account based in Mumbai, and had sent the money as according to the email they sent. The woman immediately told the bank to stop the transaction and to freeze the account. She also asked the bank to send copies of the email so that it could be used later for further investigation.

The woman came back to her office and noticed that the emails were indeed sent from her account and they were found in the trash folder of her account. She made an FIR about the incident and reported the incident to the first bank. She was refunded the amount she had lost by the bank.

How was the hacker able to send the emails to the banks?

The hacker had sent a phishing mail to the woman which was disguised as a mail to activate her account. When the woman entered her email account details, the hacker was able to store the information in his own database because the website was fake. The hacker then attempted to login to the woman's account using the credentials that she had provided. He then checked the sent folder to understand the type of transactions that take place between her and the banks and then replicated the same, entering his own bank account details this time. After he sent the mail to the bank to transfer the money to his account, he deleted the email and logged out of the woman's account, thus making it seem like nothing had happened.

What could the woman have done to stop the incident?

The woman should have enabled security for her email account. She was unaware of the different security practices for her email account and thus, she was vulnerable to the attack . She should have enabled 2-factor authentication so that the hacker would not be able to enter the account without the OTP sent to her mobile phone. The banks should have also checked with the company first before transferring the amount immediately, considering the huge sum involved.

SIM Swapping Case:

SIM swap scams are one of the most damaging and high-profile scams in the modern era. In SIM swap cases, the attacker hijacks the victim’s phone number and assigns it to the SIM card owned by the fraudster. These mobile numbers are usually linked with our banks, emails and social media accounts and hence this cybercrime is very dangerous.

SIM swapping process:

The fraudster first acquires the user's personal details through phishing or through the dark web. After this, the fraudster calls the telecom operator and requests them for a number transfer. Once the telecom provider ports the number into the fraudster’s SIM, the fraudster is now able to receive the victim’s SMS and phone calls. The fraudster is also now able to bypass other security issues which were difficult to penetrate like 2-factor authentication because now the OTP code will be sent to the person directly. The hacker is now extremely powerful and can use your details to steal all your confidential information and empty your bank account.

Case study:

In a recent case in the eastern part of India, a woman who worked in a firm lost around Rs 42000 in a SIM swap fraud. The woman lodged a complaint against the police and alleged that her SIM cards became inactive for over two hours. When the SIM card became active again, she failed to book her flight. She called her bank and got to know about the fraud that had taken place. There were a total of 13 transactions that had taken place using her bank accounts using her credit card details. All of these were done in the duration that her SIM card was inactive.

She had actually received a phishing email on the pretext that she had to upgrade her mobile's SIM. She was asked to enter her 20-digit SIM card number and Aadhar card details. After she entered the details, within a few hours, her SIM card became inactive and the fraudsters made the unauthorized transactions from her bank account.

How do you prevent SIM card swap cases?

Make sure that you do not reveal your SIM and personal details over a mail. These are always phishing emails that want to steal your information. Also make sure that the software you use on your phone is updated regularly. Install apps from trusted sources and always keep your data private.

What do you do if you have noticed that your SIM card is not activating?

Do not wait long, make a call to your telecom provider and tell them immediately that you did not make the changes to your number. They will help you recover your number and minimize any further losses that could have happened with your bank account and information.

Sextortion:

Sextortion is a way of extracting money from a victim by blackmailing them into revealing their private pictures and videos. This form of cybercrime is spreading very fast in India and needs utmost attention and awareness amongst the people. Victims of sextortion are ashamed of talking about it to the people around them and e is really shameful to the victims and they do not like to talk about it, hence the attackers are able to blackmail them into giving more and more money in exchange for not leaking their pictures and making them viral.

Case study:

Usually we read about women being the victims of sextortion. A new variant of sextortion has been trending recently which targets men.

A man was casually scrolling through his Instagram feed when he read one of the comments by a woman having a very attractive profile picture. He went to her page and saw that her bio had different links to talk to her and it also had her WhatsApp number. She was offering to do nude video calls with people for a price. The guy was unaware that this was not a real profile and it was actually a man operating the account to trap people into calling on that number. He saved the contact number and messaged the woman on whatsapp and paid the price for the call. The person behind the account then asked the customer to be ready and to be nude as during the call.

The man complied and got nude on the call. The criminal then played a pornographic video which looked like a woman was removing her clothes and the man had fallen for the trap. The man took screenshots and recordings of the victim during the video call and then after a few hours sent them to the victim and blackmailed him that he would make them viral on the internet if he did not receive Rs 50000 from the victim. The victim did not want to approach his family and the police because he was worried and embarrassed that the people around him would get to know that he was trapped and that he would have a bad image. The victim paid the money but this cycle continued over the next few days. The victim did not have money to pay and was begging the person to delete the pictures. The attacker did not delete the pictures and instead uploaded them on the internet. Out of guilt and embarrassment, the victim committed suicide the next day.

How do you identify such cases in social media?

A lot of sextortion cases have been reported from the people who post spam comments on Instagram and Facebook telling people to call them for a good time.

These profiles usually have an attractive picture to lure people into calling them.

Always avoid profiles which have attractive photos and which offer to have nude calls with you. Most of these are fake and want to make you the next victim of sextortion. If someone asks you to be nude or intimate and there is a chance that you will get recorded, then reject the offer so that there is no chance of getting blackmailed in the future.

What should you do if you have become a victim to sextortion ?

You should immediately tell your near and dear ones and then file a report to the nearby police station. Do not panic and do not fall for their blackmail traps. Trust the police to solve your case and track the culprit. If you are a girl and are afraid of revealing your identity, then you can file a complaint anonymously on the Nation’s cybercrime portal : cybercrime.gov.in.

Germany Synthetic Audio Case:

We already read about deepfakes being used in cybercrime a few chapters earlier. However this is not the only implementation of Artificial Intelligence being used in cybercrime.

Case Study:

In Germany, cybercriminals used Artificial Intelligence to make a software which can impersonate people's voices. They used this software to demand a fraudulent transfer of $243,000 dollars.

The CEO of an energy company in the UK thought that he was talking to his boss who was the owner of a German company. In the phone call, the owner told the CEO to send the amount specified to a Hungarian supplier. The caller told the CEO that it was an emergency and the amount had to be transferred within an hour itself. He received the bank details from the owner and transferred the amount to the supplier. The supplier was actually fabricated and the bank address actually pointed to the address of the caller. This way, a synthetic audio of the actual owner was used in such a way to appear as though the actual owner had called the CEO and given the orders.

How did the cybercriminal pull this off?

The cybercriminal first got the contact details of the CEO by hacking the owner's device. He then got records of the owner's speech and then used a machine learning algorithm to train it to speak a script that the criminal had written. The software was successful in replicating the owner's voice and it was very difficult to differentiate between the real and the fake voice. The criminal then called the person and used this voice spoofing technique to fool the receiver into believing the voice and complying with the orders.

What can you do in this situation?

This was a case where the user would need to apply his logic and think if the case was actually real or not. You can always call back the person to reconfirm the details to make sure that the call was legit. Apart from this there is no other way to verify if the person talking was real or not. The next best bet would be to develop a software which can detect fake voices but that would require investment into building such a software and hiring people who are skilled enough to do the job.

Final Words

Congrats on finally reaching the end of this book! We hope you had a great time learning about the different types of cybercrimes and their prevention strategies. You are now equipped with all the knowledge you need to start protecting yourself online. It is now your turn to implement whatever you have learnt in this book in the exercises that follow, as well as in your day to day lives.

As you have already read earlier, there are five types of people - the people who were needy (Job-frauds), the people who were greedy (Lottery-frauds), the people who were ignorant (sharing of OTP), the people who were negligent (used pirated software and did not update software, antivirus), and finally the people who were not at fault (Deepfakes). It is now your role to learn from these people and be responsible for all the actions you take online. Use apps like VirusTotal to verify legitimate links that you receive from messages, make sure your devices and accounts are secured by 2-factor authentication. Always preserve primary electronic evidence you have so that you would be able to present them in case you get victimized. Keep the number 1930 in the back of your mind, so that you can contact them whenever you have been scammed or duped. Go ahead and make friends online and connect with people, but always remember that no one offers anything for free. Finally, know yourself on the internet and be wary of any information you share online.

The Cyber world is huge and can be nasty to people and it is our role as netizens to be aware of the possible consequences of being online. A little practice and knowledge is all that a person needs while trying out a sport for the first time. Similarly, when you inculcate good habits and practice cyber hygiene, you will be better prepared to face challenges that may arise in cyberspace. All data that we put up on the internet, can be used by someone in another part of the world for exploitation purposes, and it is important to be psychologically prepared for anything. We hope that this book provided a clear perspective of how to approach the internet and digital data and has made you able to take informed decisions and be more confident. With the increase in technology and gadgets, the scope for exploiting people has amplified a lot, and we hope you have now gained a new perspective on them as well. Situations will demand you to stay away from devices and to carefully analyze them and the control that these devices have on your lives. It is your responsibility to ensure that you and your loved ones are safe online.

Thank you for reading Cybercrimes and Cyber Hygiene and wish you all the best in your journey to protect yourself online.

Exercises

"Any informed borrower is simply less vulnerable to fraud and abuse"

- Alan Greenspan

1. Have you enabled 2-factor authentication for the social media platforms that you have just mentioned?

2. When was the last time you changed your password?

3. Out of all your "friends" online, how many of them do you actually know personally?

4. Do these "friends" contact you frequently?

5. Do you use the same account for online transactions and social media?

6. Have you shared your password with anyone (family, friends, relatives, strangers, etc) ?

7. Have you followed any safety measures to safeguard your online presence?

8. Are your family and friends aware of these safety measures?

9. Now that you are aware of the different cybercrime types and their prevention methods, think of a real life scenario where you or your friends/ family might have been a victim of a cybercrime. Write down what happened.

10. What did you do after getting victimized?

11. What steps did you follow to receive compensation for the crime?

12. After reading this book, what steps could you have taken to prevent the crime in the first place?

13. Do you browse the internet or check the news to stay aware of the different trends in cybercrime?

14. Mark a date on your calendar when you will follow all the online security steps mentioned in the book. Promise yourself to complete them.

15. List the safety measures that you have adopted.

16. Note down the details of the nearby bank branch in your city. (Location, branch, Bank manager, important contact details, helpline number, etc)

17. Note down the details of the nearby police station and the cyber cell with whom you can contact immediately in case of cybercrime.

18. Write down the details of the IT secretary of your state

19. Pen down any safety measures that you have come across from different sources and from the personal experiences of your friends / family.

20. What have you noticed after following the different prevention measures after a week?

21. What have you noticed after following the different prevention measures after a month?

22. What have you noticed after following the different safety measures after a year?

23. What is your major takeaway from this book?

____

____

____

____

____

Social Media Protection Guide

Follow these steps to ensure your security on the most popular social media platforms on the internet. Time to protect yourself from getting hacked!

Gmail:

1. 2-factor authentication

- Open your gmail account.
- On the right hand side of the screen, select your account and click on the manage my account button.
- Open the security tab
- Click on 2-factor authentication and then enter your account and password.

- Enter the phone number of the device which should act as the device to authenticate your account.
- Enter the OTP code which will be sent to your mobile device.
- Once you have entered the OTP code, your account will now have 2-factor authentication enabled.
- Now whenever you/ or someone else logs into your account, before accessing it, a code will be sent to the device which you have selected for authentication. Only after entering the code will the user be able to login to his account on another device. This ensures that hackers will not be able to access your account from a remote location as they do not have access to your mobile device.
- You can also create printable backup codes and a backup phone number as alternatives for accessing your account. However you’ll also need to make sure that these details are not accessible to the hackers.

2. Set a recovery phone number and recovery email (should also be secure)

- To set a recovery phone number, select your account and click on manage my account button.

- Open the security tab and you will be able to see the box for entering a recovery phone number.
- Enter the phone number that you wish to use to recover your account in case of a hack .
- Enter the code which will appear in your text message box in your mobile device.
- Go back to the security tab and then select the recovery email option.
- Enter the email address of the account that you wish to use as a recovery.
- Make sure that this account is also secure using 2-factor authentication and the other safety measures that have been discussed.
- Enter the verification code that has been sent to the corresponding gmail address.
- Now this email address will be used to recover your google account in case of a hack.

3. Revoke access to 3rd party apps which you don't know about or which you have forgotten completely.

- Open the security tab after selecting manage my account from your gmail account.
- Scroll down until you see the option “Manage third-party access”
- After clicking on the link, you will be able to see

all third party applications which have access to your gmail account.

- Remove the applications which you are unaware of as they may be controlled by hackers.

4. Log out of devices which you are not aware of.

- You can also view all the devices in which your gmail account is currently logged into.
- Select the manage my google account and open the security tab.
- Scroll down until you see the option “Manage devices”.
- You will be able to see all devices and the operating system in that device. If you find any device which you do not identify, then immediately log out of that device by clicking on the three dots -> sign out.
- Also change your password, as the person who logged into the device has your password and can access it again.

5. Complete the security checklist.

- Open your gmail account and then click on manage account.

- Select the security tab and then click on the linn "Protect your account".
- Make sure to follow all the security guidelines and make sure you have green ticks in all the options that follow.
- Make a habit of rechecking your security checklist quarterly to ensure that there is no unusual activity going on with your account.

6. Check for IP addresses of your account login.

- This step can only be done on your computer.
- Click on the link to view the last 10 devices which have logged into your account.
- You will be navigated to a site where you can view the recent logins and the IP addresses of those logins.
- If you find any logins suspicious and cannot recall where they are from, then log out of that device immediately and change your password as a hacker might have already gained access to your account.

7. Turn on screen locks for added security.

8. Remove apps and browser extensions which you don't need.

9. Avoid suspicious requests, emails and web pages.

10. Regularly update your operating system because your email security depends on the security of your device. Make sure to update your OS and your browser regularly. The latest updates usually patch vulnerabilities hackers can use to break into your device.

11. General safety measures:

- Use safe and secure passwords. An ideal password should be a combination of lowercase, uppercase letters, numbers and special characters. To create a password for your account, you can use a password manager.
- Keep your password protected. (never enter your passwords on unsecure and unknown websites or the websites whose links you get on email).
- Try to avoid signing on public computers. (If you have to use it, then you must do the following things):
- Use incognito mode for signing into your account.
- Never forget to sign out when you are done.
- Clear browsing history, cache and cookies after signing out.
- Use a strong password: numbers, characters(upper and lowercase) and special characters.
- Use the right security question (not questions

which have easy to get answers as they can easily be found on social media)

- Avoid public wifi, they're insecure and make the jobs of hackers easy
- Never put your email id and password together. People put them together so they won't forget it.
- Don't share your login information. Sometimes we share login info for registration on some websites. For such cases, it is recommended to use a dedicated account for such sites instead of linking your personal account.
- Check your devices for viruses and malware.

12. Check your account filters for forwarding emails

Need to check if there are active filters in your account which are forwarding your emails to third party email addresses. You can check this by going to gmail settings and clicking on the filter tab. Look for the filters that you have not authorised and delete them. Also, check the POP/IMAP tab to ensure that there is no unauthorized forwarding address other than those approved by you.

Authenticate your emails when sending sensitive information: While sending your email, if you see a red lock beside the sender's address, then it is not safe because the person can get your passwords or other sensitive information. Avoid sending mails to these people.

13. Detect and block email trackers: People and companies can track how many times you have read their mail. You can block this by installing extensions?

14. Don't share your Gmail passwords and use Shared Inboxes instead (incase you belong to a team in an organization and use a common email address to send mails. Instead of getting the password, use shared inboxes for the group email address. This will allow you to invite relevant team members and let them manage group emails together directly from their respective inboxes.)

15. Add Password Alert to your Chrome browser. With this, you will be able to get security alerts when your google password is being used to sign in to some non Google sites.

In Google Chrome, sign in to your google account. Then go to the Chrome store and download Password Alert. Then follow all the onscreen instructions. Finally sign in to your google account again to get started.

Facebook:

1. Two step authentication. You don't want people to be able to log into your account from another device or from incognito mode. To prevent hackers from being able to log into your account, then enable facebook two step authentication.

In the computer:

- Login to your facebook account.
- Click on the account button at the top right part of the screen.
- Select the settings and privacy option.
- Open security and login.
- Check the option “Use two factor authentication . ”
- Now enter the password of the account.
- Select your authentication method. We will use a mobile phone for this tutorial.
- Enter the phone number of your mobile device and wait for a code to be sent to your mobile device through SMS.
- You can also add backup methods to recover your

2. Choose a strong password: Ideally it should be a random string of characters consisting of numbers, symbols,

special characters and lowercase and uppercase letters. It is advisable to use a password generator and a password manager to secure your accounts.

- Click the accounts button in the top right part of the screen.
- Select Settings & privacy, then click Settings.
- Click Security and login.
- Click Edit next to Change password.
- Enter your current password and new password.
- Click Save changes.

3. Protect your facebook password: Don’t use the same password anywhere else on the internet. Don’t share the password with anyone.

4. Never share your login information.

Scammers may create fake websites that look like Facebook and ask you to log in with your email and password.

Always check the website's URL before you enter your login information. When in doubt, type www.facebook.com into your browser to get to Facebook.

Don't forward emails from Facebook to other people, as they may have sensitive information about your account.

Logout of facebook on the computers which you share with other people .

5. Logout of devices remotely: You can log out of the devices remotely which you don’t know about. This can be done by opening the settings -> security and login -> where you’re logged in.

This will show a list of the devices which are currently logged into your account and their last activity.

You can choose to end the session for the device that you are not familiar with or which you don't use often by clicking on the three dots beside the device. After doing this, make sure to change your password, so that if someone had access to your account earlier you will not be able to get into your account.

6. Set up trusted 3-5 friends to contact in case you get locked out of your account.

How this works is that your trusted friends will send you a special recovery code and a url which when you click on will allow you to reassess your account.

Settings -> Security and Login -> Choose friends to contact if you get locked out -> Enter 3-5 facebook friends.

7. Don’t accept friend requests from people you don’t know about.

8. Lock your facebook profile.

No stranger will be able to see your media and all the posts that you put out.

- Can be done only on android smartphones and not ios phones.
- Open facebook -> go to profile -> tap the three dots icon -> tap lock profile.

9. Never click on any suspicious links in your facebook messages or from random posts.

10. Make sure to follow the privacy check up on facebook and follow all the instructions.

Open facebook -> Click on settings and privacy -> Click on privacy checkup -> You will see a list of many check ups that you can do. Open each of them and follow the instructions to make sure your account is safe and private.

Whatsapp

1. Enable 2-step verification in your Whatsapp account.

- Tap settings, then Account.
- Tap two step verification.
- Enter a pin number and make sure you remember this pin number so note it down somewhere.
- Enter an email address which can be used to change your pin at a later time whenever needed. (make sure that this is an active mail and you remember the password of this mail, and ensure that this email is also safe by the security features discussed earlier).

So if a hacker tries to open your account on his device by getting your mobile number, then an OTP will be generated to the mobile number that has been specified. This is pretty safe, but let's say the hacker got access to your OTP. After that he will be asked for the 6 digit pin which only you know. If he tries to reset the pin, it will again be a difficult task because the email address registered will be yours and he will have to hack your email account to reset the pin. This makes the life of hackers very difficult and hence it is safe.

2. Lock your whatsapp using fingerprint,

- To do this:
- Go to settings.
- Account -> Privacy.
- At the bottom of the screen there is an “Unlock fingerprint” option.
- Tap the option and then place your fingerprint and select the duration after which the phone will automatically lock itself.

Now you can unlock your phone using your fingerprint and any other person will not be able to access your whatsapp.

3. Set your profile photo and your abouts to “My contacts” so that you remain anonymous to the people who do not have your contact details and who don't know you.

Again this can be done by going to settings -> account -> privacy.

4. Stay aware of whatsapp forwards: This is the most important step and a lot of people get cyber victimized because they are unaware.

You should not blindly trust any links that you may receive through whatsapp forwards. Don’t go clicking any link that comes to your groups or chats. These can be spyware which can be used to steal information from your mobile device and browser. You can use some apps like VirusTotal to check if a link is safe or not. Paste the suspicious link in this app, the app will flag the link if it finds it to be unsafe.

5. Don’t download any random softwares on whatsapp. Although whatsapp messages are encrypted when they are sent from one person to another, they are not encrypted on the phone itself. So if you download a spyware from a random link, it may read your messages and then activate other functionalities like a camera on your device.

6. Keep your whatsapp updated to prevent hackers from exploiting any loophole.

7. Avoid giving your phones to strangers, because they can install malware or a spyware to spy on your device, thus compromising your whatsapp chats.

8. Check if your whatsapp backup is actually going to your email address or to another person’s address. Settings -> chats -> chat backup

9. Check the devices which your whatsapp web has been logged into and avoid sharing the qr code for your whatsapp web. If you find any device which you cannot recall, then immediately log out of all devices and make sure that you have enabled 2 step verification.

10. Turn on security notifications by going to settings -> account -> security. This will tell you about any suspicious activity on your account, however it does not prevent the hack from happening in the first place.

Emergency Action Guide

Q. What should I do if someone makes an unauthorized transaction from my account?

Lodge an FIR immediately at the nearby police station and contact the helpline number **1930** (available 24x7) to report the cybercrime. Inform the bank immediately within 72 hours so that you can receive compensation in case the bank transaction was not your fault.

Q. What should I do to report cases of cybercrimes happening around me?

Report the case to the cyber cell of the nearby police station, or you can file a complaint online at the national portal for cybercrime: cybercrime.gov.in. Once you file a complaint at this site, you will receive an email which will direct you to the police station you can report the case to. You can also contact the cybercrime helpline number: **1930**

Please make sure that you report to the correct organization, A case has been reported in Delhi, where people posed as Government officials running an online redressal system. These people cheated the individuals who tried to lodge a complaint regarding cybercrimes. They charged the victims processing fees of up to thousands of rupees just for making the complaint. One such portal was Jansurakshakendra.in which claimed to be a crime reporting portal.

The victim contacted the number provided on the website, who informed him that they are authorized persons working with the Government.They charged a fee of Rs 2850 and assured the victim that his case would get lodged under appropriate legal sections. After the payment, they blocked the people who contacted them.

The alleged persons had cheated the public for up to Rs 1.74 crores and around 3000 victims had been cheated by this scam. There are innumerable websites with similar names which pretend to be government agencies to address your complaints, but these are all fake because no government office charges any processing fee for putting government resources into action.

Q. What should I do if my Gmail account gets hacked?

- Change the password of your Gmail account if it has not been modified yet.
- If your account password has been modified and if you have enabled recovery through your mobile phone, then select "forgot password" while trying to login, and enter the recovery code that will be sent to your mobile phone and change into a strong password.
- Enable two factor authentication.

Q. What should I do if my Facebook account gets hacked?

- If you believe that your account has been hacked, then go to the link https://www.facebook.com/hacked and select the button "My Account is Compromised" and then follow the instructions that follow.
- Facebook will help you recover your account that has been compromised.

Q. What should you do if someone makes a fake profile of your account online?

If someone has created an Instagram account pretending to be you, you can make a report directly to Instagram.

If someone has created an account similar to yours on Facebook, then:

- Go to the profile that's impersonating you (If you can't find it, try searching for the name used on the profile or asking your friends if they can send you a link to it.)
- Click the three dots on the cover photo and select Report
- Follow the on-screen instructions for impersonation.

If someone has created a fake account on Twitter with the purpose of defaming you and putting out deceptive pictures, then you can open the Twitter help center and give in your details.

Q. What should you do if someone gives you an offer which seems to be too good to be true?

Ignore such calls as they are always false. No one offers anything online without a secret agenda. Please understand this!

Q. What should you do when you receive a whatsapp message from someone about something serious?

Always verify the source of the news! A lot of people spread fake news and propaganda to further their causes and you might be helping them by forwarding the same message to other people. Look online for the same message that was sent and you will almost always find a news article that tells you that the message is fake. Don't forward messages blindly!

Q. What should you do if you receive a link for some offer on whatsapp or some other social media platform?

First of all check if the link is safe through an app like VirusTotal.

If the app does not flag the link and it is safe to use, then open the link, otherwise delete the link and educate the person who sent you the link so that he/she will not share it anywhere else.