



CYBER GYAAN

By:
IT Awareness Team
Digamber Capfin Limited



Disclaimer

The information provided in this book is for educational purposes only. It is not intended to hurt any religious sentiments of any person.

We have collected data from various sources and do not take any credits for the same. The information belongs to the original owner only.

The Company does not assert any claim on the information, graphics or photos collected from third parties.

This is a work of fiction. Any names or characters, businesses or places, events or incidents, are fictitious. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.



Character Introduction

Hello Readers!

Let us meet the main characters of the Comics.

Meet **Reena!!**



She is a our Gyaan Guru. She is a cyber responsible woman who uses technology in an informed manner and believes in spreading awareness about the Cyber Security.

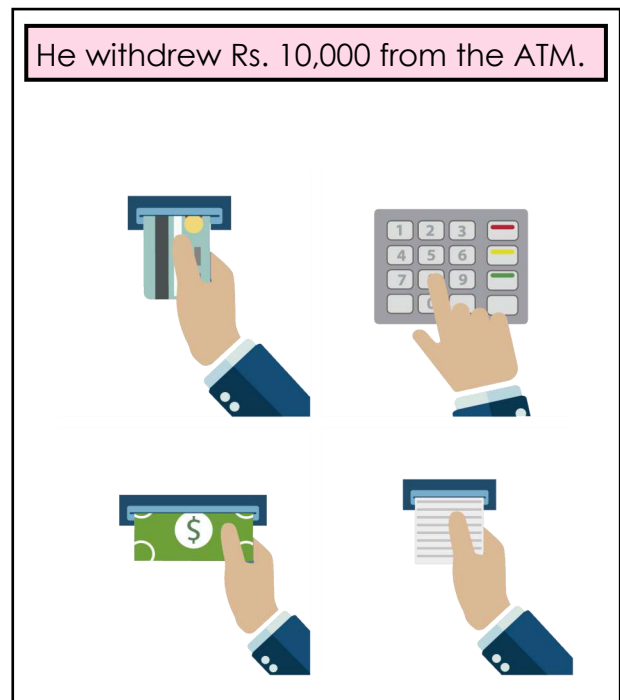
Meet **Vishal!!**

He is a friend of Reena, our Gyaan Guru. He is not well acquainted with the uses of technology and often gets himself involved in the risky situations and then needs the help of our Gyaan Guru.

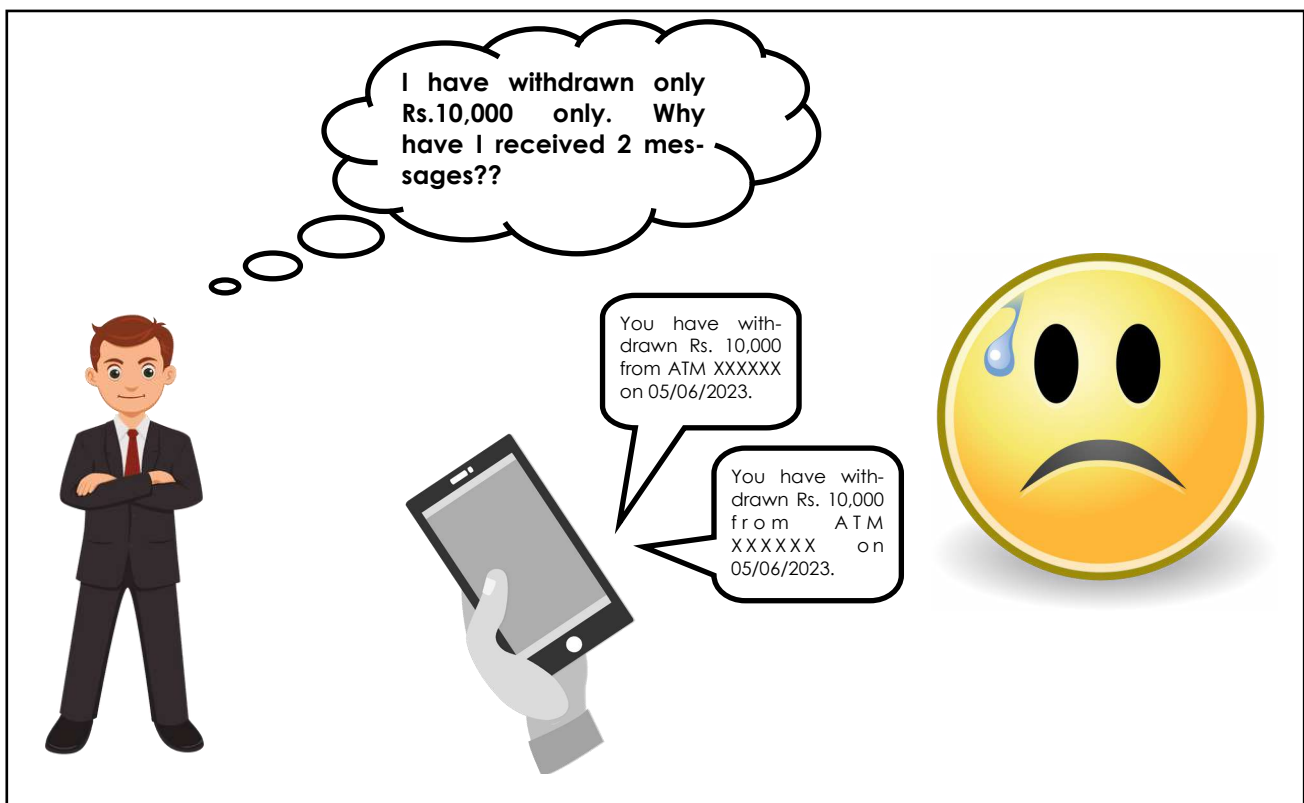


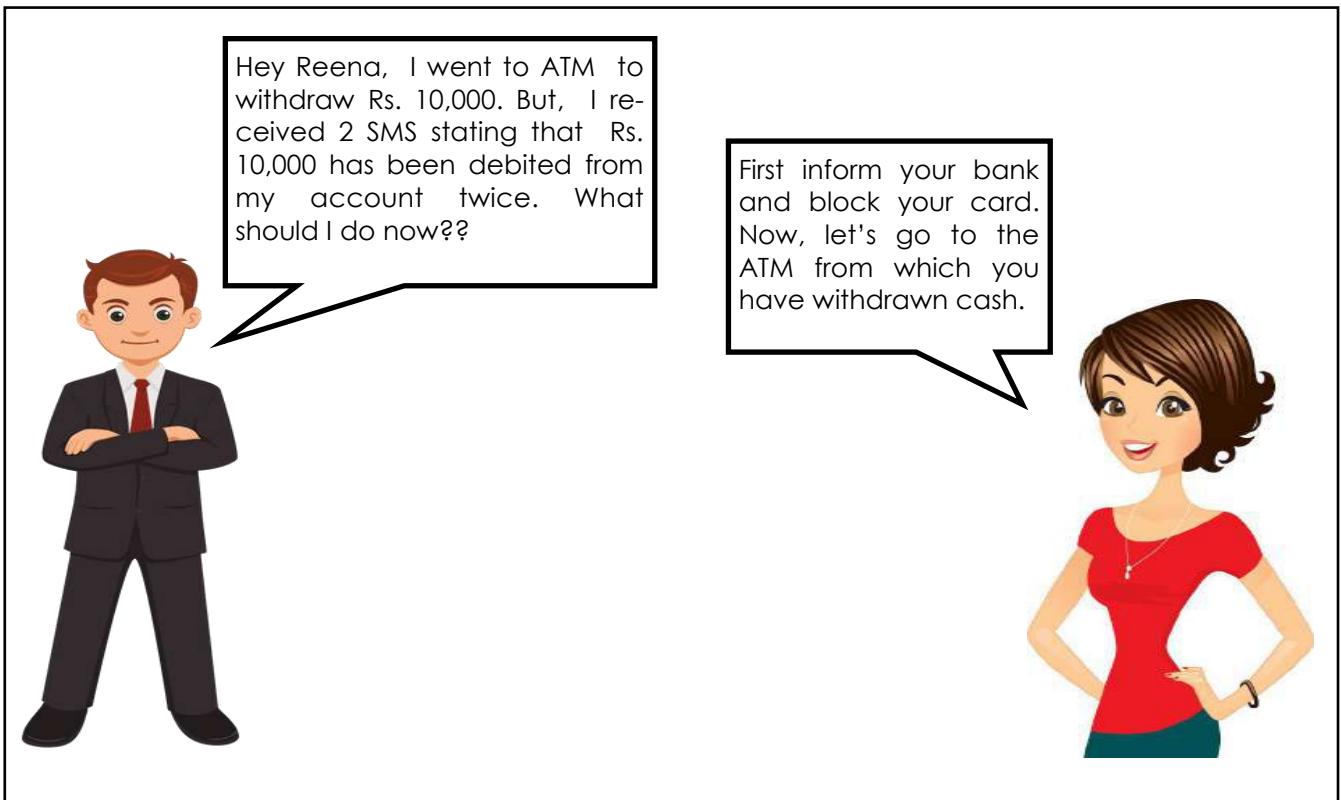


Chapter 1: Use of ATMs

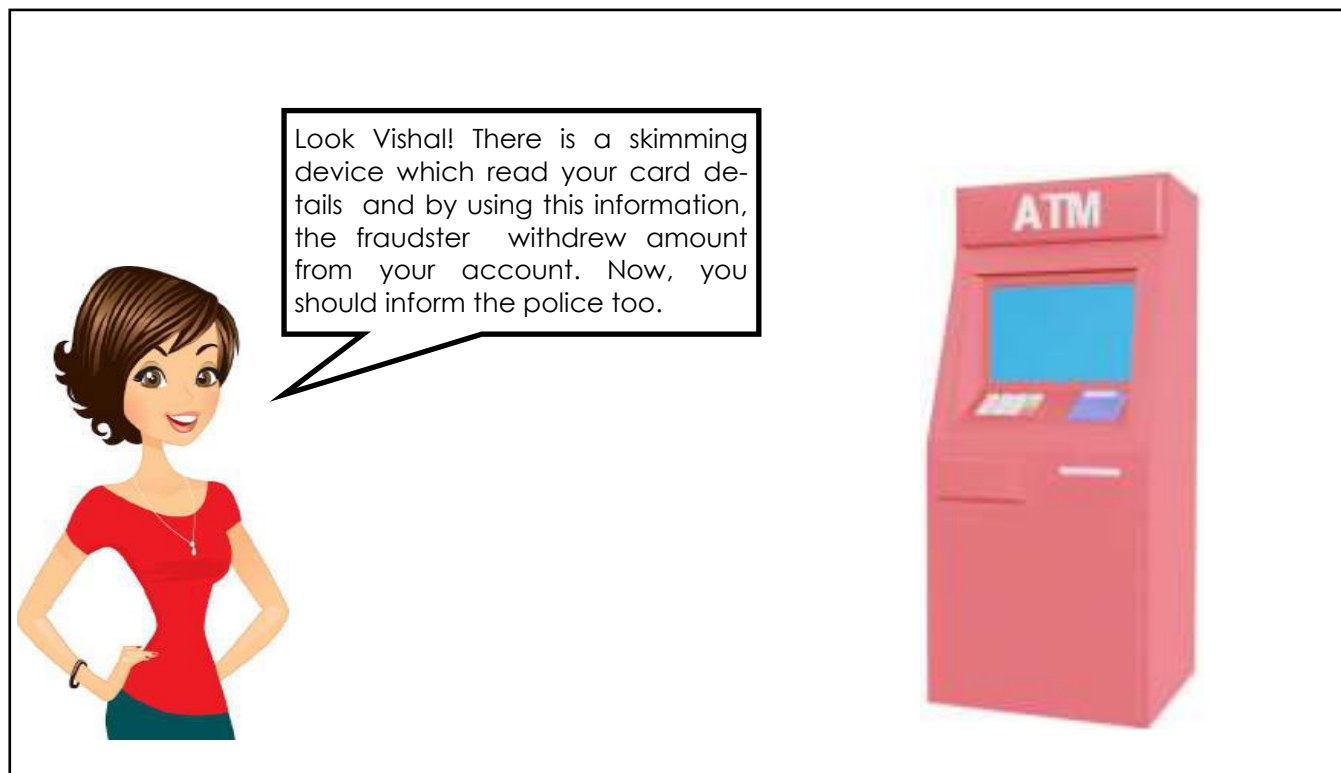


After sometime.....



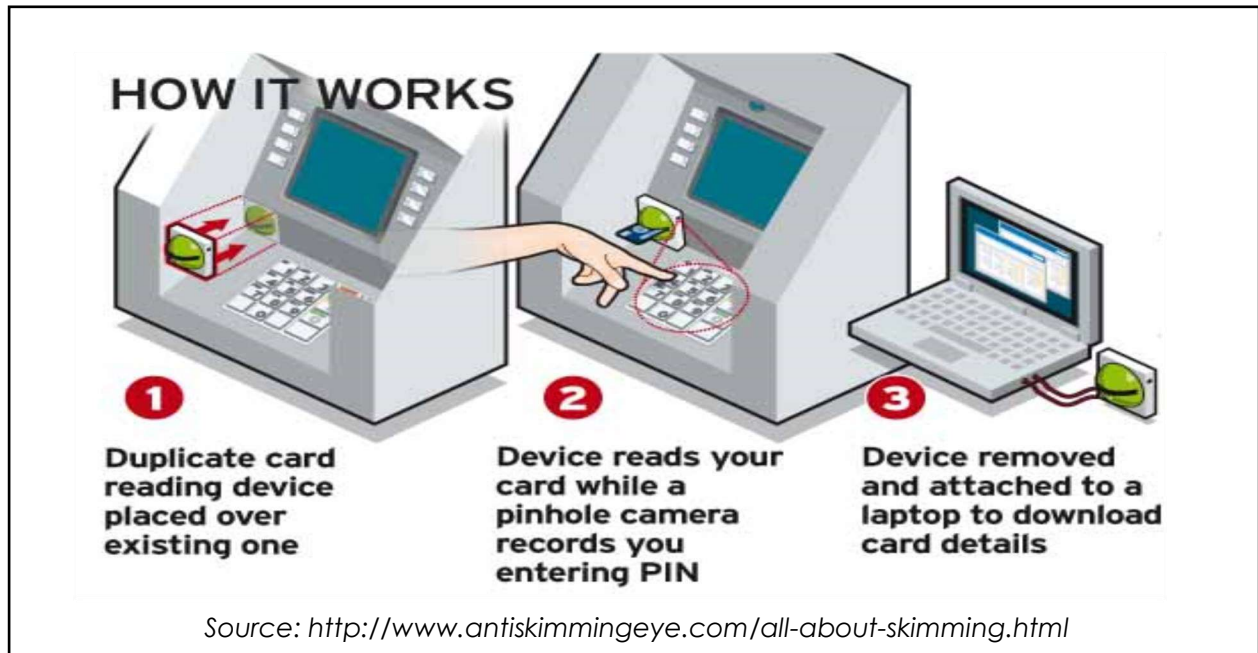


After reaching the ATM.....





GYAAN KA SAAR



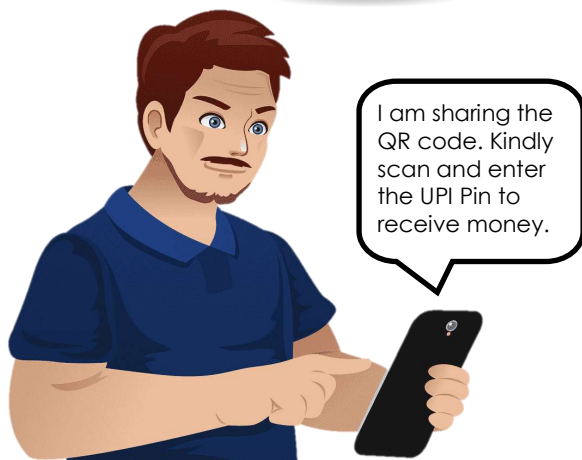
Precautions

1. Do not give your Debit Card or its details including CVV, expiry dates etc. to your family members, friends, relatives or any other person.
2. The money should be withdrawn by the cardholder only.
3. Use ATMs which are located inside the Banks.
4. Always remember to check the blinking of card reading slot of the machine. If it is not blinking do not use that ATM.
5. Report all the fraud incidences immediately on the helpline number mentioned on your Debit Card.
6. Shield your PIN from any hidden cameras by always covering the keypad with one hand when keying in the numbers.
7. If you find signs of tampering, or anything else suspicious about an ATM, don't use it, report the machine and go find another one.
8. Always press cancel button after completing your transaction.
9. Destroy the withdrawal slip after use.
10. Do not keep your cards unattended.



Chapter 2: QR Codes

Vishal posted an advertisement for selling his furniture on Resale Apps for Rs. 13,000. After two-days he received a message from Mr. X asking for the specifications of the furniture and then agreed to buy it.



Vishal scans the QR Code and enters the UPI PIN.





After scanning the QR Code

Instead of receiving the money, my account has been debited.!!

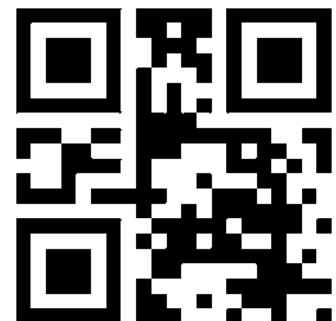


Vishal rushed to Reena

Hey Reena!! I posted an Ad on Re-sale Apps for the sale of my Furniture. A buyer contacted me and asked me to scan the QR Code provided by him and enter my UPI Pin. After scanning the code and entering my UPI Pin, instead of receiving the amount, the same amount has been debited from my Account. What should I do??



Vishal!! QR Codes are only for receiving the payments. Why did you scan his QR Code? The fraudsters also get access to your bank account details and use them later to do multiple transactions. You should first inform your Bank for the reversal of UPI Amount and then file a complaint at the Cyber Cell of the Police Station.





GYAAN KA SAAR



Precautions

1. Never ever scan QR code, if you are receiving an amount.
2. Never share your UPI ID or bank account details with people who you do not know.
3. If possible, you deal with cash if you are selling something on resale or other sites.
4. Even when sending money always cross-check the details shown by the QR code scanner.
5. Avoid scanning a QR code if it looks like a sticker covering another QR code.
6. NEVER SHARE OTP with anyone. OTPs are confidential numbers and you should treat them like that.
7. Always verify the identity of the person on an online website if you are selling or buying anything.
8. Try not to share your mobile number too if not needed.
9. Once you scan a QR code, check the URL to make sure it is the intended site and looks authentic. A fraudulent domain name may be similar to a URL with typos and misplaced letters.
10. You do not need to download any app to pay via a QR code.
11. Enable two-factor authentication such as fingerprints, Face ID etc. for passwords before making transactions through QR Codes.
12. Ensure trusted Anti-Virus software are installed in your phones.
13. Report any suspicious QR Codes to relevant authorities or organizations to help others.
14. If you recently bought something and you receive an email saying the payment failed and are asked to complete the payment through a QR code, call the company to verify this. Locate the company's phone number from a trusted site, not the phone number given in the email.
15. Avoid using a QR code to pay a bill. There are many other payment methods that are less susceptible to fraud.
16. Do not scan random QR Codes given in Newspapers, Restaurants, Social Networking Sites, Brochures, E-com shopping parcels, etc.

Chapter 3: Screen Sharing Apps



Vishal decided to buy an insurance policy and while surfing online clicked on an advertisement prompting him to enter his contact details to help an Advisor reach out to him.



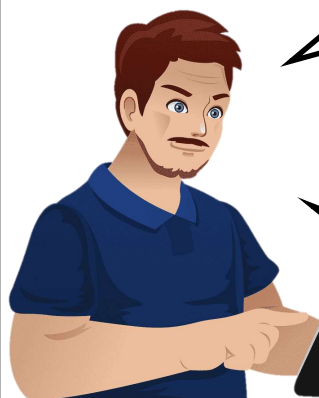
Cheapest Insurance
Starting from Rs.80/- per month
ABC Insurance
123, XYZ Building, New Delhi
Tel: 555 555 5555

General Insurance
With an attractive offer!!!!

Contact us to know more!!

Contact us!!

After sometime, Vishal receives a call from the “Advisor”



Hello Sir! I am Ajay from ABC Insurance Company and we have noticed your interest in our product. Are you looking for buying an Insurance? I am here to help you.

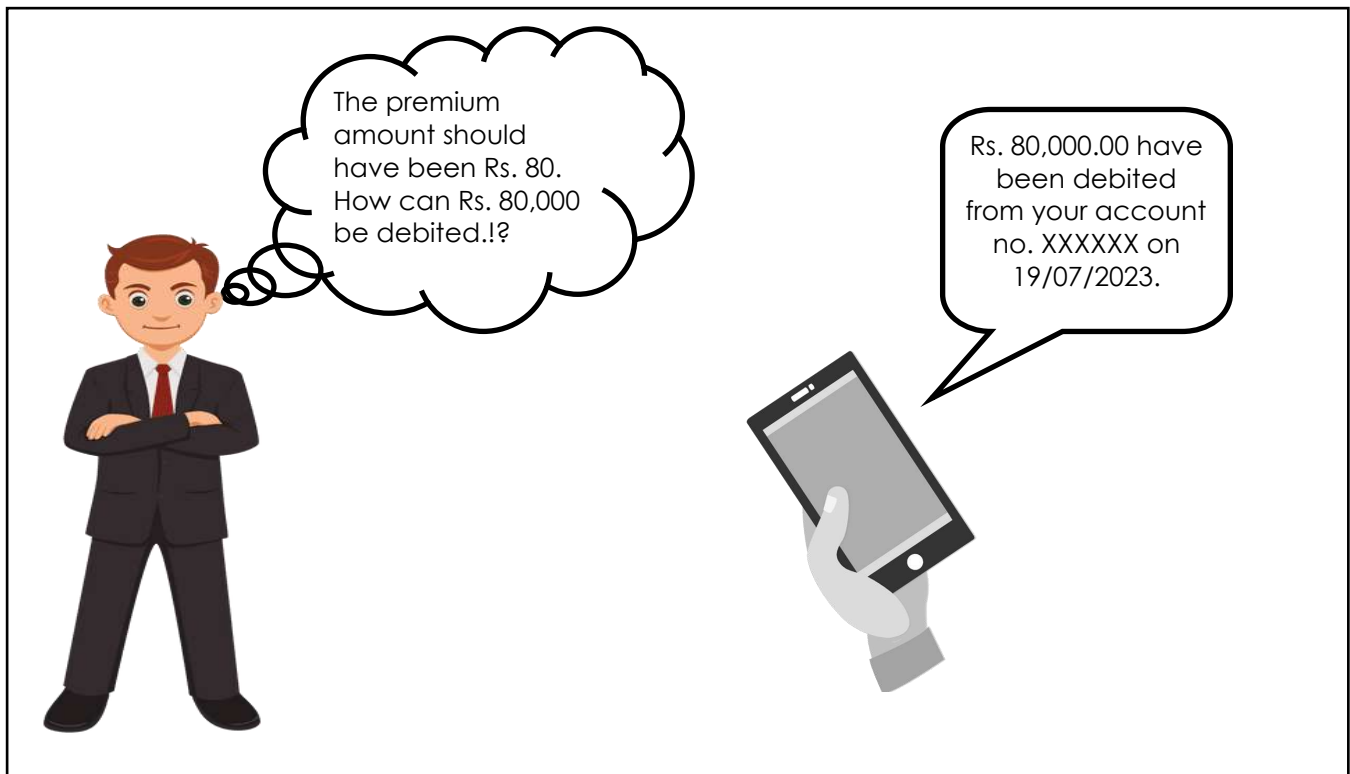
Hello Ajay! Yes, I am interested. Please guide me how to proceed further for buying the insurance.

Sir, for this you are requested to download the BCD remote desktop app from the link provided on your mail id. Then, I will help you with the payment of the premium amount. Please keep your card details ready for the payment.

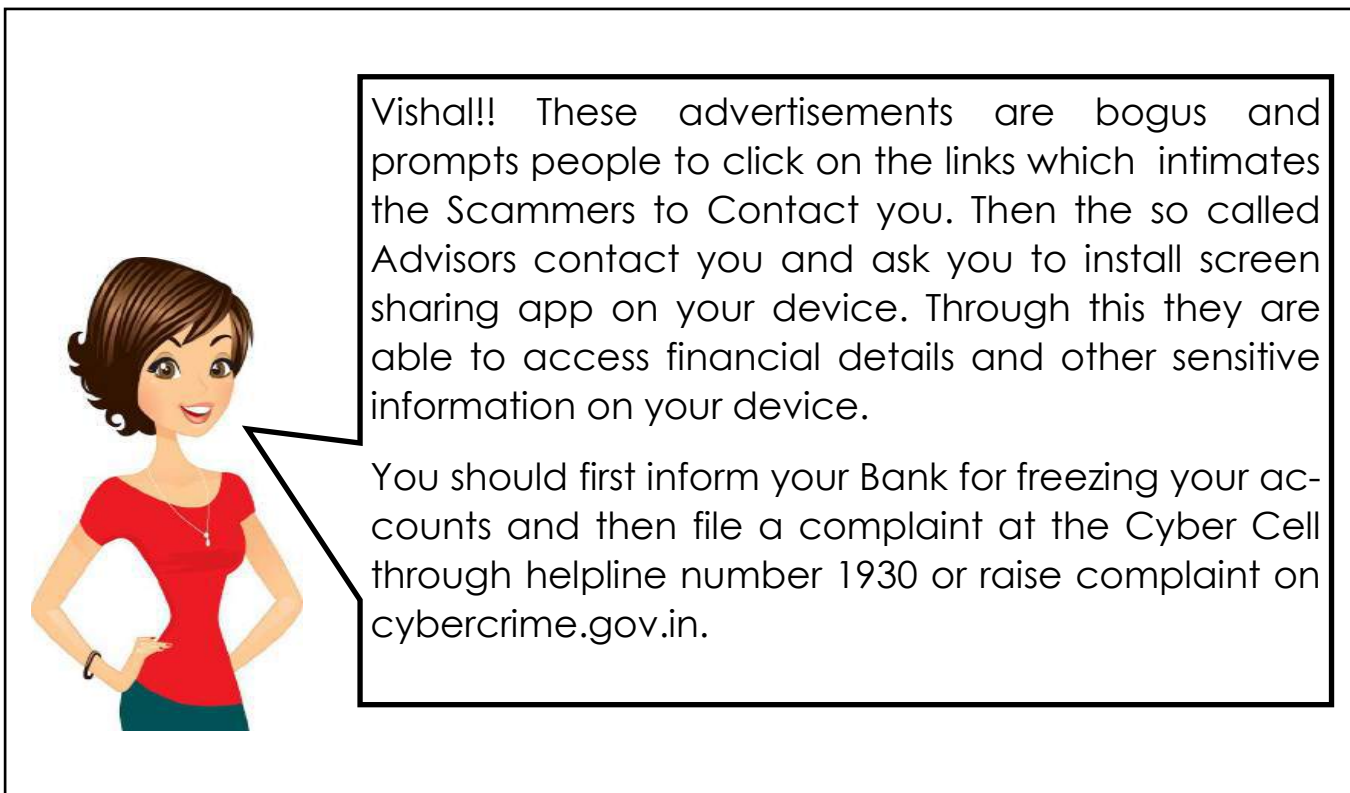


Vishal downloaded the app from the link provided on his mail id and shared his remote ID with Ajay. After giving the remote access of his desktop to Ajay, Vishal was asked to enter his bank details on the website opened by Ajay.

After making payment and disconnecting the call...



Vishal rushed to Reena and explained the entire incident.....



Precautions

1. Never download anything from the e-mails received from suspicious sources.
2. Never give unknown persons access to your devices.
3. Never insert your bank account details when you have given remote access to somebody else.
4. No bank or company will ask you over the phone to download software.
5. If someone unknown is asking to access any of your devices and wants you to download specific software: Be careful! You're at risk of becoming a victim of a remote access scam.
6. End any remote session by simply turning off your device!
7. Do not click on random links. Always use authentic sources while browsing and downloading any software.
8. Change your default settings if you feel that you have encountered a suspicious remote access transaction.
9. Install a robust anti-virus software.
10. Verify the requestor's identity when an attempt to access your device is initiated by an unfamiliar entity. This may require a phone call to the organization to ensure the request is not a fraud.
11. Another way to protect yourself is to limit access to the remote server. Only provide access to people who really need it and ensure you revoke access as soon as they no longer require it.
12. You need to monitor activity on the remote server. This will help you to detect any suspicious activity and take action accordingly.
13. Never download applications while on the phone.
14. Avoid making purchases while on call.
15. If in case you have inadvertently fallen victim, do call the Bank or Wallet Service Provider and seek help.



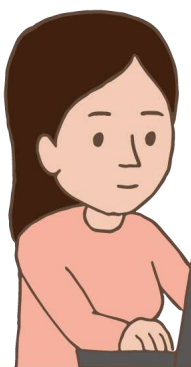
Chapter 4: Mobile Banking Frauds



Vishal recently opened a saving account with the bank and searched on Internet how to register for Internet Banking. But, Vishal was not able to understand the procedure properly.



After sometime, Vishal receives a call from the “Call Centre”...



Hello Sir! I am Sunita from ABC Bank and we have noticed you need assistance for using Internet banking. I am here to help you.



Hello Sunita! Yes, I need your assistance for registering Internet Banking. Please guide.

To initiate the process, I have sent you a registration link to your mobile number. Please click this link for the registration.




Vishal relies on her and clicks on the link and fills his personal details and Banking Credentials like Name, Account Number, ATM Card number & PIN, CVV etc. and clicks on “Register”. Then, he receives an OTP which he enters on the screen without checking the whole message.



 <p>Congratulations Sir!! You have successfully registered for Internet banking. Thank You.</p> <p>Sunita then disconnects the call.</p>	<p>After few minutes, he received a message regarding the Debit of his account. He re- alized that he has been duped.</p>  <p>Rs. 20,000.00 have been debited from your account no. XXXXXX on 26/07/2023.</p>
---	--

Vishal rushed to Reena and explained the entire incident.....

	<p>Vishal!! I have told you so many times to be cautious and not rely on the phone calls received regarding your Bank Accounts. You should have used the offi- cial website of the Bank. These fraudsters keep a track of the links created by them and once you click on them, they get information of your searches and then trap you.</p> <p>You should first inform your Bank for freezing your ac- counts and then file a complaint at the Cyber Cell through helpline number 1930 or raise complaint on cybercrime.gov.in.</p>
---	---



GYAAN KA SAAR

Precautions

1. Never search over the internet regarding help for registering the mobile banking or internet banking etc. except official website of the Bank.
2. Always confirm the Customer Care Number from the Bank's official website.
3. Always use Bank's official website and official Apps for registration of any banking facility.
4. The Banks will never ask you to download a specific software from a link and Avoid clicking on links received via text messages or emails that claim to be from your bank .
5. Never share your Card Number, CVV, PIN, expiry date, OTP, Internet Banking User ID or Password with anyone, even if the caller claims to be an employee of your Bank.
6. Install a robust anti-virus software & updates your device's regularly.
7. Always use virtual keypad while entering your Banking Login credentials.
8. Enable Two-Factor Authentication for your Banking Transactions too.
9. Never use public Wi-Fi for your banking transactions.
10. Do not click on suspicious links in SMS or MMS sent to your mobile phone.
11. Always check the complete message before entering the OTP.
12. Turn off "Allow installation of Apps from sources other than the Play store" option under Settings -> Security.
13. If in case you have inadvertently fallen victim, do call the Bank or Wallet Service Provider and seek help.
14. Always Use strong and Unique password, PIN, or biometric authentication (such as fingerprint or face recognition) to lock your mobile device and avoid using common or easily guessable passwords. This helps prevent unauthorized access if your device is lost or stolen.
15. Always log out of your mobile banking app when you're finished with your banking activities.
16. Set up transaction notifications for your mobile banking app. This way, you'll receive alerts for any account activity, helping you detect any unauthorized transactions quickly.
17. Regularly Review your account statements and transaction history to identify any suspicious or unauthorized transactions.
18. Some mobile devices offer app-locking features that allow you to lock specific apps, including your mobile banking app, with an additional layer of security.



Chapter 5: Online Lottery Frauds



Vishal received a scratch card from an identical looking email of payment App 'ABC'. The email stated that the lucky winner will win cash prize of Rs. 50000 on scratching the card.



Wow!! How nice it would be if I win the lottery. Let me scratch this card.

Vishal, then scratches the card.



On scratching the card, he receives a pop-up message.

Dear User

Congratulations!! You have won a cash prize of Rs. 5,000.00.

For claiming the amount in your Bank Account, [click here](#) and follow the steps.



Yes!!!! I won Rs. 5000. Let me follow the steps.

He clicks on the pop-up message and is redirected to ABC payment App. Out of excitement, he click on the pay and enters his UPI PIN.

Instantly, he receives a message regarding the Debit of his account. He realized that it was a fraud.



Rs. 5,000.00 have
been debited from
your account no.
X X X X X X o n
02/08/2023.



Vishal rushed to Reena and explained the entire incident.....



Vishal!! When will you understand !?!

Again you have been cheated. I have told you so many times that for receiving payment, you need not enter UPI PIN. You should have been careful. This was a fake lottery link with an attractive winning amount making you a victim of this false attractive offer. This fake link redirected to the payment app and you entered your UPI PIN and your account got debited.

You should inform your payment app and then report this fake email id. You should then inform your Bank for the wrong UPI you have done.

Precautions

1. Always verify the UPI ID before the transaction.
2. Do not click on suspicious links in SMS or MMS or email sent to your mobile phone.
3. Be careful about posting your cell phone number and email address.
4. Do not follow links sent in email or text messages. While the links may appear to be genuine, they may actually direct you to a malicious website.
5. Don't trust the good news coming from sources wherein you never contested for a lottery.
6. Never pay taxes on lottery amount upfront. That's not how the lottery system works.
7. Rely on your intellect and don't pay heed to offers sounding too good to be true.
8. Be careful , Competitions and lotteries do not require you to pay an advance fee to collect winnings.
9. Ignore all emails, texts, and social media solicitations on Lotteries.
10. If in case you have inadvertently fallen victim, do call the Bank or Wallet Service Provider and seek help.
11. Regularly Review your account statements and transaction history to identify any suspicious or unauthorized transactions.
12. Avoid entertaining or engaging with emails loaded with tons of graphics and quintals of grammar errors.
13. Never transfer funds to unknown persons or entities in anticipation of high returns. This is never going to happen.





Chapter 6: Credit Card Frauds

Vishal availed a credit card offer from his Bank. By availing this offer, he was given a physical Credit Card. After using it for some months, he started receiving the texts regarding decline of transactions.

Day One....



Please note that transaction attempt for INR 2500.00 on your Bank Credit Card No. xxxxx0123 has been declined due to insufficient authorisations.

Day Two...



Please note that transaction attempt for INR 3000.00 on your Bank Credit Card No. xxxxx0123 has been declined due to insufficient authorisations.

Upon receiving the same text message twice, Vishal decided to call his Bank to enquire about these messages.



Hello! I am receiving these text messages from the last two days stating that a transaction has been declined due to insufficient authorisations. However, I have not initiated any transaction in the last two days.

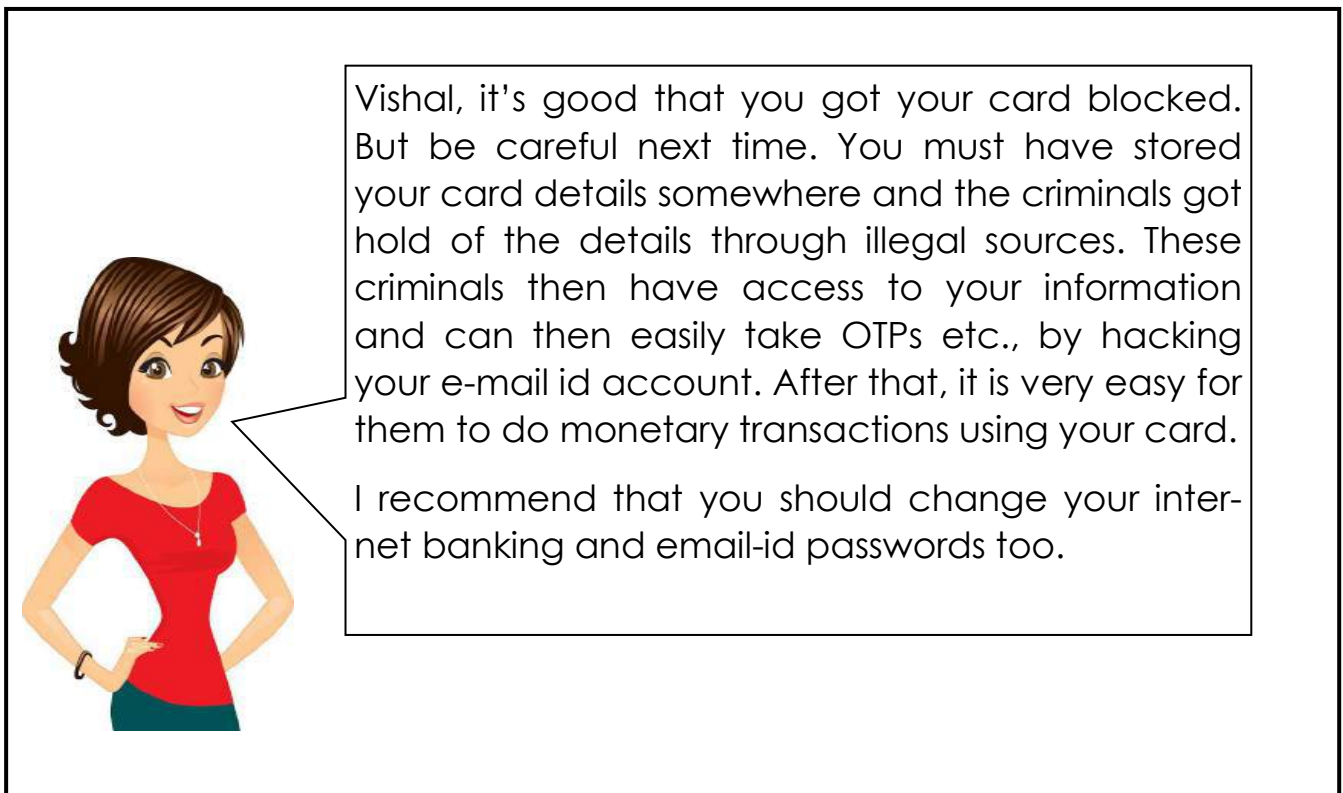
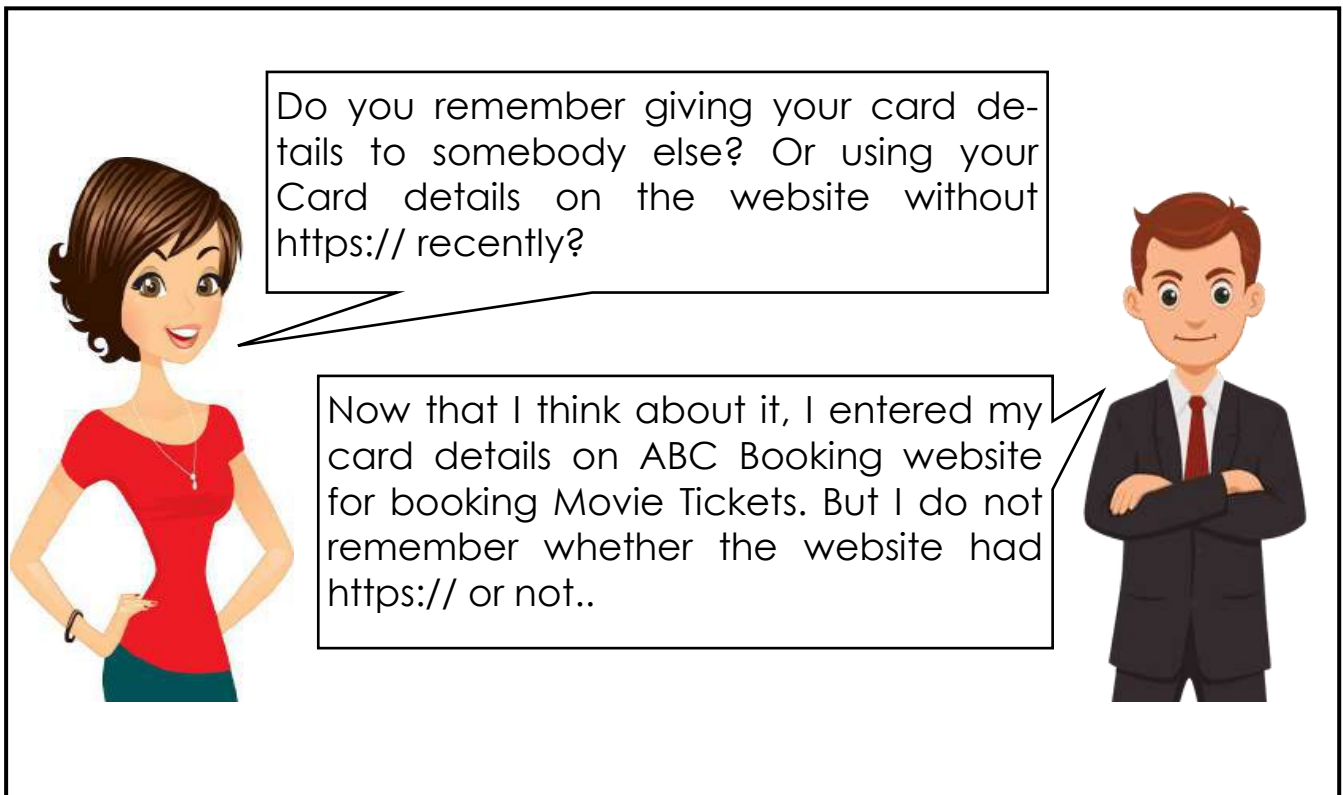
Hello Sir! Let me check. Sir, as per our records, you have tried to make a transaction at a website outside India. But, due to your Card's settings, your transactions were declined. Hence, you were not able to complete it. If you have not initiated any such transaction, you can raise a complaint with us.

Yes Sir. Please raise my complaint regarding this and block my credit card. Please issue a fresh card instead.





Vishal rushed to Reena and explained the entire incident.....





GYAAN KA SAAR

Precautions

1. Never let your card out of sight while handing it over to the operator at restaurants or at fuel stations.
2. Never share your credit card PINs, mobile application passwords, or internet banking passwords with anyone, be it a friend or a family member, or over an email.
3. It is a good habit to check the card statement each month as well as SMS alerts to keep track of transactions happening on the card.
4. If a card is lost or misplaced, the owner should immediately block the card using ATM or Internet banking. In case of a fraudulent transaction, inform the bank and the police immediately.
5. Cards should not be used when one is using public wifi
6. Do not save your information on random websites
7. Don't allow websites to "remember" your card number
8. Use Different Cards: Autopay vs. Everyday Spending
9. DO NOT swipe your card using any machine that looks tampered with.
10. NEVER give answers to questions pertaining to credit card security or personal details on unsolicited calls.
11. NEVER click on suspicious links. Look out for the tiny lock icon on the top left corner of the URL or the 'https:/' at the beginning of the URL. The 's' after http stands for 'secured'
12. Change your PIN and Banking passwords at regular intervals.
13. Notify your bank if you move to ensure statements and other information will follow you to your new address.
14. consider turning off the Autofill function in each browser that you use
15. Turn on account alerts to be notified of potential fraud on your card via phone, text or email. You can get alerts to detect charges that are unauthorized in addition to other suspicious activity.
16. Never just throw out or leave receipts behind. File what you need to keep and shred the rest to help protect your private information.





Chapter 7: Safe Downloads

Vishal wanted to buy a Bike. So, he decided to view the brochures from different Two-Wheeler Sellers.



He clicked on the first link available and downloaded the Brochure available on the website.



Once the download was completed, he decided to open the file. When he opened the file he noticed that his Laptop started functioning slow. He tried opening other files available on his Laptop, but was unable to do. He decided to take the Laptop to the Service Center.



Hello! My Laptop is running slow and I am not able to open any existing file in my system. Kindly check.

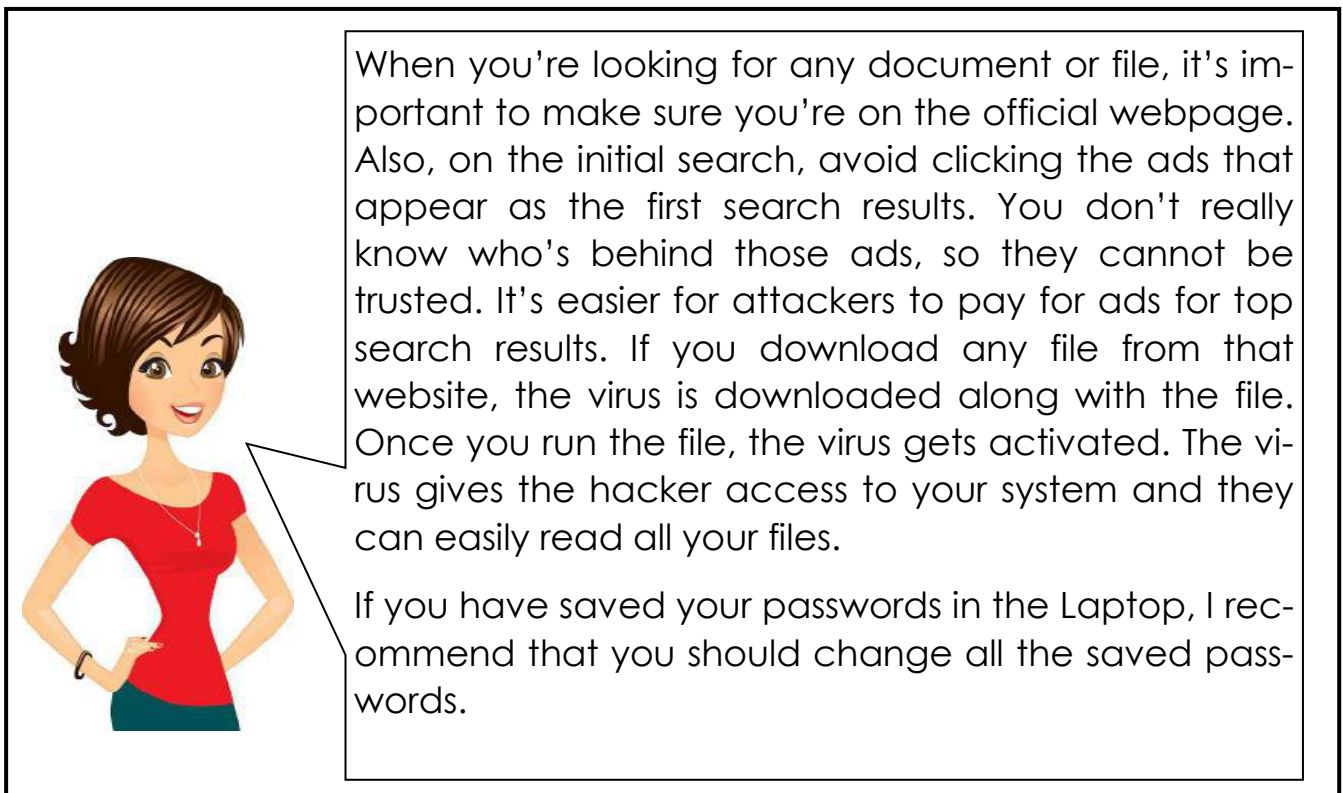
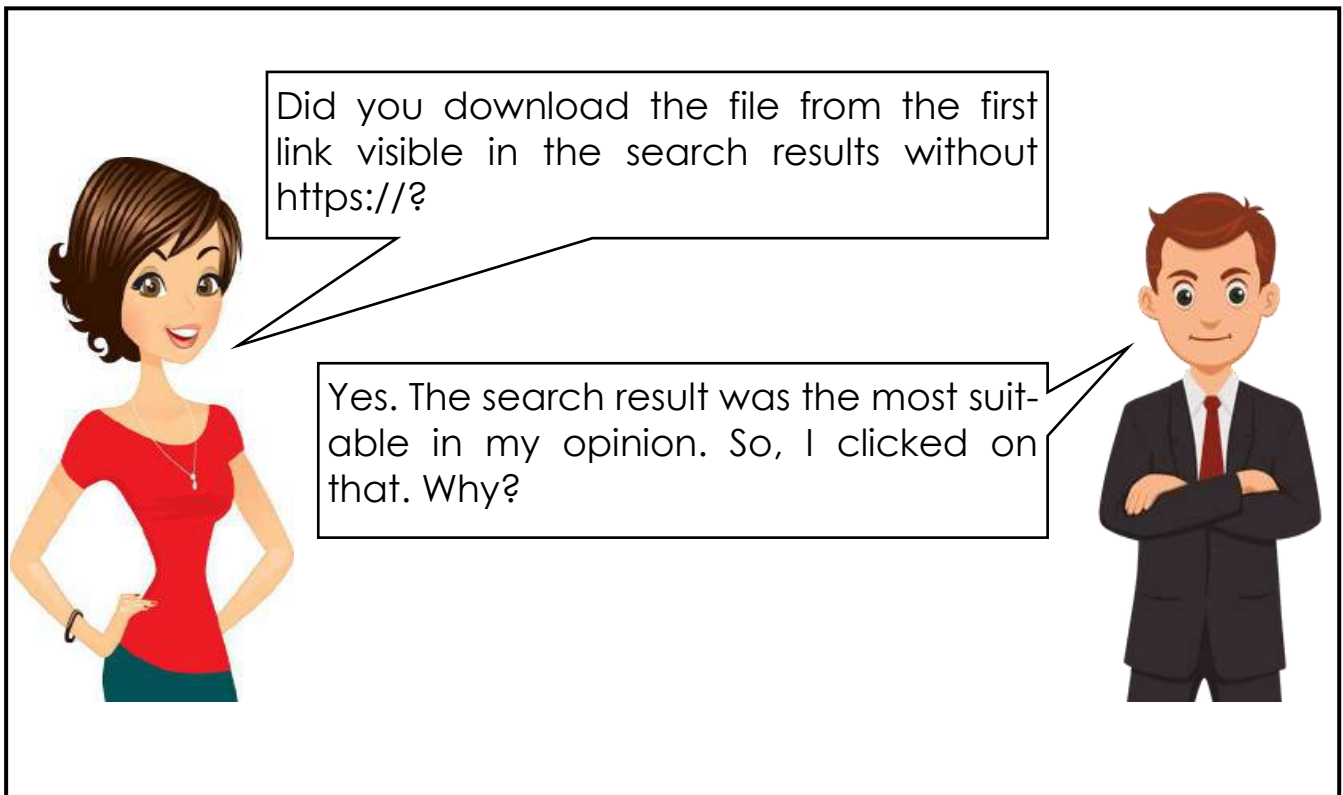
Hello Sir! Let me check. Sir, it seems your Laptop has been affected with some kind of virus through a file you have downloaded. As there was no anti-virus software in the system, the Virus has corrupted all your files. Even if I remove the virus, all your data will still be lost.

Oh God!! I do not have a backup of my data with me. How will I be able to access my data? 😞





Vishal rushed to Reena and explained the entire incident.....





Precautions

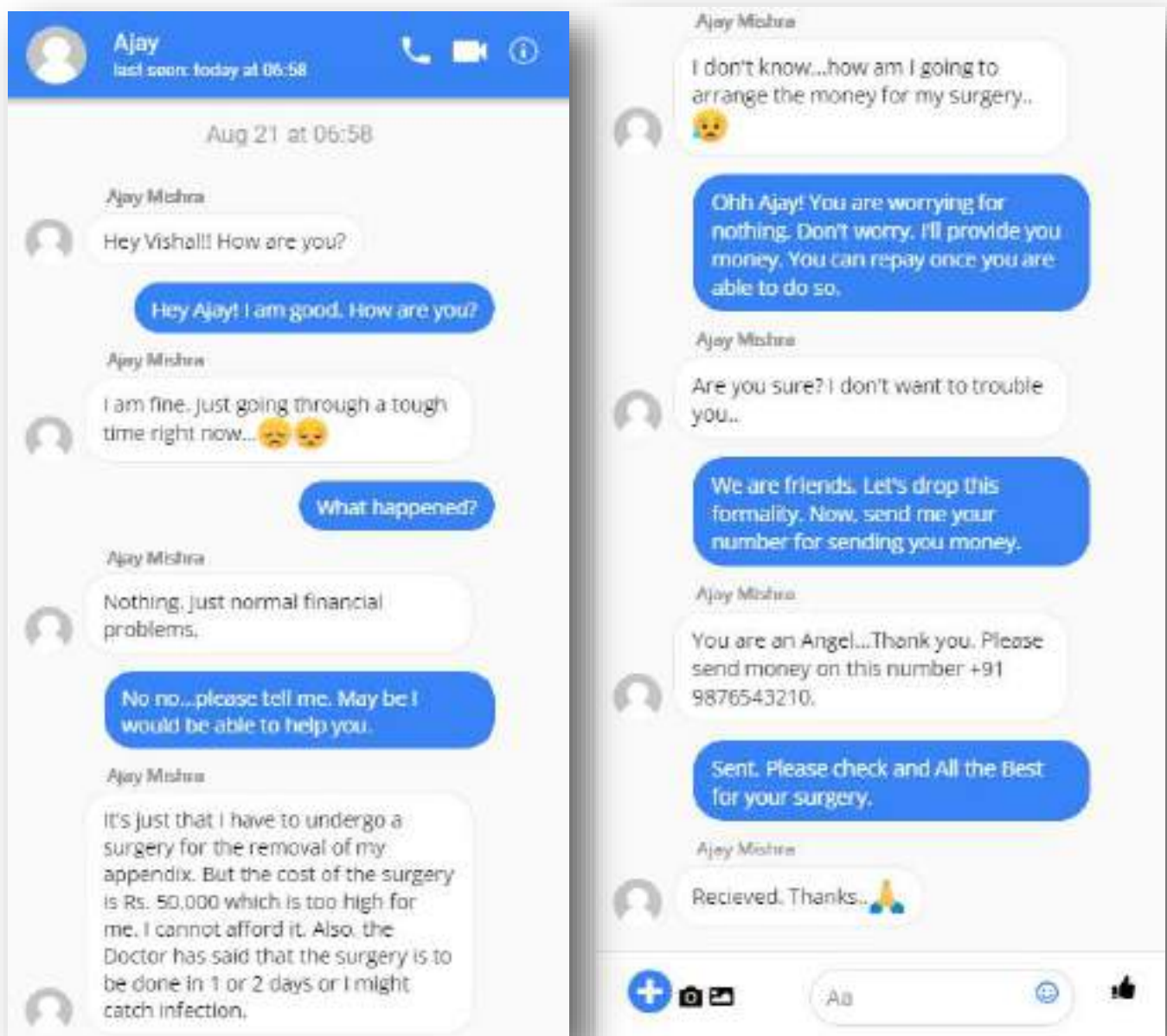
1. NEVER click on suspicious links. Look out for the tiny lock icon on the top left corner of the URL or the 'https://' at the beginning of the URL. The 's' after http stands for 'secured'
2. Before downloading any file, check the file's name, size, and format to ensure they match what you are expecting. Some malicious files may have misleading names or extensions to trick users into downloading them. Always download files from trusted websites.
3. Keep all website components up to date.
4. Use strong passwords and usernames for your admin accounts.
5. Keep your antivirus software up to date to ensure it can effectively protect your system against the latest threats.
6. Regularly scan your downloaded files and your entire system to identify and eliminate any potential threats.
7. Stay away from any illegal or unethical downloading practices, and always use a secure internet network.
8. Don't write sensitive information in text notes, Word documents or spreadsheets.
9. Consider using adblockers to protect yourself from fake ads.
10. Carefully read and examine security popups on the web before clicking.
11. Avoid downloading files on public Wi-Fi networks, as they may not be secure and can expose your data to potential threats.
12. Executable files such as .exe or .scr are often considered dangerous and should be avoided.
13. Take regular back-ups of your device to protect your files, photos, and data.
14. If you do have suspicious or unknown links, do not click them, especially if they will initiate a download. The links may even be shorter as a way for the criminals to hide where it actually leads.
15. Avoid signing-in through your Google Account on different websites. It is recommended to create separate user id and passwords for separate websites.
16. You should never give away private information or passwords.



Chapter 8: Social Media Frauds

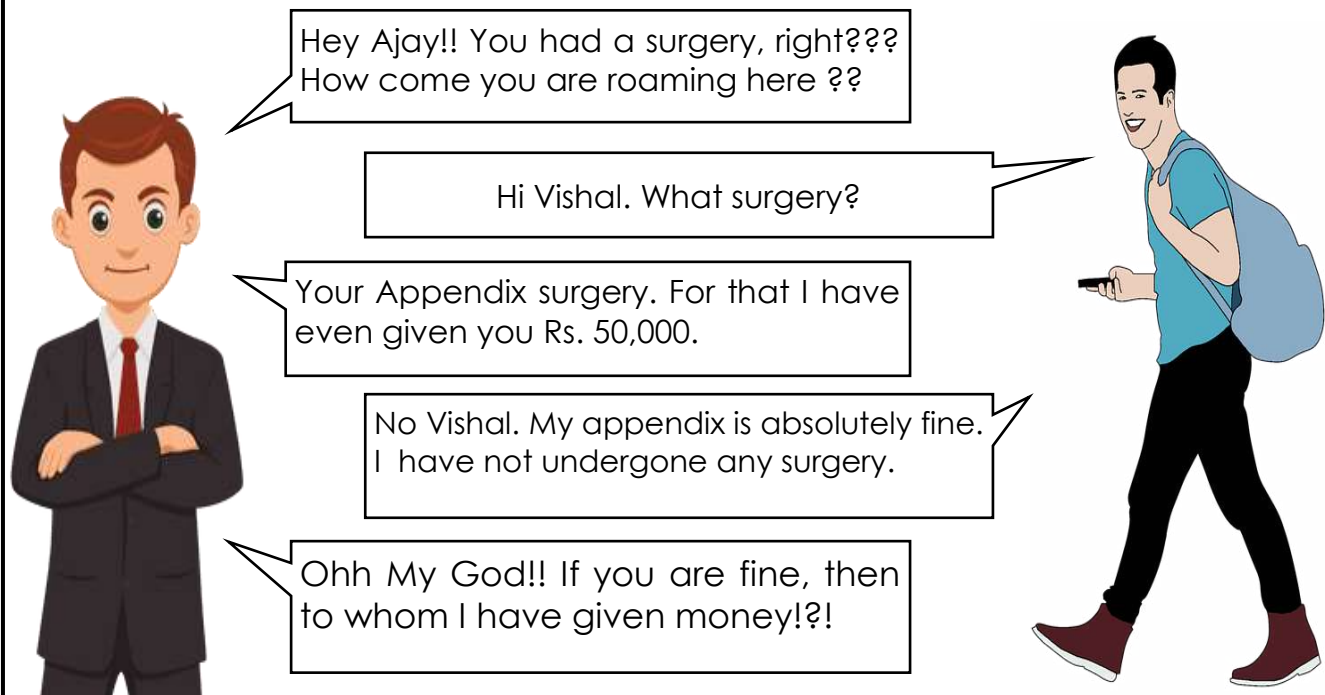
Vishal is an active 'Friends-book' Social Media website user. But, he is not an aware user. He accepts all the friend requests he receives without properly checking the profile. He has also not enable privacy settings in his account.

One day, he received a message from a profile named Ajay Mishra, whom he thought to be his classmate.

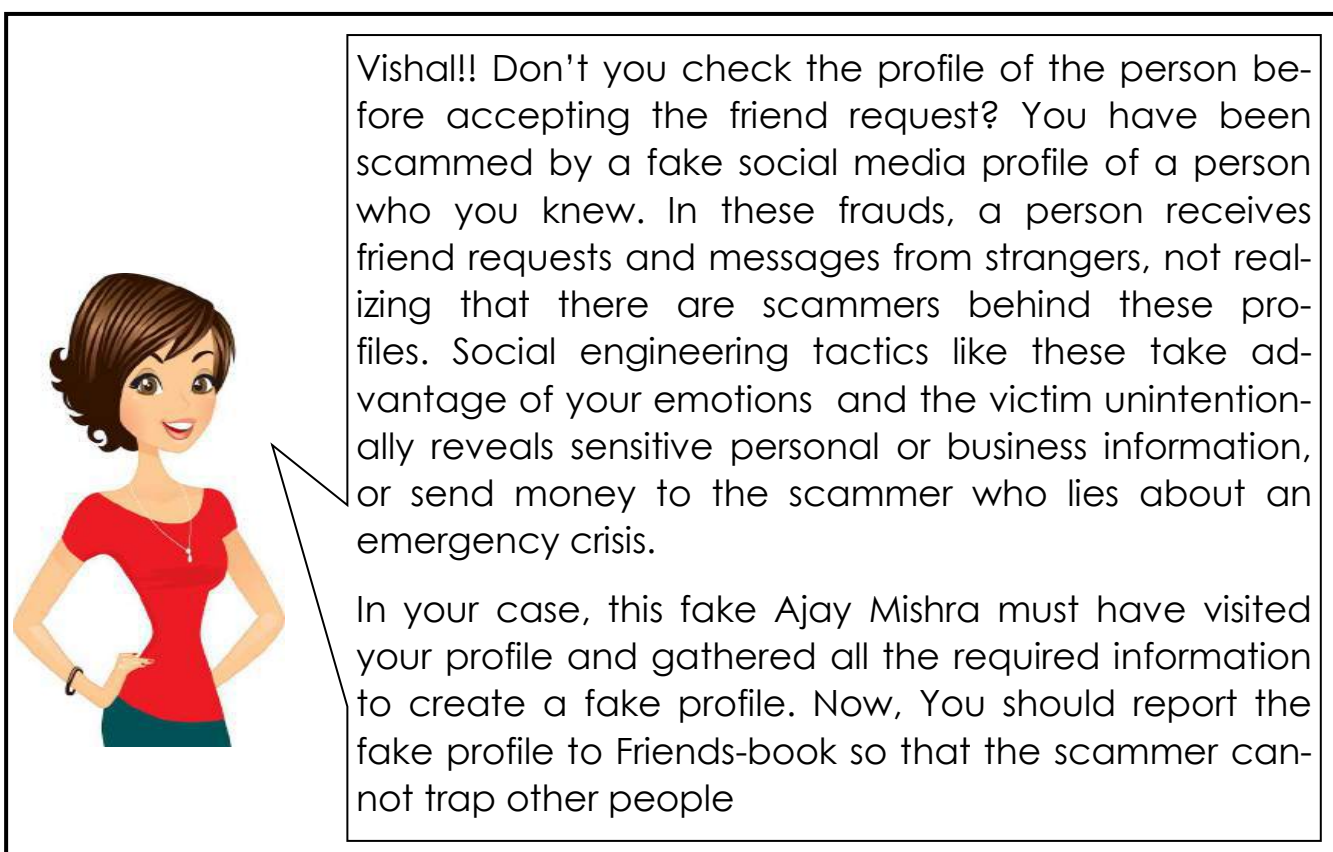




After two days, on his way to Home, Vishal met Ajay Mishra



Vishal rushed to Reena and explained the entire incident.....





GYAAN KA SAAR

Precautions

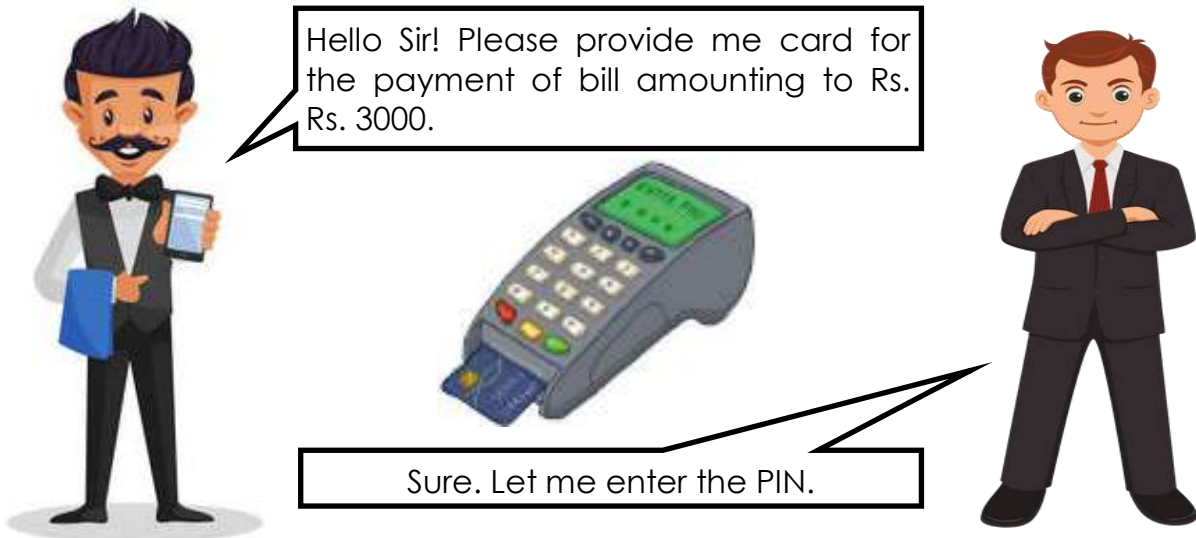
1. Ensure that you are using different passwords for all your online accounts, including email and each social platform.
2. Make your accounts private or have limited details showing on anything that can be viewed by the public. That way only trusted friends and family can see what you're posting.
3. If someone contacts you on social media asking for personal details, be very careful. Always make sure they are genuine and you're providing details for the right reason.
4. Before transferring the money requested via facebook, whatsapp or other social media accounts, verify the authenticity of the message by meeting the concerned person or calling him.
5. Legitimate brands on many social media platforms are verified with a blue checkmark next to their names. If they do not have this, there is a chance that they may be fraudulent.
6. Avoid clicking on any link that does not appear legitimate. Whether a link appears in a post in your feed, directly on your page, in a group, or via a direct message or email, always double-check. Unsolicited or malicious links usually include promotional language which can tempt users into clicking, so be wary.
7. Limiting who can see your posts on social media websites which reduces the likelihood of a cybercriminal conducting "watch" on you. Doing this will prevent them from reaching out to you with a scam or fake offer or friend request.
8. A lot of the time, online quizzes, polls, and games link to phishing and other malicious websites. It's best to not engage with these types of posts and links as a general rule.
9. What you post online is permanent, even after a social media account is deleted. So be cautious about what you share.
10. Always remember what you've posted about yourself. A common way that hackers break into financial or other accounts is by clicking the "Forgot your password?" link on the account login page. To break into your account, they search for the answers to your security questions, such as your birthday, hometown, high school class, father's middle name, on your social networking site. If the site allows, make up your own password questions, and don't draw them from material anyone could find with a quick search.
11. Be wary of links that come across your timelines in social media; they could be part of a phishing attack that redirects you to a fraudulent website.
12. Before accepting a friend request, verify the following-
 - Check the profile of the person
 - Check number of followers and following or likes
 - Check profile photo and friend list
 - Recent joining date
 - Mutual friends
 - Their Bio includes grammatical and spelling errors.



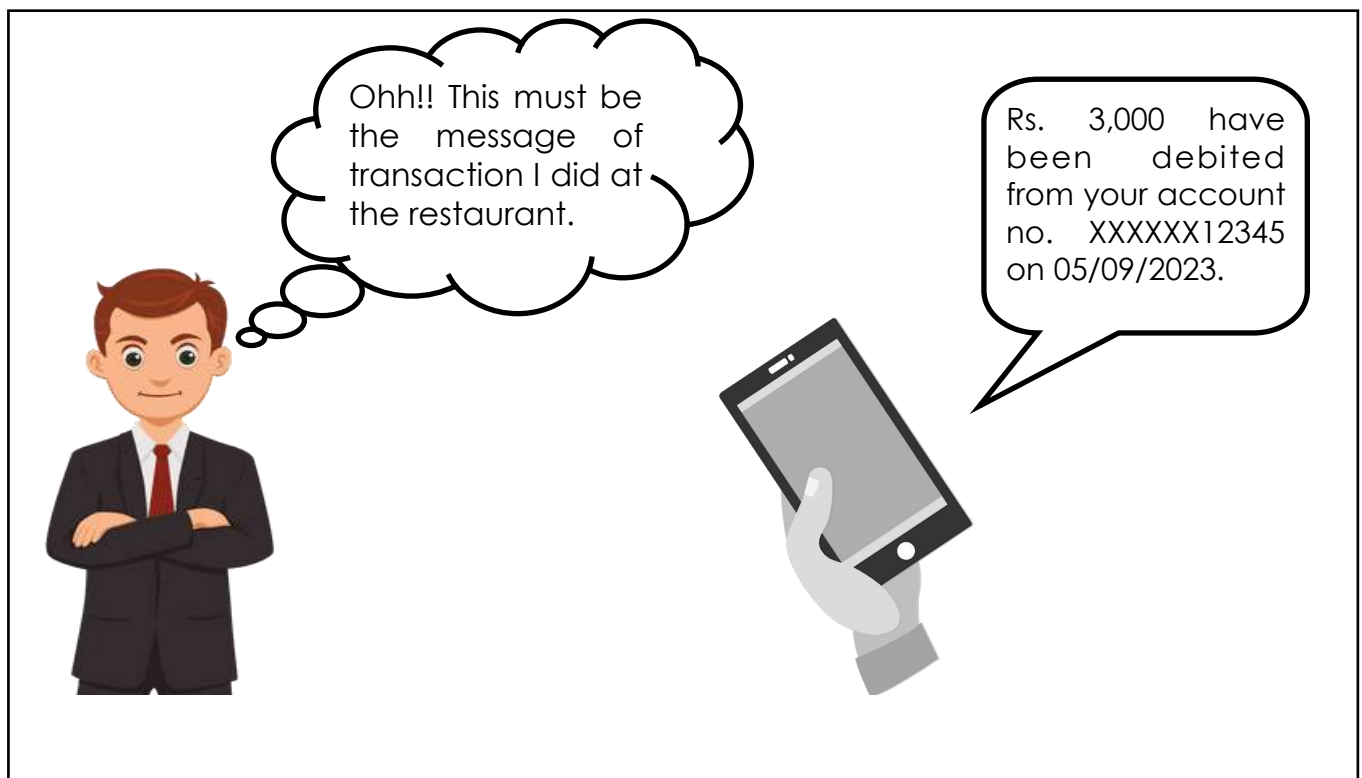
Chapter 9: PoS Machine Frauds



Vishal and his family goes to 'ABC' Restaurant for family dinner. After eating the food, Vishal asked for Point of Sale (PoS) Machine for paying the Bill.

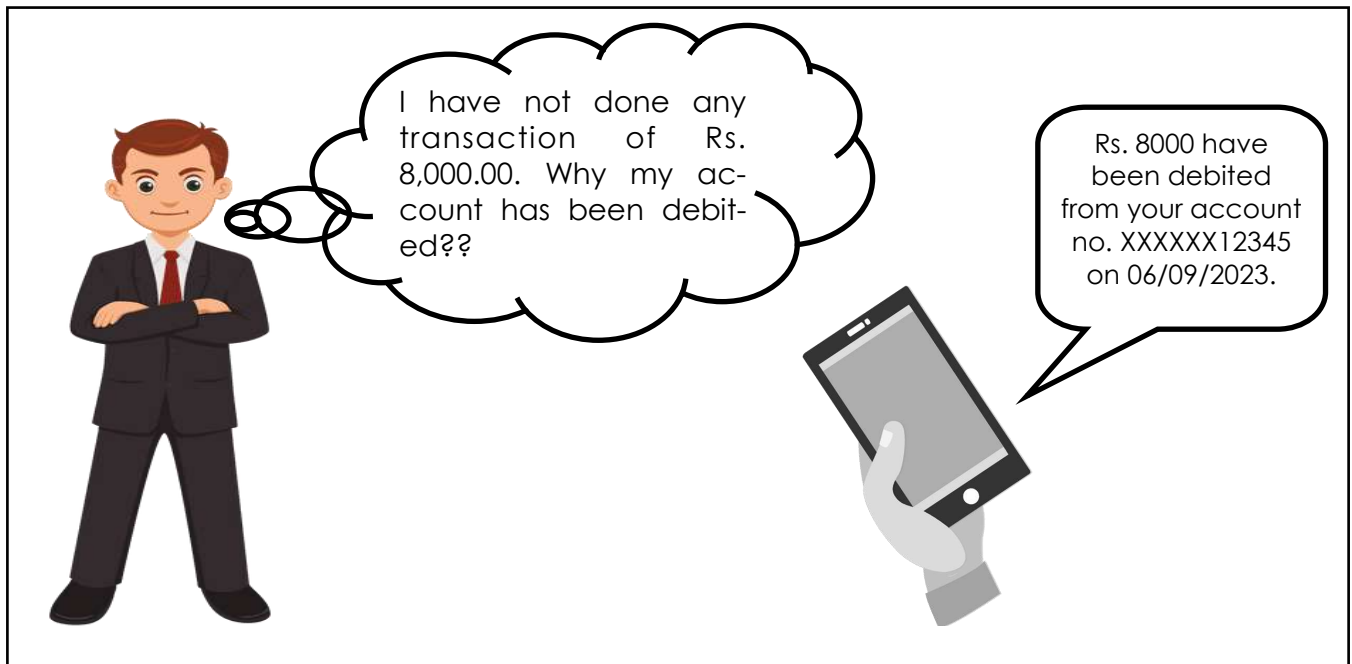


After reaching home.....

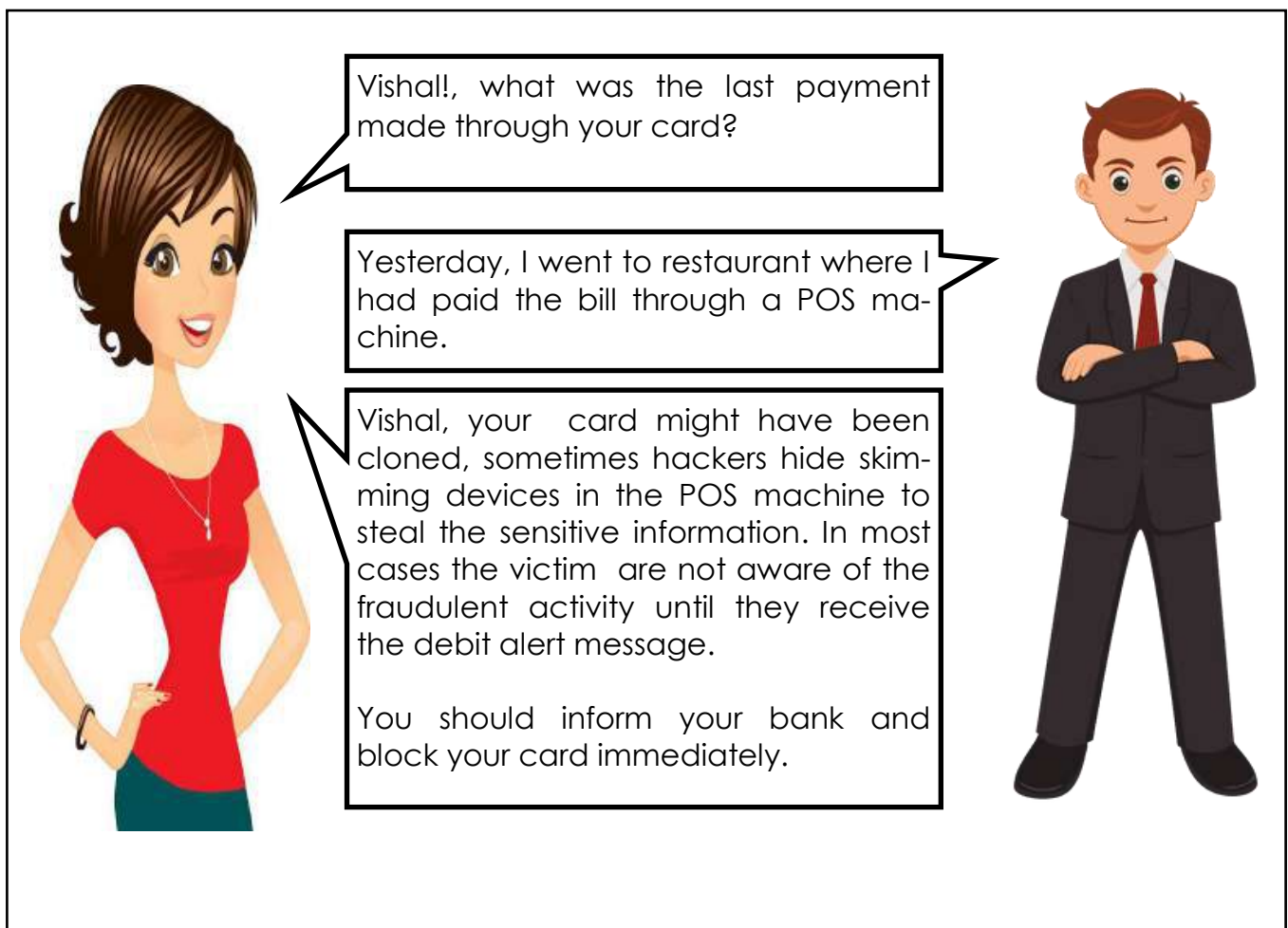




In the morning next day.....



Vishal rushed to Reena and explained the entire incident.....



Precautions

1. Before using any machine, inspect the machine to make sure that it is not tampered. If anything is suspicious do not use the machine
2. Don't allow anyone to assist you to insert your card into the ATM or POS terminal.
3. Don't use the ATM or POS in a dark environment.
4. Always take receipt of payment.
5. It is advisable to disable Wi-Fi tap feature in your cards.
6. Make sure no one is watching you from behind when you are entering your PIN.
7. Cover your hand when entering your PIN at the point of sale terminal, if required. Make a habit of doing this even when you are alone.
8. Don't provide any personal information to merchants other than your ID
9. Don't ever sign a blank transaction receipt
10. Don't share your PIN to anyone, not even family.
11. Be aware of your surroundings and have your card ready, as you approach the POS terminal.
12. Don't let your card out of sight.
13. Verify the transaction value prior to finalizing your payment.
14. Check your statements regularly or review all your transaction activity
15. If you are a victim of ATM or POS skimming fraud, report immediately to your bank.





About the Chapter

IT for business can be the 'life-blood' of a company, but it can easily be taken for granted. When someone gains access to someone's bank account, that's all they have access to. When someone gains access to your computer, they could potentially gain access to far more.

The person can do the following from your system:

- ⇒ Stealing confidential corporate data*
- ⇒ Credential theft*
- ⇒ Unauthorized access to private information*
- ⇒ Sending emails or messages as you*
- ⇒ Identity fraud / theft*
- ⇒ Installation of Malware, Trojan and other viruses.*

This Chapter covers one of the situation arisen due to leaving of systems unattended.



Chapter 10: Misuse of Un-attended Computer Systems

Vishal worked in ABC Limited as a Senior Manager. Due to his designation he often had access of many confidential and sensitive data which he stored in his desktop system. One day, while working on the system, his friend called him and he left the system on his desk unattended.



Aakash, Vishal's colleague noticed this. He got the opportunity and accessed the confidential files present in computer system of Vishal.

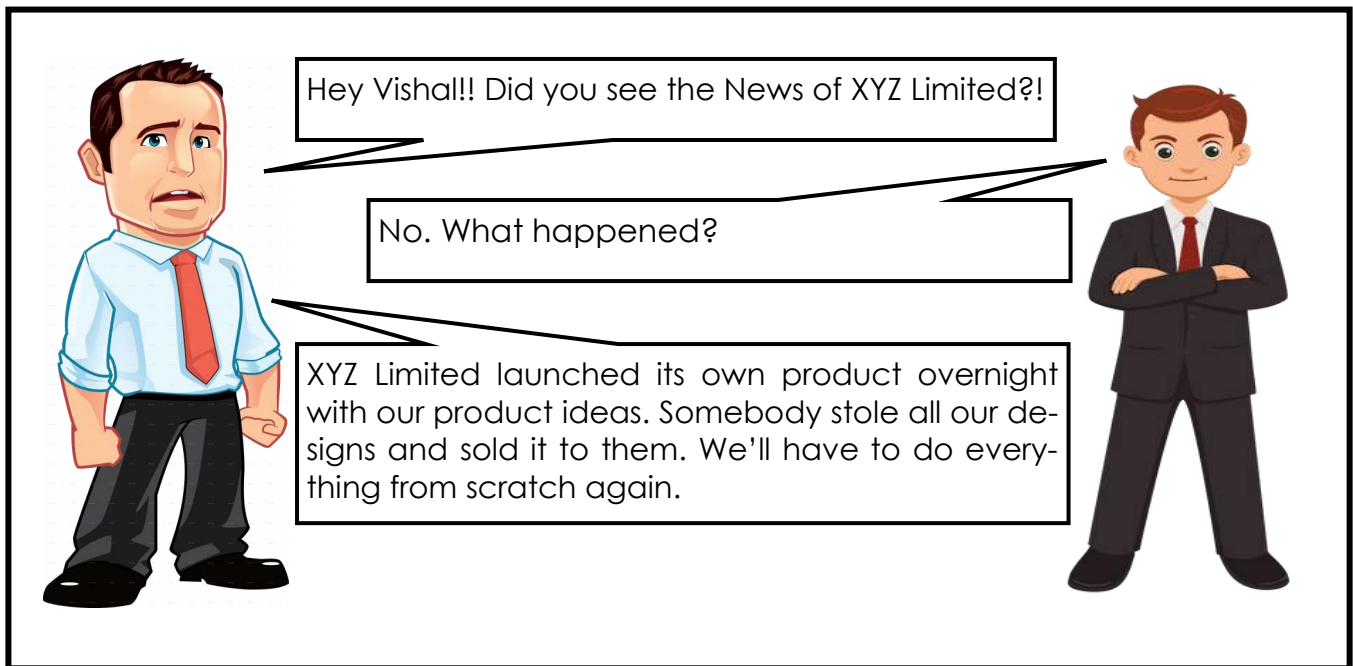


Ohh wow!! Now, I can access all the files which I did not have access to. I can sell this information to XYZ Limited and earn money!!

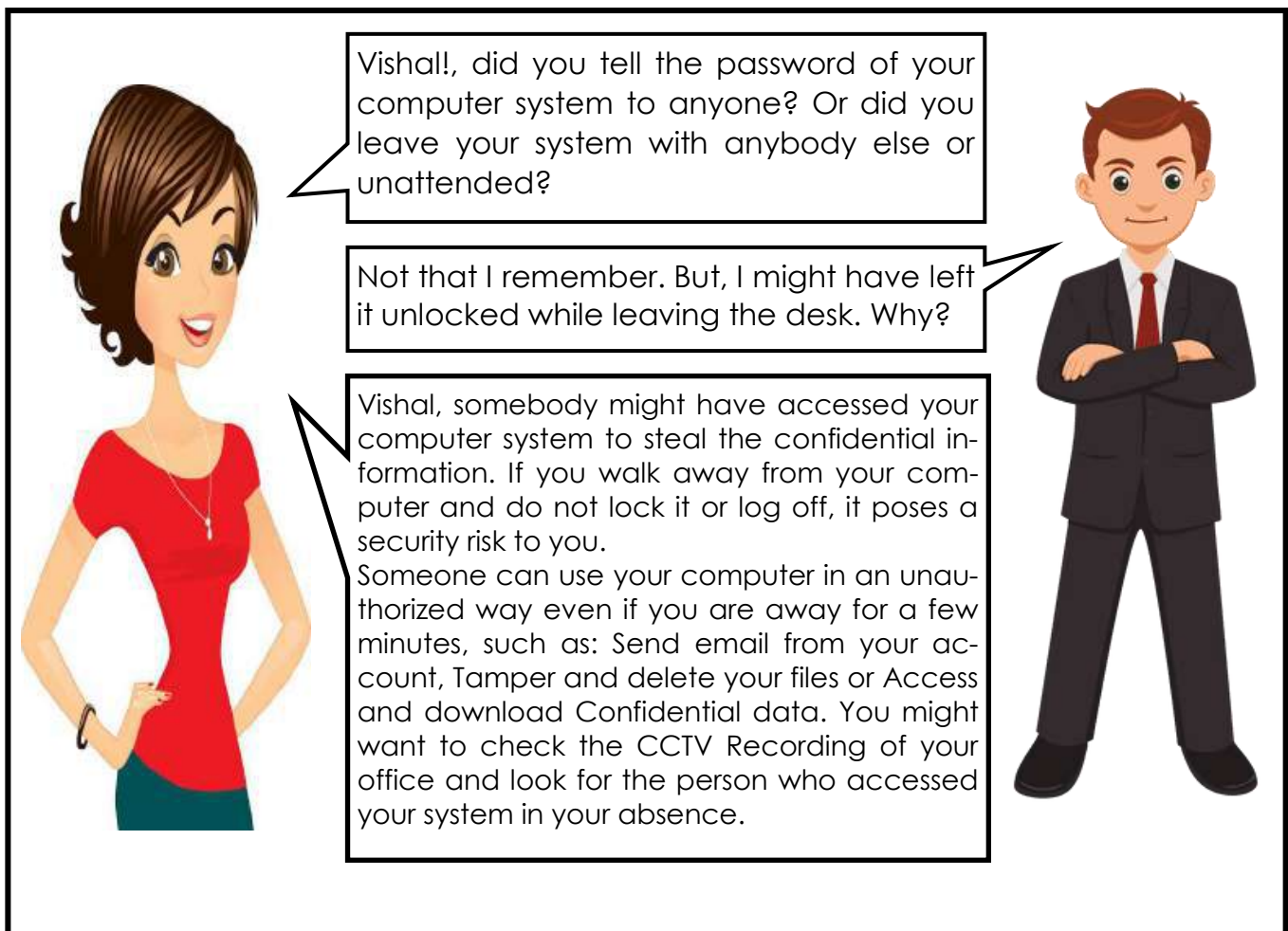
He copied all the data from Vishal's System and sold it to XYZ Limited.



In the morning next day.....



Vishal discussed the entire incident with Reena.....





Precautions

1. The easiest way to prevent unauthorized access to your desktop is to lock it when you are away. On a PC, the easiest way to lock it is by pressing Win+L. With a Mac computer, you can easily lock your computer by pressing Ctrl + Command + Q.
2. To be safe, don't allow your internet browser to save your passwords.
3. If you need to step away from where you are working, take your laptop with you. Or if you must leave it, make sure you log out of your user account or set a password-protected screen-saver.
4. Don't let other people access your user account when you are not with them.
5. Secure your area, files and portable equipment before leaving them unattended.
6. Don't leave sensitive information lying around unprotected, including on printers, fax machines, copiers, or in storage.
7. Change the settings on your systems to lock itself after certain minutes of inactivity.
8. Do not keep your confidential files in the visible location on your systems.
9. To secure your personal computer when you leave it unattended, either log off when you leave, requiring a password to log back on, or use a password-protected screen saver.
10. You can use Dynamic Lock that automatically locks your PC after you step away from it. It is based on Bluetooth network. When the signal drops, Windows assumes you've left the immediate area of your PC and locks it for you. This works on the basis of pairing done between your Computer and Smartphone.



About the Chapter

"From Google searches to Amazon purchases, they're listening, adding more and more data points on you to their records"

If you have a smartphone, it's a probably listening to you to some extent. Popular virtual assistant apps like Google Assistant or Alexa work by listening to your conversation and any app with access to your microphone can listen if you give access. In this chapter, we'll explore privacy issues related to how our phones listen to us.

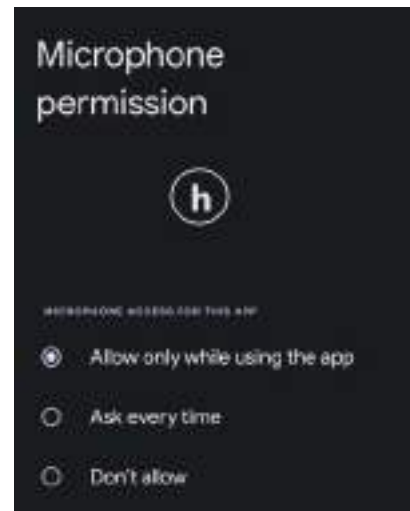
Remember, your digital security and privacy should always be a top priority, so be vigilant about the apps you use and the permissions you grant.

This Chapter covers one of the situation explain how the apps are listening to us and how we can stop the same.



Chapter 11: Apps are listening to you

Vishal downloaded a shopping app and after downloading the app, he granted access to all permission requested.



Next Morning.....

He was talking to his friend for buying shoes. After some time, while surfing on Google, he noticed some ads displaying shoes.





In the evening.....

He was discussing with his colleague about a holiday trip. After this discussion he again noticed some ads for trips packages. He was shocked.



Vishal discussed the entire incident with Reena.....



Vishal, our phones listen to us to virtually assist us. That's through voice assistant apps, but also through personalized advertisements that follow conversations had on them. See, it's no coincidence that you're sometimes served advertisements that directly relate to a phone conversation you just had.

We grant unnecessary permissions to the app which they do not need. Refrain from granting access to these sensitive permissions, unless essential for the app's primary function:

1. Contacts
2. Microphone
3. Camera
4. Call logs
5. Text messages
6. Location, unless it is a navigation app.

Precautions

1. Do not install any app without checking the details and assessing its actual use.
2. Always use official app stores for downloading and installing any app on your smartphone.
3. Avoid apps that ask for unnecessary access to your data or device functions. For example, if a flashlight app asks for access to your contacts, call logs or location, it is a red flag.
4. Be cautious when granting permissions to the app. Allow only those permissions that are necessary for the app to function.
5. If possible, make sure you grant selective permission to the app. Grant permission 'while using' or 'only while using the app' instead of 'always'.
6. Do not download any application which is not necessary and uninstall the applications which do not have any further use.
7. Consider using web-based tools when possible to avoid cluttering your device with single-use apps.
8. Some single-use apps may try to sell or pressure you into making in-app purchases. Be cautious and buy, if needed, only from trustworthy apps.
9. Do read user reviews and check the app's permissions before installing it.
10. Do not leave your phone unattended.
11. Disable microphone access to google assistant, Siri or Alexa.
12. Keep your software up to date to stay ahead of cybercriminals seeking to exploit security vulnerabilities, as software updates patch these holes.





About the Chapter

"Ponzi schemes has been carried out over decades. Investigators suspect Madoff's Ponzi scheme was started in the early 1980's and lasted over 30 years "

A Ponzi scheme is an investment fraud in which clients are promised a large profit at little to no risk. The Companies that engage in a Ponzi scheme focus all of their energy into attracting new clients to make investments.

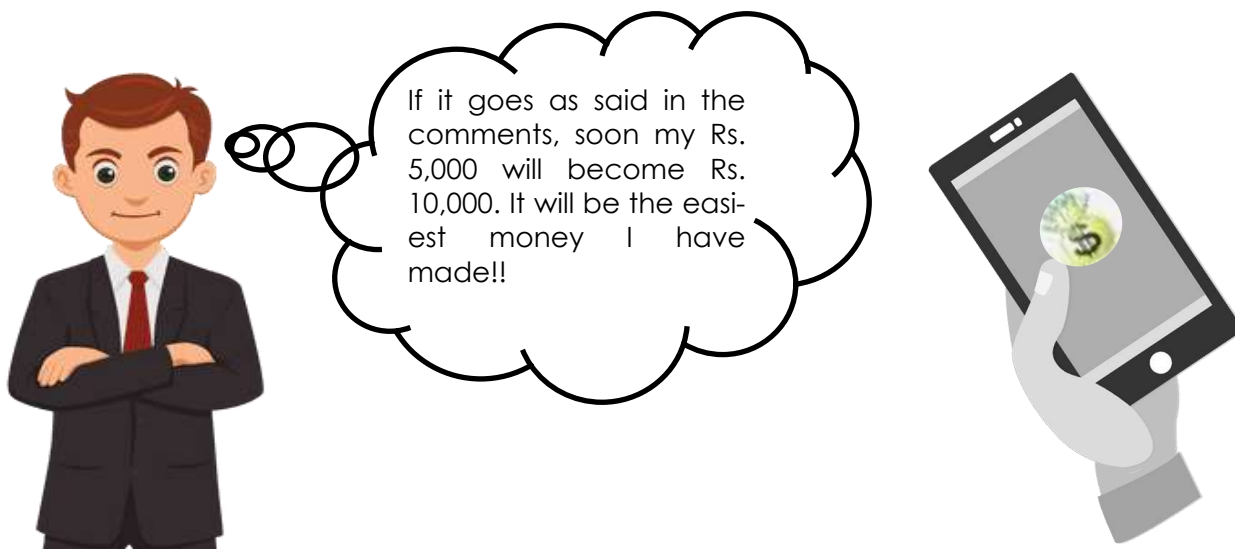
This income is used to pay original investors their returns, marked as a profit from a legitimate transaction. Ponzi schemes rely on a constant flow of new investments to continue to provide returns to older investors. When this flow runs out, the scheme falls apart.

This Chapter covers one of the situation explain how a person falls under the trap of Ponzi Scheme and what we can do to come out of it.



Chapter 12: Ponzi Scheme

While surfing through his play store, he came across an app named “Money Double\$!!”. He checked the reviews and found that the money invested through this app can be doubled. Finding the offer interesting, he downloaded the app and invested Rs. 5,000/-.



Fifteen Days later.....

He was excited to see how much his grew in one night. He quickly opened the app and decided to view his statement.



Balance as on	Transaction ID	Amount
01/08/2023	1234567890	₹ 5,000.00
15/08/2023	9876543210	₹ 10,000.00

Seeing his money doubled, he got greedy and decided to re-invest the whole amount.

One Month Later....

He was happy that his initial investment of Rs. 5000 has now become Rs. 20,000. He decided to withdraw the entire amount. When he tried to withdraw the amount, the app was crashed. Even after numerous tries, he was unable to withdraw the amount.



Vishal discussed the entire incident with Reena.....



Vishal!! When are you going to learn that your money cannot be doubled without doing anything in such a short time.

These attractive looking schemes are frauds. You should have understood that these schemes are nothing but frauds. These schemes are known as Ponzi Scheme.

With little or no legitimate earnings, Ponzi schemes require a constant flow of new money to survive. When it becomes hard to recruit new investors, or when large numbers of existing investors cash out, these schemes collapse. As a result, most investors end up losing all or much of the money they invested. In some cases, the operator of the scheme may simply disappear with the money.

You should uninstall this app and report it with the Google Play Store and also register a Police Complaint.

Precautions

1. Every investment carries some degree of risk, and investments yielding higher returns typically involve more risk. Be highly suspicious of any “guaranteed” investment opportunities.
2. Be suspicious if you don't receive a payment or have difficulty cashing out. Ponzi scheme promoters sometimes try to prevent participants from cashing out by offering even higher returns for staying put.
3. Account statement errors may be a sign that funds are not being invested as promised.
4. Avoid investments if you don't understand them or can't get complete information about them.
5. Before investing, read terms and conditions carefully and ensure that the scheme is registered. Most Ponzi schemes involve unlicensed individuals or unregistered firms.
6. Check the credentials of the Company through which you are investing money.
7. Check the number of downloads while downloading any app.
8. Always invest through trusted investor advisor.
9. Do not take investment decisions in haste.
10. Warn your family and friends to stop them from becoming victims.
11. Invest depending upon your risk tolerance capacity.
12. Know your investment time frame.
13. Diversify your portfolio. Do not keep all your eggs in one basket.





About the Chapter

If you're like most people, you like to stay connected whether you are traveling or just on the go. That's why it can be tempting to connect to free, public Wi-Fi networks, but you should know that these networks could open you up to some serious risks.

Public Wi-Fi networks often lack a security measure called encryption, which sends the information quickly from your computer or device to the router so strangers cannot read it. Without this security measure in place, the information you send over these networks can potentially be intercepted by cyber crooks. This information could include your banking and social media passwords, as well as your identity information.

We all know cybercriminals always try to take advantage of every situation. So, they come up with a new conning technique. They are using public Wi-Fi as a weapon to trick people into their trap.

In fact, every day thousands of innocent people are becoming the victim of public Wi-Fi scams. Its cases are rapidly rising in India. Here, we are with one incident which took place when Vishal used Public WiFi.



Chapter 13: Public Wi-Fi

Vishal was waiting at the railway station. His train was set to arrive in 30 minutes. While waiting, he decided to do some work on his laptop.



Wow!! This railway station has free Wi-Fi connection. Since I have time, let me connect the Wi-Fi and pay my credit card bill.

After few minutes...

Vishal connected with the Public Wi-Fi available and logged into his net banking to pay his credit card bill.



Finally!! Because of this Public Wi-Fi, instead of waiting, I was able to complete one important transaction.



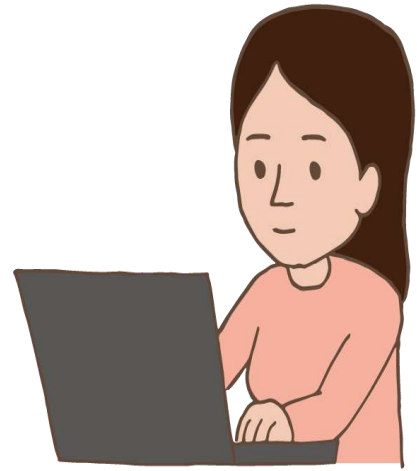
One Hour Later...

Vishal receives an OTP on his mobile for log in of net banking. Thinking that this might be OTP for his previous login, he ignored it. After few minutes, he again receives another message containing OTP. This time he got worried and thought of calling his bank.



Hello Madam, I am receiving an OTP for log in into net banking. But I am not logging in my account. I think some fraudster might have tried it. What should I do?

Yes, your net banking credentials might have been compromised. You should change your net banking password and other authentications. On your request we can temporarily freeze your account.



Vishal discussed the entire incident with Reena.....



Vishal!! You are impossible!!

I have told you so many times to be careful. But you just don't listen. But, it's good that you informed your Bank.

See!! Public Wi-Fis are very dangerous. One of the biggest risks associated with using public Wi-Fi is that they have low security and firewall settings and are thus vulnerable to attacks. Hackers can easily access your personal information or install malicious software on your devices without your information.

When you accessed your Bank details through Net banking, the hacker might have stolen your internet banking ID and password. Be careful. Do not use Public Wi-Fi again.



Precautions

1. Avoid accessing sensitive information while using Public Wi-Fi.
2. Only browse websites that include an SSL certificate while on public Wi-Fi. A website has an SSL certificate when the URL begins with "HTTPS."
3. Using antivirus software is another great way to stay safe while using public Wi-Fi.
4. When you're done browsing, be sure to log out of any services you were using.
5. Check your settings to make sure your device will "forget the network" and not automatically reconnect to that network again if you're within range without your permission.
6. It's crucial to always update your operating system (OS). OS updates often include important security patches that can further protect your device from Wi-Fi threats.
7. When you're using public Wi-Fi, cyber snoops could gain access to your passwords. One way to enhance your protection is by enabling two-factor authentication (2FA) on any services that offer it.
8. Make sure you turn off file sharing before accessing public Wi-Fi.
9. While using public Wi-Fi, you should avoid visiting sites that require you to enter personal information such as passwords or credit card numbers.
10. Verify that the network is legitimate.
11. Turning on the firewall can prevent hackers' unauthorized external access to your system.
12. Connecting through VPN prevents web browsers and unwanted visitors from accessing your data.
13. The riskiest places to use public Wi-Fi, as perceived by the respondents, are hotels, airports, and cafes or restaurants. These places saw a considerable increase in their perceived riskiness compared to other locations. Schools were seen as relatively low-risk places to connect to public Wi-Fi.





About the Chapter

Online betting scams are used to steal personal information and could take several forms. Fraudsters may send you a link to click on to download a gaming file which then installs malicious software onto your device which logs your keystrokes.

Another tactic is account takeovers where fraudsters exploit a real betting online account to send other innocent players free skins and points when they put in their username and password. In addition, players could be offered free trials or other 'freebies' such weapons or tokens if they click on a link.

There are even a fake game apps which can be downloaded at a cost from the Google Play or Apple's App Store onto one's mobile phone.

Fake competition video game are also prevalent and are designed with the intent to dupe users into paying fraudulent entrance fees and steal personal banking details. Finally, legitimate online gaming marketplaces may sell 'keys' that are stolen or are fake.

Apart from these, these online gaming platforms have a significant impact on your mental health too. In this chapter, we'll be learning how you can be scammed through online betting..



Chapter 14: Online Betting

Vishal recently started playing an Online Betting Game named 'Wizingo' which was a card game. While playing the game, he realised that he needs to buy some points his Bank Account to move to next level. Finding the game interesting, he decided to buy some points.



It's only Rs. 200 for 20,000 points. It's not a big deal. I might be able to win Rs, 2000 by spending Rs. 200. Let me just make the payment.

Vishal started playing the game regularly....

To clear next level, he purchased a booster of Rs. 10 through his Bank Account to Skip Ads while playing the game.



Now, I can peacefully play my game without ad interruptions.



Next Day.....

He reviewed his Bank Statement randomly. He noticed that there were debit transactions in his account which was not done by him.



The last transaction I remember making was to pay for the booster. After that, I have not made any single transaction. Then why there are entries for debit of Rs. 1,000 and Rs. 2,000 twice?!



Vishal discussed the entire incident with Reena.....



Vishal!! Did you check the authenticity of the Betting App before downloading it?

The cyber criminals often build a fake mobile game, usually a replica of a popular online game. Then when a cyber victim downloads it, this software installs malware on their device. This could be a mobile phone, tablet, or, on rare occasions, a desktop computer. The malware in question targets details of gamers' online accounts, which usually include personal user information.

Once installed, malware can log credit card information, phone numbers, or even addresses, which could be exploited in numerous ways. This is what happened with you.

Also, many banks do not offer SMS facility for transactions involving small amounts. So that's why you didn't receive the message for the Transaction.

Now report that app to the Play Store and uninstall the app. Remember, to install any app after checking its credentials.

Precautions

1. Activate two-factor (2FA) or multi-factor authentication (MFA) where possible and regularly change the password for your account.
2. Install a local security solution to block and detect malicious software and alert you to any phishing attempts.
3. Use the privacy settings on your online account to control how your profile appears to other members of the gaming community. Some platforms allow you to choose between public, friends-only or private options.
4. Log out of your account when using shared or public machines.
5. Don't click on unsolicited emails that portray a sense of urgency or ask you to provide particular information to confirm your identity. Be especially suspicious of any request to verify your password.
6. Download apps and extensions from the official website.
7. Don't provide your personal or financial information to someone you've just met in an in-game chatroom
8. Make your in-game purchases from official sources.
9. Report any suspicious activity to the gaming platform.
10. Never follow instructions provided by someone who says he reported you by mistake and asks you to contact an authorized representative via communications channels such as Discord to solve the issue.
11. Keep an eye on your accounts and monitor them for any unusual activity. If you notice any suspicious transactions or changes, report them immediately.
12. If your account was compromised, you should change your passwords immediately. Choose a strong and unique password that is not used for any other accounts.





About the Chapter

Hackers and attackers are constantly trying to infiltrate the safety of corporate firewalls. These individuals are becoming increasingly clever and creative in finding new ways to infiltrate a company's network. No longer are they limited to trying to break into the network from the outside.

Hackers can also use USB drives to gain access to sensitive information kept on a computer or network. Hackers may infect one or more USB drives with a virus or Trojan, that when run, will provide hackers with access to logins, passwords, and information on the user's computer or the network the computer is connected to. The hacker may then leave the infected USB untended on the floor, in or next to a cluster machine, in hallways, restrooms or any areas with a relatively high volume of traffic. A user who finds a USB drive will often install the device on their computer or on a cluster machine to search for identifiable information that can be used to locate the owner of the USB device.

In many cases, plugging the USB into a computer will trigger a virus alert and encourage people to call a customer support line, where a scammer will take over the computer and demand payment.

In this Chapter you will learn how using a random USB may cost you to lose your data...

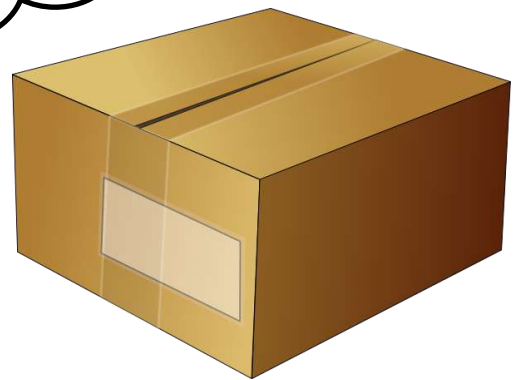


Chapter 15: Scam through USB Devices

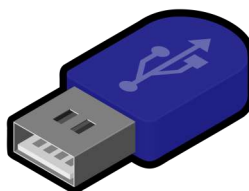
One day Vishal received a package from "MegaSoft" which provides the Software used in Computer Systems. When he opened the package he found something....



What is this? I don't remember ordering anything from MegaSoft.



He opened the Box and found a USB Drive with a letter.



Dear User

As a gift for your continuous trust in the organization, we are giving you a PenDrive through which you can download free software update which will improve your device's performance.

To run this update, please follow the steps which will be displayed when you connect the PenDrive with your device.

Thanking You

Yours sincerely
MegaSoft

He connected the PenDrive with his Computer without scanning its contents.



When he connected the PenDrive, his system immediately malfunctioned and crashed.

Vishal discussed the entire incident with Reena.....



Vishal!!! When will you learn? Never trust something which is free.

Did you check the authentication of the courier you received? If you don't remember ordering anything, this means you have not ordered anything. So, probably this is a bogus courier.

The only reason behind crashing of your system is that Pen-Drive you connected with your system. When you connected it, the virus in the PenDrive got activated and infected your system and the system crashed.

That's why, it is advised to not connect your system to any unknown devices without scanning.

You should take your system to the Authorised Service Center and get it formatted.

Precautions

1. If you're using a USB drive to transfer files across several host devices, it can make you vulnerable to malware – and you can never be too careful when it comes to USB security, particularly if you're handling sensitive data.
2. Always scan your USB Drive after connecting it with your computer and use decent USB Anti-virus.
3. Always check the authenticity of the external devices before connecting it with your computer.
4. If you see a USB key lying around within the grounds of your workplace, bring it to your security department. If it is lying outside of your workplace, it is better not to pick it up.
5. Install and update anti-malware software (e.g. Windows Defender).
6. Install and maintain a firewall .
7. Disable Autorun on your machine. Autorun is a feature that allows Windows to automatically run the startup program when a CD, DVD, or USB device is inserted into a drive.
8. Do not connect any USB Drive which you have received randomly through mails or couriers.
9. Be cautious of anything that comes in the mail that you didn't ask for.
10. Password protect your removable media devices.
11. When you have finished transferring sensitive data from a USB drive, be sure to delete it using a secure delete utility. .
12. Keep your personal and business data separate. Don't plug your personal audio player into your work PC or your work jump drive into your home PC.





About the Chapter

While a new scam is born nearly every day, most scammers use the same bag of tricks. As a new scam technique, they allegedly lure people with fake loan schemes through apps, and the money that is extorted using their personal data would be sent to their associates in China via cryptocurrency. They would seek permission from users to access their data and steal all their contact details, chats, photos, etc. These would then be uploaded on servers based in Hong Kong.

Then they would refer themselves as recovery agents and then call the users and extort money using their morphed photos by operating from call centres. The person in fear would then pay-off them in lakhs.

Victims, often downloading these apps without proper research, are harassed and scammed out of lakhs of rupees. Despite warnings from the police to people, these apps continue to be popular.

In this Chapter, you will see how Vishal got trapped into one of these scams....



Chapter 16: Fake Loan Apps

One day, Reena received a call from an unknown number. Being curious, she picked the call.



Hello! Who is this?

Hello Ms. Reena. I am calling from ABC Financiers. Mr. Vishal has taken a Loan from us for Rs. 1 Lakh and has missed its instalments. Please ask him to repay our amount or else we will take strict action against him.

Sir I have no idea about this transaction. But, I'll talk to Vishal about this.



Reena found this a little strange but decided to talk to Vishal about this first. She decided to visit Vishal.



Vishal I have received a call from ABC Financiers today. They told me you have borrowed Rs. 1 Lakh from them and have missed your instalments. And if you do not repay them, they will take strict action against you.

What I don't understand is why are they calling me? Did you give my number to them or something?

Ohh Reena! This time I have landed myself into a huge mess. I have taken a loan of Rs. 10,000 only. But now in repayment, they are asking me to pay them Rs. 1 Lakh or they will start calling people known to me and tarnish my reputation.





Explain in detail what happened?

I was in a need of money. I heard about this app named ABC Financiers, which provide small amount loans at the rate of interest of 5 % p.a for a period of 7 days. I thought of downloading this app. In the excitement of taking loan at such a low rate of interest, I didn't properly check the permissions of the app and completed the procedures for borrowing money. Rs. 9,200 was disbursed in my account after deducting the processing fees.

On the due date of repayment, due to some errors in the app, my repayment was not processed. Now, they are harassing me to repay them Rs. 1 Lakh or else they will contact my relatives from my Contact List and tarnish my reputation.



Vishal!! This is not a way to fulfil your financial needs. You should have checked the authenticity of the app before applying for loan and you should be very careful while giving the permissions.

Fraudsters mostly target people from low or medium income groups. They are offered small amounts (Rs 10,000- Rs 20,000) as loan. The victim is asked to upload their KYC details and accept the terms and conditions of these loan apps. The amount is transferred to the victims' bank accounts after deduction of processing fees. If the remaining amount is not repaid within the stipulated time the interest and penalties together take upto 200% of the loan amount.

After few days, the victims start getting calls and messages on their Whatsapp and phone to repay the loan amount. The tricky catch here is that the amount of money being demanded from the victims is much higher. If the victims start questioning or arguing, the scammers threaten the victims to morph their personal photos in an obscene manner and make them go viral by sending them to their contacts in the phone or even threaten to upload their vulgar photos and videos on social media platforms in order to mentally pressurize them.

Now you should report this app on App Store platform and lodge Cyber Complaint. And remember the loans are never this cheap.

Precautions

1. Consumers should never share copies of KYC (Know Your Customer) documents with unidentified persons, unverified/unauthorised apps and should report such apps/bank account information associated with the apps to the law enforcement agencies concerned or use the Sachet portal.
2. Remember that the real and original loan app companies would always be registered with the Reserve Bank of India (RBI). Before downloading them from the Google Play Store, ensure to check the registration number of these loan companies from the RBI's website. All legal lending companies are required to clearly show the same along with their Company Identification Number (CIN) and details of the Certificate of Registration (CoR) with RBI.
3. Always read the reviews of these loan apps before downloading them. Most of these loan apps have a very less rating and if you carefully scrutinize the comments on the user reviews, you might come across people who have already been a victim of them.
4. If a loan app appears to be too good to true, it is surely a scam. Always get the loan from RBI authenticated and verified lenders.
5. If a loan app is asking for unwarranted permissions from the user to access their contact lists and media gallery including photographs and videos from the phone, it is a sure-shot sign of a scam app.
6. If you get threatening calls and messages from the scammers to repay an unjustified amount of money, simply block them and uninstall the loan app from your phone. Also, revert to factory settings on your phone so that the scammers do not have any access to your phones.
7. Tell your contacts that you have been a victim of these fake loan apps and politely request them to ignore the calls and messages of these scammers.
8. Report the matter to the RBI and also report these fake loan apps to the Google Play Store to be removed. Be a responsible citizen and an aware consumer to educate the people.
9. Unsubscribe to mails providing links to a bank, e-commerce and/or search engine website. Block the sender's ID before deleting the email.
10. Always check the list of fake apps before downloading them.
11. When downloading an app, only give permissions that are absolutely essential for using the application.





About the Chapter

With evolving technology, the cybersecurity space is facing new threats everyday. People are getting ease with the gadgets but are also getting vulnerable to cyber attacks like phishing. In a recent call out, Researchers have highlighted the surge in OTP bots and SMS senders which are being used by cyber criminals to amplify their malicious activities.

Less of a cyber security threat and closer to a scam, Vishing refers to attempts to steal information or money over the phone by convincing the victim. Attackers may pose as employees of a trusted company, such as a bank or government agency, in order to gain the victim's trust.

A recent report by CloudCEK, a cybersecurity firm, has raised alarm over the growing number of scams that combine vishing techniques (tricking people over the phone) with OTP grabber services (to steal one-time passwords) to trick people into sharing their personal information, particularly for financial gain.

Highlighting the seriousness of the growing threat, it is advisable to be careful while sharing any information over call.

Here, we are with one of the situation where Vishal got trapped in vishing attack.....



Chapter 17: VISHING ATTACK

One day, Vishal received a call from a person named Ajay, who introduced himself as a representative from ABC Bank. Since Vishal had savings account with ABC Bank, he did not suspect irregularity.



Hello Sir! I am Ajay calling from ABC Bank. You have a saving account with our bank.

Yes, I have.

Sir, there is a problem with your account. Therefore I need you to verify your identity. When I will generate the OTP you need to share the same for verification.



Vishal, without giving a second thought shared the OTP instantly with Ajay.

After few minutes....



I did not make any transaction amounting to Rs. 20,000 right now. How come my account is debited with this amount? Let me check my bank statement.



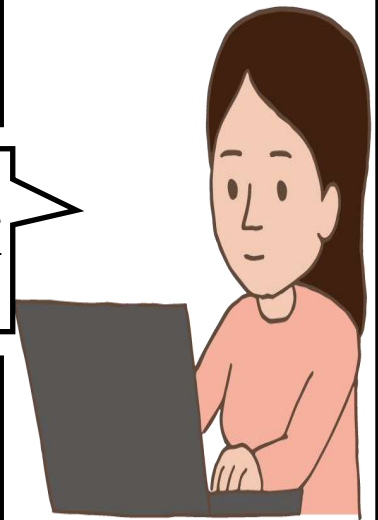
After checking his bank statement, he identified a transfer of Rs. 20,000 which was not done by him. He, instantly decided to call his bank



Hello! I am Vishal. There is fraudulent transaction of Rs. 20,000 from my bank account. What should I do now?

Hello Sir ! Don't worry. I am here to help. But prior to that can you please confirm your details of the fraudulent transaction?

There is transfer of Rs. 20000 from my account today which was not carried out me. I request you to block my account till further instructions.



The Customer Care executive blocked his account for further transfers.

Vishal rushed to Reena and explained the entire incident.....



Vishal!!! I have explained you so many times but you are not going to understand.

But thank god!! This time you had immediately informed of the fraudulent transaction.

This was Vishing attack, where an attacker calls a victim and pose as a bank employee. The attacker might make convincing excuse ask the victim to give their OTP. After receiving the OTP, they access victim's bank account and steal their money.

Since, you have informed your bank immediately of financial frauds, any loss suffered after reporting of the unauthorized transaction shall be borne by the bank.

You should also report the fraud with National Cybercrime Reporting Portal (<https://cybercrime.gov.in/>).



Precautions

1. Do not provide personal and sensitive information in order to receive prize/lottery/gift/ updating KYC etc. Legitimate organizations will never ask for this information over the phone.
2. Use the customer care service numbers available on authorized websites of the institute/ organizations/ banks etc.
3. Verify the caller's identity: If you're uncertain about the caller's identity, hang up and contact the organization directly. Use contact information from the organization's website or a trusted source, not from the caller.
4. Do not respond to unsolicited calls: Vishing scams often begin with an unsolicited call from someone claiming to be from a legitimate organization. If the call seems suspicious, do not provide any personal information and hang up immediately.
5. In case of any incident, users should call 1930 and change the password of their account immediately or block the card/ freeze the account to prevent financial loss.
6. Block Robo-call. Scammers also use technologies to do their job. They frequently use automated calls with an automatic delivery message for you. When you respond to that call, they come online and start talking with you, which looks very real.
7. Register for the National Do Not Call Registry to avoid spam calls.
8. Do not follow instructions to call a number provided. If the caller directs you to call a certain number, do not follow it. This could be an attempt to get you to call a spoofed number that looks legitimate but is actually a scam.
9. Attackers could request remote access to your computer under the guise of removing malware or fixing some issue. You should never grant anyone access to your computer, unless they are a verified member of an IT department.
10. Use mobile applications to verify any unknown number that calls you.
11. Don't respond to emails or social media messages that ask for your phone number. This tactic is often the first step in a targeted vishing attack. Instead, report these emails and messages to your IT team.
12. Explore and enable protection features on your phone that block or filter out spam calls.





About the Chapter

Top-notch browser protection starts with you. That is why you need to have enough knowledge on how to browse the mobile web more securely. By adopting the best mobile web browsing behavior, you can lessen the risk of mobile security threats infiltrating your phone.

To ensure browser protection, avoid clicking unfamiliar links. Cybercriminals often use these to direct their victims to a phishing page, a malicious web page designed to look like a legitimate one (e.g., your bank) and lure you into giving up your sensitive data.

You can also execute proper web browsing behavior by providing sensitive info only to secured websites. To determine if a website is secure, check if a padlock is present on the web browser's address bar. This way, you can ensure that the traffic between you and the mobile website is encrypted, which means that if you sent private information to a secured website, it remains private.

In this Chapter, you will learn how to change your browser settings to make it more secure...



Chapter 18: Browser Safety Settings

Vishal and Reena met with their friends for Diwali get-together. A conversation came up regarding the safety features for mobile browsers. Since Reena is our Cyber Guru, she told them some safety settings for their browsers...



Which browser do you commonly use? Do you know if it is safe?

Google Chrome. Safe? How can we check that?

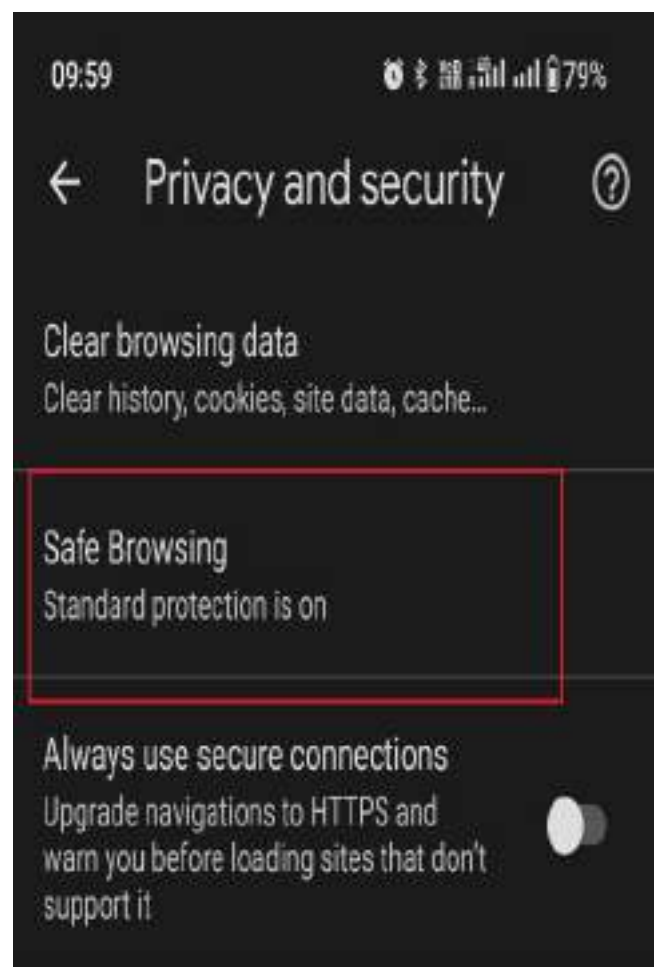
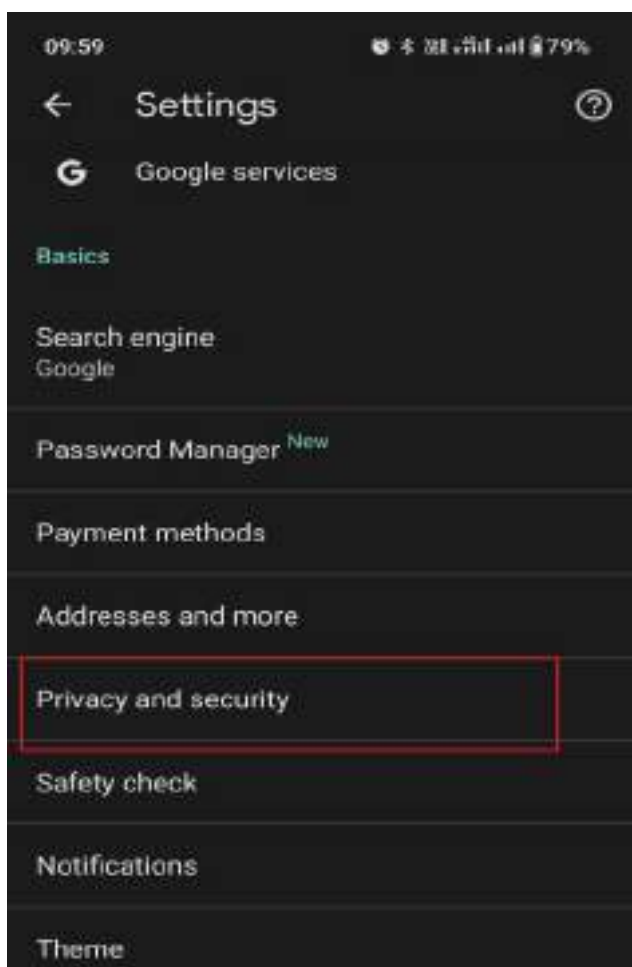
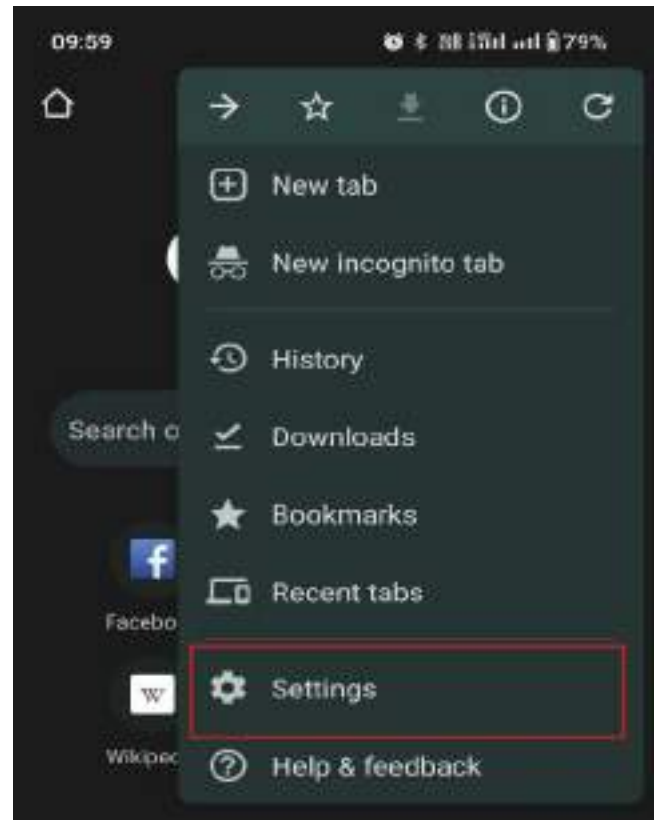
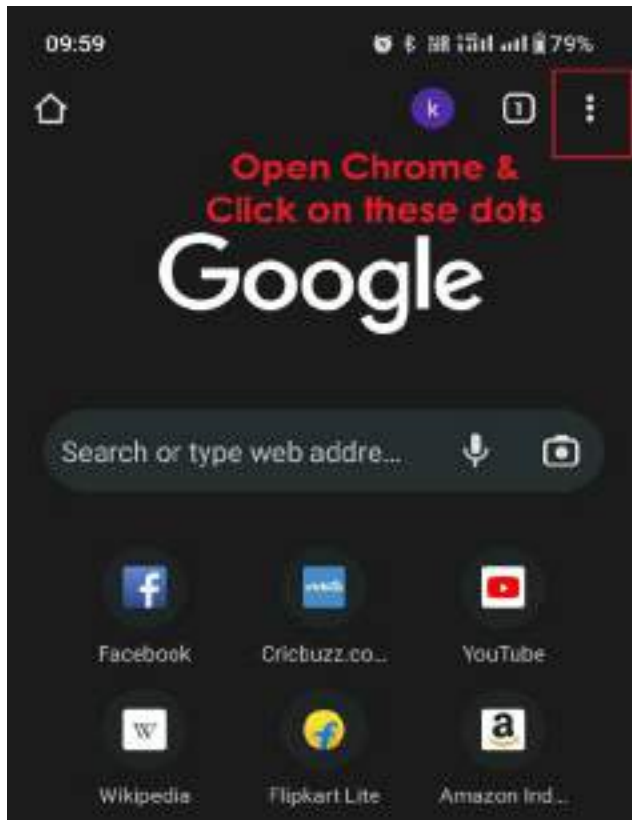
Let me tell you why is it important. Then I'll show you how you can enable them.

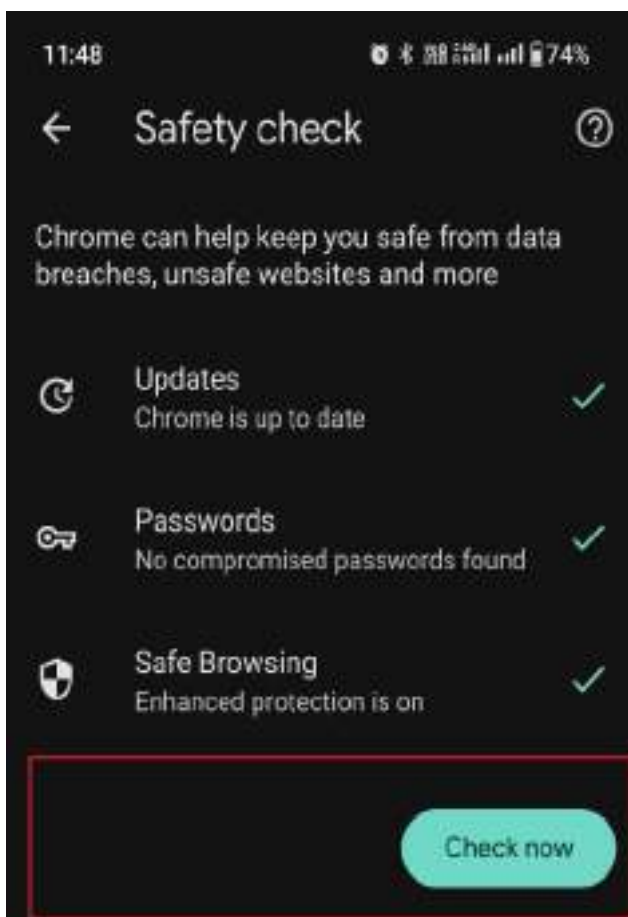
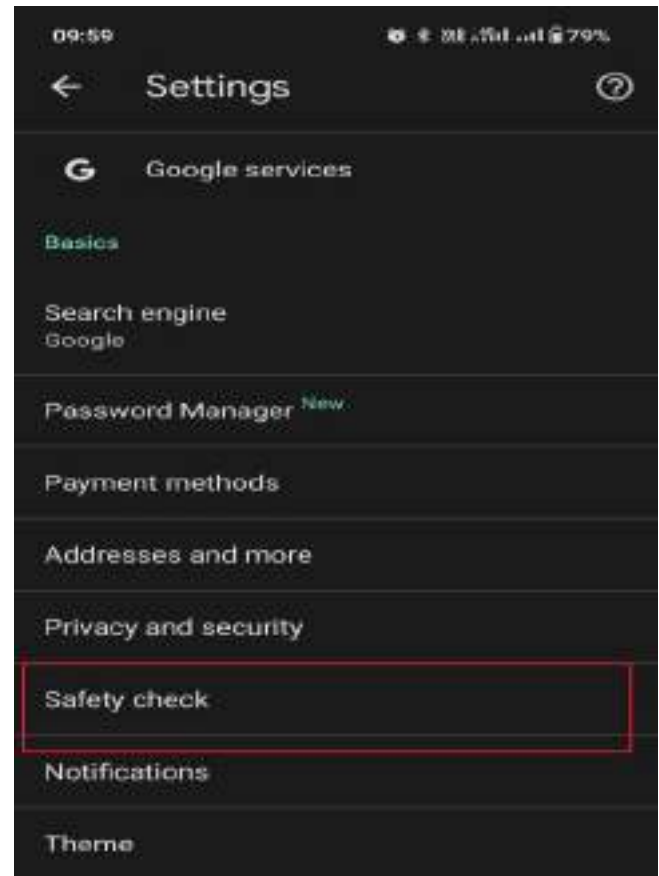
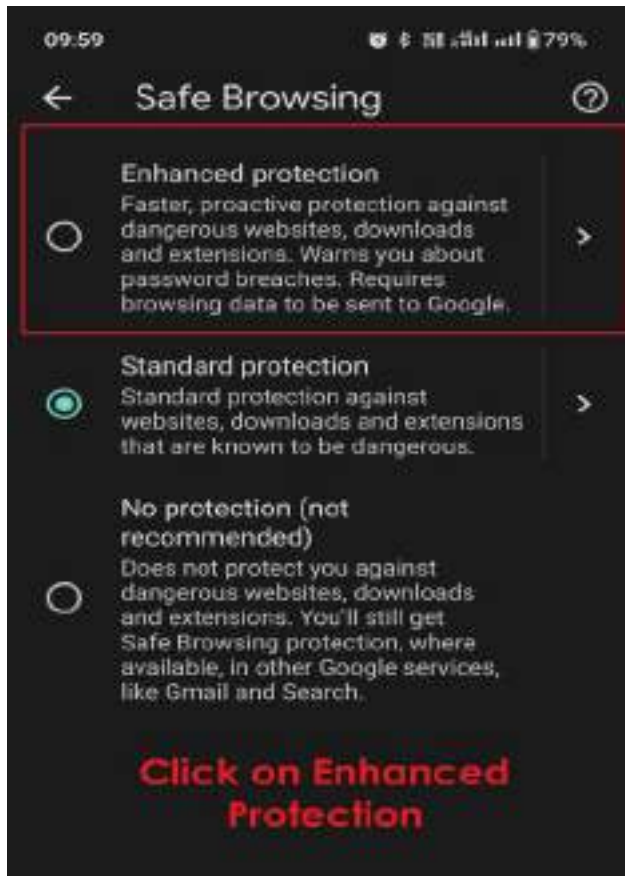
A secure browser is one that has extra security measures to help you avoid illicit third-party actions while you're online. These browsers have a list of permitted applications and activities, and they don't allow functions that aren't on that list to run.

Safe browsers prevent certain behaviors from occurring in the first place, making it a more proactive approach to remain protected on the internet. Third-party technologies, such as cookies, are blocked by safe browsers. Cookies save information about you, such as the websites you've visited, usernames and passwords, and other tracking information. Safe browsers don't divulge your identity. You're only masking your IP address, location, and data in transit if you utilize a VPN. Through leaks or browser fingerprinting, your browser can still reveal your identity, however, safe browsers help you hide your identity for safety reasons.

Now follow the steps to enable the security feature...







Guys!! I have enabled these settings. You should do it too.





About the Chapter

The dark web is a part of the internet that can usually only be accessed using a specialized browser. While it's infamous for illegal and other criminal activities, people also turn to the dark web for valuable anonymous activities like bypassing censorship, journalism, and whistle-blowing.

The dark web can be a dangerous place. It's also important to note that smartphones, in general, aren't the most privacy-friendly devices (think GPS tracking) and have plenty of vulnerabilities that can be exploited.

"Most organizations don't find out their information has been compromised and that their employees or clients have been put at risk until they read about it along with the general public," says John M. "By that point, it is much harder to recover the leaked information and implement damage control."

In this Chapter, you will learn how to check your data shared on dark web and ways to protect yourself from the dark web...



Chapter 19: Dark Web

Vishal and Reena were having discussion on cyber security. Since Reena is our Cyber Guru, she told Vishal about the dark web...



Vishal, the dark web refers to encrypted online content that is not indexed by conventional search engines.

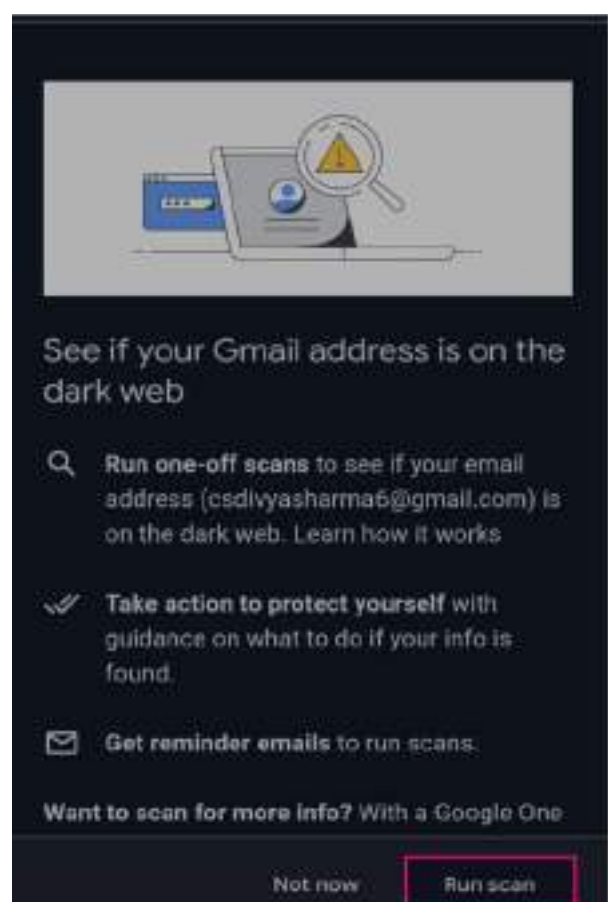
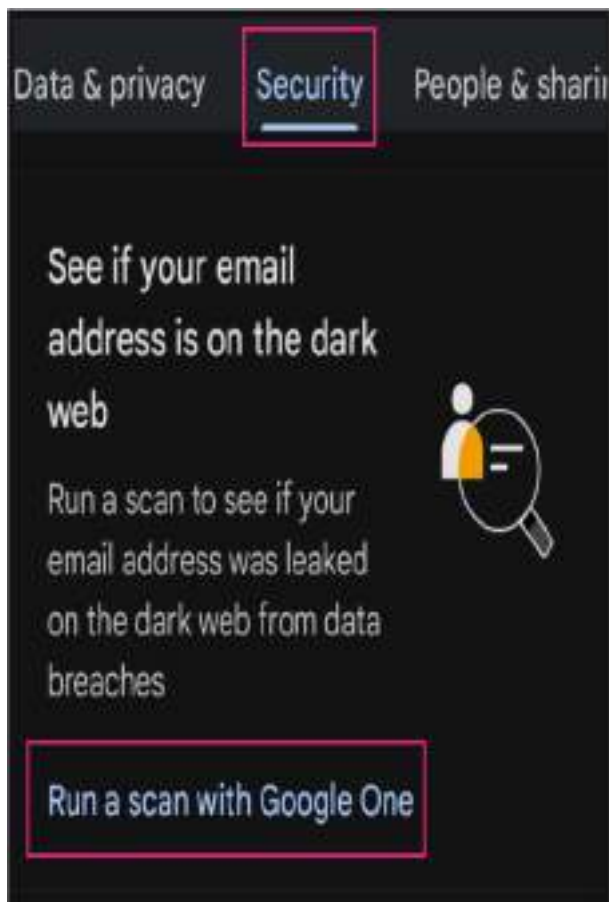
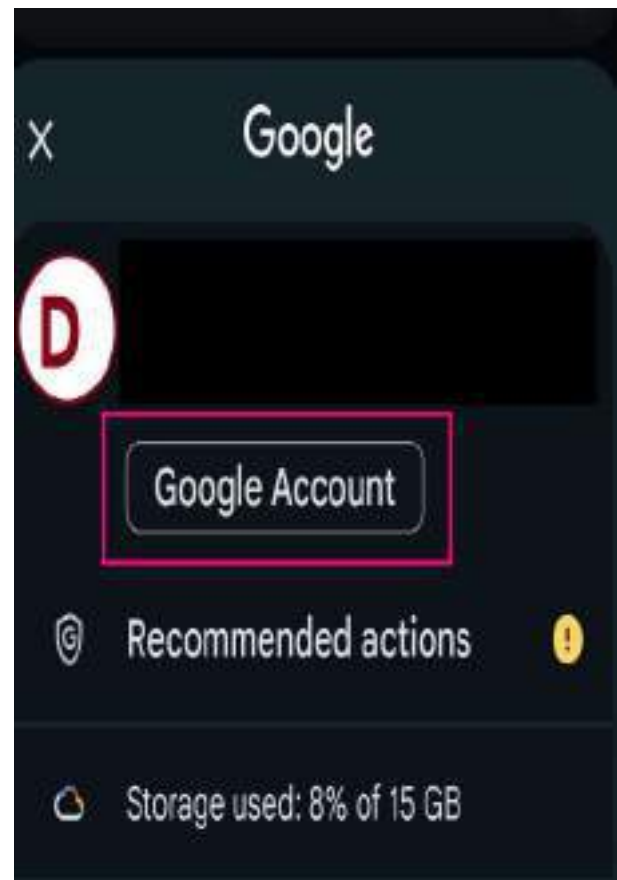
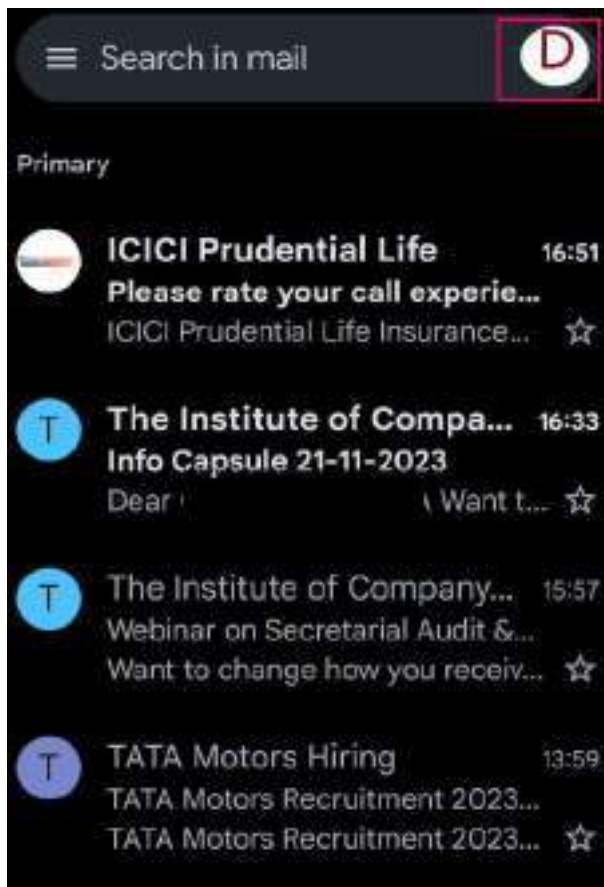
Specific browsers, such as Tor Browser, are required to reach the dark web. The dark web pulls up sites using information that isn't indexed online, such as bank accounts, email accounts, and databases.

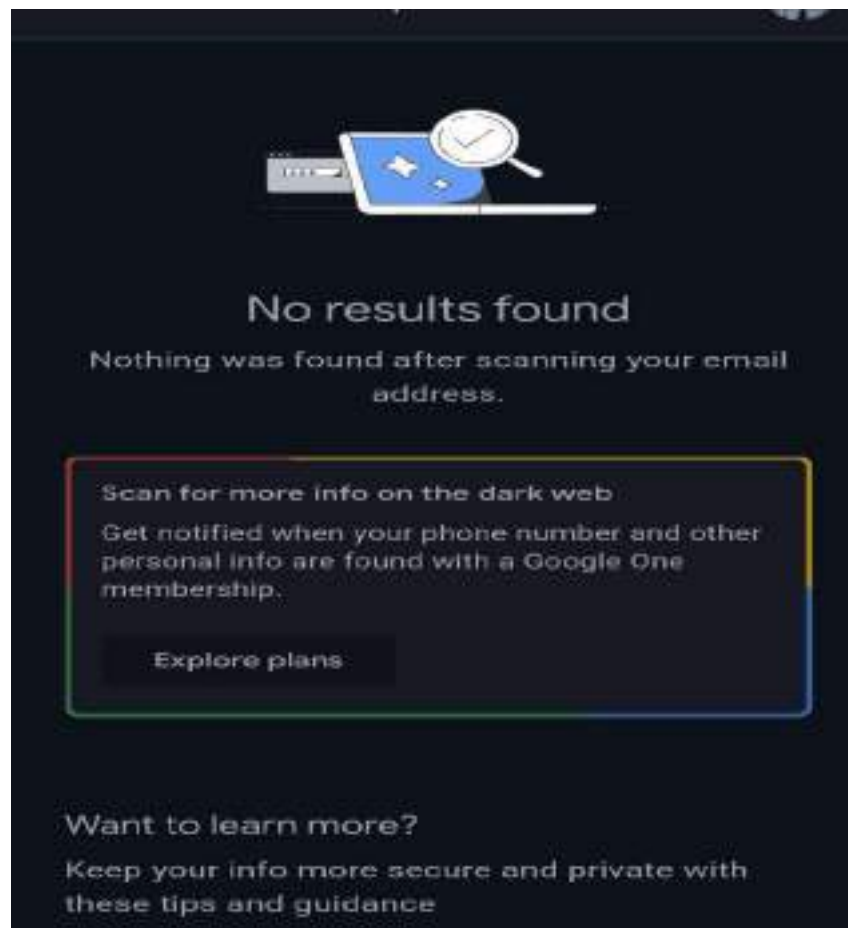
People who use the dark web can maintain their privacy and freely express their views. It also has a reputation for being associated with illicit and unethical activities.

You can check for data on the dark web that might be associated with your email address or other info you add to your monitoring profile. Breach results may contain information including

- Your name
- Address
- Phone number
- Email
- Social Security Number (SSN)
- Username
- Password

You can check your data shared on dark web using your gmail account:-





If you find any name in place of no result found this means your data has been shared with those persons...

Thank you Reena...
I will also check this.





Precautions

1. Create strong, unique passwords for each of your online accounts
2. Use a password manager on your computer and mobile devices
3. Enable two-factor authentication
4. Use a VPN
5. Don't enter sensitive information on public computers.
6. Stay away from unsecure sites such as those without a secure socket layer (SSL) — especially if the site sells products and services, or asks for financial information.
7. Do not reply to unsolicited email messages.
8. Refrain from publishing personal information on social networks.
9. Keep your device up to date.
10. Install a robust antivirus.
11. Use caution with suspicious emails.
12. Use a good dark web monitoring service to detect and anticipate cybersecurity threats. These tools help to find leaked or stolen information such as compromised passwords, breached credentials, intellectual property and other sensitive data that is being shared and sold among malicious actors operating on the dark web.



About the Chapter

Google Play Protect is a malware protection and detection service built into Android devices that use Google Mobile Services. It helps protect mobile devices by scanning for malicious applications on Android devices and removing any potentially harmful software. It also warns users about apps that violate the Unwanted Software Policy by hiding or misrepresenting important information.

Applications are automatically checked when installed and are periodically scanned in the background. Users can also initiate a scan directly.

When a potentially harmful app is detected, Android users receive a notification and the option to uninstall the app. Google Play Protect can also disable such apps and keep them from running until users uninstall them. Particularly concerning apps could be removed automatically, in which case the user is notified. The users can also change their mobile settings so that installation from unknown sources are disabled.

Let's see how we can do it.



Chapter 20:

Google Play Protect Feature

One day, Vishal was downloading an app from Play Store. He noticed that while downloading the app, a line was written below the downloading status. He decided to ask Reena about this.



Hey Reena! I was downloading this app and noticed a line written below the downloading status stating "Verified by Play Protect".

What is this?



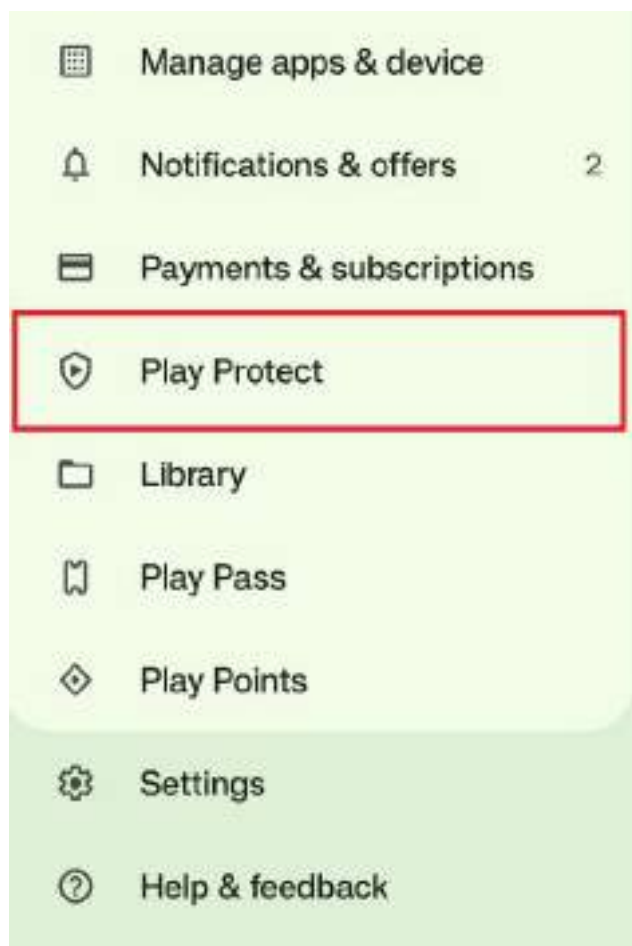
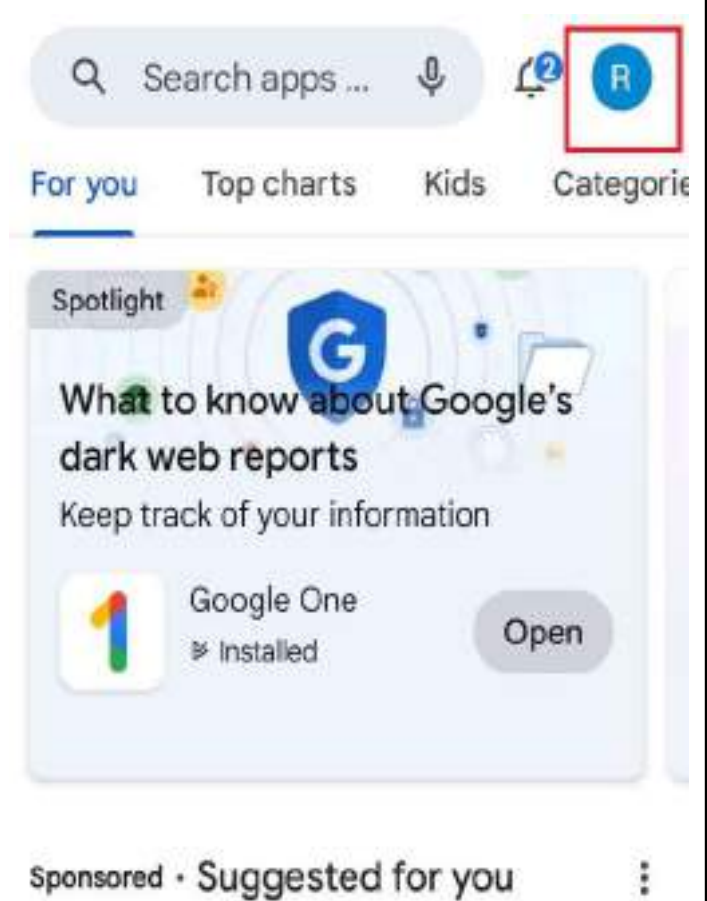
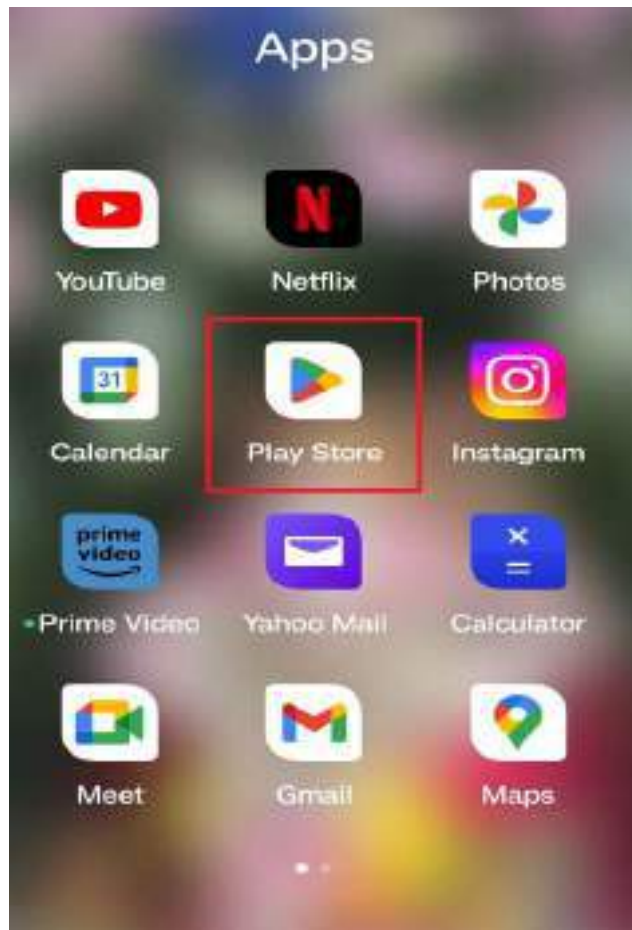
Vishal, Google Play Protect is a feature of Google Play Store which helps protect mobile devices by scanning for malicious applications on Android devices and removing any potentially harmful software.

It also warns users about apps that violate the Unwanted Software Policy by hiding or misrepresenting important information.

Applications are automatically checked when installed and are periodically scanned in the background. Users can also initiate a scan directly. Google Play Protect is found on a device by opening the Play Store and selecting "My Apps & Games."

You can also check whether this feature is enabled without downloading any app. Let me show you how you can do it....





← Play Protect settings

General

Scan apps with Play Protect

Play Protect can scan this device and warn you about harmful apps



Improve harmful app detection

Send unknown apps to Google for better detection



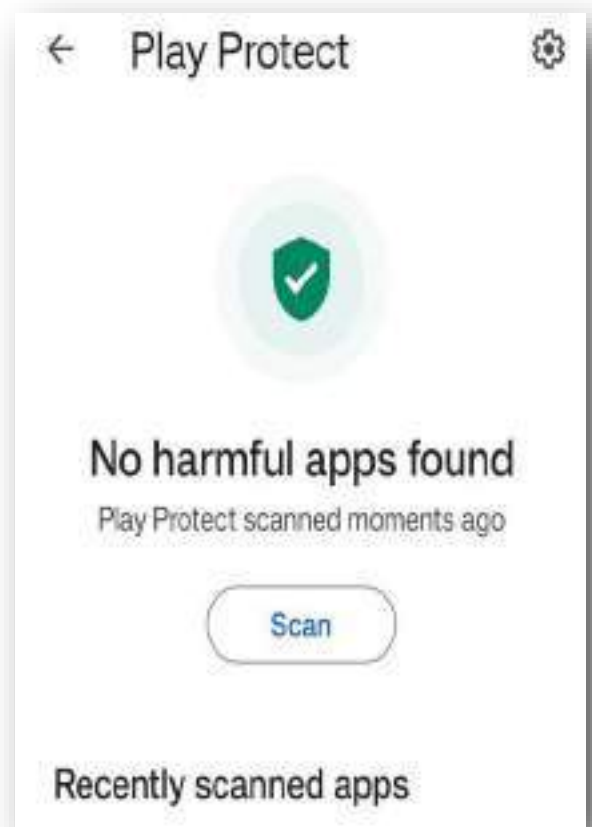
App privacy

Permissions for unused apps
Review permissions for apps that you haven't used in a few months



You can also scan your existing apps through Play Protect Feature.

Just Click on Scan and it will run a thorough check on your mobile phone.

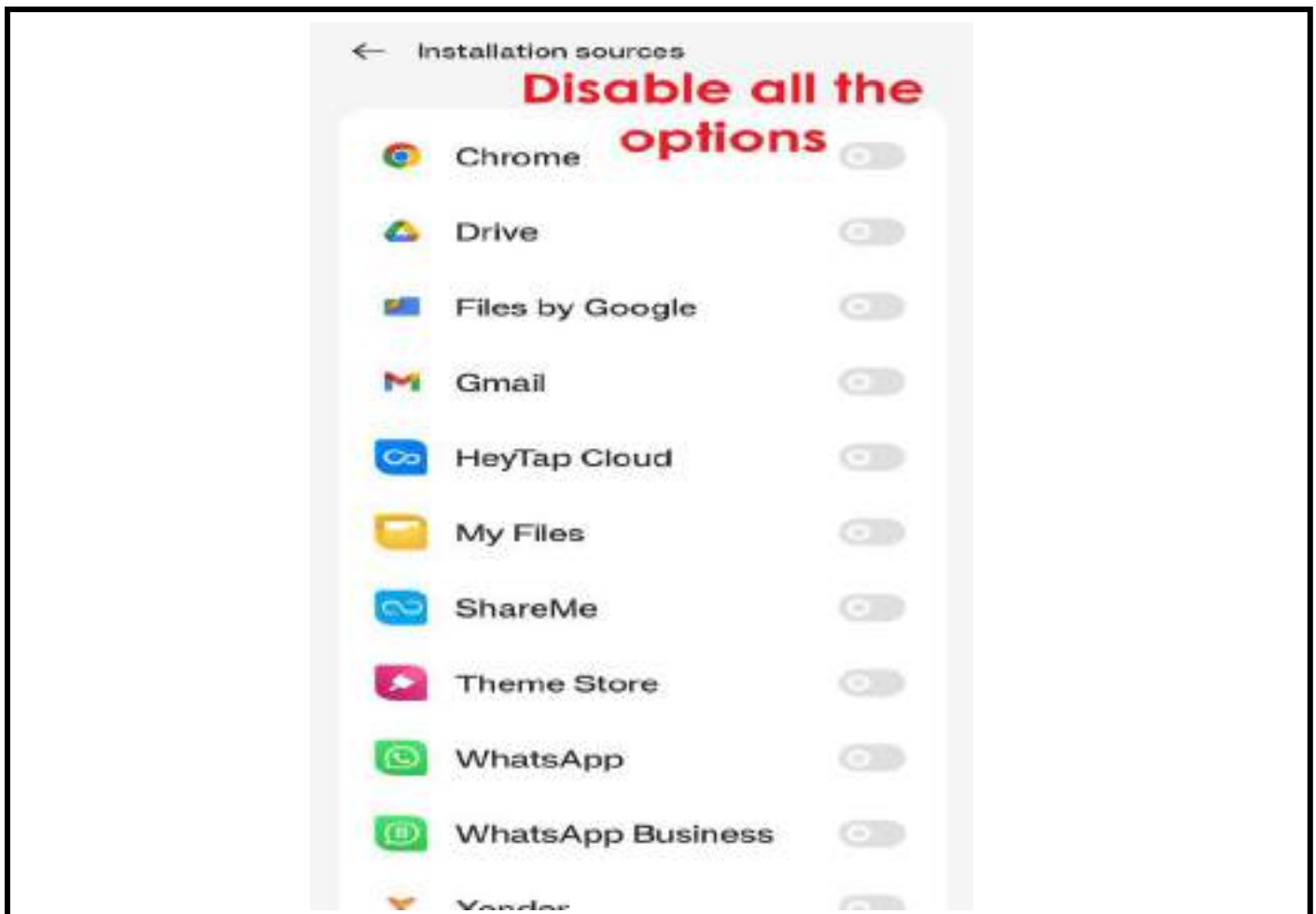
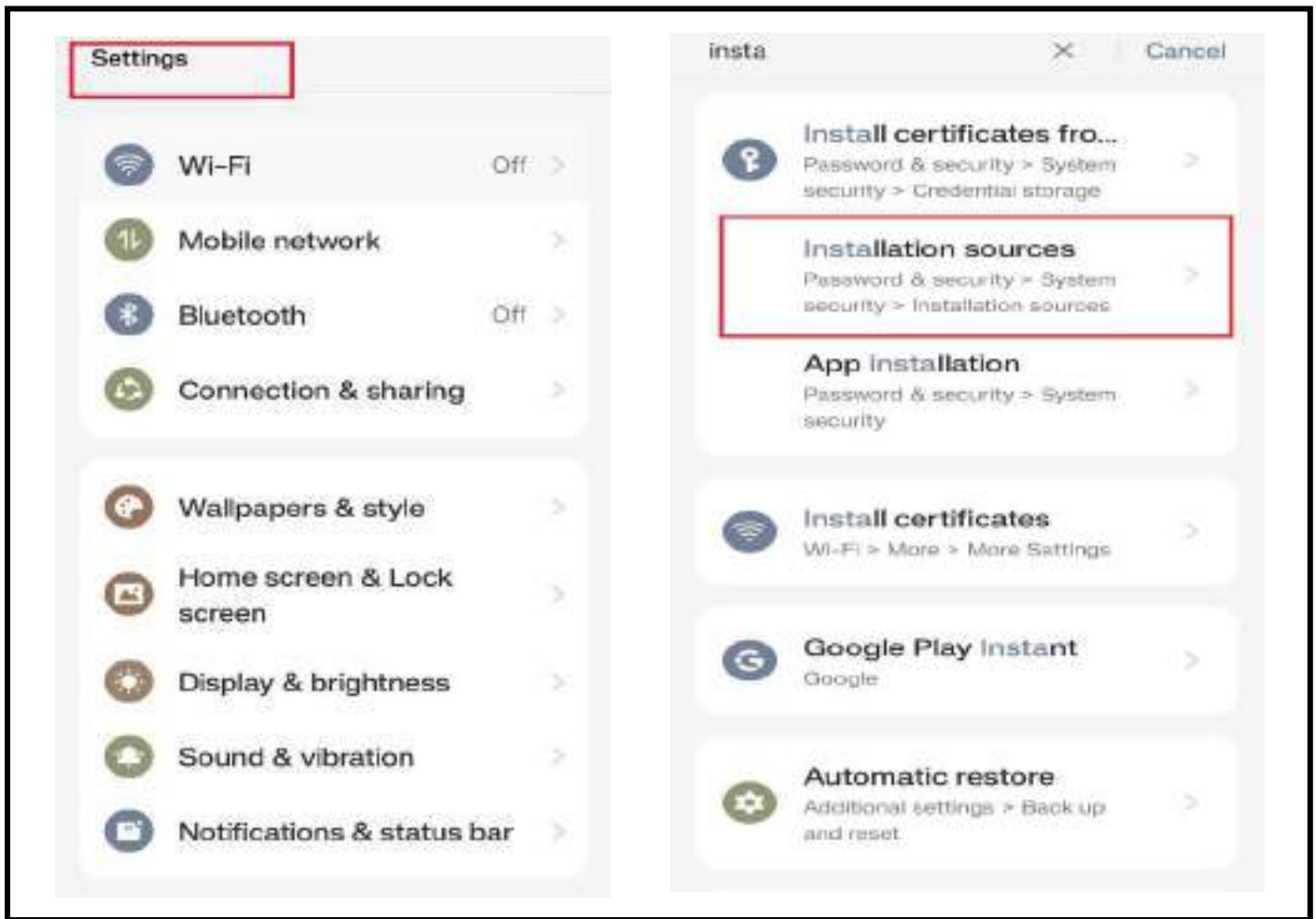


Also, You should always download the apps from Google Play Store/ App Store.

Apps downloaded from untrusted sources often cause a malware attack on your mobile phone.

You should disable Downloading/ installation from untrusted sources in your phone settings.

Let me show you....





GYAAN KA SAAR



Precautions

1. Uninstall those apps which are not in use as it will improve your phone's performance and make it more Secure.
2. Review the App permissions twice before granting them.
3. Download apps only after reading its reviews, ratings and number of downloads.
4. If you are not sure about the app you just downloaded, it's always safe to browse the internet and know more about it.
5. Keep your device and apps updated so that latest security features are available and your personal data is protected at all times.
6. Many apps will request specific permissions on your device, such as access to your camera for taking photos, the gallery for media editing, or your contact list for making calls. Common permissions requested by apps include access to:
 - Contacts
 - Photo Gallery
 - Location
 - Calendar
 - Browsing history
 - Microphone
 - Camera
 - Storage
 - Calls

Grant only those permissions which are absolutely necessary for the purpose of the app.



About the Chapter

Truecaller is a mobile app available for Android and iOS devices that automatically filters and block untrustworthy calls to prevent spam.

Users will simply need to provide their phone number to start using the service. The app will then access their contacts to build up its phonebook and improve its spam database. It even blocks malicious messages before they can reach your device.

Truecaller is generally considered a safe app, but like any software that collects and uses personal data, there are potential security and privacy concerns. The app collects and stores data such as phone numbers, email addresses, and names, which could be vulnerable to cyberattacks. Additionally, the app requires access to a user's phone contacts and call logs, which some users may find intrusive.

Truecaller is generally considered safe, it's important for users to weigh the potential risks and benefits before using the app and to take steps to protect their privacy, such as regularly updating their security software and avoiding sharing sensitive information through the app.



Chapter 21: Truecaller App

One day, Vishal received a call from unknown number. He instantly searched the number on Truecaller. Reena noticed this and decided to ask him about this.



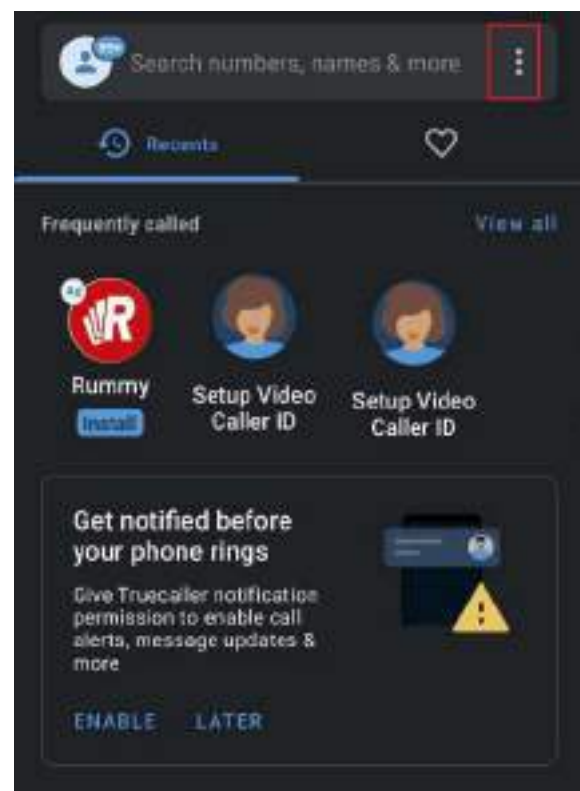
Vishal!! Are you still using Truecaller? Do you know that data of almost 5 crore Indians was leaked on dark Web through Truecaller.

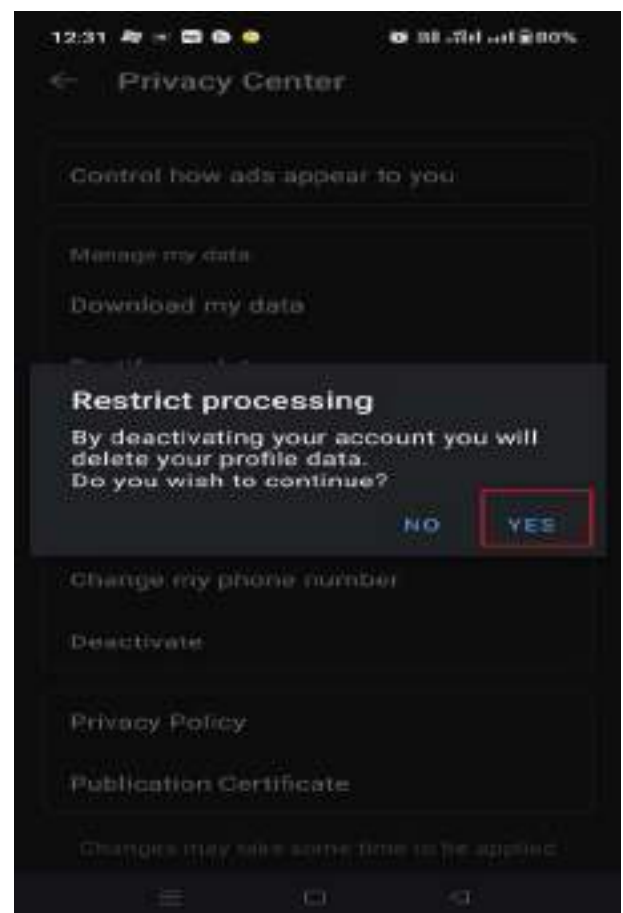
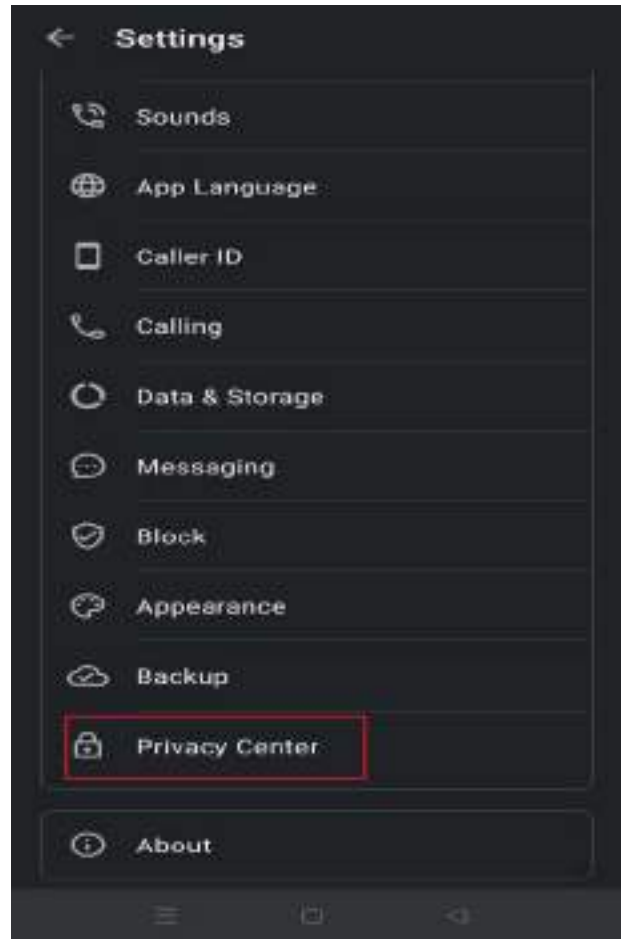
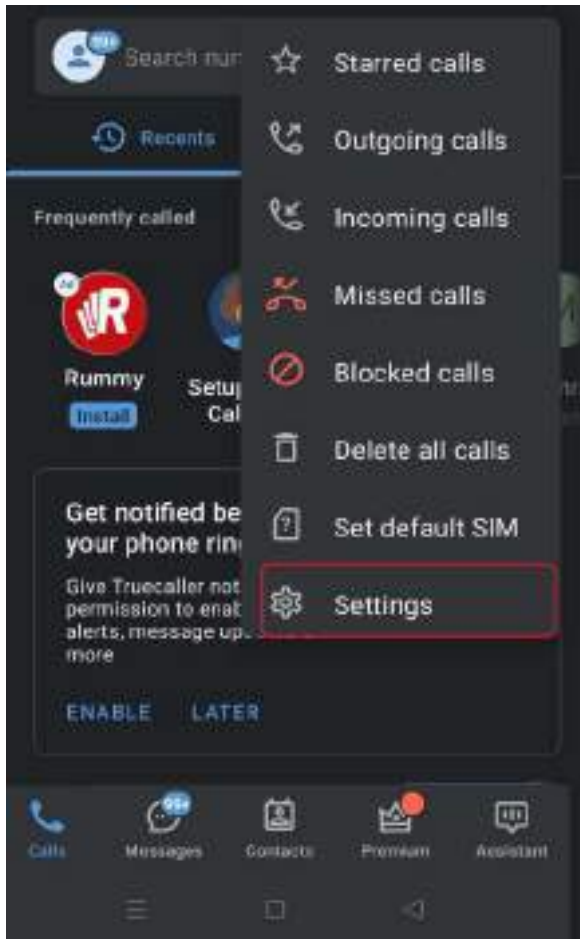
Is it? I didn't know that. Is it possible to delete my data from Truecaller now?

Don't worry Vishal !! I will teach you how to restrict the processing of your data and unlist your number from Truecaller.

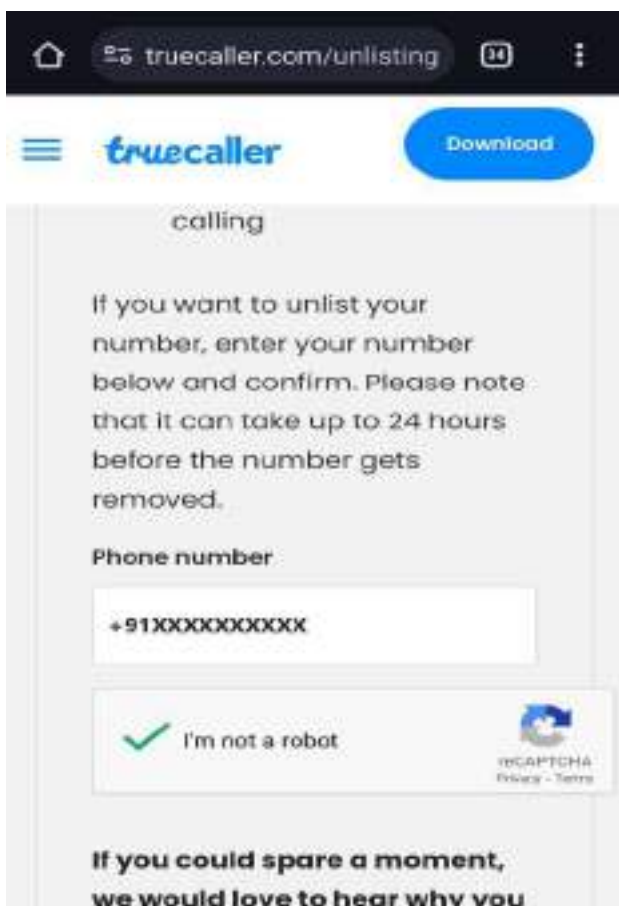
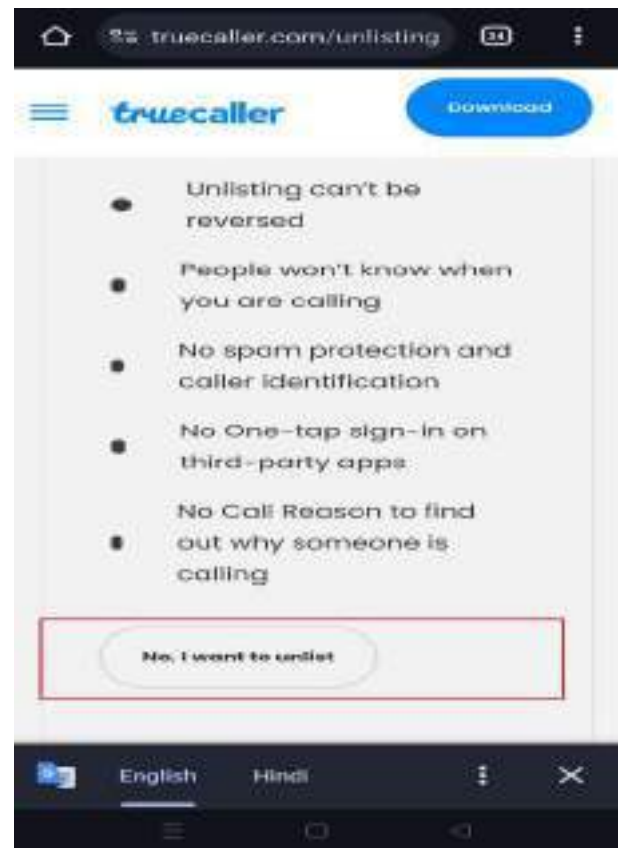
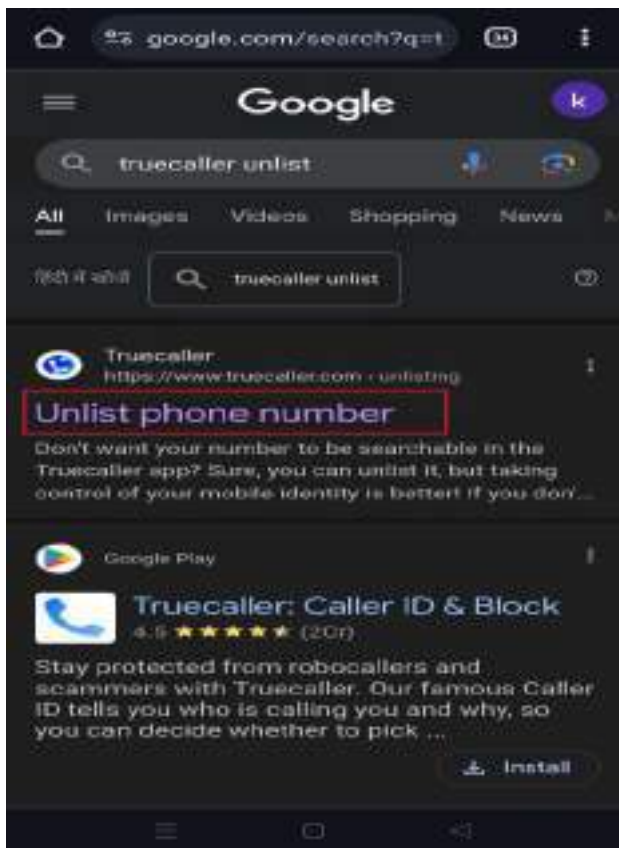


You can deactivate your Truecaller account by opening the Truecaller app in your mobile and following these steps:





Now, open Google account and delist your number from truecaller....





GYAAN KA SAAR



Precautions

1. Keep your device and apps updated so that latest security features are available and your personal data is protected at all times.
2. Pay attention to the permissions the app requests. Grant only those permissions which are absolutely necessary for the purpose of the app.
3. Use different passwords for all your online account.
4. Download apps in official stores
5. Download apps only after reading its reviews, ratings and number of downloads. Also, download the apps after proper knowledge of the app.
6. If you are not sure about the app you just downloaded, it's always safe to browse the internet and know more about it.
7. Do not use truecaller as phone directory.
8. To ignore spam calls, subscribe to DND services of telecom service provider
9. The app should have appropriate security measures in place to protect the privacy and security of the user's personal information
10. Make sure you have an antivirus installed on your phone.



About the Chapter

You need to give certain permissions to apps to work properly. For example, some apps need your location to give location-related information like flight ticket booking, navigation, hotel search, etc. Is it necessary to revert the permission given to an app at the time of uninstalling or after uninstalling?

Unused apps are taking up storage space that you could be using for other things. Some apps are bigger than others. Games, in particular, typically take up a lot of space. If you downloaded a trendy game and played it for a while, it's still sitting there taking up space.

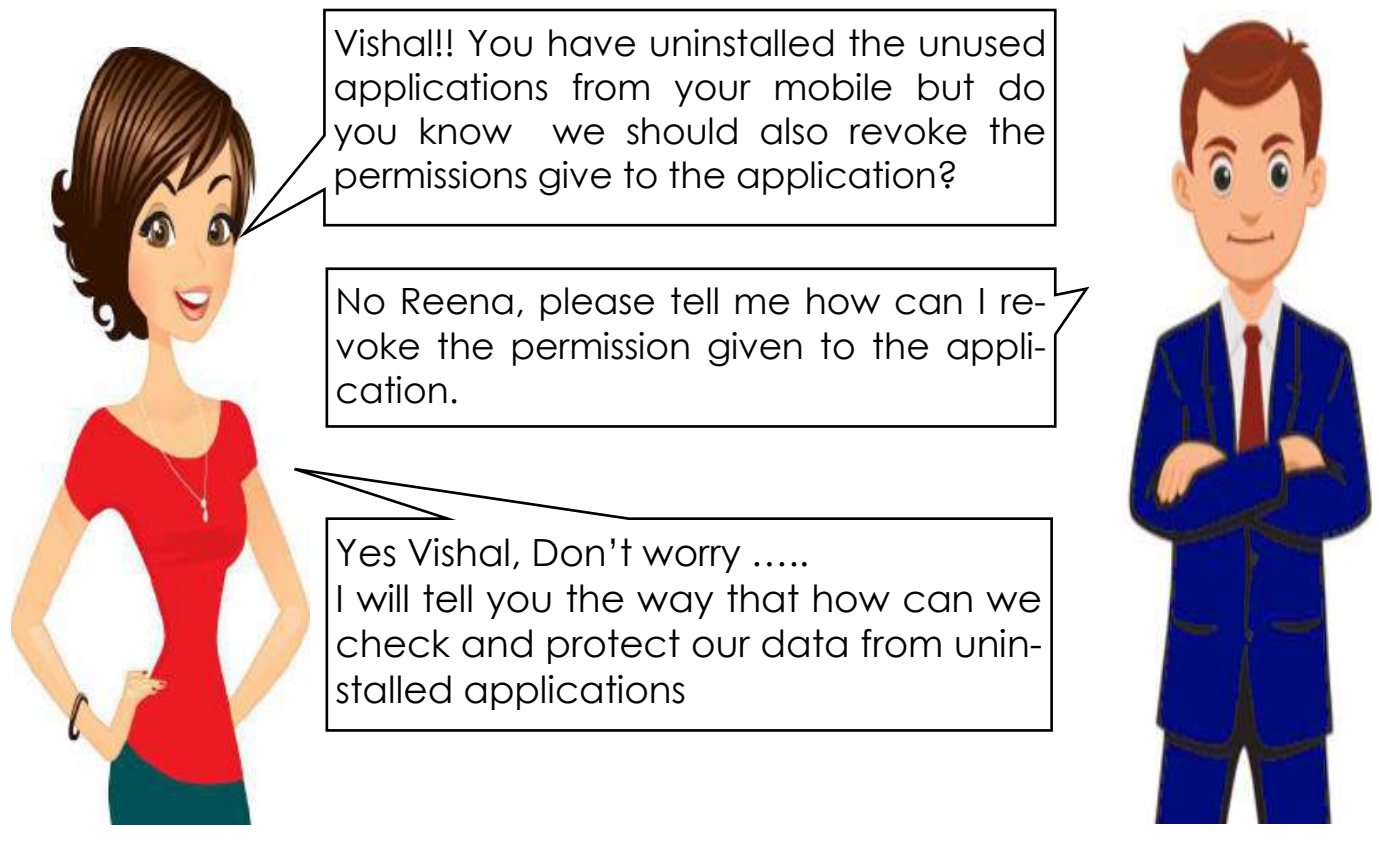
Lastly, cleaning up your phone is a good way to eliminate distractions. A more focused phone experience can make it much more pleasant to use.

This chapter of our Cyber Gyaan will let you know how to remove permission given to uninstalled Android apps.

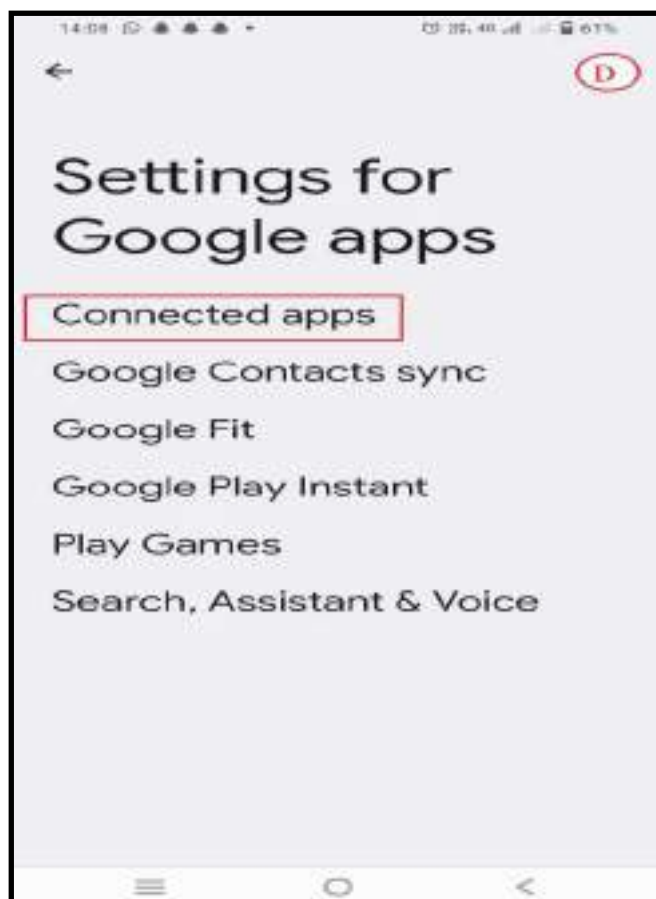
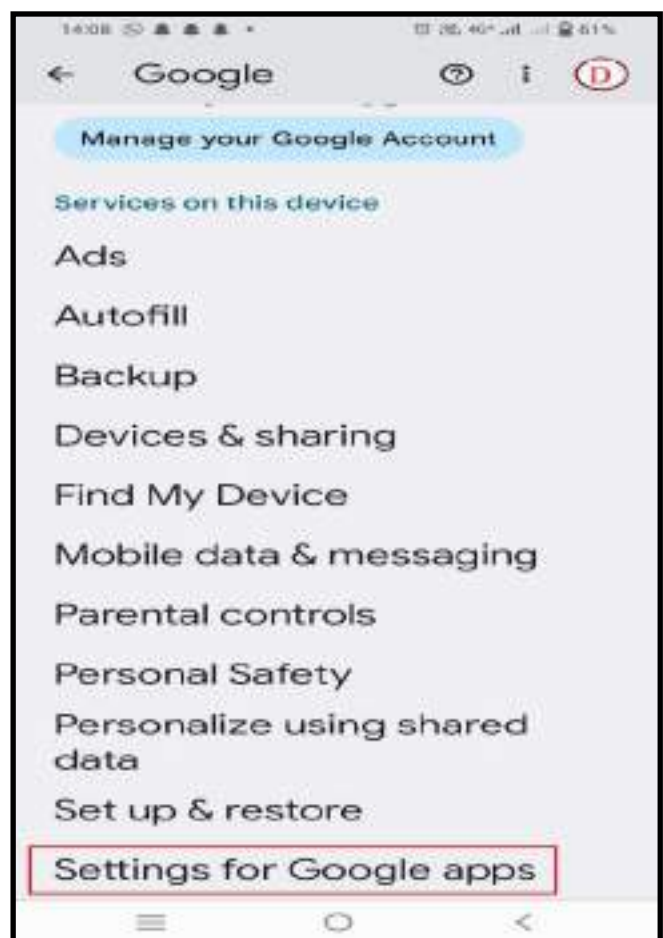
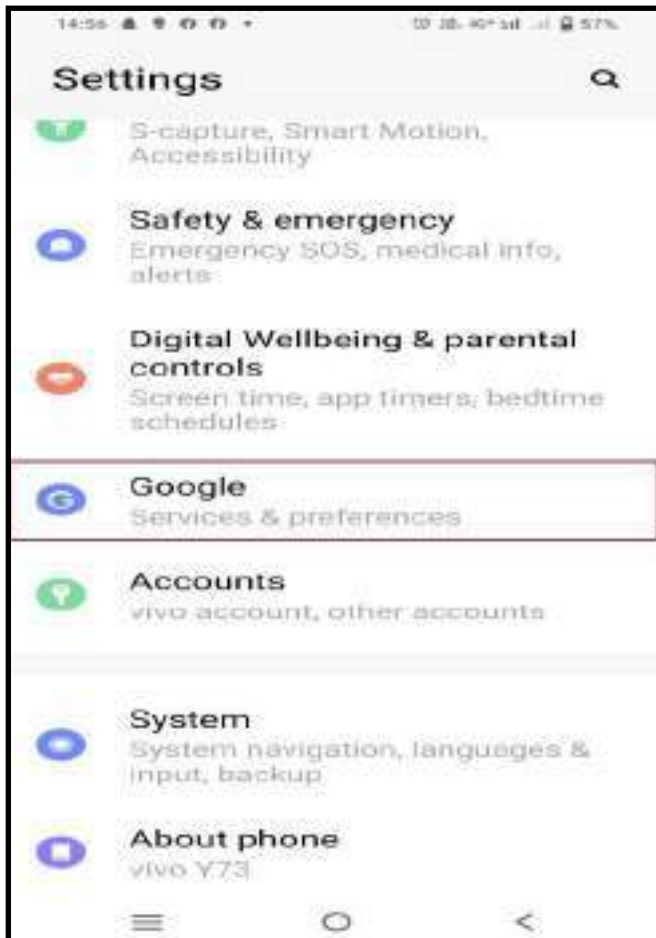


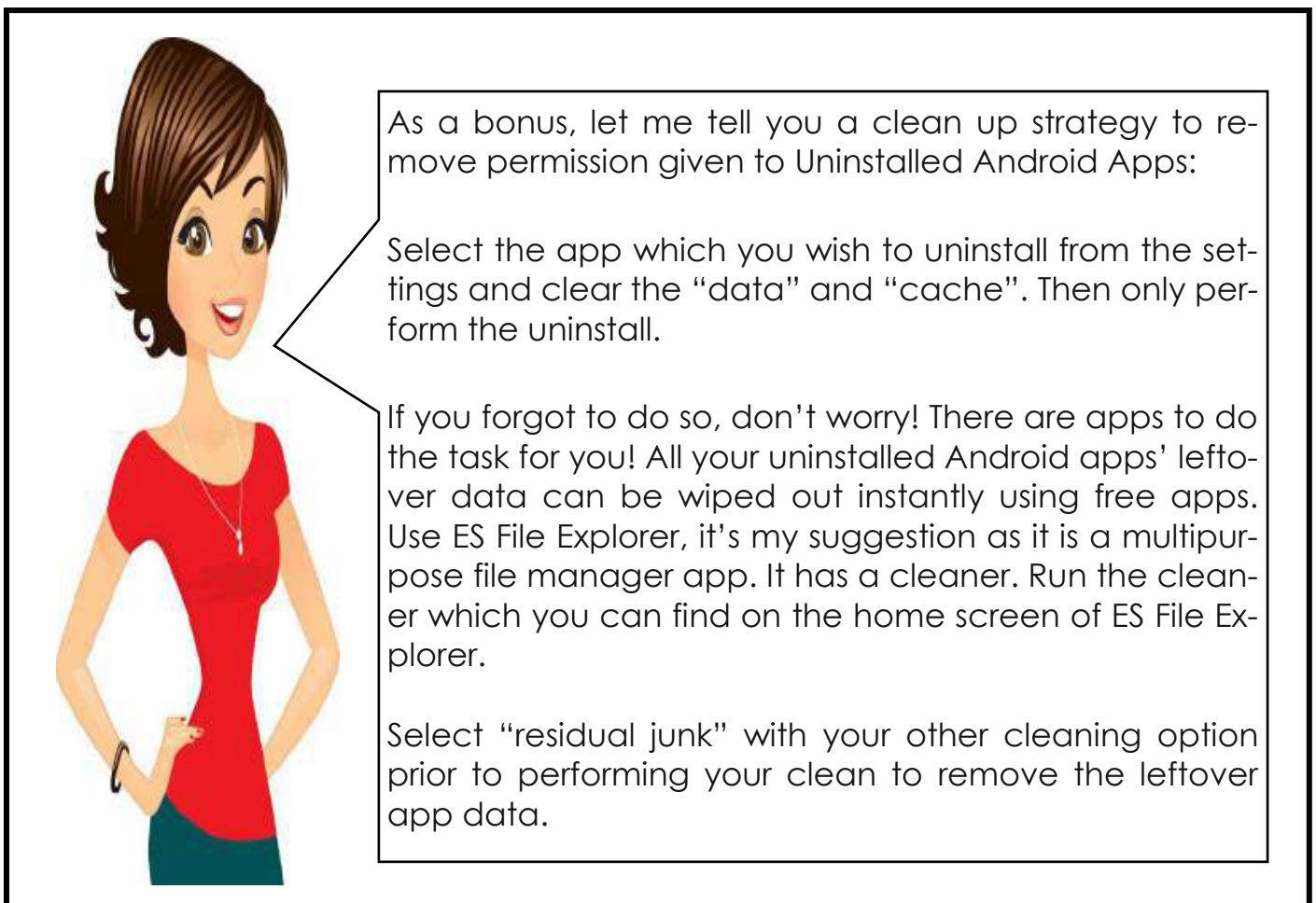
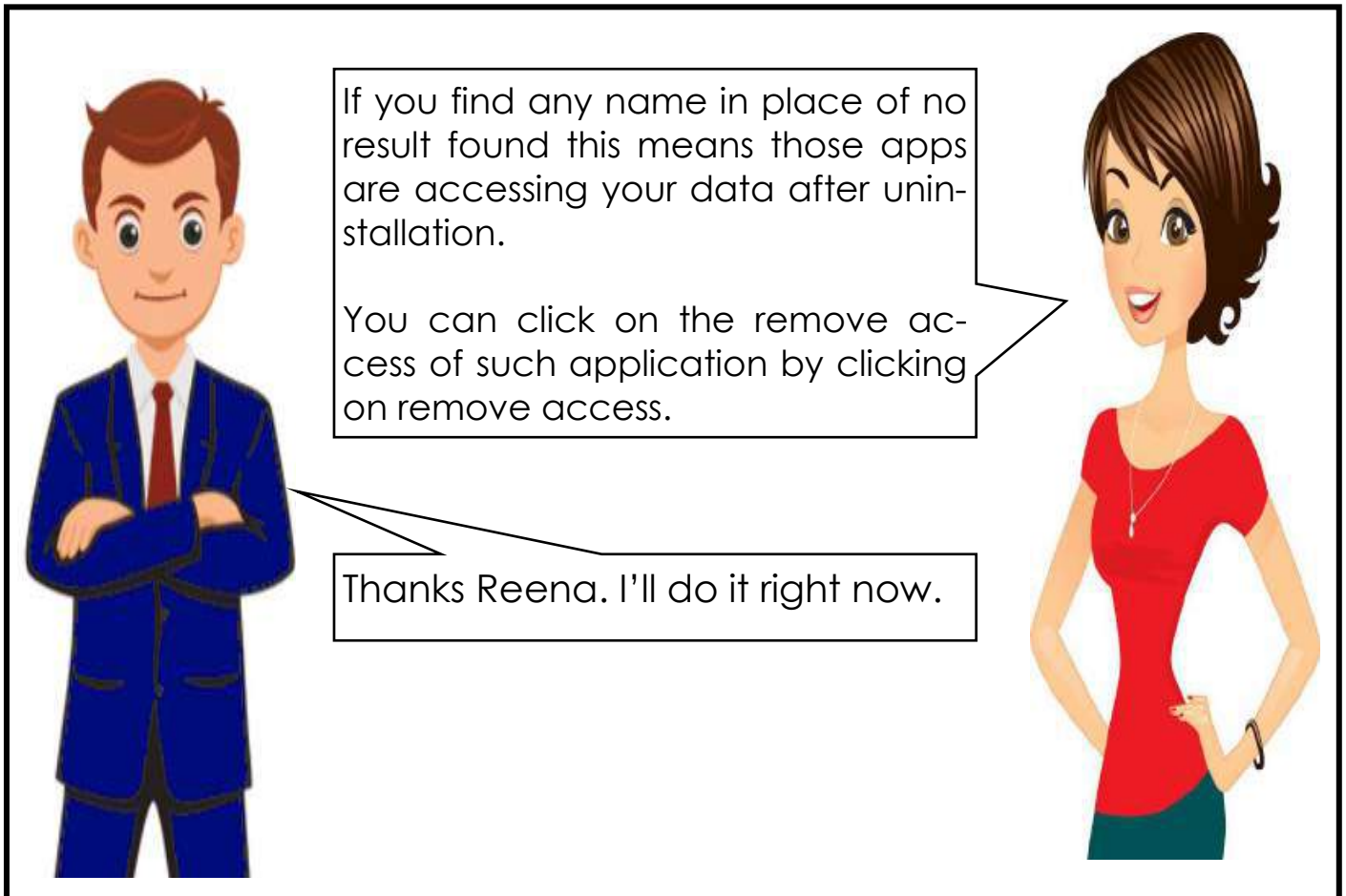
Chapter 22: Stop Uninstalled apps from accessing your Data

One day, Vishal was uninstalling unused applications from his phone. Reena noticed this and decided to ask him about the permissions given to the applications during installation.



You can follow the steps mentioned for checking and preventing the data from uninstalled apps...







GYAAN KA SAAR



Listed below are the primary reasons why users should uninstall unused apps on their smartphones.

1. Privacy is a most important concern when installing new apps. Apps that ask for the way to lot permissions may get discarded instantly.
2. Apps that send many related or unrelated push notifications; end up annoying the user particularly if the notifications are not relevant to the user.
3. Users might get into a uninstall frenzy and discard your app along with many others if they require some free space on the phone memory.
4. Generally Users don't like to exhaust their expensive, hi-speed data over apps running in the background.
5. Many smartphone users worried about rapid battery drain and if your app happens to be the cause of this battery drain, chances of it being uninstalled are very high.
6. Users might uninstall mobile apps; if they notice a sudden spike in the many numbers of times the phone freezes or hangs after they have installed it.
7. Uninstalling an addictive app is a ploy to get rid of the addiction.



About the Chapter

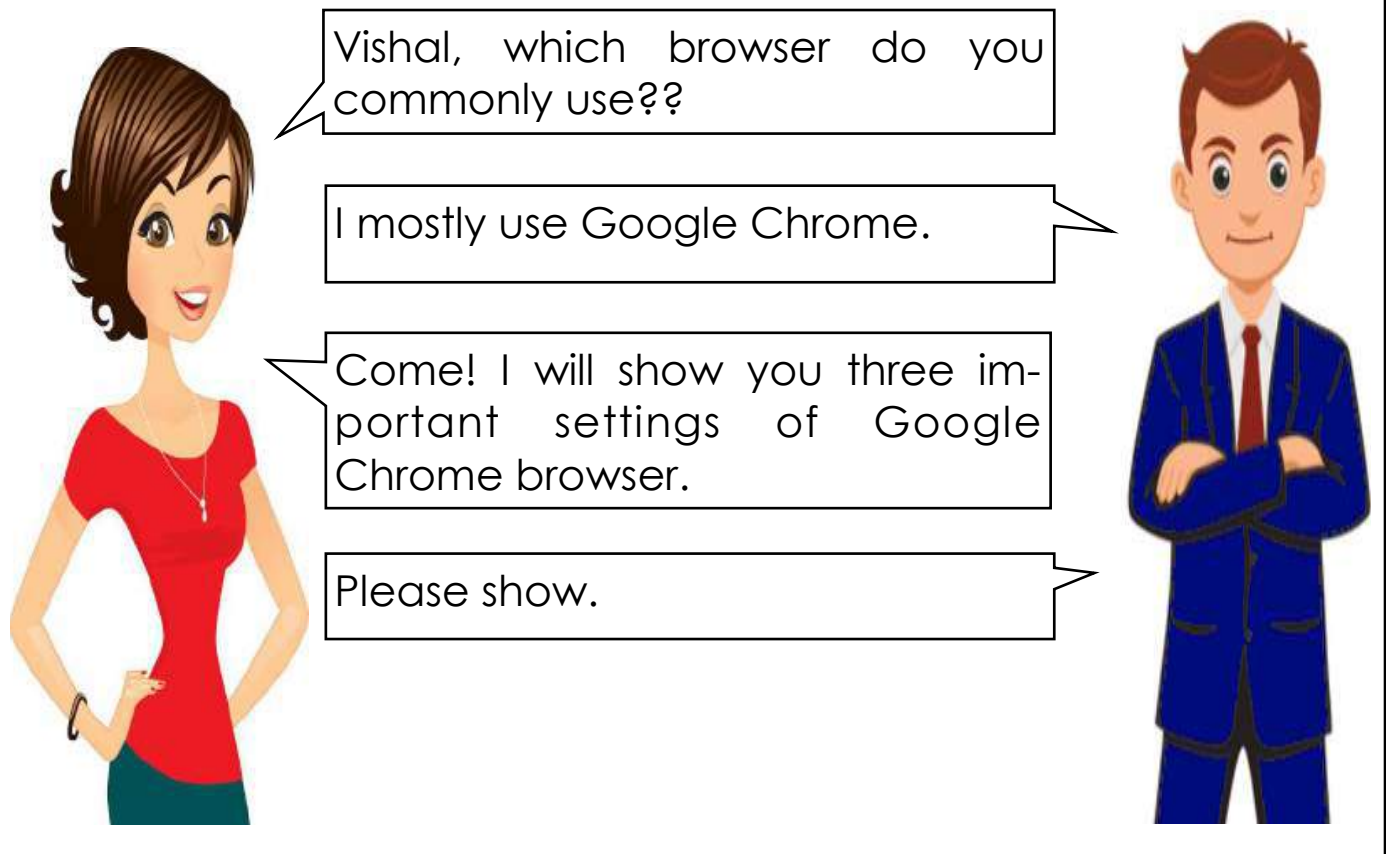
The mobile web can be a dangerous place — countless web-based mobile security threats can infect your phone. Without proper browser protection, your phone can be the next mobile cyber-threat victim.

Most people use their phone to connect to the internet, typically using the mobile web browser. Private information is being sent to and from your phone when browsing the mobile web. By lacking adequate browser protection, security issues caused by mobile cybersecurity threats may arise. These include phishing attacks and browser hijacking.

In this chapter of our Cyber Gyaan, we will learn three important safety features of Google Chrome Application.

Chapter 23: Important settings of Google Chrome

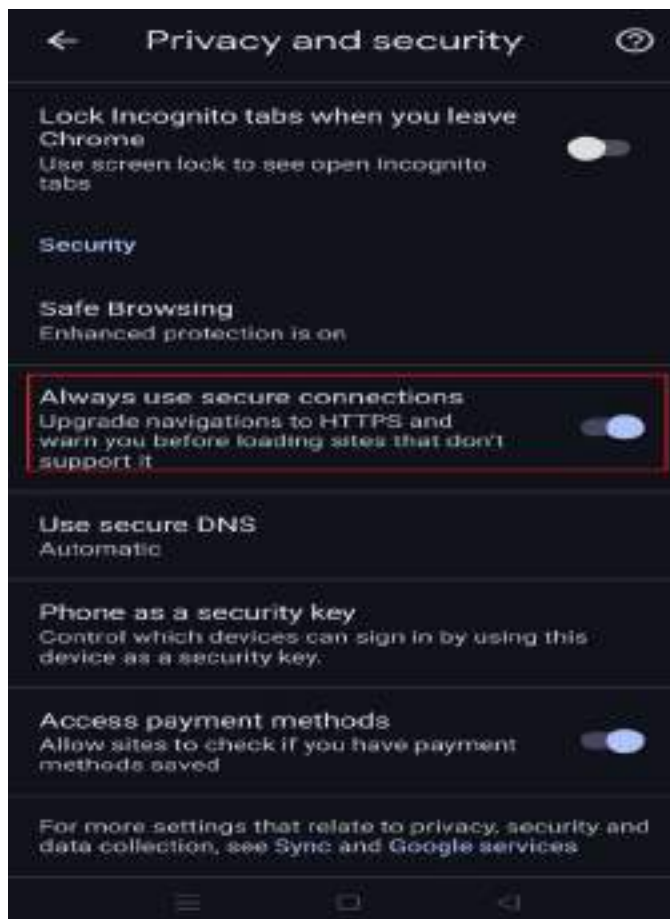
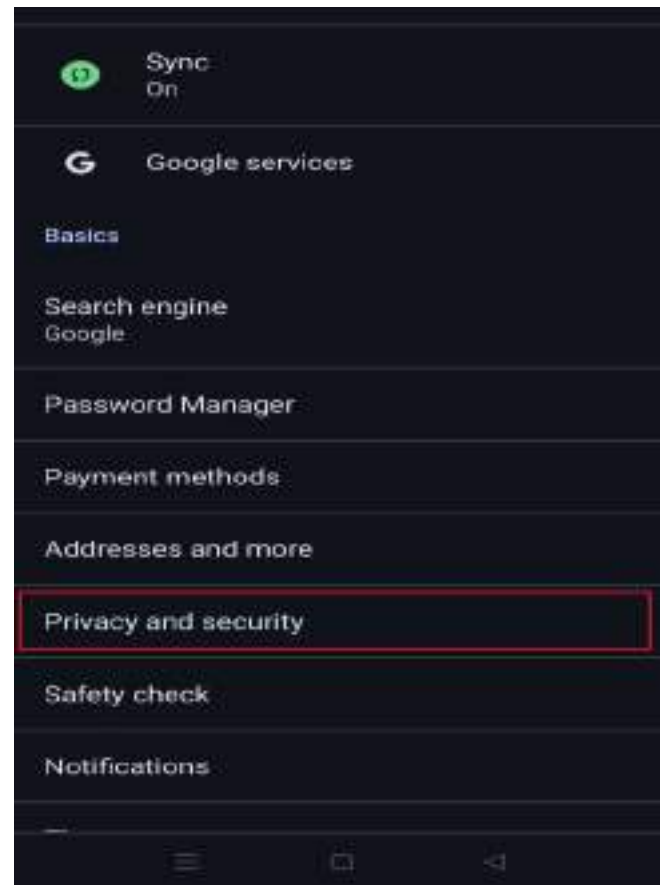
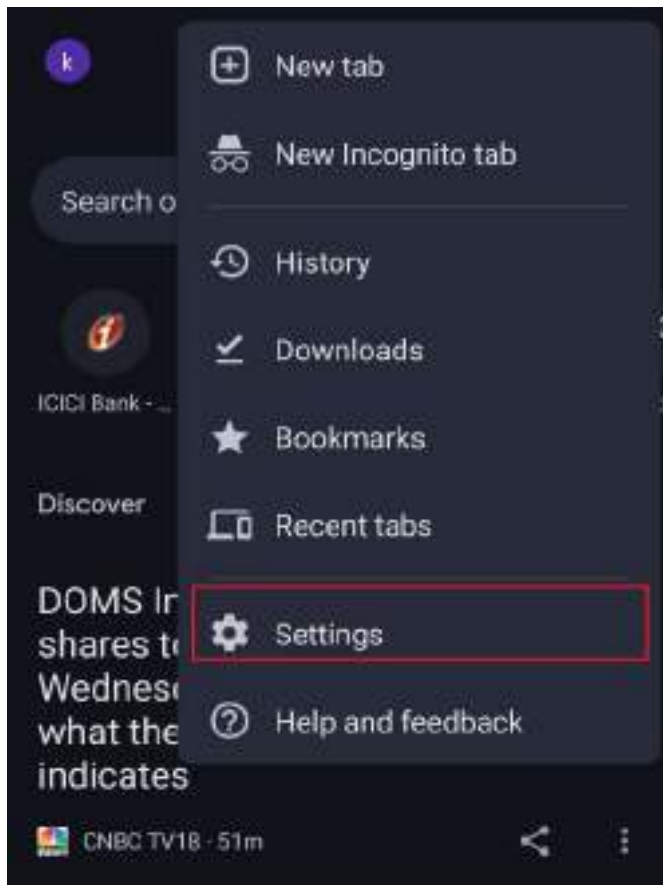
One day, Reena and Vishal were having a discussion about web browsers.



You can follow the steps mentioned for reviewing the setting of the Google Chrome



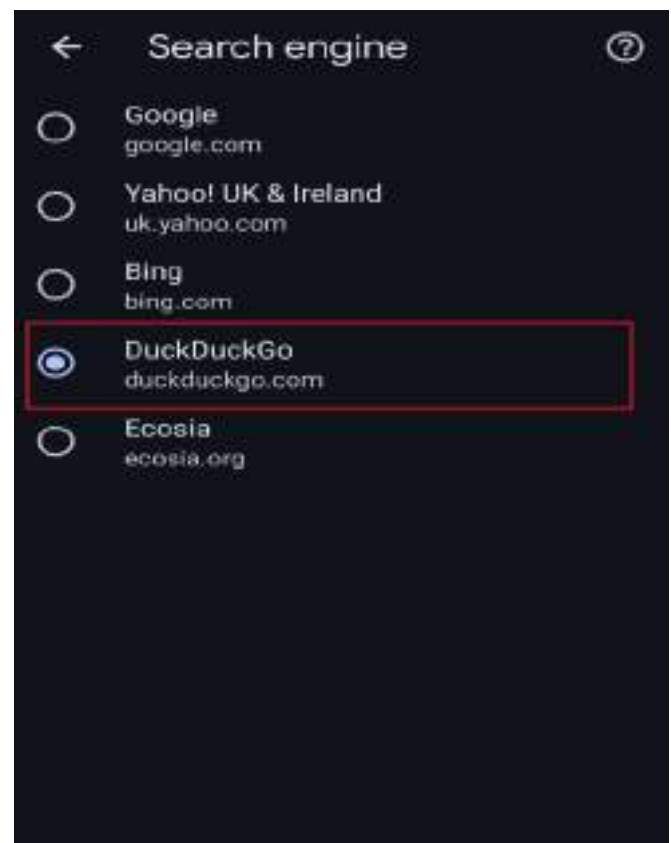
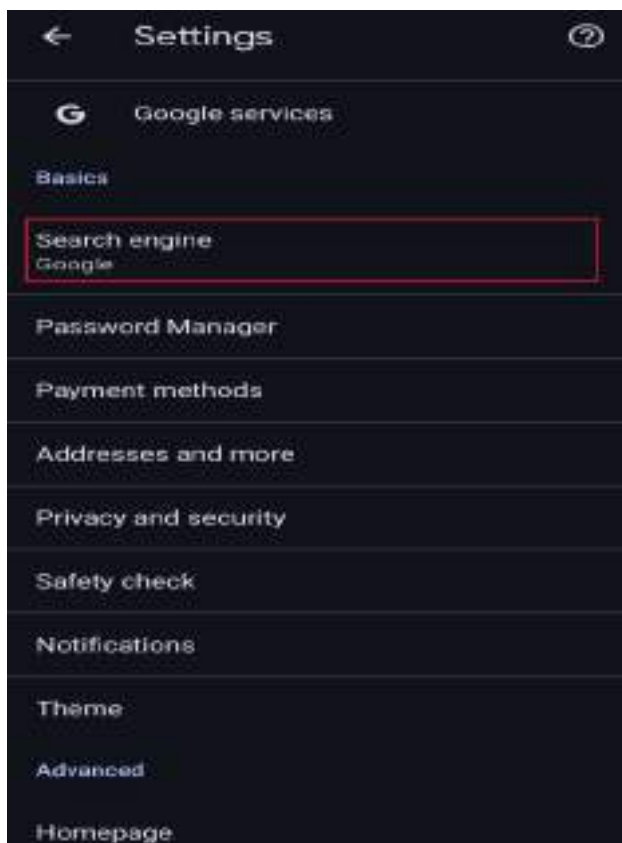
Open Google Chrome application on your mobile phone.



By doing this your chrome will access only the secured website and chances of virus infecting your phone will decrease.

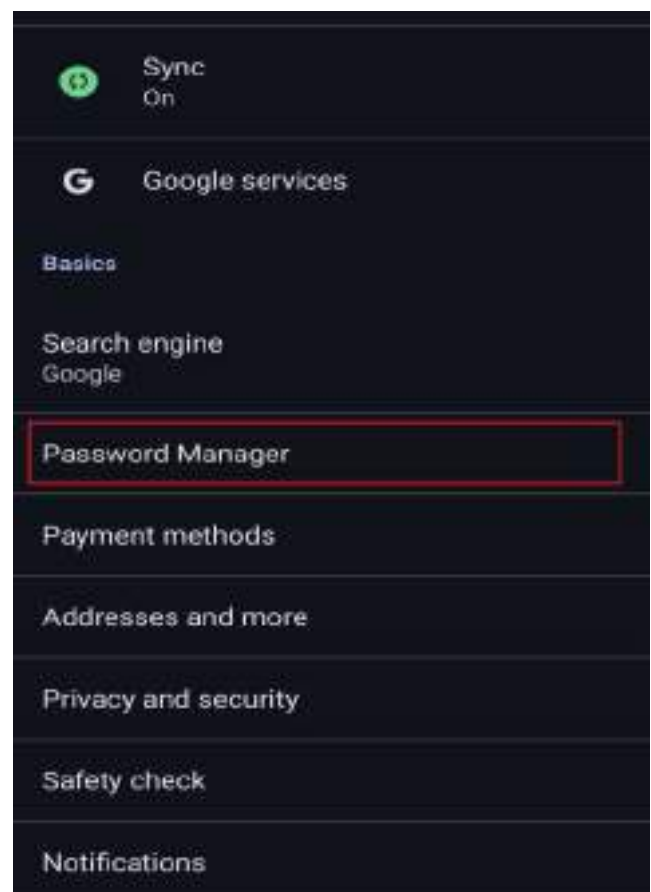


Again, go to settings options of your google Chrome browser

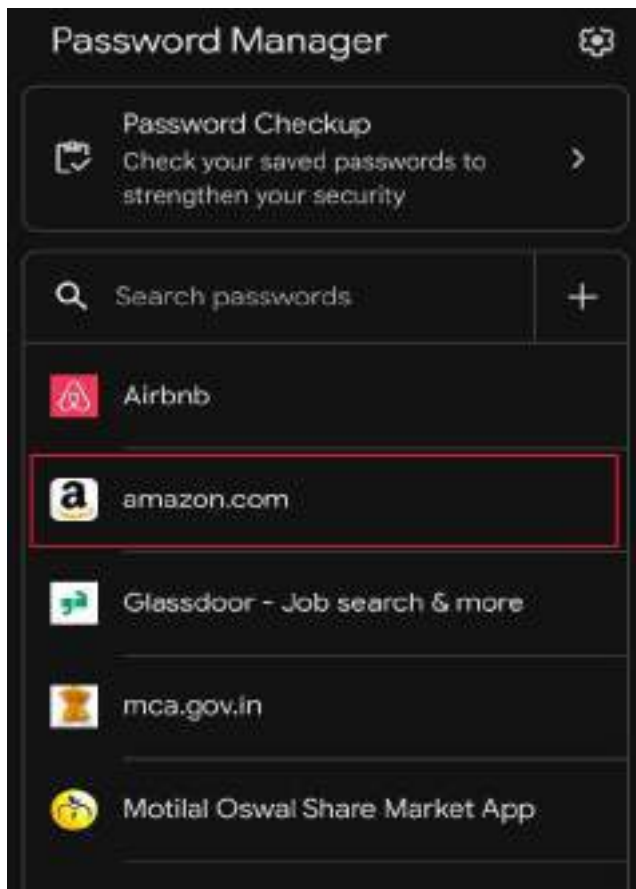


Enabling these settings will reduce unnecessary ads and your browser history will also not be saved.

Next safety security setting is to retrieve your forgotten password. For this again go to setting and follow the upcoming steps.



Clicking on the application for which you wish to check the password and then click on eye bottom.



I have been using Google Chrome since long time, but I didn't knew these settings. I will check these setting and make necessary changes.

Thanks Reena.





GYAAN KA SAAR



Precautions

1. Pay attention to the permissions the app requests. Grant only those permissions which are absolutely necessary for the purpose of the app.
2. Use different passwords for all your online account.
3. Download apps in official stores
4. Keep all your apps up to date
5. Make sure you have an antivirus installed on your phone.
6. Download apps only after reading its reviews, ratings and number of downloads. Also, download the apps after proper knowledge of the app.
7. Do not leave your phone unattended
8. Back up your data
9. Log out of sites after you make a payment
10. Turn off Wi-Fi and Bluetooth when not in use.



About the Chapter

While the Internet has been about sharing information, many users out there trust it to keep their personal data safe and accessible only to them. Understanding the origins of the Internet and where it's heading are both critical to keeping your Google account's best interests in mind. Google account services include Google Drive, Calendar, and Google Plus, all are in sync with your Gmail account.

Nowadays, almost everyone has an email id, more particularly a gmail account. Therefore, it is important to know how we can protect our gmail account.

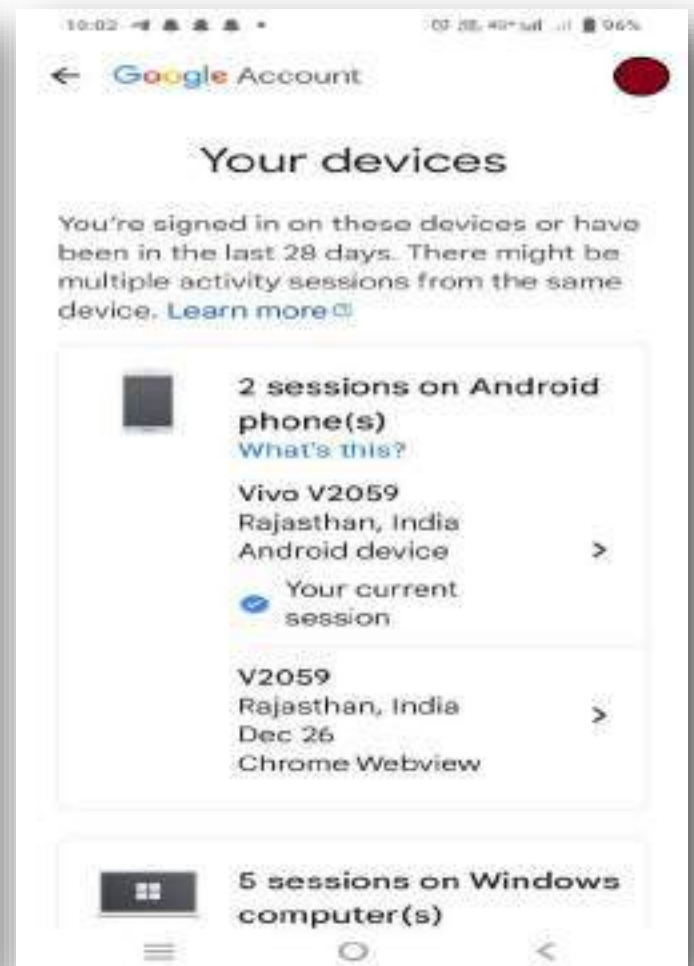
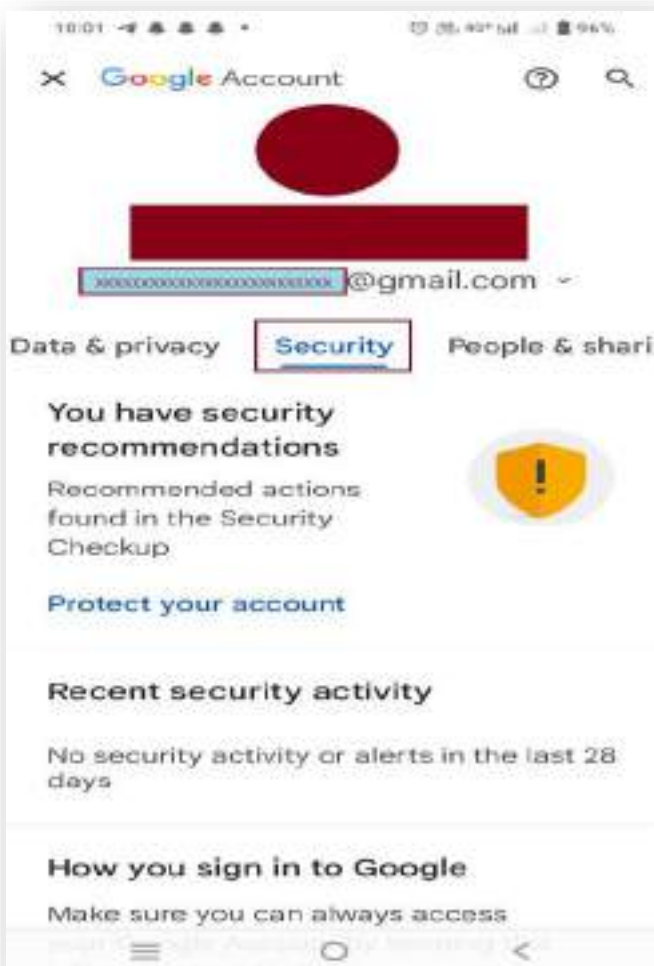
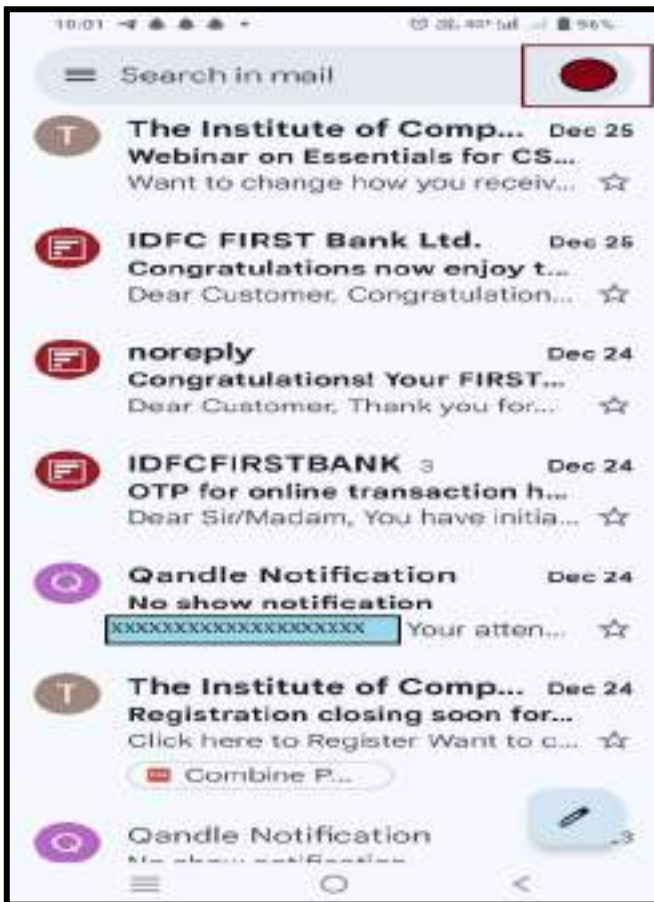
In this chapter of our Cyber Gyaan, we will learn the important safety features of Gmail.

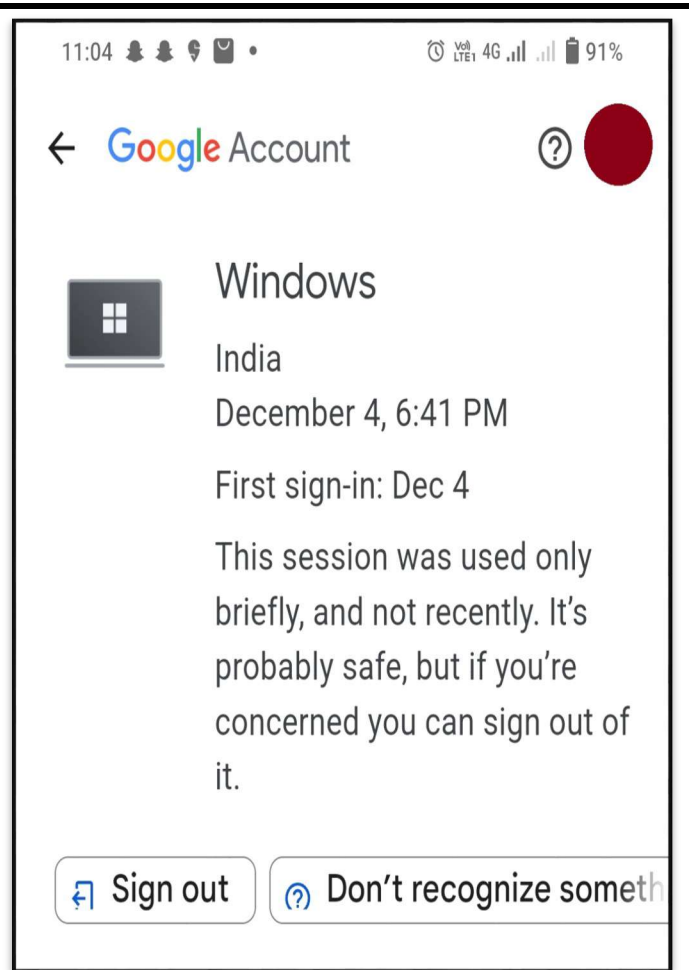
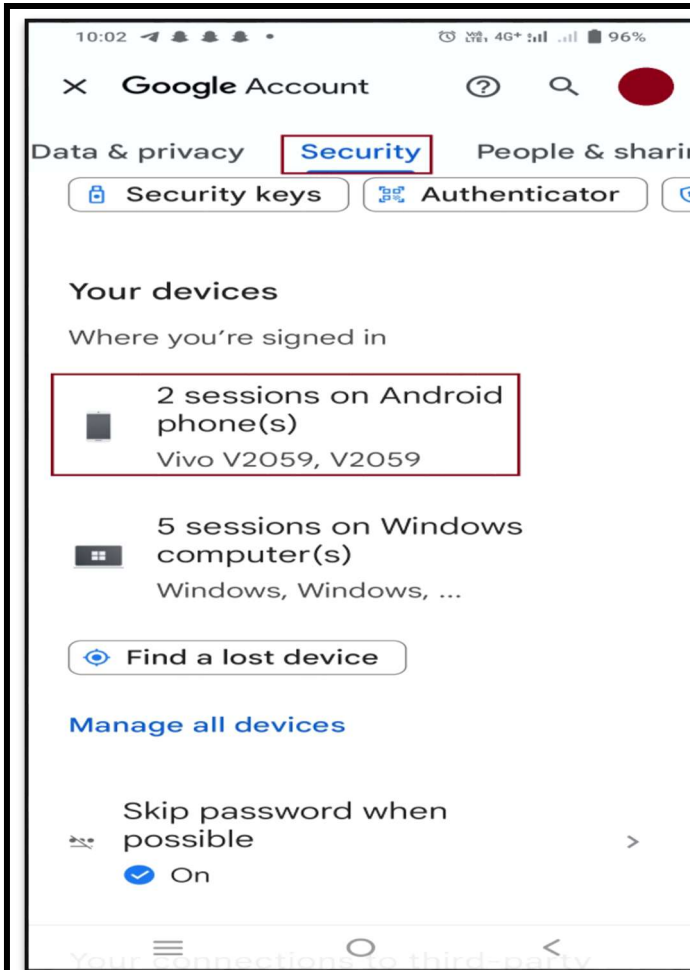
Chapter 24: Safety Features of Gmail





Open Gmail application on your mobile phone.





So this is how you can keep a check on the devices which have active access to your Gmail Account.

Thanks Reena. I have reviewed the list of devices and have also removed the unnecessary device access.



GYAAN KA SAAR



Precautions

1. Enable Two-factor authentication
2. Use a strong password
3. Don't click on suspicious links
4. Set up a recovery phone number or email address, and keep it updated.
5. Don't use public Wi-Fi to access Gmail
6. Be careful with app permissions
7. Keep your browser up to date
8. Look at account activity
9. Use separate email accounts
10. Don't open an attachment unless you know who the sender is.
11. Check your backup contact method
12. Choose A Unique Security Question
13. Backup Your Emails
14. Check Email Settings and Options Regularly.
15. Revoke unauthorized access.



About the Chapter

Detectives look for footprints and fingerprints because they're instant proof of where someone's been, what they touched, and where they're headed. The concept holds online, too.

Your digital footprint is a map of where you (and your devices) have been, what you do online, how you behave, and where you're probably headed next in the cyber sphere.

Our digital footprints are more than personal expressions. Businesses use them to shape our experience on the web. Websites use them to pre-select our language preferences. Marketers use them to show us relevant content and make appropriate product and service recommendations.

In this chapter of our Cyber Gyaan, we will learn the about the Digital Footprints.

Chapter 25: Digital Footprints

One day Vishal was looking for a blog on the internet. While doing so, he noticed something which got his attention..



I have never visited this site before.. then how does this website know that I was recently looking for wallets to buy?

How is this possible?

I think I should ask Reena..



Hey Reena!

Is it possible that a site which we have never visited shows something which we were earlier looking for?

Hello Vishal! I think what you are talking about is called Digital Footprint.

It is basically a person's record of online or mobile device actions. It's a record of your cyber presence, online behaviour, and web preferences. Think of it as your digital shadow.





What details are recorded as Digital Footprints?

All the details which we search online are recorded. This may include your Online shopping details, Registering for brand newsletters or publications, Online banking, Using a mobile banking app, Buying or selling stocks, Social media, Sharing information, data, and photos with your contacts, Joining a dating site or app, Reading the news, Subscribing to an online news source, reposting articles and information you read, Using fitness trackers, Registering your email address with a gym, etc.



Do they matter?

They matter because:

- They are relatively permanent, and once the data is public, the owner has little control over how others will use it.
- They can determine a person's digital reputation.
- Employers can check their potential employees' digital footprints, before making hiring decisions.
- Words and photos which you post online can be misinterpreted or altered, causing unintentional offense.
- Cybercriminals can exploit your digital footprint using it for cyber crime purpose.

You cannot delete your data, but you can manage it. You may follow the Precautions mentioned in the next page.





GYAAN KA SAAR



Precautions

1. Use search engines to check your digital footprint.
2. Reduce the number of information sources that mention you by limiting the amount of data you share.
3. Begin customizing your privacy settings to limit access to personal data.
4. Avoid unsafe websites and disclosing private data on public Wi-Fi.
5. Deactivate or delete old or unused accounts on social media platforms, e-commerce websites and email addresses.
6. Use strong unique passwords and enable 2 Factor Authentication or Multiple Factor Authentication on all of your accounts. Never share it with anyone.
7. Don't log in with Facebook or other social media accounts on other websites.
8. Keep your software up to date.
9. Review your mobile use. When installing an app, read the user agreement. Many apps disclose what kind of information they collect and what it may be used for.
10. Use a VPN and check your browser for cookies.



About the Chapter

Money muling is a type of money laundering. A money mule is a person who receives money from a third party in their bank account and transfers it to another one or takes it out in cash and gives it to someone else, obtaining a commission for it. Simply put, money mules help criminal syndicates to remain anonymous while moving funds around the world. Since these are normal people with no criminal background and legit income, the criminals use them to disguise their illegal funds.

It can be easy to fall into a money mule scheme because the perpetrators know how to make their offers appealing. They might reach out via phone, email, mail or social media. Or they might put up a job ad and wait for you to apply.

In this chapter of our Cyber Gyaan, we will learn the about how money mules uses innocent people to achieve their objectives.

Chapter 26: Money Mules

One day Vishal was watching TV and he heard of a word called "Money Mules". He thought of search the same of internet. However, his concept was not clear, so he visited Reena



Hey Reena!
I came across a word called Money Mules. Do you know what is it?

Hi Vishal!!
Yes, I can explain you in detail.



Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen/illegal money via their bank account(s).

Money mules are frequently innocent individuals who are drawn into the plan by a variety of tactics, such as job offers, online classified ads, or social media postings. Some money mules know they are assisting with criminal activity, but others are unaware that their actions are helping fraudsters.

How do these fraudsters operate?



Step 1: Fraudsters contact customers via emails, chat rooms, job websites or blogs, and convince them to receive money into their bank accounts, in exchange of attractive commissions.

Step 2: The fraudsters then transfer the illegal money into the money mule's account.

Step 3: The money mule is then directed to transfer the money to another money mule's account – starting a chain that ultimately results in the money getting transferred to the fraudster's account.

Step 4: When such frauds are reported, the money mule becomes the target of police investigations.



Ohh!! Now, I understand, the term money mules. It facilitates the movement of illicit funds,.

Thank you so much Reena for explaining it and clearing my doubts.



GYAAN KA SAAR



Precautions

1. Do not allow others to use your account to receive or transfer money for a fee / payment.
2. Do not respond to emails asking for your bank account details.
3. Do not get carried away by attractive offers / commissions and give consent to receive unauthorised money and to transfer them to others or withdraw cash and give it out for a handsome fee
4. Don't agree to receive or send money or packages for people you don't know or haven't met in person
5. Don't pay to collect a prize or send someone money out of your "winnings."
6. Be cautious of unsolicited emails and social posts
7. Do not accept job offers that require transfer of money to other unknown accounts
8. Do not accept any award money for which part of it is to be transferred elsewhere
9. Don't take a job that promises easy money - especially if it involves sending or receiving money or packages.
10. If you fall prey to money mule scam, reach out to National Cyber Crime Reporting helpline 1930 and portal <https://cybercrime.gov.in/>



About the Chapter

More than ever, the electronic devices that are critical to everyday life, to the larger infrastructure, and to national defense are dependent on increasingly sophisticated semiconductor integrated circuits, also referred to as “chips”. For example, laptop computers and tablets, smartphones, the financial system, the Internet, aircraft flight controls, automobile antilock braking, the power grid, and an almost endless list of other devices and systems can be trusted to run properly only if the chips they contain are free of hidden malicious circuits inserted during the design or manufacturing process.

Cyber security can be a complex subject to tackle. Hackers have become more adept at infiltrating systems because they continually experiment with ways to exploit back doors and vulnerabilities. While cyber security strategies frequently focus on preventing software vulnerabilities, hardware also needs to be a priority.

In addition to cyber attacks, other elements at home or in an office can harm hardware components: damaged hard disks, faulty power supply and human error, both intentional and unintentional, can all present challenges. Upgrading hardware along with updating software is crucial to protecting computer systems and IT networks from cyber criminals.

This chapter of our Cyber Gyaan will let you know Hardware Attacks, their types and Hardware Security.

Chapter 27: Hardware Attacks and Security

One day, Vishal was reading a newspaper and he read a news about the Hardware Attacks. He decided to ask to Reena about the same....



Hi Reena, In the morning I was reading the news paper and I read about Hardware Attacks .
Do you know about it?

Hello Vishal...
Yes I know about the Hardware Attacks .
I'll tell about the same.

Hardware attacks Hardware attacks include Attack vectors—as they relate to hardware security—are means or paths for bad actors (attackers) to get access to hardware components for malicious purposes, for example, to compromise it or extract secret assets stored in hardware.

It includes invasive and non-invasive attacks.

Non Invasive attacks include covert channels attacks or data leakage attacks and involve closely observing a device's emissions to gain access to unauthorized data.

Invasive attacks involve direct electrical access to the internal components of the device.





Let me tell you some of the common hardware vulnerabilities.

Hard disks: Hard disks are delicate pieces of technology, so they're vulnerable to physical damage. The owner may harm the disk by dropping it or via any other mishap.

Power: An inconsistent power supply can damage components within the hardware and risk failure.

People: People are essential for your business to function, but they can also be the reason as to why hardware fails. They may unintentionally harm a computer, perhaps by spilling their beverage or dropping important equipment; or they could cause purposeful harm, perhaps by knowingly downloading attachments with malware or intentionally sabotaging equipment.

Hardware Trojans: Hardware Trojans are malicious modifications or insertions of circuitry or logic in a hardware device, such as a chip, that can alter its functionality or leak sensitive information.

Side-Channel Attacks

Side-channel attacks are passive or active attacks that exploit the physical characteristics or behavior of a hardware device, such as power consumption, electromagnetic radiation, timing, or acoustic signals, to infer or manipulate confidential data or operations.

Fault Injection Attacks :

Fault injection attacks can cause denial of service, authentication bypass, code injection, or model inversion.



GYAAN KA SAAR



Listed below are the some measures for securing your Hardware and Data:-

1. Keep all software up to date .
2. Use antivirus software and keep it current .
3. Make sure your passwords are well-chosen and protected .
4. Browse the web safely .
5. Don't use USBs or other external devices unless you own them.
6. Don't open suspicious attachments or click unusual links in messages.
7. Data, Software, technologies, everything is moving so fast. Keep track of them, keep in touch with news to see what is new on the market.
8. Prevention is the best way to keep your Data safe.
9. Antivirus and anti-malware are indispensable to protecting your Data. They are designed to prevent, search for, detect and remove viruses but also adware, worms, trojans, and so on.
10. In order to protect your network, firewalls are an important initiative to consider. They are a must-have for any company, as they control the internet traffic coming and leaving your business.



About the Chapter

Fake Job Scams have existed for a long time but technology has made this scam easier and more lucrative. Cyber criminals now pose as legitimate employers by spoofing company websites and posting fake job openings on popular online job boards. They conduct false interviews with unsuspecting applicant victims, then request personal information and/or money from these individuals.

Job fraud is the scamming of people who are seeking employment or already employed, giving them false hope of earning wages of which they are often desperately in need. The victims are often contacted via Email or phone.

Fraudsters use numerous schemes such as easy hire, easy work, flexible hours or other attractive offers to lure victims. Virtually all of them ask victims to pay money as a security deposit, bonds etc.

This chapter of our Cyber Gyaan will let you know how these scams happen and how you can safeguard yourself against them...

Chapter 28: Job Scams

Vishal was looking for switching jobs. He decided to create his profile on the Job seeking platform named "SearchJob". Two days after creation of profile, he received a call.

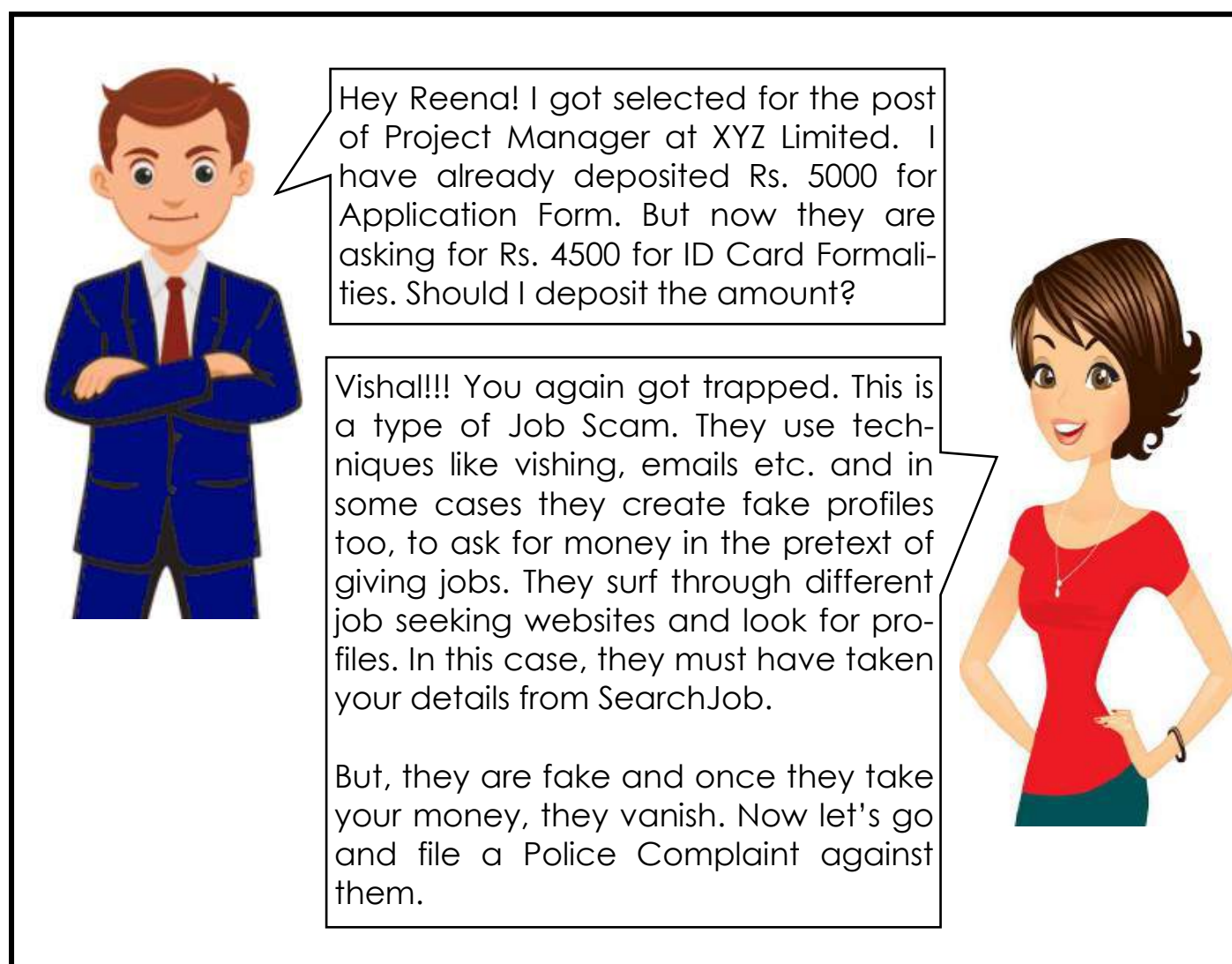
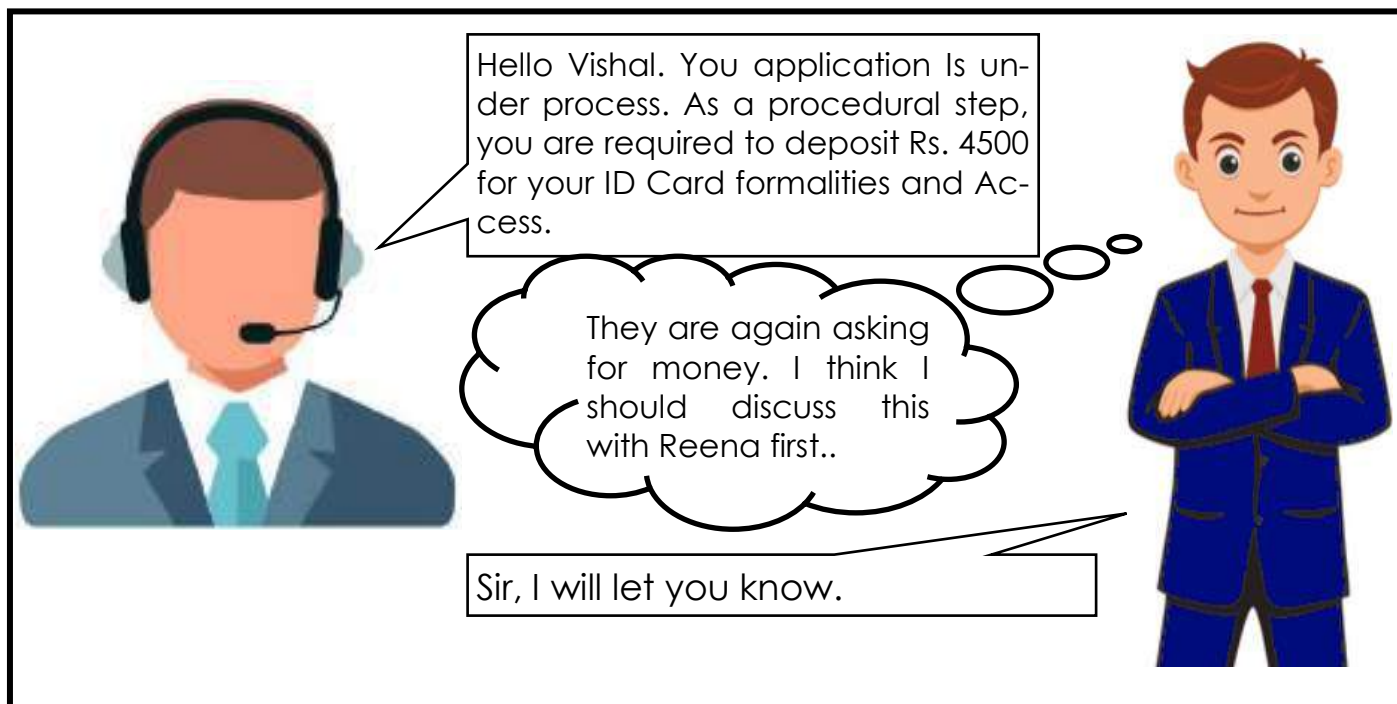


After interview....



He thought that it is routine, therefore he deposited the amount.

After some days....





GYAAN KA SAAR



Precautions

1. If you receive an unexpected job offer, especially without having applied, proceed with caution.
2. Scammers often resort to free email services or slightly modify the company's domain. Be cautious if the email address seems unprofessional or suspicious.
3. Double-check the job posting details on multiple platforms or job portals. Scammers may post fake job ads on less popular websites or use slight variations in the company name to appear legitimate. Suspicious or unfamiliar platforms should raise red flags.
4. Conduct thorough research on the company before applying. Visit their official website, verify contact information, and search for online reviews or news articles.
5. Avoid upfront payment requests. Such requests are often signs of a scam.
6. If something feels off or too good to be true, trust your instincts. Scammers often use high-pressure tactics, make unrealistic promises, or rush you into making decisions.
7. Conduct a background check on the company. Look for registration details like incorporation certificates or business licenses.
8. Ensure reliable contact information. Legitimate companies provide trustworthy contact details, including a physical address and valid phone number.
9. Rely on online reviews and testimonials. Seek out reviews or testimonials from current or former employees of the company. While reviews alone may not be conclusive, multiple negative reviews or a lack of online presence should raise concerns.
10. Scrutinize the email domain. Legitimate companies typically use their own domain names for email addresses.



About the Chapter

In the digital world, the cyber criminals are finding new ways for scamming people. Nowadays, the most used messaging app has become the platform for cyber fraud where people are getting scammed through various tricks.

Some of the common frauds through WhatsApp are:

- ⇒ Impersonation scams: Scammers pretend to be someone you know to gain your trust to scam money.*
- ⇒ Phishing Scams: Scammers send messages with urgent warnings and contains links which when clicked, takes the user to fake site for entering their personal information.*
- ⇒ Investment Scams: Scammers promise high returns on investments and will pressurise you to invest in them quickly .*
- ⇒ Loan Scams: Scammers offer quick and easy loans with low rate of interest and once you apply for it they will ask you for some fee etc.*


To combat the same, there are several privacy and security features launched by WhatsApp through which we can prevent ourselves from frauds.

In this Chapter, you will learn how to enable them..



Chapter 29: Whatsapp Privacy Features

Vishal was reading an article on “WhatsApp Privacy in the world of cybercrimes”. He realised that he has not yet activated the safety settings on his WhatsApp account.



Hey Reena! I was reading this article where they were telling about the security features of WhatsApp. But I have not yet enabled it. Am I at risk?

Vishal nowadays everyone uses WhatsApp. As a result, it has become a new platform for spreading cyber crimes.

Earlier such frauds were attempted via other social media platforms. But now the latest modus operandi is to send messages, pretending to be acquaintances and offering freebies, over the WhatsApp.

There are many instances in which there were attempts of frauds using fake identities.

Therefore, to avoid these instances, it is necessary that you enable your Privacy Settings.

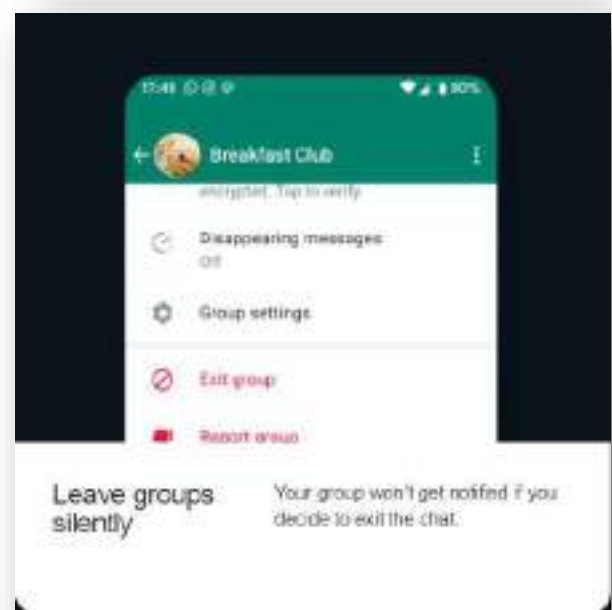
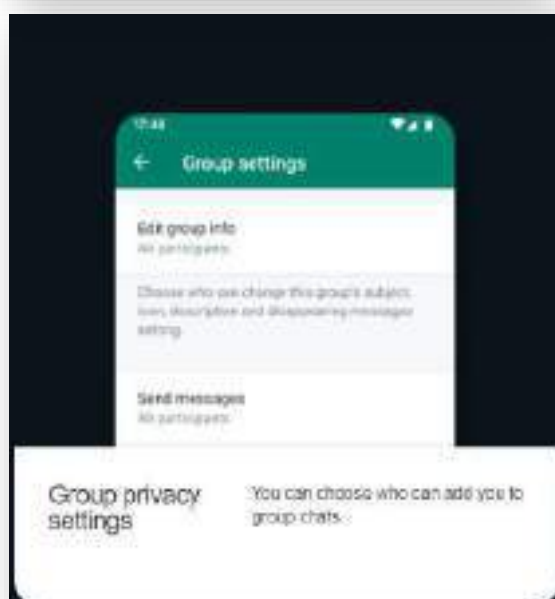
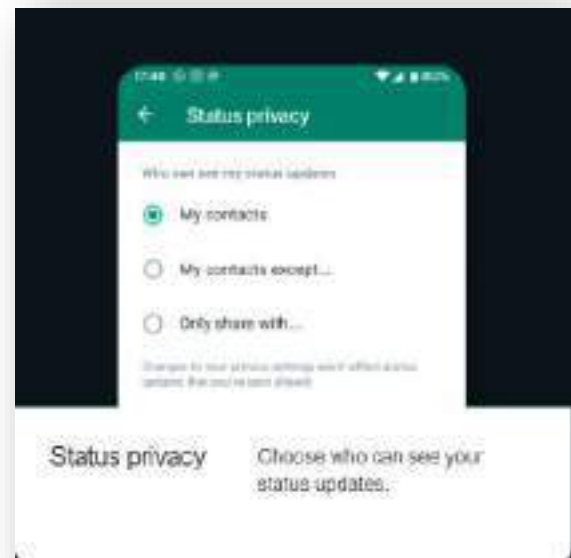
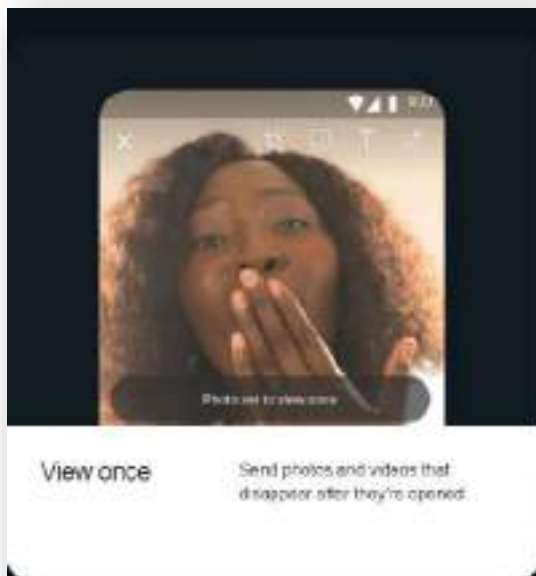
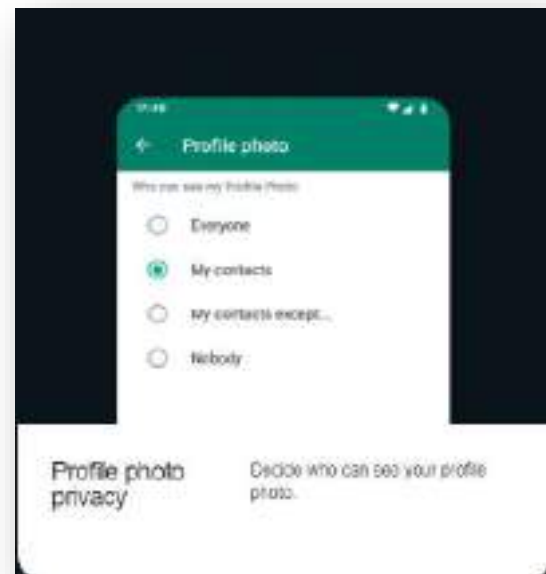
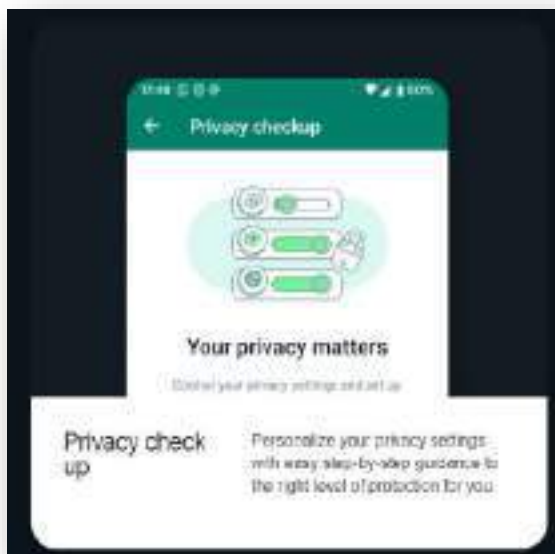
Can you help me in enabling these settings?

Sure Vishal. You can see the Privacy & Security Features as follows...



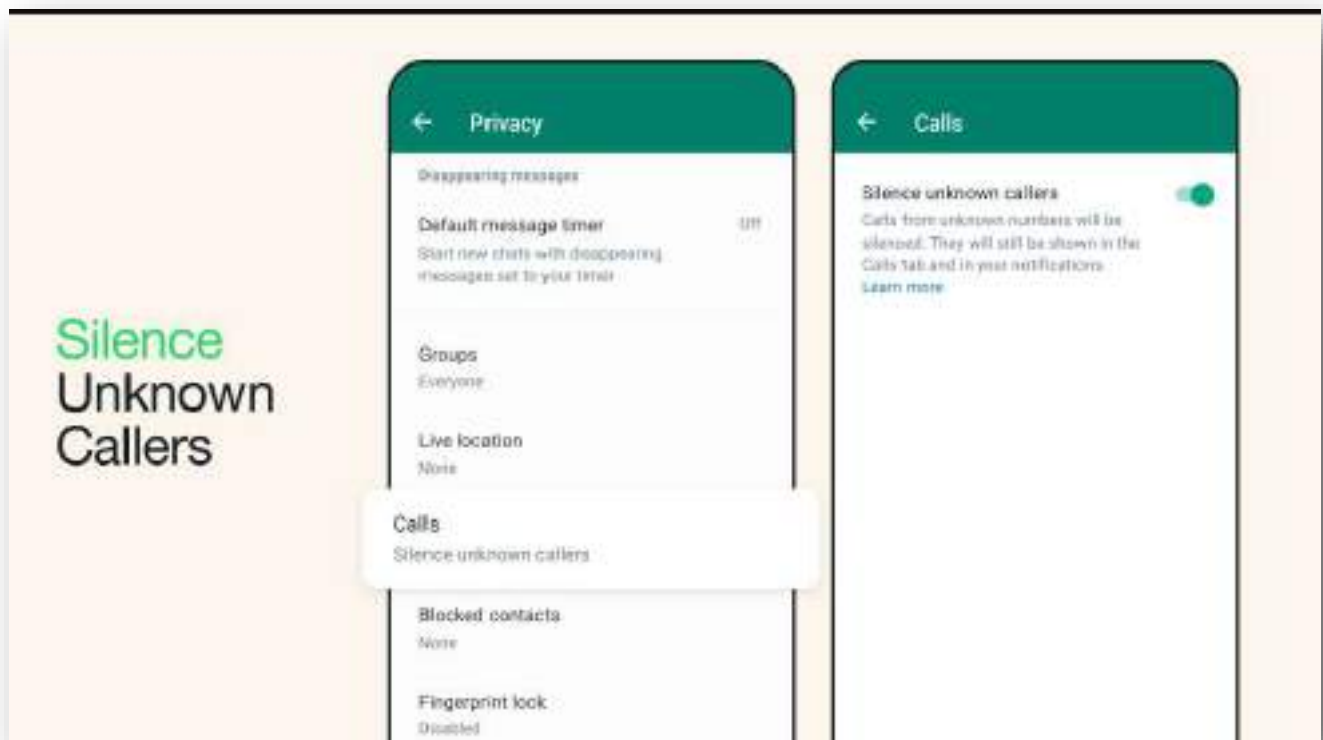
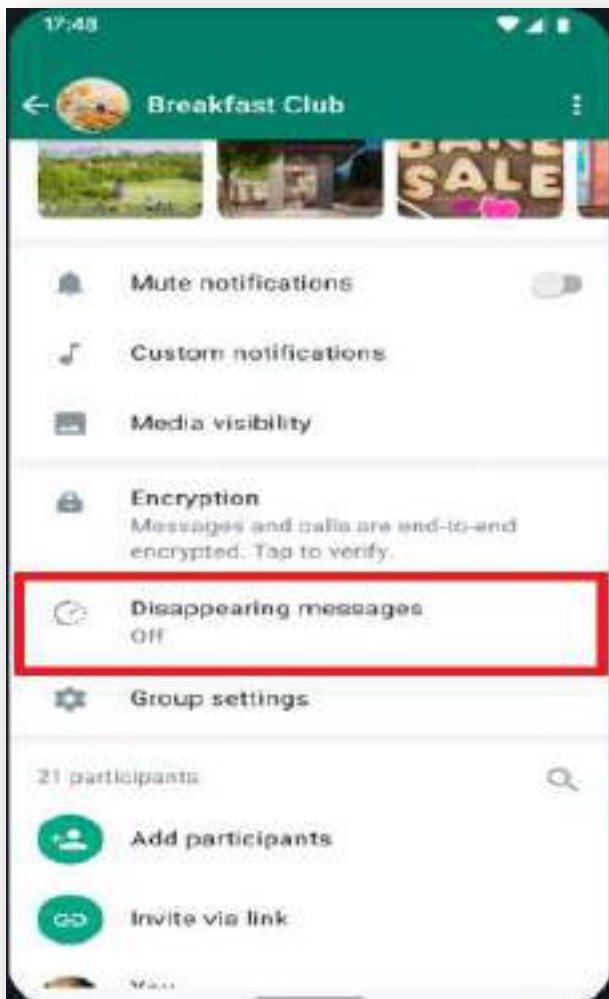


Privacy Settings



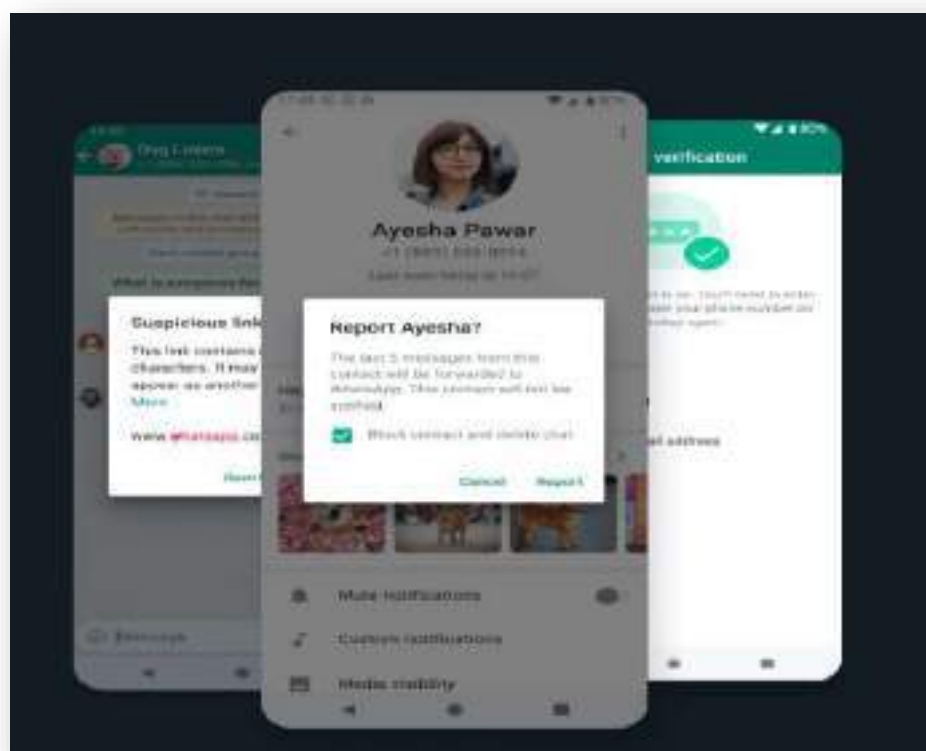
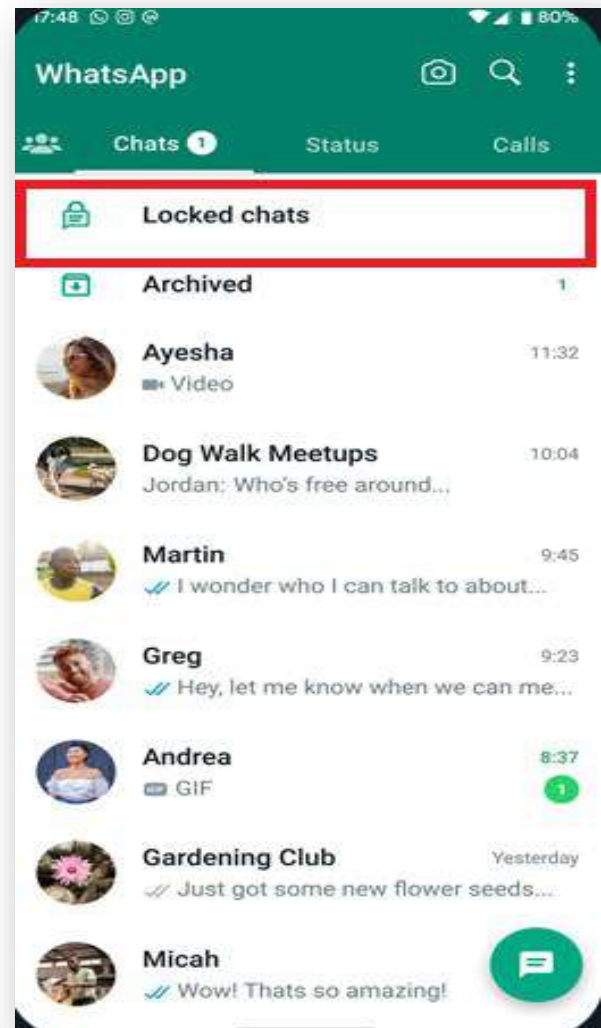
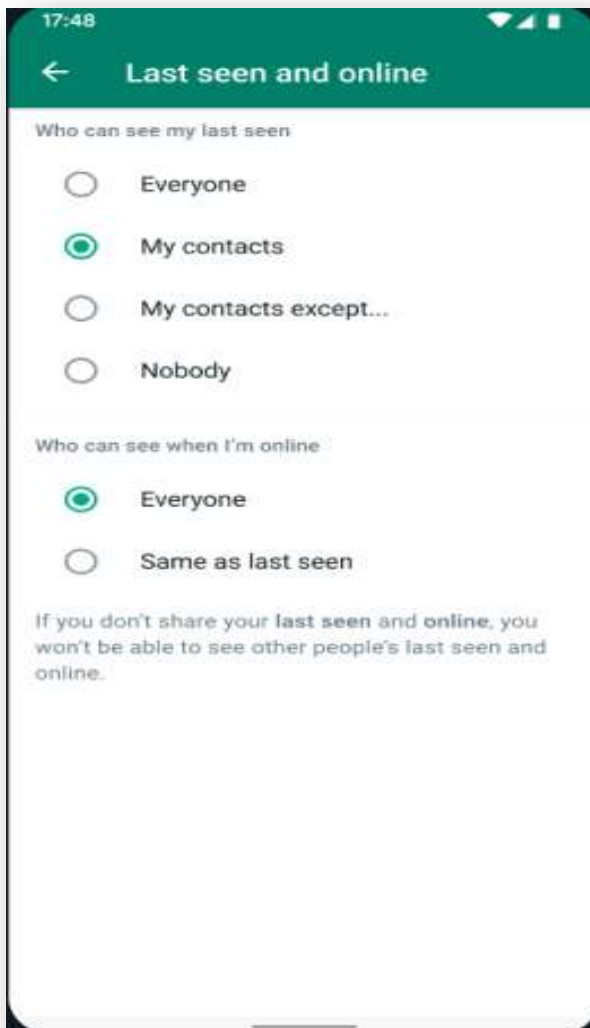


Security Settings





Security Settings





About the Chapter

Cyberbullying is a form of bullying or harassment using electronic means. It is often known as online bullying. It is increasingly common among teenagers and adolescents. Cyberbullying is a recent issue with increasing numbers of people using the Internet.

It is a very serious issue affecting not just the young victims, but also the victims' families, the bully, and those who witness instances of cyberbullying. However, the effect of cyberbullying can be most detrimental to the victim, of course, as they may experience a number of emotional issues that affect their social and academic performance as well as their overall mental health.

In this chapter we are going to learn how cyberbullying has affected Vishal's niece.



Chapter 30: Cyber Bullying

Vishal was visiting his relatives. He noticed that Kimi, his niece was being isolated. She was sad and depressed. He decided to ask her about this.

Hey Kimi! I have noticed that you are sitting alone since I have come here. What happened?



Vishal Uncle, it's just that I posted this video on my social media profile a few days back and since then I am receiving rude messages. People are harassing me and I feel really bad about this.



Ohh Kimi! Do not worry. We will find a solution. First tell me, did you try blocking or reporting those social media accounts? Is the video still available on your profile?

I have blocked and reported all those accounts and have also removed the video from my profile but still I am receiving the hateful comments and messages.

It's Okay. I have a friend Reena. Let's ask her about this. I think she will be able to help us.

Vishal contacts Reena...



Hey Reena! I need your help. My niece Kimi posted a video on her social media profile a few days back and since then she is receiving rude messages. She has even blocked and reported all those accounts and has also removed the video from her profile but still she is receiving the hateful comments and messages.

She has become sad and depressed because of this. Please tell us how we can get out of this.

Vishal this is called Cyber Bullying. Cyberbullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behavior, aimed at scaring, angering or shaming those who are targeted.

The First step against them is blocking and reporting the accounts and then removing the content from your profile.

But since you have done this and still the problem persists, you can file a complaint with National Cyber Crime Reporting Portal.

Always remember, cyber bullying is a crime and should not be ignored.



Effects of Cyberbullying

Psychological Effects

- Low Self-Esteem
- Isolation and Withdrawal
- Harmful habits

Physical Effects

- Headaches
- Stomach aches
- Sleeping problems

Mental Effects

- Anxiety
- Loss of concentration
- Self-harm
- Suicidal thoughts

Emotional Effects

- Depression
- Shame
- Guilt
- Embarrassment



Social Media
Victims
Law Center

GYAAN KA SAAR



Precautions

1. Do not share private information like passwords, name and address, phone numbers with people you don't know. This can also include sharing of photos of yourself, your friends and your family
2. Do not respond to messages when you are angry or hurt. Log out and stop messaging if you feel you are being harassed.
3. You can block, delete and report anyone who is harassing you online and on your mobile.
4. Find out how to report bullying and harassment on each of the different social networks that you use.
5. Keep a record of calls, messages, posts and emails that may be hurtful or harmful to you.
6. Set up the privacy options on your social networking sites like Facebook in a way you are comfortable with
7. Don't post anything that is very private.
8. Stay safe online
9. Never Open Unidentified or Unsolicited Messages
10. Regularly search your name in every major search engine (e.g., Google, Bing, Yahoo). If any personal information or content comes up which may be used by someone to target you, take action to have it removed before it becomes a problem.
11. Restrict access to your online profile to trusted friends only
12. Don't save passwords in form fields within websites or your web browser for convenience
13. If you are being bullied, then get the help of someone you trust.
14. Don't support inappropriate content. If someone you know posts something mean, offensive, or harassing, don't like, repost, or share it.



About the Chapter

Unlike other phishing scams, frauds related to the unauthorised use of Aadhar biometrics neither involve clicking on unknown links nor sharing One Time Passwords (OTPs). The victims only become aware when they receive a debit message from their banks.

Scammers have utilised leaked biometric details to circumvent the need for One-Time Passwords (OTPs), facilitating the draining of funds from unsuspecting victims. A spate of recent scams has laid bare the vulnerabilities of Aadhaar-Enabled Payment System (AePS), exposing how cyber criminals exploit loopholes in the system to defraud unsuspecting customers.

In this chapter we are going to learn how we can secure our Aadhaar Biometrics...

Chapter 31: Aadhaar-Enabled Payment System (AePS)

Vishal and Reena were having Lunch at a restaurant. While waiting for their food, Vishal decided to ask about the AePS.



Reena.. Nowadays, Aadhaar Enabled Payment Systems are in news. What is it?

Aadhaar Enabled Payment System (AEPS) is a payment service that allows a bank customer to use Aadhaar as his/her identity to access his/her Aadhaar enabled bank account and perform basic banking transactions like balance enquiry, cash withdrawal, remittances through a Business Correspondent.

It is a nice facility. But why is it in news nowadays?

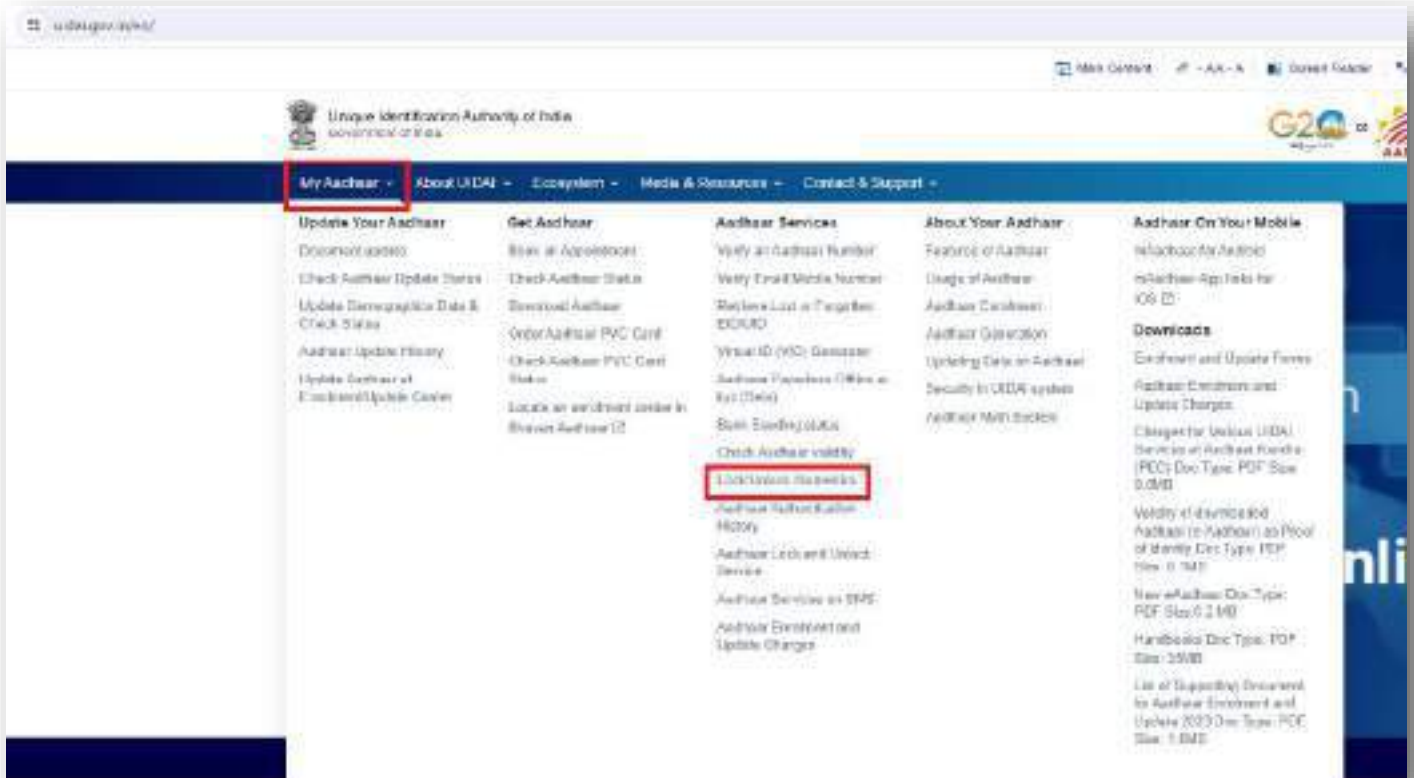
It is in news due to increasing frauds. Let me tell you how frauds take place through AePS.

Fraudsters gets access to Aadhaar card numbers and cloned fingerprints to perpetrate the fraud. Biometric information of the victim is illegally obtained from land records and / or physical documents. Hence, always verify the authenticity of the person / agency seeking your biometrics for any purported scheme like government subsidy etc. Victim's Aadhaar linked biometric fingerprints are cloned by creating silicon fingerprint replicas. Using the cloned fingerprints. AePS transactions are authenticated, and money is withdrawn from the victim's bank account.





You can protect yourselves from this fraud by Locking your Aadhaar Biometrics. This can be done by visiting the website of UIDAI and following the below mentioned procedure...





Login to Aadhaar via OTP

Enter Aadhaar Number

Enter Captcha

9eZr2R

Login With OTP

Enter Aadhaar Number and Captcha,
then click on Login with OTP

Services

Following bouquet of online Aadhaar services are available for access. Click on the tab to navigate to the service-specific page.



Document Update

Click here to upload your Proof of Identity (POI) and Proof of Address (POA) Documents. **This service is free of cost till 14/03/2024.**



Download Aadhaar

Click here to download digitally signed and password protected electronic copy of the Aadhaar



Order Aadhaar PVC Card

Click here to order a secure, water-proof Aadhaar PVC card



Address Update

Click here to update the address of your Aadhaar. For any other update kindly visit nearest Aadhaar Seva Kendra.



Bank Seeding Status

Click here to find your bank Seeding Status.



Generate Virtual ID

Virtual ID (VID) can be used in lieu of the Aadhaar number. Click here to download 16-digits random VID.



Lock / Unlock Biometrics

Click here to temporarily lock/unlock your biometrics information.



Authentication History

Click here to view the authentication history.



Offline eKYC

Click here to access secure and sharable eKYC document, used for offline identification verification.



Payment History

Click here to view the payment and refund status.



My Head of Family (HoF) Requests

Click here to check HoF based Address Sharing Requests.



Aadhaar Update History

Click here to find your Aadhaar update history.

Requests

Status of various requests originated by you in the recent past. You can check the detailed status of the request by clicking on the "downward" arrow icon.



How Lock/Unlock Biometrics Works

The Lock/Unlock feature prevents possible misuse of the Resident's Biometrics Data. Locked Biometrics prevents the use of Biometric information for authentications. Users of this Service are cautioned to do so with care to prevent denial of Authentication services.



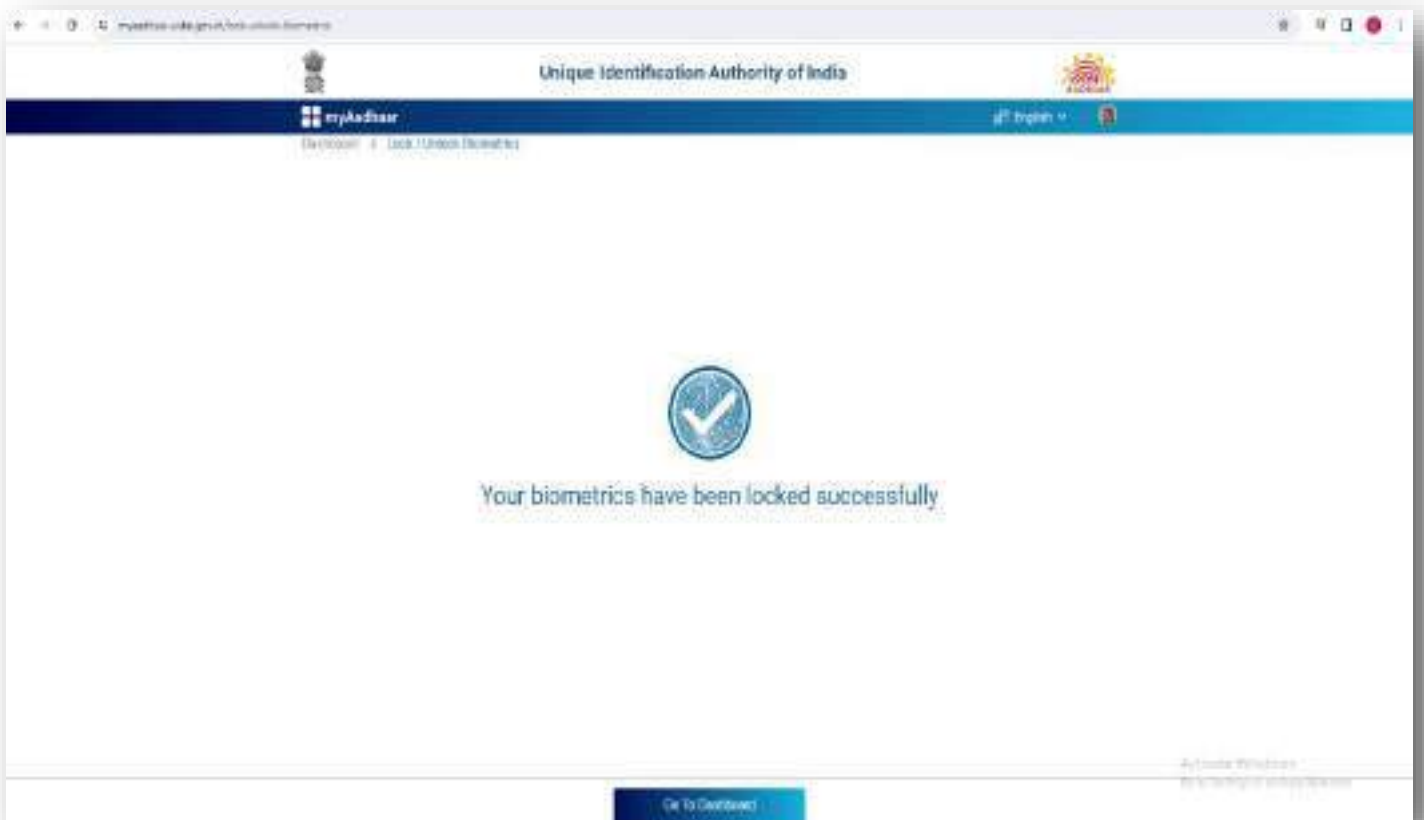
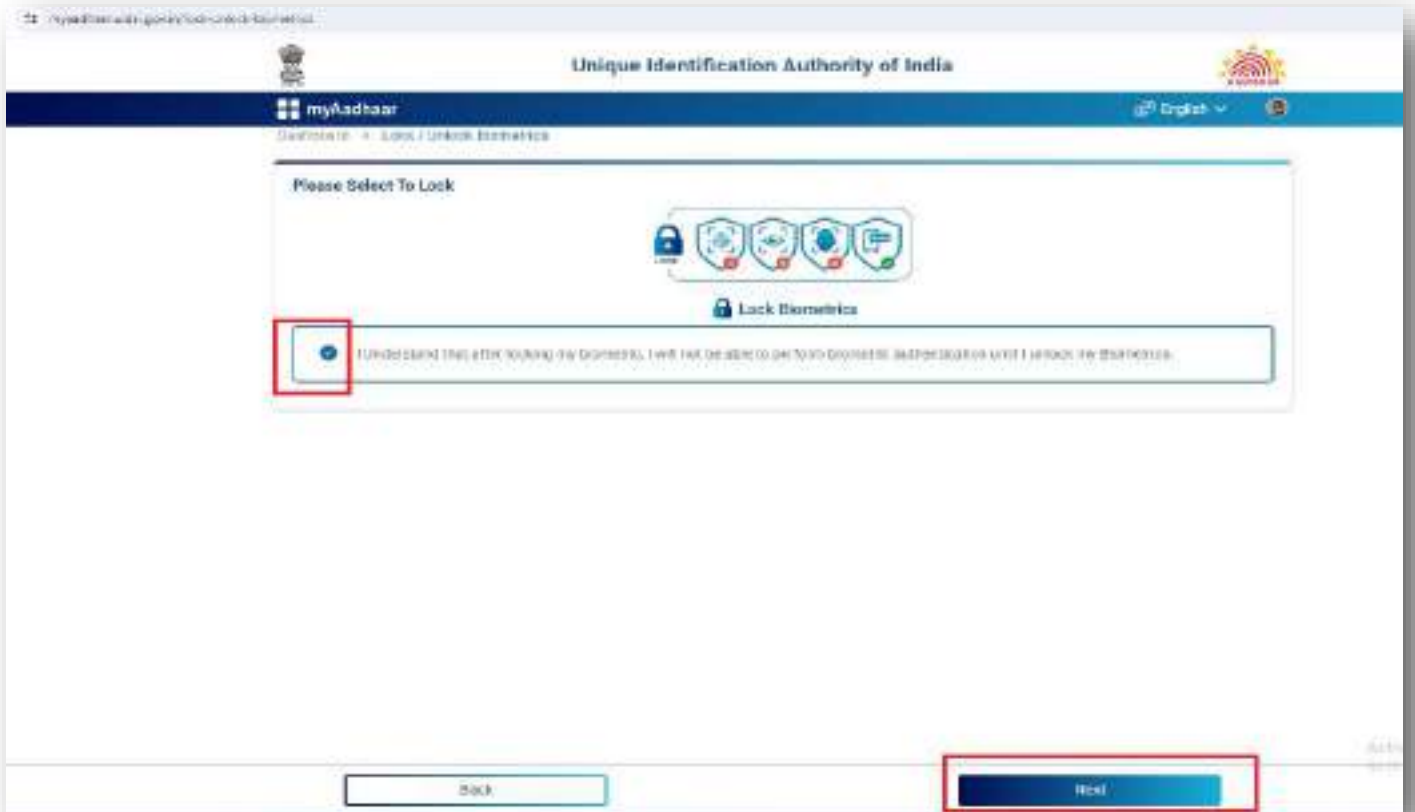
Please use this service from the Dashboard to lock your biometrics. When you lock your biometrics (fingerprint, iris, and face), they can no longer be used for Authentication. Moreover, OTP-based authentications would continue to be (as usual) as intended.



Please return to this page and proceed to unlock Biometrics upon unlocking your Biometrics (Fingerprint + Iris + Face). will be enabled along with OTP based Authentication.

Back

Unlock



GYAAN KA SAAR



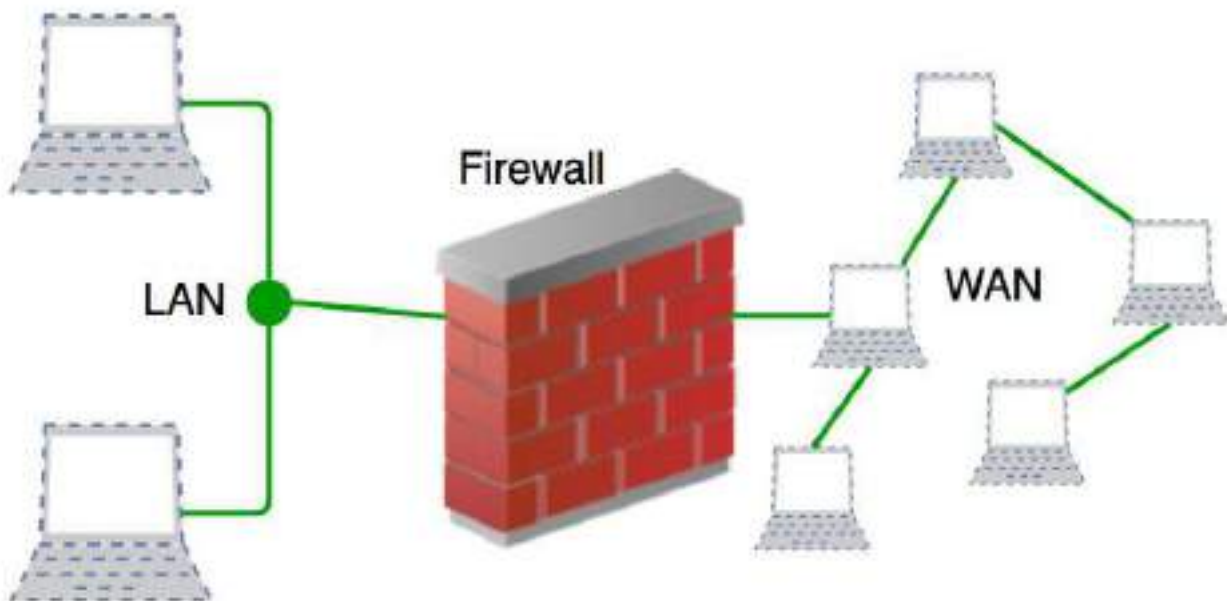
Precautions

1. Never share your Aadhaar number and biometric information with anyone, unless required by a trusted authority.
2. Regularly check transaction and transaction alerts - Monitor your SMS / Email alerts and bank statements for transactions regularly.
3. Be cautious- Be wary of calls, messages or emails requesting your Aadhaar or banking information or any similar red flags.
4. Report frauds - If you are a victim of such frauds, file a complaint via the complaint portal (<https://www.npci.org.in/register-a-complaint>) or dial helpline number 1930 to report the incident on National Cybercrime Reporting Portal www.cybercrime.gov.in and to your Bank also.
5. Create a virtual ID (VID) to use instead of your Aadhaar number for online transactions.
6. Lock or unlock your biometrics, to prevent any unauthorized access.
7. Update your mobile number and email ID with your Aadhaar. to receive OTPs and alerts.
8. Don't leave your Aadhaar letter or card unattended or share it on social media or public platforms.
9. Don't store your biometric information or Aadhaar data in any unprotected devices.
10. Don't print or display your personally identifiable Aadhaar data mapped with other sensitive information.

About the Chapter

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

The basic structure of Firewall is as follows:



In this chapter we are going to learn about Firewall and its features...

Chapter 32: Firewall Security

Vishal had often heard about “Firewall” related to Network Security. He decided to ask Reena about this.

Reena.. What is a Firewall?



A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

A firewall establishes a barrier between secured internal networks and internal networks and outside untrusted network, such as the Internet. A firewall establishes a barrier between secured internal networks and internal networks and outside untrusted network, such as the Internet.

How does it work?

It works in the following manner:

1. Accept : allow the traffic.
2. Reject : block the traffic but reply with an “unreachable error”
3. Drop : block the traffic with no reply.

Tell me more about it.



Okay. So let me tell you about the types of firewalls:

1. **Hardware Firewalls:** These firewalls are implemented as a physical appliance deployed in an organization's server room or data center.
2. **Software Firewalls:** Software firewalls are implemented as code on a computer. These firewalls include both the firewalls built into common operating systems and virtual appliances that contain the full functionality of a hardware firewall but are implemented as a virtual machine.
3. **Cloud Firewalls:** These virtual appliances are specifically designed to be deployed in the cloud and may be available as either standalone virtual machines or as a Software as a Service (SaaS) offering.



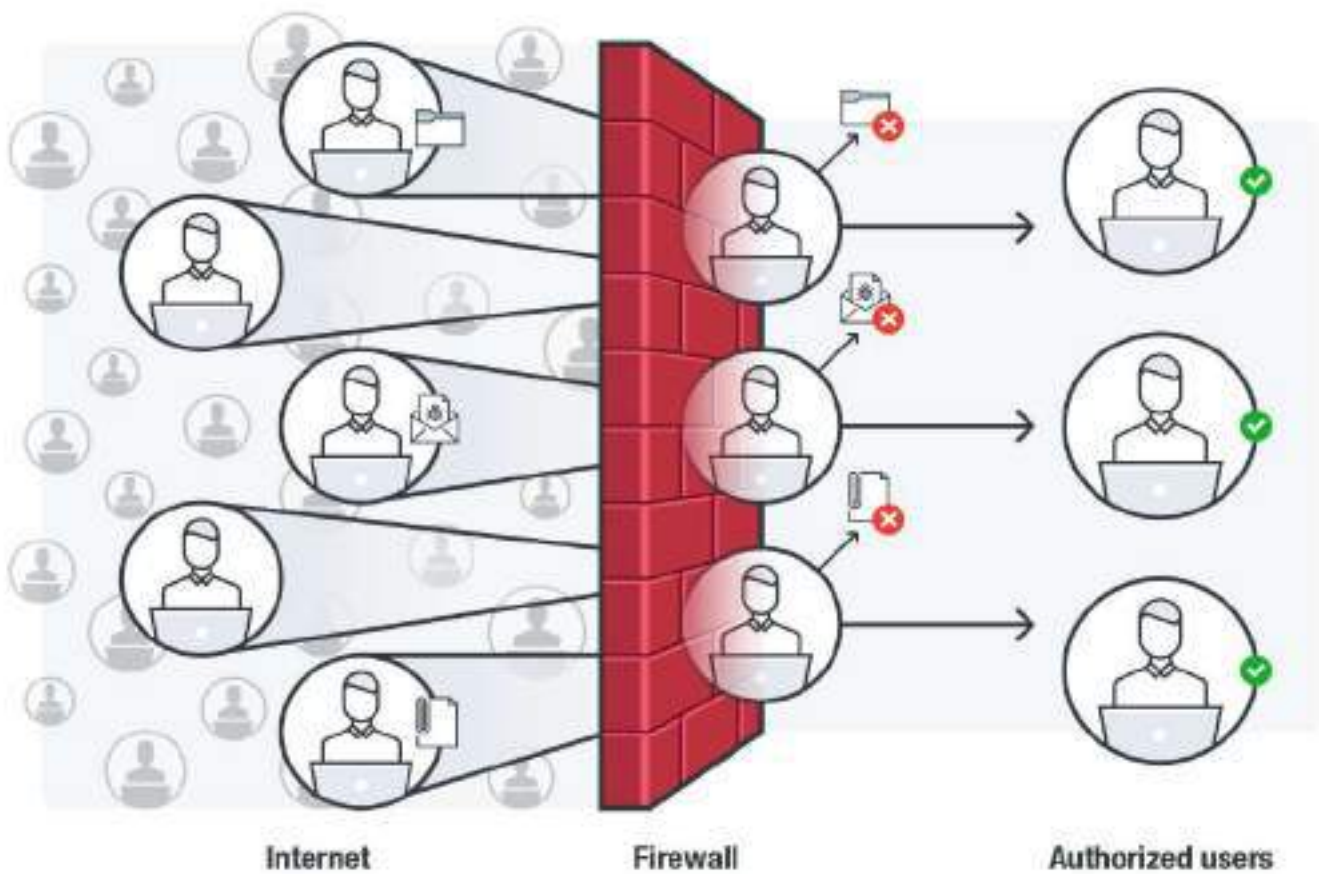
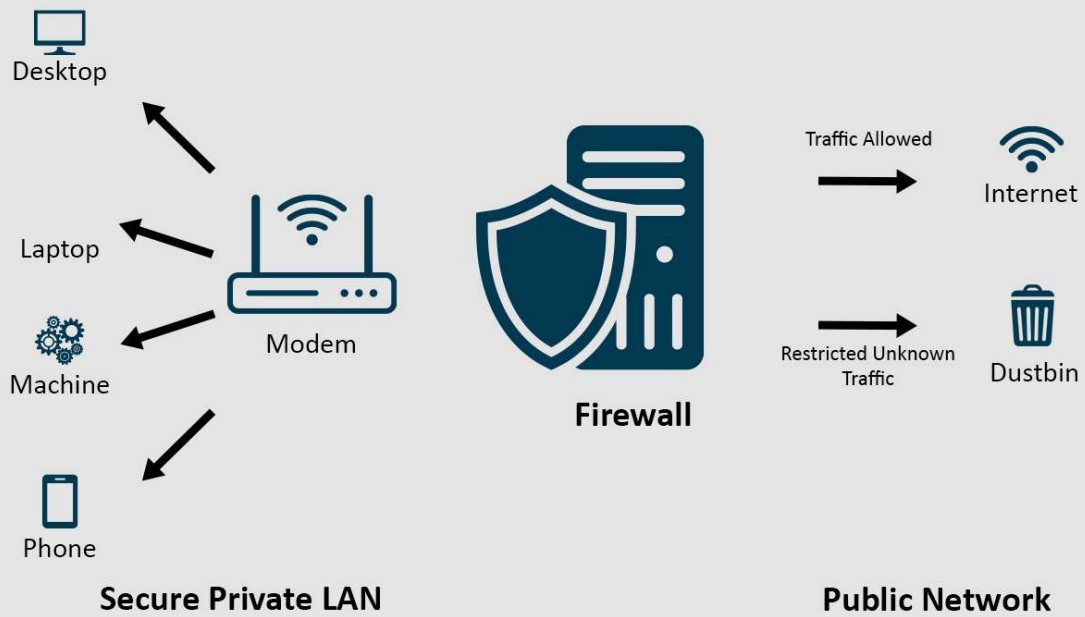
What are its advantages?

1. Protection from unauthorized access.
2. Prevention of malware and other threats.
3. By limiting access to specified individuals or groups for particular servers or applications, firewalls can be used to restrict access to particular network resources or services.
4. Firewalls can be set up to record and keep track of all network activity.
5. By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.





 **TOOLBOX**



<https://www.trendmicro.com/vinfo/hk-en/security/news/security-technology/best-practices-deploying-an-effective-firewall>



About the Chapter

The Indian Computer Emergency Response Team (CERT-In) is a Government Organization under Ministry of Electronics and Information Technology (MeitY), Government of India established with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

CERT-In takes several initiatives for the creation of awareness in the area of cyber security as well as training/ upgrading the technical knowhow of various stakeholders. The CERT-In as a part of awareness initiatives, issued cyber security alerts.

The CERT-In has recently issued a high-risk alert for those using the desktop version of the world's most popular browser – Google Chrome.

In this chapter we are going to learn about the alert issued by CERT-In...

Chapter 33: Cyber Security Alert issued by CERT-In



The Indian Computer Emergency Response Team (CERT-In) is a Government Organization under Ministry of Electronics and Information Technology (MeitY), Government of India established with the objective of securing Indian cyber space.

In a recent alert issued by CERT-In, it has stated that 'multiple vulnerabilities have been reported in Google Chrome which could allow a remote attacker to execute arbitrary code on the targeted system'.

According to CERT-In, these vulnerabilities affect Google Chrome v122.0.6261.57 or earlier on Windows, Mac and Linux. Google says the latest Chrome version includes 12 security fixes, out of which two were marked as high-severity flaws, five were medium-severity vulnerabilities and one was marked as low severity.

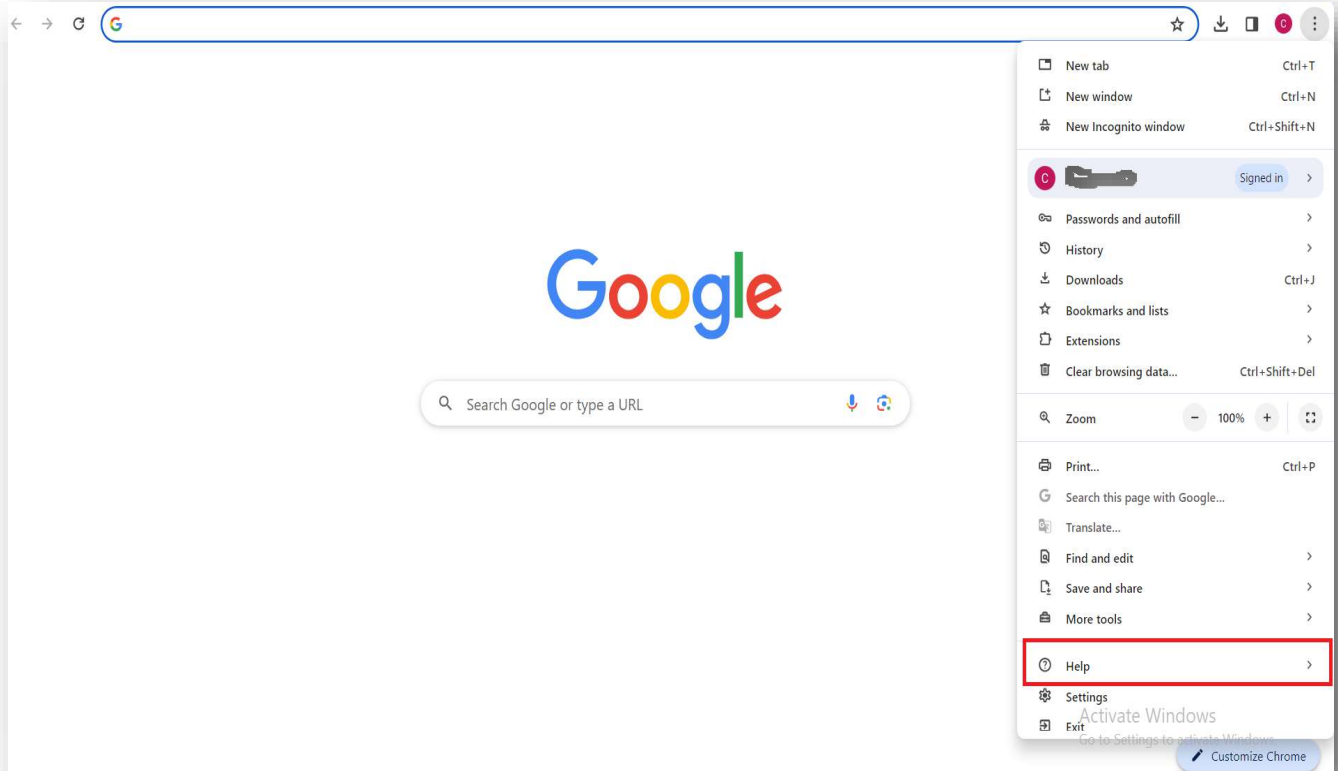
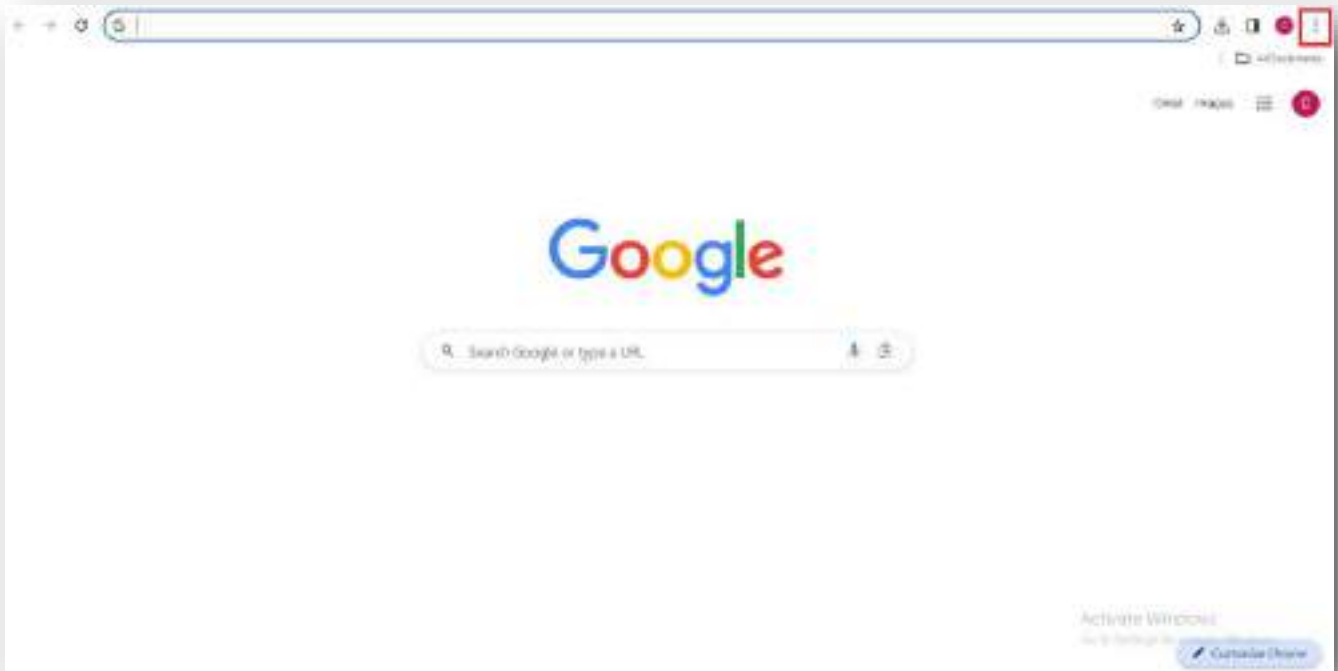
These vulnerabilities exist in Google Chrome due to inappropriate implementation in Payments, Downloads and WebApp Provider; Insufficient data validation in USB; Integer overflow in USB; Incorrect security UI in Downloads and Picture in Picture; Use after free in Printing, Profiles, Reading mode and Side Panel.

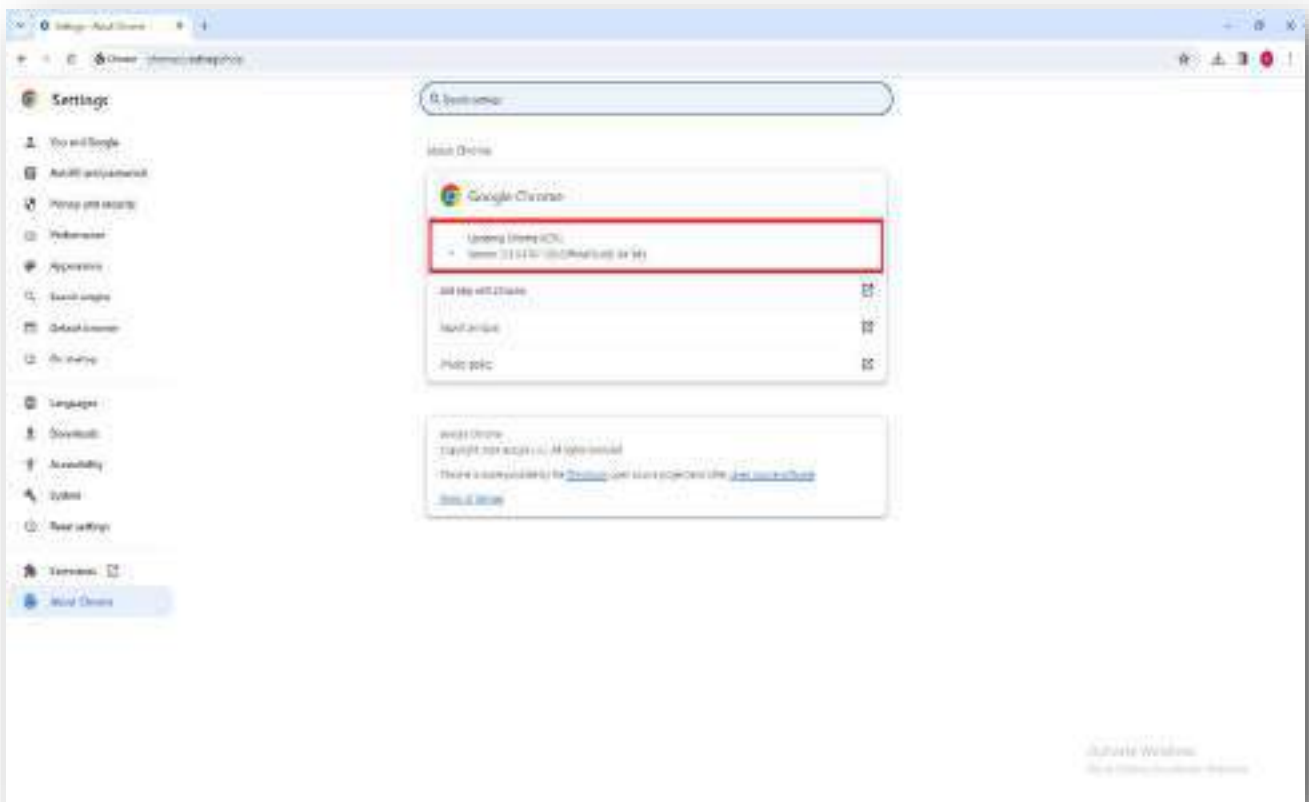
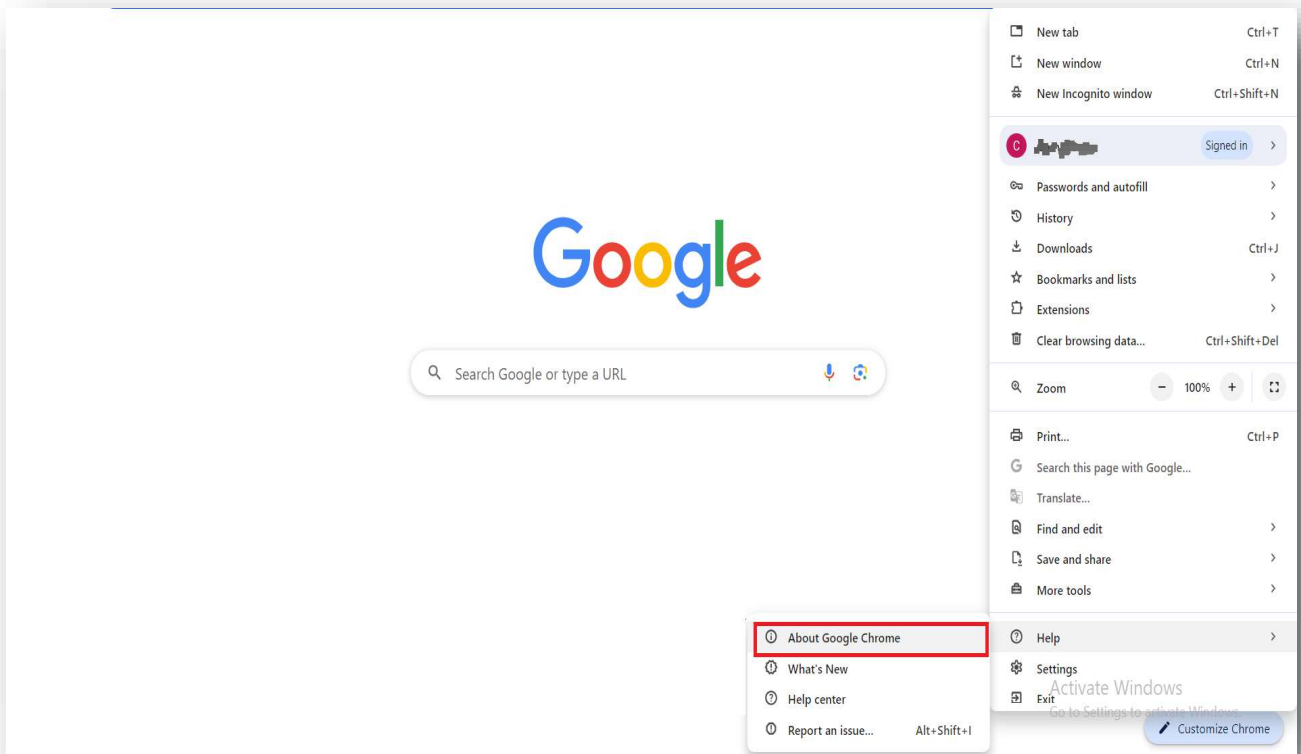
A remote attacker could exploit these vulnerabilities by persuading a victim to visit a specially crafted website. Successful exploitation of these vulnerabilities could allow a remote attacker to execute arbitrary code, information disclosure or cause denial of service condition on the targeted system.

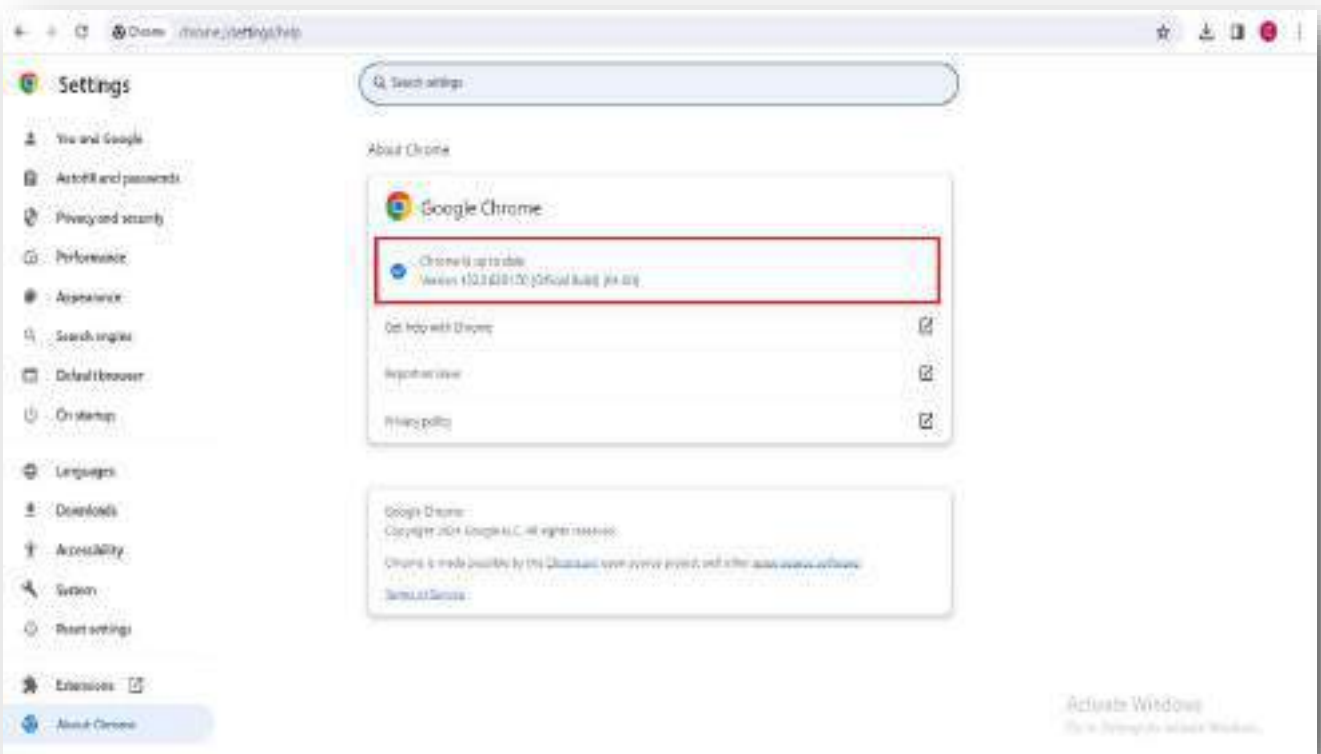
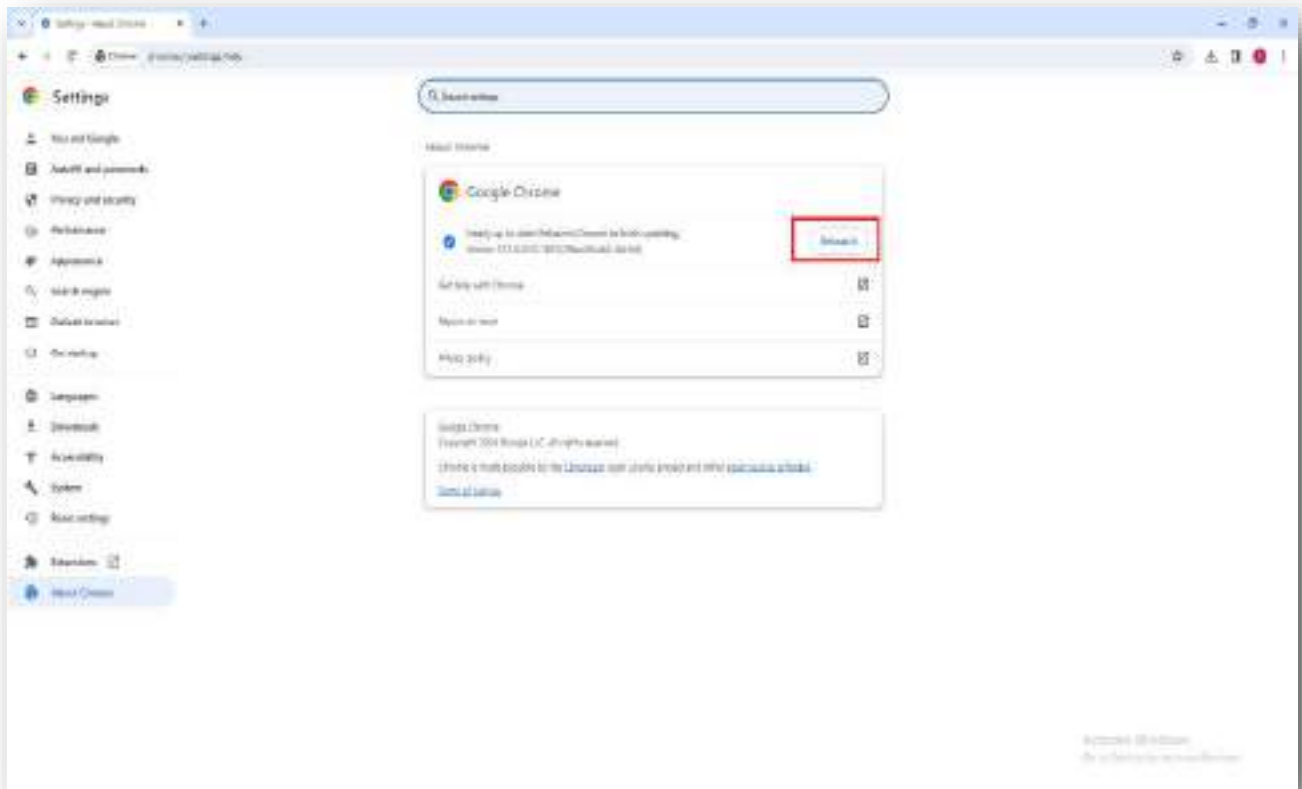
You can remove these vulnerabilities by manually updating Google Chrome to the latest version.



You can update your Google Chrome Browser by following the below mentioned steps:









Character Introduction

Hello Readers!

Vishal, with the help of Reena have now become well informed person with respect to cyber security.

So, we are introducing our new characters of the Comics Ms. Sayani and Mr. Pappu.



Meet **Sayani!!**

She is a Cyber Expert. She is also aware about the threat that are attracted with the usage of technology and the ways to use it responsibly.

Meet **Pappu!!**

He is a friend of Sayani, our Cyber Expert. He is a sound user of technology but does not know the specifics of it. He understands the Cyber situation but cannot resolve them without the help of our Cyber Expert.





About the Chapter

Email is a cost-effective and efficient way to communicate with others using the internet. Both companies and individuals can use email to convey important information and improve security for profiles and accounts.


Email is a critical component of organizational communication because it enables users to communicate quickly, easily, and with a variety of devices. Further, email can be used to send a number of different types of media, and communications can be tracked, stored, and organized according to attributes such as time and date stamps and size.

Email security is important because email contains sensitive information, which is used by everyone in the organization, and is therefore one of a company's largest targets for attacks. The shift to cloud-based email like Gmail and others comes with several benefits, but cloud-based email has become a tempting attack surface for cyber criminals.

Here, in this chapter, we are going to learn about the email usage policy of our Company...

Chapter 34: Email Security

Pappu has recently joined a new organization. He is adopting to the new culture of the organization. He randomly met Sayani and they were having an conversation about his new organization.



Hi! Pappu. How are you. How is your job at new Company going on???

Hi! Sayani. I am fine, trying to adjust with the environment at the new Company.

You know they are too vigilant with the security of their IT infrastructure. One thing which grabbed my attention was the email security.

Ohh!! This is nice. Considering the increase in the number of cyber instances, it is very important to have strong IT infrastructure.

Email security allows an individual or organization to protect the overall access to one or more email addresses or accounts.

Email Security is important considering the following reasons-

- A. To avoid Business Risks and Remain Compliant
 - B. To protect Confidential Information
 - C. To avoid Identity Theft
 - D. To unprotected Backups
- 



You know DCL also has its own Email Usage Policy, which states as follows:

Overview

This section of policy describes Digamber Capfin Limited's policy with regards to access to and disclosure of electronic mail messages sent or received by employees through Digamber Capfin Limited email system. The Company respects the individual privacy of its employees. However, employee privacy does not extend to the employee's work-related conduct or to the use of Company-provided equipment or supplies. Therefore, all employees are expected to exercise responsible and ethical behaviour when using the Company's Information Technology facilities.

Policy

1. E-mail must be used primarily for the conducting of Company business, and must not be used in any illegal, offensive, or unethical manner. The Company also prohibits such access for conducting non-Company commercial business, and for excessive personal use.
2. All the emails containing sensitive / critical data should be accessed from a dedicated machine which can be used by authorized personnel only.
3. Creation of email IDs of new employees and removal of email IDs of employees leaving the Digamber Capfin Limited shall be done as per the procedure specified in IT Procedures.
4. Employees are prohibited from accessing other associate's e-mail messages. However, Digamber Capfin Limited reserves the right to access any associate's e-mail for any business purpose, and also for inspection for disciplinary or legal actions.
5. Chain Mails, Jokes, multiple forwards, large attachments are strictly prohibited
6. Emails must be checked regularly.
7. Set the "Out of Office" flag and arrange for someone to deal with your email if you are away.
8. Delete unwanted or unnecessary email. It is the employee's responsibility to manage their own email folders and stay within the storage limits set.
9. Unsolicited emails, especially with an attachment, may contain a virus. If in doubt, delete the email or contact the sender for verification.
10. An employee shall be given a set message capacity for sending e-mails by default. In case additional capacity is required then employee will have to make a written request to the System Admin department along with a copy to his Department Head. Additional capacity shall be provided only after the approval of the respective Department Head.
11. Printing of electronic mail shall be avoided unless absolutely necessary.
12. All employees are required to take necessary backups or archive old but important mails required for any future reference. (this is applicable for important mails only)
13. PAN numbers, Aadhar Number or any other sensitive information will not be sent unencrypted via email.



GYAAN KA SAAR



Precautions

1. To minimize the potential damage and devastation in a ransomware attack, enterprises should back up critical files regularly and automatically.
2. In situations where a corporate email account's credentials are successfully stolen, multifactor authentication (MFA) can prevent an attacker from gaining access to the account and wreaking havoc in the organization.
3. Use Spam Filter. You can get hundreds of unknown emails in a day, which is why it is so important to use a spam filter.
4. Always log out after using your email account whenever you log into your email account, whether it is on your own device or on someone else's.
5. Do not open emails sent by someone you do not know or trust.
6. Avoid sending sensitive information over email.
7. It is suggested to change your passwords at least after every 60 days, mainly if you view and manage your mail on any public system.
8. Creating a strong, unique password for every account is one of the most critical steps you can take to protect your privacy. Never share your password.
9. Check where that link will direct you before clicking on any link in an email message. If the link looks suspicious, don't click on it even if it seems to be from someone you know. Instead, call or text that person and ask if they sent the message.
10. When opening commonly infected formats such as pdf, xls, and doc, use the built-in functionality of your webmail provider for scanning the attachments before downloading them. (Eg. Gmail has a virus scanner for attachments).
11. Never download .exe files received on mails.
12. Keep your Anti virus software up-to-date.



About the Chapter

A Domain Name System (DNS) attack is where cyber-criminals exploit vulnerabilities found in the Domain Name System (DNS) of a server. The purpose of the domain name system is to translate user-friendly domain names into machine-readable IP addresses, via a DNS resolver.


The DNS Attacks are of following types:

1. **Volumetric DoS attacks:** Attempt to overwhelm the DNS server by flooding it with a very high number of requests from one or multiple sources, leading to degradation or unavailability of the service.
2. **Exploits:** Attacks exploiting bugs and/or flaws in DNS services, protocol or on operating systems running DNS services.
3. **Stealth/Slow drip DoS attacks:** Low volume of specific DNS requests causing the DNS to slowdown and leading to degradation or unavailability of the service.
4. **Protocol abuse:** Attacks using the DNS in a different manner than the original intention leading to data exfiltration and phishing.
5. **DNS Hijacking:** In this attack, the attacker diverts the DNS query traffic to a malicious DNS server, leading users to fraudulent websites or intercepting internet traffic.

Here, in this chapter, we are going to learn about the DNS Attacks and how to prevent from them...


Chapter 35: DNS Attacks

One day Pappu was called by Mr. Rajesh, his Reporting Manager. Mr. Rajesh was tensed about the increasing complaints received from their customers due to non-fulfilment of orders placed through their website. Also, he was concerned about the decreasing traffic on his website.



Good Morning Pappu. I have called you here to discuss an issue which is bothering me.

Good Morning Sir. Please let me know what is it about?



You know from the past 10-15 days, we have received so many complaints from our customers for not receiving their orders which they have paid from our Website, but I have checked from the online order fulfilment department that there are no such orders.

I have also noticed from Website Reports that the number of people visiting our website has also decreased. I think there is something wrong.

You need to look into the matter and resolve it.

Pappu decided to discuss about the issue with Sayani for her expert advice...



Hey Sayani! I need your expert opinion on something. Please help me.

Hey Pappu! I'll help you. Tell me what happened?

My Reporting Manager called me today and told me that the Company is receiving customer complaints from the past 10-15 days for not receiving their orders which they have paid from our Website, but we have not received any such order requests.

Also, the number of people visiting our website has also decreased. He has told me to resolve this issue.

I need your help.

Hmm. Can you tell me the website address of your Company?

Here: **www.buyonline.com**

Let me check. See Pappu, I entered **www.buyonline.com** in search box but I was redirected to some other site with name was **www.byuonline.com**. Somebody has conducted a DNS Hijacking-Phishing Cyber Attack on the website of the Company.

The fake website looks identical to the original website of your Company.



Hey Sayani! What is a DNS Hijacking-Phishing Cyber Attack? And what should we do now?

Let me tell you what it is.

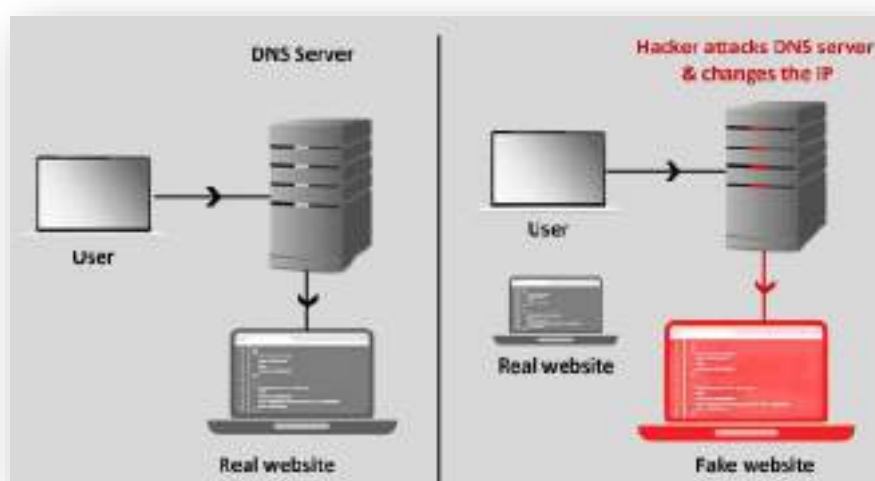
The Domain Name System (DNS) is a critical component of the internet infrastructure, responsible for translating human-readable domain names into IP addresses that computers can then use to communicate with each other. These are vulnerable to attacks.

The attacks faced by your Company is a DNS Hijacking-Phishing where, the attacker diverts the DNS query traffic to a malicious DNS server, leading users to fraudulent websites or intercepting internet traffic.

As a result of this, people are unable to view your website and are instead redirected to the fake websites.

I think you should report this fake domain to the Domain service provider so that the fake site can be shut down and issue a public disclosure telling your customers to exercise caution for this.

Also, I suggest you to file a complaint with the Cyber Crime Cell of Police.



<https://www.valencynetworks.com/blogs/cyber-attacks-explained-dns-invasion/>



GYAAN KA SAAR



Precautions

1. Conduct regular checks for your DNS.
2. Keep your DNS updated so as to ensure that vulnerabilities are treated well in time and the risk for exploitation of those vulnerabilities are reduced.
3. Restrict DNS resolver usage to only users on the network and never leave it open to external users. This can prevent its cache from being poisoned by external actors.
4. For mitigation, identify the source of attacks and analyze the vulnerabilities responsible for it.
5. Run malware scanning tools on all network devices, starting with the machines responsible for the most DNS requests.
6. Blacklisting the IPs that are flooding your server is an absolute must if you intend to stop the attack, and blacklisting entire subnets may be necessary.
7. Using a VPN solution will prevent the hijacking of local DNS settings and redirection of end-user devices.
8. Be vigilant while visiting any site and be cautious towards the redirecting of websites.
9. Implement firewalls and keep firewall definitions up to date.
10. DNS filtering examines the URLs requested by users and the URLs sending data through the DNS. Known-malicious URLs will be blocked and suspicious URLs will be quarantined.
11. You should use strong and unique passwords for your domain registrar and email accounts.
12. You should enable two-factor authentication and monitor your domain name records for any unauthorized changes.



About the Chapter

A distributed denial of service (DDoS) attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server.


The objective of a DDoS attack is to prevent legitimate users from accessing your website. Unlike other types of attacks, attackers do not use DDoS to breach your security perimeter. Instead, DDoS attacks are used to take down your website and prevent legitimate traffic, or used as a smokescreen for other malicious activities.

DDoS attacks cannot steal website visitors information. The sole purpose of a DDoS attack is to overload the website resources. However, DDoS attacks can be used as a way of extortion and blackmailing. For example, website owners can be asked to pay a ransom for attackers to stop a DDoS attack.

Here, in this chapter, we are going to learn about the DDOS Attacks and how to prevent from them...

Chapter 36: Distributed Denial of Service (DDoS) attack

One day Pappu came across a news article mentioned Distributed Denial of Service attack (DDoS) attack. He thought of approaching Sayani for understanding it.



Hi, Sayani ! How are you. Today I have come here to ask something

Hi Pappu! I am fine. Tell me how can I help you.

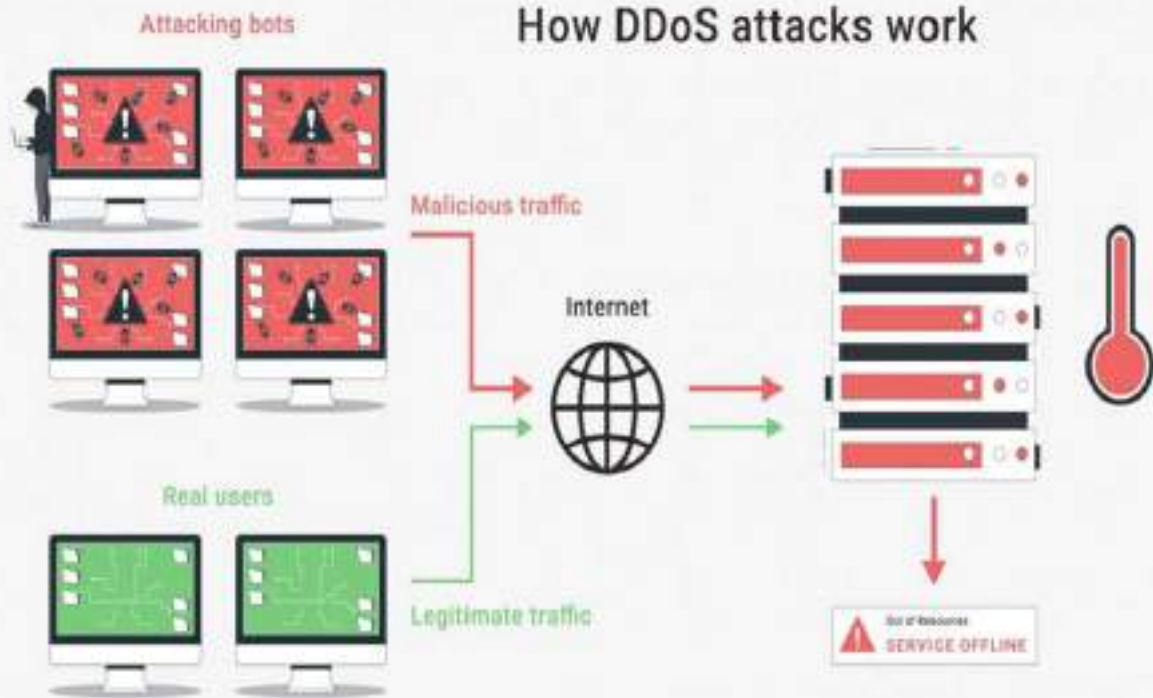
Actually I came across an article on Distributed Denial of service (DDoS) attack. Do you have an idea what it is ?

Oh !! Yes. I can explain you in details what it is and how does it work. I will also share precautions for safeguarding from it.

Look, A distributed denial-of-service (DDoS) attack is an attempt to disrupt the traffic of a targeted server, service, or network by overwhelming it with a flood of Internet traffic. A DDoS attack aims to infect a network. This is done by infecting devices with malware, creating botnets that can remotely carry out an attack. The bots in a botnet will overload a network by sending disruptive requests to the IP address of the network, which can eventually result in a denial-of-service.



How DDoS attacks work



<https://gcore.com/learning/how-to-protect-against-ddos-attacks/>



A DDoS attack will test the limits of a web server, network, and application resources by sending spikes of fake traffic. Some attacks are just short bursts of malicious requests on vulnerable end-points such as search functions. DDoS attacks use an army of zombie devices called a botnet. These botnets generally consist of compromised IoT devices, websites, and computers.

When a DDoS attack is launched, the botnet will attack the target and deplete the application resources. A successful DDoS attack can prevent users from accessing a website or slow it down enough to increase bounce rate, resulting in financial losses and performance issues.

The main goal of an attacker for leveraging a Denial of Service (DoS) attack method is to disrupt a website availability:

- The website can become slow to respond to legitimate requests.
- The website can be disabled entirely, making it impossible for legitimate users to access it.

DDoS attacks cannot steal website visitors information. The sole purpose of a DDoS attack is to overload the website resources. However, DDoS attacks can be used as a way of extortion and blackmailing. For example, website owners can be asked to pay a ransom for attackers to stop a DDoS attack.

DDoS attacks can have many other motivations including political, hacktivist, terrorist, and business competition. Anyone with a financial or ideological motive can damage an organization by launching a DDoS attack against it.



Different Types of DDoS Attacks

Volume-based Attacks



Goal: Flood a site with a high volume of traffic and connections, overwhelming its bandwidth, network equipment, or servers until it crashes.

Protocol Attacks



Goal: Disable resources that websites use to protect themselves like firewalls and load balancers to more easily disable targeted websites and/or servers.

Application Attacks



Goal: Use zombie networks to overwhelm the layer of a network that generates web pages and responds to application requests.

GYAAN KA SAAR



Precautions

1. Conduct routine cyber security exercises to check the vulnerabilities in the system and then take necessary steps.
2. Encrypt sensitive data when it is at rest and in motion to reduce the risk of data loss, leakage or theft.
3. Use only secure connection while using the internet facilities.
4. Keep your devices and software up to date
5. Use strong and unique passwords
6. Be cautious of suspicious emails and attachments
7. Use a reputable anti-malware solution
8. Use a reputable VPN
9. Practice good cyber hygiene
10. Regular patch update can prevent DDoS attacks
11. Some of the warning signs for a DDoS attack are:
 - Unusually high traffic volume
 - Slow or unresponsive website
 - Network connectivity issues
 - Unusual traffic patterns
 - Unexpected server errors
 - Unusual spikes in resource usage



About the Chapter

Voice clone fraud has been on the rise in India. A report published in May last year revealed that 47% of surveyed Indians have either been a victim or knew someone who had fallen prey to an AI generated voice scam.

It has come to light that scammers are using voice cloning tech to trick people, and create fake voices of anyone in seconds.

A voice cloning scam involves using artificial intelligence (AI) technology to replicate someone's voice, typically for fraudulent purposes. Scammers can use these clones to impersonate individuals and trick them or others into giving up personal information, money, or access to accounts.

These scams can be particularly hard to detect, as the voice sounds genuine. However, there are some red flags to watch out for:

- *Unexpected calls or messages: Be wary of unsolicited calls or messages, especially from unknown numbers or claiming urgency.*
- *Suspicious requests: Don't share personal information or authorize transactions over the phone without verifying the caller's identity through other means.*
- *Unnatural speech: Pay attention to any inconsistencies in the voice, like robotic-sounding delivery or unnatural pauses.*

Here, in this chapter, we are going to learn about the Voice Cloning Scams and how to prevent from them...

Chapter 37: AI Voice Cloning Scams

One day Pappu was working at his home. He received a phone call from an unknown number, which left him in confusion. Let's see what was the phone call about...



Hello? Who is this?

Mr. Pappu! We have your daughter with us. If you want her back safe and sound, do as we say.

Who are you? What are you talking about?

Mr. Pappu, if you do not believe us, hear your daughter calling out to you.

The unknown caller makes Pappu hear the sound of a crying girl whose voice sounds similar to his daughter.

Mr. Pappu, if you want your daughter safe, you need to pay Rs. 50,000

Hearing this Pappu immediately disconnects the call.



How is this possible, when Riya, my daughter is playing around me!! This might be some kind of scam. I must talk to Siyani about this

Pappu went to Sayani's place and described her the entire incident.

Pappu, these types of frauds are called voice cloning fraud. You were lucky that Riya was around you and you did not fall prey to his attempt.

A voice cloning scam involves using artificial intelligence (AI) technology to replicate someone's voice, typically for fraudulent purposes. Scammers can use these clones to impersonate individuals and trick them or others into giving up personal information, money, or access to accounts.

These scams are hard to detect as the voice sounds genuine. However, there are some red flags to watch out for:

- Unexpected calls or messages
- Suspicious requests
- Unnatural speech



STEP 1: Voice Gathering: Scammers might collect voice samples from various sources, like social media videos, public speeches, or even intercepted phone calls.

STEP 2: AI Training: These samples are used to train AI algorithms to learn and mimic the target's voice patterns, intonation, and speech characteristics.

STEP 3: Voice Cloning: After training, the AI can generate realistic audio that sounds like the target, even saying new phrases or sentences.

STEP 4: The Scam: Scammers then use the cloned voice to carry out fraudulent activities, such as:

- * Phishing: They call or leave voicemail messages impersonating trusted entities like banks, companies, or even the victim's friends or family, attempting to steal personal information or money.
- * Social Engineering: They impersonate the victim themselves to manipulate someone into taking an action, like transferring funds or revealing sensitive details.
- * Fraudulent Orders: They use the cloned voice to place orders or make transactions over the phone, pretending to be the real person.



GYAAN KA SAAR



Precautions

1. Be cautious about sharing your voice online: Limit the amount of personal information you share publicly, including audio recordings.
2. Enable two-factor authentication (2FA): This adds an extra layer of security when accessing your accounts.
3. Verify caller identity: Don't trust caller ID alone. Always try to verify the caller's identity through other channels before sharing any personal information.
4. Report suspicious activity: If you receive a suspicious call or message, report it to the authorities and the relevant organisation the scammer was impersonating.
5. If you decide to answer a call from an unknown number and it sounds like a panicked family member is asking you for money, try not to panic yourself. Instead, end the call and try calling or texting the person using the number they've given you, rather than the one that called, to check that they're OK.
6. The same goes if you receive a call from a scammer pretending to be your bank. Don't immediately believe their claims. Instead, end the call and call the number listed on your bank's website or on the back of your debit or credit card.
7. Try to minimise the words you speak while on call with unknown callers or blank calls, as they may have made arrangements for cloning your voice.
8. It's essential to protect yourself from future scams by blocking the scammer's phone number or email address.
9. If you've been impersonated online, warn your friends and contacts about the scam, as they could be next.
10. Given the capability of scammers to replicate voices, establish a unique family or friendly password known exclusively to trusted individuals.



About the Chapter

As more services go digital, instances of identity theft have become increasingly prevalent, posing significant risks to individuals and national security. Stolen identities are often exploited to procure mobile numbers or SIM cards, which can subsequently be utilised for illegal activities.

Considering the seriousness of the situation, the Department of Telecommunications (DoT) of Government of India issues advisories from to time to warn the citizens.

Department of Telecommunications (DoT), Ministry of Communications, has issued an advisory to citizens that calls are being received by the citizens wherein callers, in the name of DoT, are threatening that all of their mobile numbers would be disconnected or their mobile numbers are being misused in some illegal activities. The DoT has also issued advisory about WhatsApp calls from foreign origin mobile numbers (like +92-xxxxxxxxxx) impersonating government officials and duping the people.

Cyber criminals through such calls try to threat/steal personal information to carry out cyber-crime/financial frauds. The DoT does not authorise anyone to make such call on its behalf and has advised people to stay vigilant and asked not to share any information on receiving such calls.

The DoT has advised citizens to report such fraud communications at 'Chakshu-Report Suspected Fraud Communications' facility of Sanchar Saathi portal (www.sancharsaathi.gov.in). Such proactive reporting helps DoT in prevention of misuse of telecom resources for cyber-crime, financial frauds, etc.

Further, citizens can check the mobile connections in their name at 'Know Your Mobile Connections' facility of Sanchar Saathi portal (www.sancharsaathi.gov.in) and report any mobile connection not taken by them or not required.

Here, in this chapter, we are going to learn about the precautions we need to take in this regard...

Chapter 38: Mobile Number Scams

One Sunday morning, Pappu was watching News on his TV. The News Anchor covered a latest advisory issued by the Department of Telecommunication. When he heard the news, something suddenly struck in his mind.

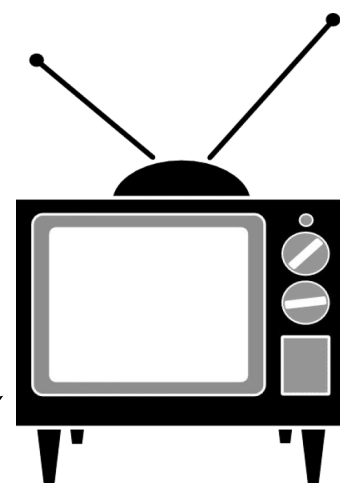
The DoT has also issued advisory about WhatsApp calls from foreign origin mobile numbers (like +92-xxxxxxx) impersonating government officials and duping the people. The Citizens are requested to stay alert.

Further, citizens can check the mobile connections in their name at 'Know Your Mobile Connections' facility of Sanchar Saathi portal (www.sancharsaathi.gov.in) and report any mobile connection not taken by them or not required.

This is interesting. Thank God I haven't received any WhatsApp calls from foreign origin mobile numbers (like +92-xxxxxxx). But I need to be careful.

But regarding the phone connections, even I don't know about the phone numbers issued with my ID.

Let me ask Sayani how to do it.





Hey Sayani! Did you hear about the advisory issued by the DOT regarding checking the mobile connections associated with our Ids?

Yes Pappu, I have heard about the Advisory. Have you checked your mobile connections?

I tried to. But I was not able to do it. Can you guide me?

Sure Pappu. But before that, let me tell you something about this initiative of DoT.

The DoT has launched a web portal called Telecom Analytics for Fraud Management & Consumer Protection or TAFMCP. Users can also deactivate those unknown numbers and register with the ID.

On the portal, you can check and ensure that all the active mobile numbers belong to you or to your relatives, like parents, siblings and other family members.

In case of any doubt, this website gives 03 options; "Not my number", "Not required" and "Required".

You can report a number that is registered with your ID but does not belong to any of your family members by clicking "Not my number".





You can check the mobile connections by following the below-mentioned steps:



You can check the mobile connections by following the below-mentioned steps:

Not my number: This option is to raise request of disconnection of selected mobile connection(s) which are active in your name and without your knowledge.

Not required: This option is to raise request of disconnection of selected mobile connection(s) which are active in your name and not required anymore.

Required: This option is to inform that selected mobile connection(s) are active in your name and No action is required.



About the Chapter

What would be the job of a key if there wouldn't be a lock and what would be the role of a lock if there wouldn't be a key? Useless, right? Where there is a crime, there is precaution and protection. Cyber Security's existence in this world is because of cybercrime. The more cybercrime tries to become a part of our lives, the more we try to adopt cybersecurity.

Cybersecurity, also known as IT security refers to a technique of protecting networks, computers, programs, and data from any activity aimed at exploitation, or unauthorized access. It helps to protect information from being stolen, requiring an understanding of potential threats, like viruses or other malicious code.

Despite lots of government efforts and specialized inputs, cyber-crime is not ready to slow down. With constant technical innovation, new dangers are continually coming to the surface. Cybersecurity is all about building confidence and safety for the IT world.

Here, in this chapter, we are going to learn how a world without Cyber Security looks like...

Chapter 39: World Without Cyber Security

On one morning, when Pappu woke up he experienced something which he never thought could happen.

It seems that the Cyber Security System has collapsed. The whole world is in chaos right now. The systems are failing right now.

People are losing money!! Rapid Debits shook the world!!

Then, there is Traffic chaos. People are colliding at the junctions due to improper traffic management!!

The data of patients have been stolen, leaving the Doctors confused about the treatment to be given to patients!!

The Companies are reporting that the data of their customers have been leaked and stolen!! Causing data breaches all over the world!!

What is this?! Let me call Sayani & ask about this!!



Pappu tries to call Sayani multiple times. But all goes in waste. The calls could not be connected! All this made Pappu worry.



Ohh My God!! My accounts have been debited. I am unable to report it to the Bank. Now what should I do? Here I am unable to connect to Sayani!!

Rs. 20,000.00 have been debited from your account no. XXXXXX.

Rs. 30,000.00 have been debited from your account no. XXXXXX.



He started sweating. Suddenly, he woke up panting, realizing that this was only a bad dream. He decided to call Sayani.



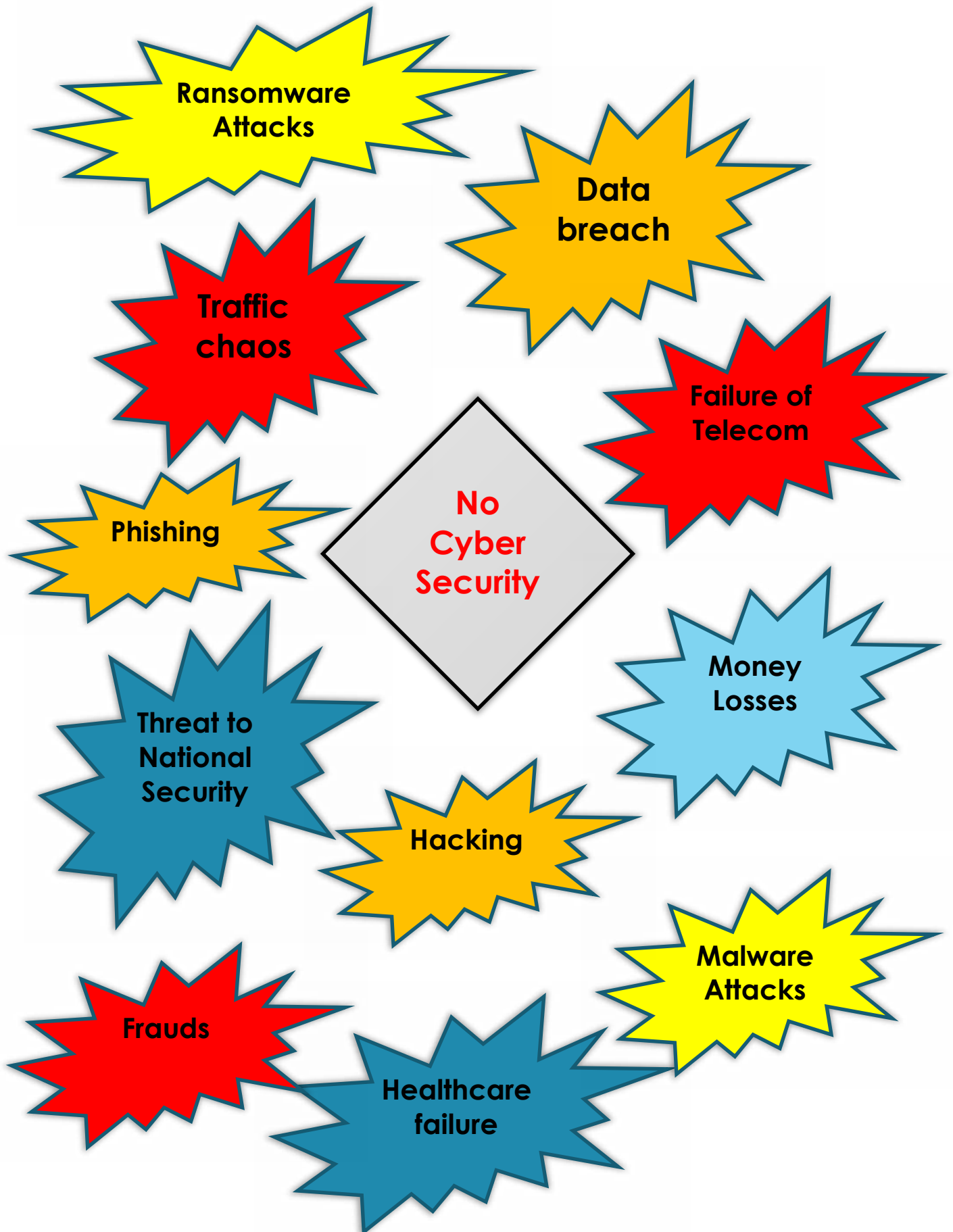
You know Sayani, I had a horrible dream today. In the dream, the Cyber Security system of the world collapsed. It was utter chaos. I lost a lot of money as a result of it.

Hahaha! You should thank god that it was just a bad dream. Just imagine, if it becomes the reality! Therefore you should all our my advices which I had shared till now otherwise the world would become worse to worst.





What would a world without Cyber Security looks like?



So be cautious regarding your Cyber Security.



About the Chapter


For technology professionals, the internet is an indispensable resource. However, the line can become blurred between what activities constitute personal use and inappropriate online behaviour.

Not having an enforceable internet usage policy can create significant liability issues for a company, not to mention diminished productivity resulting from personal business conducted on company time and equipment.


Therefore, employers need to have a clear, specific internet usage policy that is widely communicated and consistently enforced.

Chapter 40: Internet Usage Policy

Pappu and his colleague were searching some content on the internet in the office but the some of the sites did not open. There was a restriction on connection. He decided to ask Sayani about this.



Hi! Pappu. How are you. How is your job going on?



Hi! Sayani. I am fine, My job is also going well. I have learnt many new things here.

I wanted to ask you something? You know yesterday, we were searching some content on internet in office but the sites did not open.

Do you know why our company has imposed these restrictions.

Ohh.!!! This might be the internet usage policy.

It is important for a business to have an internet usage policy in place that sets and establishes guidelines for employees to follow while using the internet at work.



You know DCL also has its own Internet Usage Policy, which states as follows:

Overview

Internet is a great resource for our organization; it is the responsibility of each employee to use this resource responsibly and in a lawful manner. The (organization's) internal network will not be connected to the Internet. It is assumed that the predominant use of these resources will be for work use, and that any personal use of e-mail or the World Wide Web services will be limited; never a priority over work matters. If an employee is found spending excessive time on personal use of these resources, this privilege may be revoked for that employee. This document establishes the acceptable use of the Internet.

Policy

1. Internet access is limited to official business and purposes only.
2. As a security measure Internet system which are part of a different network in no circumstance a user will link these systems with the internal LAN & WAN network.
3. Employees who need an access to the internet shall make a request to the concerned HOD who in turn shall approve and forward the same to System Admin.
4. On receipt of such request, System Admin shall forward the same to Head – IT who shall grant the final approval for giving internet access to the requesting employee as per the availability of network and resources.
5. Eligible individuals may be authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system.
6. Users may not, under any circumstances, transfer or confer these privileges to other individuals.
7. Users shall not use any account assigned to an individual without written permission from the systems administrator.
8. The authorized user is responsible for the proper use of the system, including password protection.
9. The introduction of viruses, or malicious tampering with any computer system, is strictly prohibited.
10. Files that are downloaded from the Internet must be scanned with virus detection software before being accessed. Files downloaded through the terminal server will have to be scanned by the IT dept.
11. The truth or accuracy of information on the Internet and in e-mail should be considered suspect until confirmed by a separate (reliable) source.
12. Employees shall not place company material (copyrighted software, internal correspondence, etc.) on any publicly accessible Internet computer.
13. Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third party. Employees must exercise caution and care when transferring such material over the Internet.
14. Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, employees are prohibited from downloading software and/or modifying any such files without permission from the copyright holder.
15. Any infringing activity by an employee may be the responsibility of the organization. Therefore, the organization may choose to hold the employee liable for the employee's actions.
16. This organization reserves the right to inspect an employee's computer system for violations of this policy.
17. Any form of Messengers should not be loaded on any terminals. IT personnel have the right to delete such software without notification and without the consent of any employee.




About the Chapter

On 11th August, 2023, the President of India gave assent for the enactment of the Digital Personal Data Protection Act, 2023 for the protection of privacy of citizens.

This Act provides for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

In this Chapter, let's learn about this Act through Sayani and Pappu.

Chapter 41: Digital Data Protection



Hey Sayani! Can you tell me something about the Digital Personal Data Protection Act, 2023?

Sure Pappu. Ask what you want to know.

What are the main features of this Act?

The Act protects the digital personal data by providing for the following:


- ⇒ The obligations of persons that process data.
- ⇒ The rights and duties of individuals for their data.
- ⇒ Financial penalties for breach of rights, duties and obligations.

Okay. So, what is data as per the Act?

Data means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means;

What is personal data?

It means any data about an individual who is identifiable by or in relation to such data.



Can anybody process my data?

Your data can be processed by anybody with your consent or for any lawful reason.

What are my rights under the Act?

Your rights are:

1. The right to access information about personal data processed;
2. The right to correction and erasure of data;
3. The right to grievance redressal and right to withdraw consent; and
4. The right to nominate a person to exercise rights in case of death or incapacity.

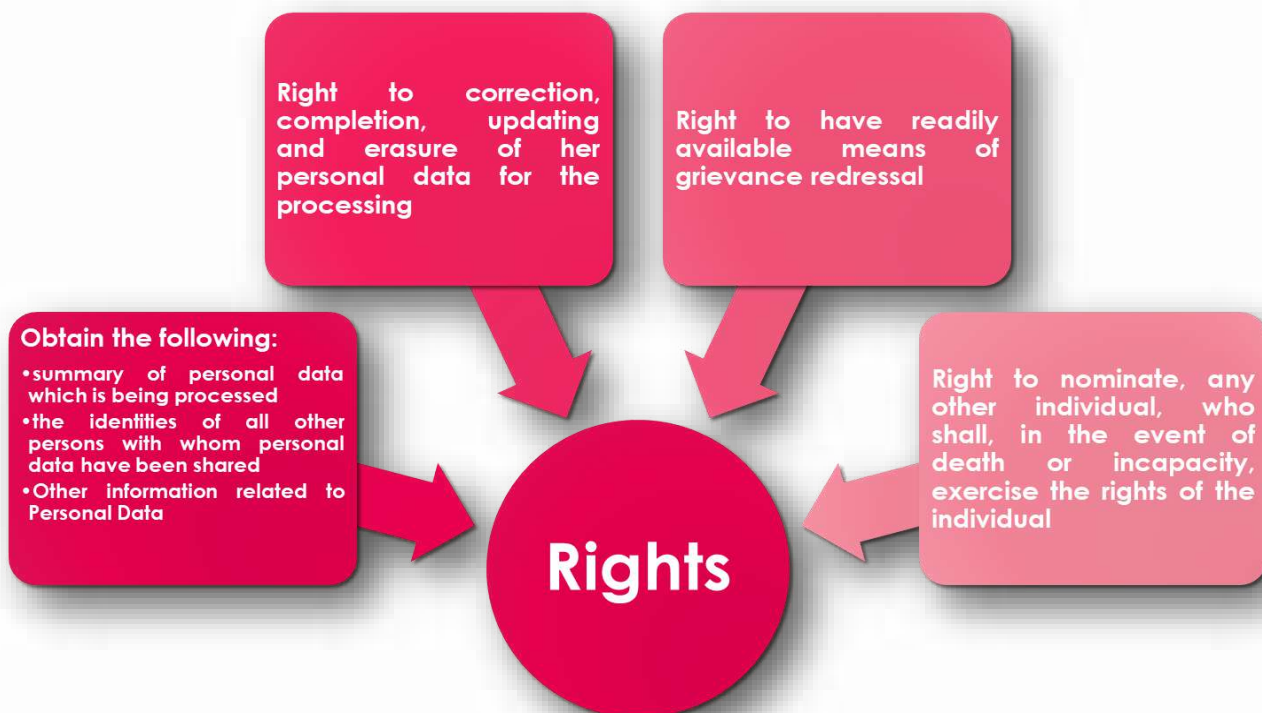
What are my duties under the Act?

Your duties are:

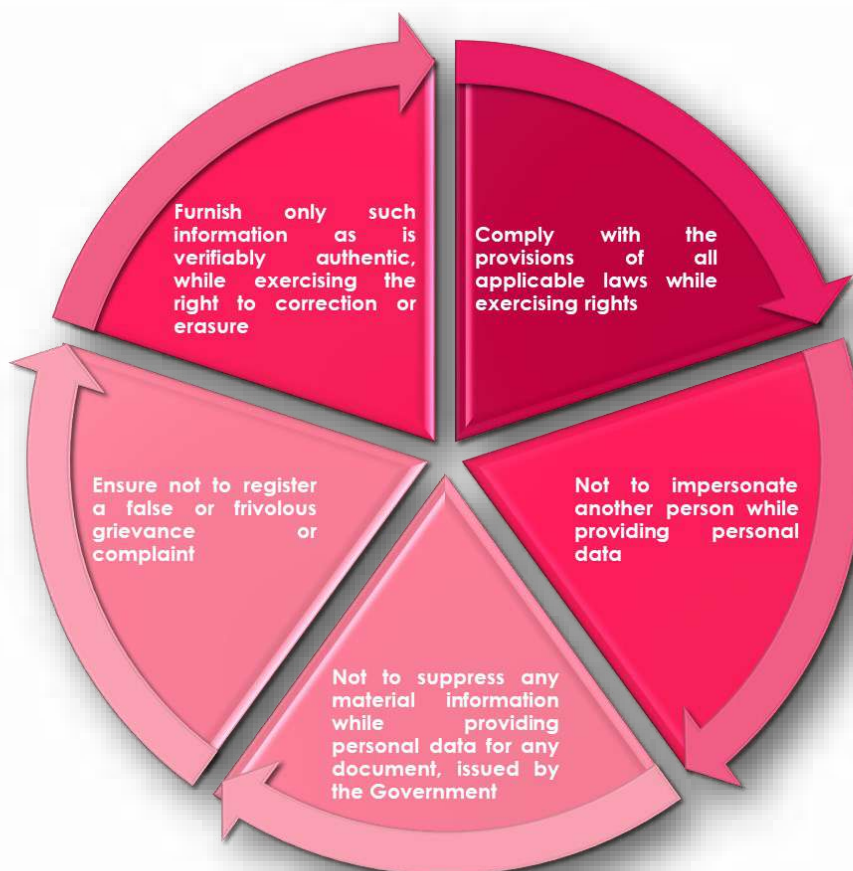
1. Comply with the provisions of all applicable laws while exercising rights.
2. Not to act as another person while providing personal data
3. Not to suppress any material information while providing personal data for any document, issued by Government.
4. Ensure not to register a false or frivolous grievance or complaint.
5. Furnish only such information as is verifiably authentic, while exercising the right to correction or erasure.



Rights



Duties





About the Chapter

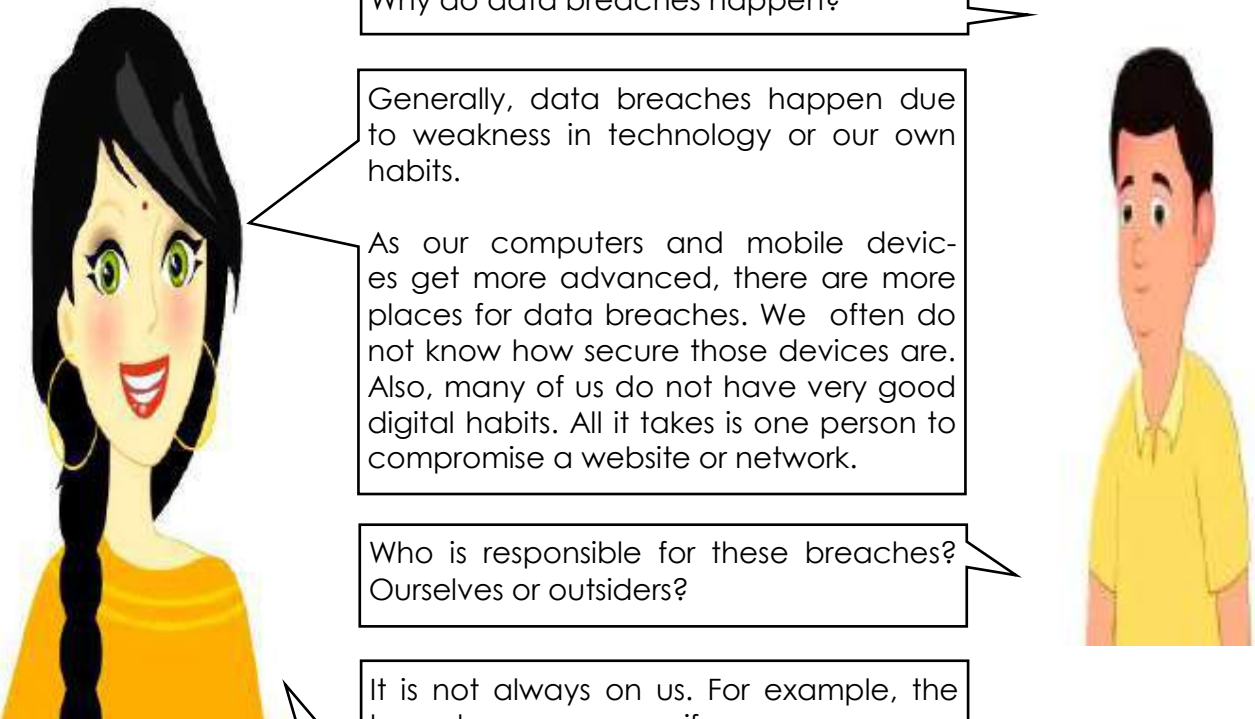
Data privacy generally means the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. This personal information can be one's name, location, contact information, or online or real-world behaviour.

Personal data can be misused in a number of ways if it is not kept private or if people don't have the ability to control how their information is used:

- ⇒ Criminals can use personal data to defraud or harass users.*
- ⇒ Entities may sell personal data to advertisers or other outside parties without user consent, which can result in users receiving unwanted marketing or advertising.*
- ⇒ When a person's activities are tracked and monitored, this may restrict their ability to express themselves freely*

In this Chapter, let's learn about how we can take care of our data privacy.

Chapter 42: Data Privacy Breach



Hey Sayani! Nowadays, I have heard so many instances of data privacy breach. I don't know how to ensure that my online data privacy is being maintained?

Pappu, anything which is online is always at the risk of being breached. However, if you take care of it, you can avoid it to some extent.

Why do data breaches happen?

Generally, data breaches happen due to weakness in technology or our own habits.

As our computers and mobile devices get more advanced, there are more places for data breaches. We often do not know how secure those devices are. Also, many of us do not have very good digital habits. All it takes is one person to compromise a website or network.

Who is responsible for these breaches? Ourselves or outsiders?

It is not always on us. For example, the breaches can occur if a person uses a co-worker's computer and reads files without having the proper authorization permissions. The access is unintentional, and no information is shared. However, because it was viewed by an unauthorized person, the data is considered breached.

Another example would be, that somebody purposely accesses and/or shares data with the intent of causing harm to an individual or company. He may have access, but his intention was to cause harm.

Other things can be losing your device or hacking by any outsider.

How to prevent being a Data Breach victim?

You can protect yourself from Data Privacy Breach by:

- ⇒ Patching and updating software as soon as options are available.
- ⇒ High-grade encryption for sensitive data.
- ⇒ Upgrading devices when the software is no longer supported by the manufacturer.
- ⇒ Checking Privacy & Security Policies of the website or App while uploading your data.
- ⇒ Using strong credentials, passwords and multi-factor authentication to encourage better user cybersecurity practices.
- ⇒ Avoid sharing your sensitive data online unless you are sure about it.
- ⇒ Grant only that access to apps and websites which you feel is necessary for them. Do not grant them full access.
- ⇒ Please keep your anti-virus software and firewalls updated.
- ⇒ Do not make your private information public. Be careful while posting on social media.
- ⇒ Make sure to safely store any paper documents that contains personally identifiable information (PII) and shred these documents before discarding them.
- ⇒ Frequently clearing your cookie cache or browser histories can also limit the amount of data collected about you online.
- ⇒ Some smartphones and services have an option that will erase your data after 3 or 10 failed attempts. Turn this on to protect yourself from thieves or if you lose your phone.

Thank You Sayani for sharing this information.





About the Chapter

A web server is a computer system capable of delivering web content to end users over the internet via a web browser.

The end user processes a request via a web browser installed on a web server. The communication between a web server or browser and the end user takes place using Hypertext Transfer Protocol (HTTP). The primary role of a web server is to store, process, and deliver requested information or webpages to end users.


It uses:

Physical Storage: All website data is stored on a physical web server to ensure its safety.

Web browser: The role of web browsers such as Firefox, Chrome, or Internet Explorer is to find the web server on which your website data is located.

In this Chapter, we will learn about web server.

Chapter 43: Web Server



Hey Sayani! Can you tell me about the web server ? I heard about it many times but don't know how it works.

Pappu,
A web server is computer software and underlying hardware that accepts requests via HTTP (the network protocol created to distribute web content) or its secure variant HTTPS.

How do web servers work?

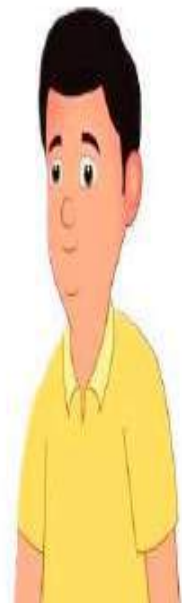
Web server software is accessed through the domain names of websites and ensures the delivery of the site's content to the requesting user. The software side is also comprised of several components, with at least an HTTP server. The HTTP server is able to understand HTTP and URLs. As hardware, a web server is a computer that stores web server software and other files related to a website, such as HTML documents, images and JavaScript files.

Multiple domains also can be hosted on one web server.



There are different types of web server-

- ⇒ **Apache HTTP Server.** Developed by Apache Software Foundation, it is a free and open source web server for Windows, Mac OS X, Unix, Linux, Solaris and other operating systems; it needs the Apache license.
- ⇒ **Microsoft Internet Information Services (IIS).** Developed by Microsoft for Microsoft platforms; it is not open sourced, but widely used.
- ⇒ **Nginx.** A popular open source web server for administrators because of its light resource utilization and scalability. It can handle many concurrent sessions due to its event-driven architecture. Nginx also can be used as a proxy server and load balancer.
- ⇒ **Lighttpd.** A free web server that comes with the FreeBSD operating system. It is seen as fast and secure, while consuming less CPU power.
- ⇒ **Sun Java System Web Server.** A free web server from Sun Microsystems that can run on Windows, Linux and Unix. It is well-equipped to handle medium to large websites.
- ⇒ **Node.js Web Server.** Node.js is known for executing the JavaScript code outside of a browser. It is an open-source, cross-platform, JavaScript runtime environment and enables developers to use JavaScript for writing commands.
- ⇒ **Jigsaw Web Server.** Jigsaw is an object-oriented, full-functioning Web Server that offers an array of distinguishing features along with an advanced architecture that is written in Java.



Why is Web Server Security Essential?

- ⇒ Data Protection: Your web server often contains sensitive user data, financial information, and intellectual property. Without robust security, this valuable data is at risk of theft or compromise.
- ⇒ Business Continuity: A breach or downtime due to an attack can translate into significant financial losses and damage to your reputation. A secure web server ensures uninterrupted business operations.
- ⇒ User Trust: Users expect their data to be handled with care and protected from cyber threats. A secure web server fosters trust among your audience.
- ⇒ Legal and Regulatory Compliance: Many industries have strict regulations regarding data protection. Failure to meet these requirements can lead to legal

How can we secure the web server?

- ⇒ Keeping your server software and applications up-to-date is a fundamental security measure.
- ⇒ Implement strong authentication mechanisms to thwart unauthorized access attempts.
- ⇒ Firewalls act as a barrier between your web server and the internet, filtering incoming and outgoing traffic.
- ⇒ Enable HTTPS and use SSL/TLS protocols to encrypt data in transit.
- ⇒ Continuous monitoring of server activity and maintaining comprehensive logs is crucial for early threat detection and incident response.
- ⇒ Create regular backups of your server data and configurations.

Thank You Sayani for sharing this information.





About the Chapter


Cloud computing has revolutionised businesses, the way data is stored and accessed. These digital applications are transforming businesses, however, with large amounts of private data being stored remotely comes the risk of large-scale hacks. By choosing the right cloud service provider, cloud storage can be a much safer and cost-effective way of storing your data.

Cloud Storage Security includes keeping data private and safe across online-based infrastructure, applications, and platforms. Securing these systems involves the efforts of cloud providers and the persons that use them.

Cloud security is the whole bundle of technology, protocols, and best practices that protect cloud storage environments, applications running in the cloud, and data held in the cloud.

In this Chapter, we will learn about Cloud Storage Security.

Chapter 44: Cloud Storage Security




Hey Sayani! I want to store my digital data in such a manner that I can access it anytime and anywhere I want and it does not impact the storage capacity of my device. Do you know any option?

Pappu, you can always use Cloud Storage for that. Cloud storage is a cloud computing model that enables storing data and files on the internet through a cloud computing provider that you can access using internet.

Tell me something more about it.

Okay. Let me tell you the benefits of Cloud Storage Systems.

1. You can always see what data you have and who else has access to your data.
 2. Data Backups and data retrieval/recovery is easy and you have the option to choose Automatic Back-ups.
 3. Your data is encrypted. Cloud service providers help you tackle secure cloud data transfer, storage, and sharing by implementing several layers of advanced encryption for securing cloud data, both in transit and at rest.
 4. Also, maintaining the data on cloud is cheaper and safer than maintaining it in physical form.
 5. Cloud service providers provide you the tools that help you automatically scan for suspicious activity to identify and respond to security incidents quickly.
- 

How can I ensure that my data on cloud storage is secure on my part?

The data which you put online is at risk partially because of your own practices. If you adopt healthy practices for cloud storage, you can minimize the risk for data breach on your part.

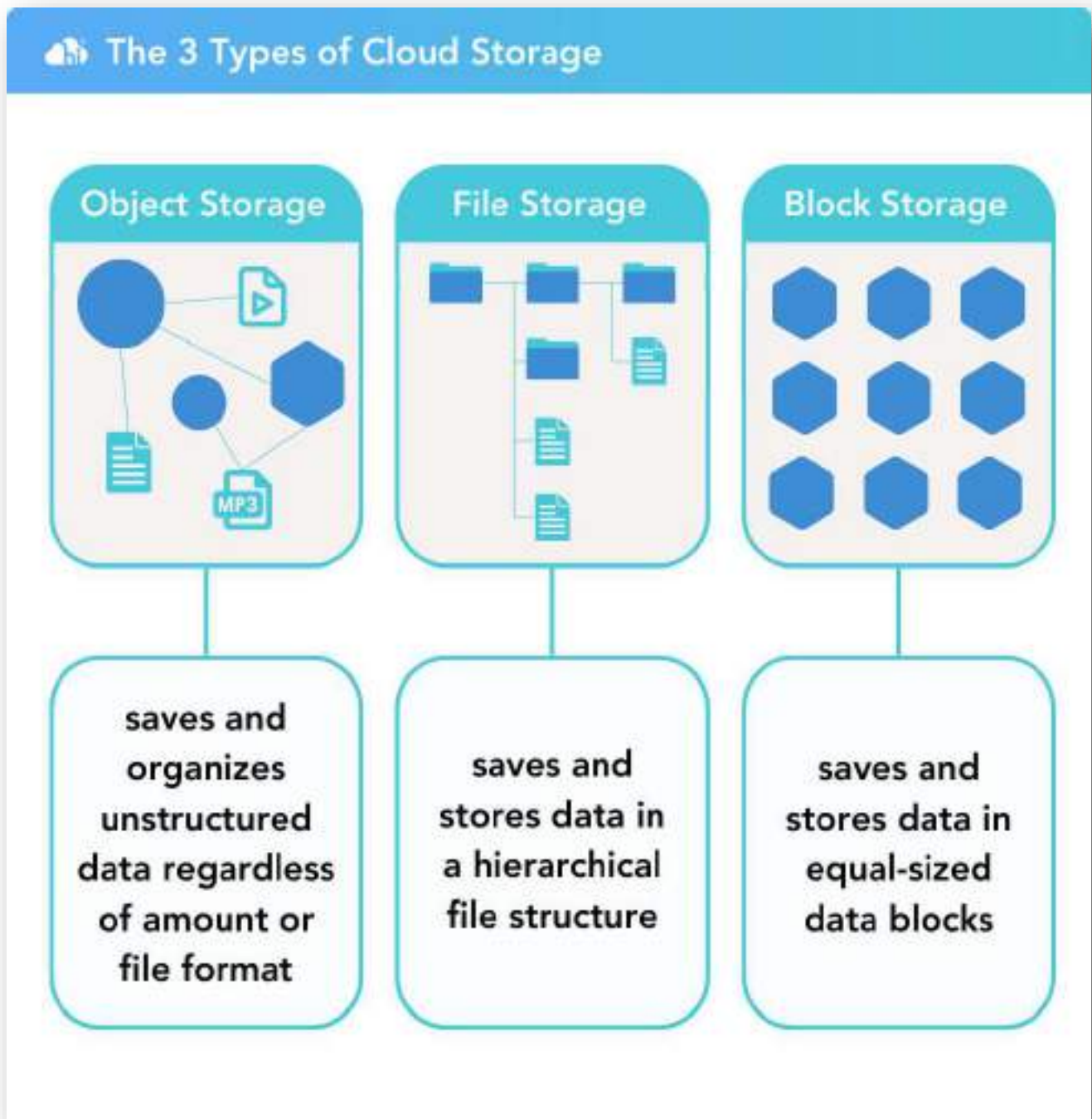
You should keep the following in mind:

- ⇒ Data can only be accessed or modified by authorized people or processes. In other words, you need to ensure that your data is kept private.
- ⇒ Be vigilant what you share online and where you link your cloud storage. We often use cloud storage for uploading a file on some websites. We should link our cloud storage only on secured and trustworthy websites.
- ⇒ You should not ignore cyber security warnings received from your security provider.
- ⇒ Maintain secrecy of your passwords and data by not sharing it with people, unless absolutely necessary.
- ⇒ Maintain backups for easy recovery of data in case of emergencies.



Thank You Sayani for sharing this information.

Types of Cloud Storage



<https://www.hicloud.sg/news/blog/cloud-storage>



About the Chapter

Scammers have also turned heavily to videos as lures. Whether from stock footage or an elaborate deepfake, scammers are using all video varieties in their threats. One of the most widespread techniques involves exploiting famous individuals and significant media events to attract large audiences.

Nowadays, the scammers are using reviews of the products as a tool for scamming people. They make people believe that they will get rewards if they submit the product reviews. Once the user submits the review, they receive links for submitting their financial information which is then used for cyber crimes.

In this Chapter, we will learn about these Review Links Scams.

Chapter 45: Review Links Scam

One day Pappu and Sayani were watching videos on TubeU videos regarding product reviews. Pappu saw a link on the description of a video which promised to give rewards on submitting the reviews.

Hey Sayani! Look there is a link in the video for submitting review of the product. Let's click on the link and submit the review and earn some rewards.

Pappu. Wait!!

This link might be malicious.

This is not malicious. I have seen people doing this and earning rewards.

Infact, one of my friend has earned reward of Rs. 500 by reviewing the products.

He might have come across an authentic link. Because in many cases, these links are found to be fraudulent and are not cyber-safe.



Despite warnings of Sayani, Pappu clicked on the link and submitted the review. On submitting the review, he received a SMS.

Thank you for submitting your review. To collect your reward, click on link mentioned below and provide your details: <http://www.xyz.reeview.rewards.hvhdfrefrefnfnrnmfmrjdjvdfndfeojdhsfrddgerf012462552262.com>



Look Sayani, I have received a SMS for my reward. You just watch me collecting it.

First show me the link.

See Sayani.

Pappu, this is not a valid link. Look at the link closely. It is a malicious link as it does not have https.

Also, do you think that a valid link is this much long?

You are right Sayani. I should be more careful and vigilant. I got greedy.



GYAAN KA SAAR



Precautions

1. Never share your UPI ID or bank account details with people who you do not know or the sites you do not know.
2. NEVER SHARE OTP with anyone. OTPs are confidential numbers and you should treat them like that.
3. Always verify the identity of the person on an online website if you are selling or buying anything.
4. Try not to share your mobile number too if not needed.
5. Check the URL to make sure it is the intended site and looks authentic. A fraudulent domain name may be similar to a URL with typos and misplaced letters.
6. Ensure trusted Anti-Virus software are installed in your phones or computer systems.
7. Report any suspicious links to relevant authorities or organizations to help others.
8. Before clicking on any link, preview it to make sure that it's redirecting you where you expect it to. To preview a link on mobile, tap and hold the link. Check for typos or for very long and complicated strings of letters and numbers.
9. Avoid risky websites. It makes sense that risky websites are home to risky links. Practice safe downloading practices and be extra vigilant about the websites you visit.
10. Avoid pirated content hubs as they're often a haven of dangerous links.
11. Never click shortened URLs in email or messages – clicking links using Bit.ly and other shortening services are risky since you cannot hover over shortened URLs to see where they go. They can easily be hiding a malicious website.
12. Be wary of social media stores that are new and selling products at very low prices.
13. Check that a website you want to buy from has information about privacy, terms and conditions of use, dispute resolution and contact details, plus a secure payment service like PayPal or credit card.



About the Chapter

Android Package Kit (APK) files form the backbone of Android apps. While users are seldom exposed to these .apk extensions during installations, tech-savvy individuals can manually manage them.

This accessibility allows hackers to tamper with APKs for nefarious purposes, usually by tweaking the code to provide additional features without any charges.

For gaming apps, this could mean extra lives, whereas for streaming apps, it could translate to unrestricted content access.

By tampering with the APKs of the Apps, hackers can easily execute a Malware Attack on any User.

In this Chapter, we will learn about how Malware Attacks happen through App Piracy.

Chapter 46: Malware Attacks Through App Piracy

Pappu was fond of watching latest movies and series. Considering the current concept of OTT Platform for video content, he was looking for purchasing the subscription of Apps that provides him with best and latest content.

I want to watch this movie which has just released on OTT. Let me check the subscription for this App.

It is too costly. Rs. 500 per month is too high for me to pay for watching a Single Movie.

(After Searching) Yes!! I found one option. Through this App, I can view the content of the Original OTT App for free. I just need to install this App through my Web Browser on my phone. This is nice. I should tell about this App to Sayani too.

Hey Sayani! Look I found an App which lets me watch the content available on other Apps for free. I just need to download this App from my Browser and install it on my Phone. That's good, Right? I won't have to pay Rs. 500. Let us both install it.

Please stop Pappu! Do not install that App. That App is a pirated App.



So what? It is cheaper and it works. I'll just watch the movie and uninstall the App.

These Pirated Apps contain Malwares which can infect your device.

What are Malwares?

Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.

Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware. These malicious programs steal, encrypt and delete sensitive data; alter or hijack core device functions and monitor end users' device activity.

The Hackers are using these Pirated Apps for inserting Malwares in the devices of Users.

As soon as you run that application file and install it, the Malware files hidden in the installation files are activated and start attacking your device's security. So, please don't do it.

Thank You Sayani. You stopped me at the right time.



GYAAN KA SAAR



Precautions

1. Check the URL to make sure it is the intended site and looks authentic. A fraudulent domain name may be similar to a URL with typos and misplaced letters.
2. Ensure trusted Anti-Virus or anti-spyware software are installed in your phones or computer systems.
3. Report any suspicious links to relevant authorities or organizations to help others.
4. Avoid risky websites. It makes sense that risky websites are home to risky links. Practice safe downloading practices and be extra vigilant about the websites you visit.
5. Avoid pirated content hubs as they're often a haven of dangerous links.
6. Never click shortened URLs in email or messages – clicking links using Bit.ly and other shortening services are risky since you cannot hover over shortened URLs to see where they go. They can easily be hiding a malicious website.
7. Keep your computer or device and its software up-to-date.
8. Use a non-administrator account whenever possible.
9. Be careful about opening email attachments or images
10. Don't trust pop-up windows that ask you to download software
11. Limit your file-sharing and monitor for suspicious activities.
12. Implement email security and spam protection.
13. Implement robust security policies such as whitelists or allow lists
14. Use your firewall and keep it updated.
15. Implement strong access controls and user privileges.
16. Regularly conduct vulnerability assessments and penetration testing
17. Use Strong Passwords and Two-Factor Authentication.



About the Chapter

The unprecedented ways in which individuals are engaging themselves with the digital devices has made it a cause of concern for them from various perspectives. These concerns mainly relate to the users health & wellbeing and includes security issues related to user data, finance, network, system etc.

Digital detox is a primary step in this direction which encourages digital users to make responsible and hygienic choices in proper usage of digital devices and data consumption, and inculcate healthy digital device practices the encourages the 'me time' and make time for connecting in real world rather than be hooked to virtual world.

In this Chapter, we will learn about how Digital detox .

Chapter 47: Digital Detox

Pappu was scrolling on internet and he read about the Digital detox. He decided to ask Sayani about the Digital detox.

Hi Sayani,
Do you have any idea about Digital Detox?



Hello Pappu.

Digital Detox is a trend these days.

It is a process that refers to a time period of conscious restrain in using digital devices like smartphones, televisions, computers, tablets and social media sites. It may include activities like avoiding scrolling social media and constant checking of mails, avoiding texting etc., The purpose of the effort is to avoid digital distractions to reconnect with the real world around you and relax yourself to enjoy the moment.

Sayani....Is it necessary to go for the Digital Detox?



These days we all are lost in the digital world. We constantly use internet and other Digital devices. Digital Platforms keep us connected to friends and family, while also serving as an outlet to find inspiring people. However, the constant comparison, fear of missing out and highly curated content we're exposed to on social media can come with some drawbacks.



Signs You Might Need a Digital Detox-

- You feel anxious or stressed out if you can't find your phone
- You feel compelled to check your phone every few minutes
- You feel depressed, anxious, or angry after spending time on social media
- You are preoccupied with the like, comment, or re-share counts on your social posts
- You're afraid that you'll miss something if you don't keep checking your device
- You often find yourself staying up late or getting up early to play on your phone
- You have trouble concentrating on one thing without having to check your phone

The Benefits of Digital detox are as follows:-

- Reduces stress and anxiety
- Better sleep
- Better work-life balance
- Promotes physical and mental health
- Helps unwind n relax
- Helps build healthy hobbies
- Productive and efficient usage of time
- Promotes healthy social life and better interpersonal relations
- Increased Self-Awareness and Mindfulness
- Increased Productivity and Creativity



Few ways and means of Digital Detox

1. Know where you stand in your digital device usage habits and accordingly set your goals for necessary corrective action in that direction setting timely goals with required commitment.
2. Set limits and make it work for you.
3. Focus on achieving long term benefits of developing an healthy body and mind, better interpersonal relations, efficient time management etc., as a goal and keep working on accordingly managing your digital device usage habits .
4. Gather required support from family members, close friends to encourage you and provide accountability. Share your goals with like-minded and supportive people. You can share ideas on how to stop your targeted behavior.
5. Evaluate your progress toward achieving hygienic digital usage practices regularly, asses the benefits and barriers you experienced during the digital detox, and appropriately regulate your actions on any aspect of the change moving forward.
6. Look into putting in practice some tips for effective time management like – deleting time-consuming apps and disabling distracting features like notification alerts, auto-push notifications, setting screen to gray scale to keep you from waking at night, creating a screen lock with questions like 'what is the need?' ; Why now? Etc.,
7. Have digital device/ mobile free zones and make it a practice to keep it out of sight during bed time, food time and family time. For example You may plan to have a charge your phone outside your bedroom. Use a non-administrator account whenever possible.
8. Develop healthy hobbies that you really like and feed your soul giving yourself the 'me time', it may include things like making time for quite walks, playing board games with family, outing with family, cooking, gardening, painting , meeting up with friends, reading good books, volunteering etc.,



About the Chapter

Parcel scams are a type of fraud that typically involves unsolicited contact about a supposed parcel delivery. Typically, scammers pose as a legitimate courier company, customs official, or even a law enforcement agency to trick people into believing they are receiving a parcel.

The scam begins with convincing communication from the fraudster, such as an email or text message that claims to be from a reputable delivery service. The message may state that the recipient is expecting a parcel or that there are problems with the parcel during transit. The victim is then asked to provide sensitive personal information or financial information, or to pay for alleged customs fees or parcel charges. The scammer may also direct victims to a fake website that masquerades as a legitimate courier service.

In this Chapter, we will learn about how these scams take place.

Chapter 48: Parcel Scam

Pappu was fond of Online Shopping. He often used to buy products from different online sellers. This time his online shopping gave him a lesson for a lifetime. It all began with a Phone Call.

Hello Mr. Pappu. I am calling from X-Delivery Service regarding your parcel from abc.com.

Yes Sir. I placed an order from abc.com. Is it out for delivery?

Your parcel has reached the nearest courier partner location and was out of delivery but, before we could reach your location, the delivery person was intercepted by the Police. The Police inspected and found out that your package contain some goods on which Custom Duty of Rs. 500 was required to be paid and has not been paid. You are requested to make payment of the Custom Duty.

Ohh! I had no idea that the product I ordered attracted Custom Duty. Anyways, please let me know the way to pay the custom duty.

Sir, I have just sent you an SMS with a link for making the payment of Custom Duty. You just need to click on your link and then make payment through your Net Banking.



Without even checking the validity of the call and SMS, he decided to click on the link received in SMS. On clicking the link, he was re-directed to a website where he entered his Banking credentials and made payment. Rs. 500 was deducted from his account. After few minutes, he received another notification for deduction of Rs. 5000 from his Account. He understood that he has been scammed.

Pappu rushes to Sayani and explains her the entire incident.

Pappu I am so disappointed with you. I thought you were aware of these scams.

I am sorry Sayani! I got excited for my parcel and ignored all the warning signals.

You must have searched the status of your parcel on some fake website from where they got the details of your parcel.

In these cases, the scammers often call the victims by pretending to be someone from the courier company. Then they make some excuses which seem genuine to the victims. They then trick victims for making payments through a link and ask the victim to make a small payment to release the parcel. When the victim clicks on the link, a screen mirroring app gets downloaded in the background. As the victim makes the payment, the criminals steal the details of his bank account or wallet and subsequently steal a larger amount.

The same thing happened with you too.

What should I do now to get my hard-earned money back?

Let's first register our Complaint at <https://cybercrime.gov.in/> now without any delay.

Pappu and Sayani registered the complaint within 24 hours of occurrence of fraud. Within 2-3 months, the authorities were able to find the scammers and recovered Rs. 5000 from them.

GYAAN KA SAAR



Precautions

1. If you suspect fraud, disconnect from the callers, take a moment to reflect on whether their requests are normal, and consult with experts and law enforcement to determine if you are being scammed.
2. Avoid rushing into any financial transactions or disclosing personal information.
3. When searching via Google, verify the authenticity of the website you are led to by closely examining the URL. Avoid ordering from lesser-known websites, especially those discovered through a search engine or a social media platform.
4. If you are informed that a cross-border shipment has been detained by Customs, request an official summons and avoid paying up.
5. Verify the source of the call independently. Contact the supposed delivery company directly using contact information obtained from their official website or previous correspondence.
6. Do not click on links in SMS carrying failed delivery notification without verifying the authenticity of the source. Use any tracking ID provided to check on delivery status at the courier service's official website only.
7. Avoid sharing sensitive personal or financial information or giving OTP (one-time password) unless you are certain of the recipient's legitimacy.
8. Check who is calling from an independent source: Customs or police officers do not typically call in this manner.
9. Become especially wary if someone calls instructing you to make a payment or click on a link.
10. If unsure, contact your bank immediately. Report any suspicious activity related to your accounts, including unauthorized transactions.
11. Set up two-step verification (2SV) wherever possible, particularly on your most important accounts.
12. Delivery scams are often vague and won't be specific about where the parcel is coming from – or what's inside.



About the Chapter

Until a few years ago, it was the good old family connections that played a crucial role in arranging marriages, introducing the bride's family to the groom's, even if not the bride to the groom. Though proposals came through familiar members of the family, parents went the extra mile, even employing private eyes to do a background check. However, increasingly over the last decade or so, the matrimonial process has undergone a big change, and has almost migrated online. Various kinds of matrimonial sites, offering to find life partners for various communities and groups, have since begun to take precedence in the big hunt. But as things went digital, a number of issues popped up, the important ones being the anonymity for users, the inability to gauge the true nature of people hiding behind aliases, and doctored photos.

In this Chapter, we will learn about Matrimonial Frauds.

Chapter 49: Online Matrimonial Frauds

Pappu was talking to a girl found on a matrimonial site since 15 days. One day this girl requested for transfer of money. Pappu found this suspicious and he decided to speak to Sayani about the matter.

Hey Sayani! I was talking to a girl through matrimonial site. She has requested me for financial help.

Hi Pappu.
What happened?
Tell me the whole story first.

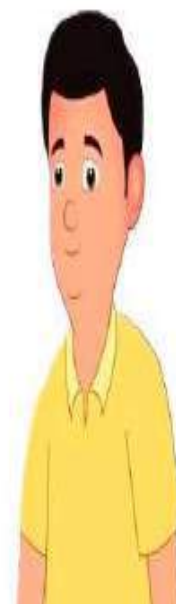


I had created my profile on a matrimonial site wherein I was talking to a girl. When I sought her details, she messaged me. Two days later, she called me up. Though I sent my details and photos, she did not share anything in return, nor did she show any interest when I proposed letting their parents discuss the alliance.

5 days later She requested me to help her with ₹10,000 and promised to return the money once she received her salary. Thinking that everything was going good and she was going to be my wife and the amount she sought was meagre, I transferred the amount to her bank account.

Today also she has messaged me that her mother required a surgery and she would needs ₹1 lakh urgently.

I think she is trying to dupe me. Should I transfer the amount.??





Pappu this is not expected from you.

I always tell you not to do any work related to cyber without checking the integrity of someone. You just don't understand.

Fraudsters often create fake profiles impersonating someone else. They use attractive photos and fabricated personal details to attract more people to choose their profiles.

And you also duped by that girl.

Sayani...What should I do know??

Pappu, You can file a complaint on cybercrime.gov.in to Seek justice and ensure that criminals do not harm you or others.

You are right Sayani. I will file a complaint.
Thank you so much for preventing me from losing my money from the fraudsters.





How to identify fake profiles on matrimonial sites

1) Unrealistic profiles

Be cautious of profiles that seem too good and everything looks perfect. Some pointers include highly attractive photos, impressive achievements, moderate needs and expectations, high salaries, etc. You should verify the information provided by cross-referencing it with other sources like social media and mutual connections.

2) Inconsistencies in information

This is a huge red flag and is often easily identifiable. Fraudsters often make mistakes or provide conflicting details in the stories they tell you as compared to the information being displayed in their profile. When you begin talking with someone online, try to know more about them. Pay attention to inconsistencies in educational backgrounds, job details or personal narratives they tell.

3) Too quick to share personal information

You should be wary of individuals who quickly share personal information or request sensitive details from you. Legitimate matches will take time to establish trust before sharing personal details and information.

4) Financial requests

This is the biggest red flag you can easily identify. You should never send money to someone you've met online. Fraudsters fabricate sad stories to take advantage of emotional connection and sympathy. What follows is a financial request with a promise to return the funds shortly. Once you transfer the money, they may disappear suddenly with no trail. Genuine individuals seeking relationships will not ask for financial assistance so early in the relationship.

5) Reluctance to meet in person

Fraudsters often avoid in-person meetings and may provide excuses for not being able to meet, especially when they are using fake profiles or photographs. This is a potential red flag. You should insist on meeting in a public place before committing to a serious relationship. If the other person consistently refuses, then you should part ways quickly.

6) Fraudsters never involve their family on matrimonial sites.

Fake profiles on the marriage bureau don't involve their guardians. When you ask them, they will probably say they deal with all the marriage talks themselves. In our culture, we love to involve our parents before making any big decisions in our life, especially when we are looking for prospects on marriage sites.

7) Fake Profiles show off more than usual

Usually, fake profiles show off that they are super-rich, mention they have 3-4 houses, share fake property details and even upload fake pictures with luxurious cars. They boast about themselves to grab the attention of all their prospective matches. If you feel that they are flashy about their bank balance, properties, or standards, stop conversing with them and bid adieu.

8. No Social Media presence

When you connect with any prospective profile, check their social media profiles to verify their identity. Today, everyone has found their prime interest on Facebook, Twitter or Instagram. A person's social media says a lot about their personality, choices, friends, and regular activities. If she/he doesn't have any social media profiles connected to an online matchmaking site, ask them directly or try searching with their full name. You can also check their posts, activities, comments and learn a bit more about how serious they are about matrimony. Beware of accounts that have no activity or has a smaller number of followers as it can be a real deal-breaker.

9. Other ways to detect fake profile on online matrimony sites

If you find other missing information that is necessary, like educational background, job position, age, then stay away from such matrimonial profiles. Similarly, if someone is bragging about her/his status to an unexpected level without any sign of verification, stop conversing with such people. A well-qualified person will never hesitate to share his original position.



About the Chapter

Almost two decades after they were developed, the pandemic saved the Quick Response (QR) code from extinction. They have consequently expanded far beyond their original scope and while many uses are legitimate, threat actors are now leveraging the technology for malicious purposes.

Invented in 1994, QR codes originally provided quick tracking information for car parts. This technology was adopted by other businesses and upgraded to facilitate access to websites and other information.

In 2022, QR codes are used for tasks such as facilitating payments, downloading applications, distributing documents, and confirming event tickets. They even support security mechanisms, including the deployment of multi-factor authentication.

This evolution has persuaded users that QR code mechanisms can be trusted. However, threat actors are exploiting this trust to collect sensitive information or to deploy malware. The QR code's associated URL may coax victims into downloading seemingly harmless files, ultimately installing malware. In sophisticated cases, victims may not initiate downloads willingly but can be forced through manipulated QR codes.

In this Chapter we will learn how we can protect ourselves from this cyber threat...

Chapter 50: Hacking Through QR Codes

Pappu was reading news paper and he read that hacking can be happen through QR Codes. He decided to learn more about this from Sayani.

Hey Sayani!
Do you know that hacking can happen through QR Codes?

Hi Pappu. Yes, nowadays the hackers also doing frauds through QR Codes.

Let me tell you about this.

As you know that a QR code, is a type of bar code that can be used to provide easy access to online information.

To use them, all you need to do is use open the camera on your smart device to scan the code, but as with most technology to-day you need to be careful. Cybercriminals are taking advantage of this technology by using QR codes to direct victims to malicious sites to steal personal information, download malware to their devices, and even redirect payments.



Like phishing attacks, cyber criminals use different lures and tactics to trick users into scanning the malicious QR code. The types of QR code attacks include:

1. Quishing

In a Quishing attack, threat actors send a phishing email containing a malicious QR code attachment. Once the user scans the QR code, it will direct the user to a phishing page that captures sensitive data like users' login credentials.

2. QRL Jacking

Most organizations use Quick Response Code Login (QRL) as an alternative to password-based authentication procedures. A QRL allows users to log in to their accounts by scanning a QR code, which is encrypted with the user's login credentials.

QRL Jacking is like a social engineering attack capable of session hijacking affecting all accounts that rely on the Log-in with the QR code feature. In a QRL jacking attack, the scammers trick unwitting users into scanning a specially crafted QRL rather than the legitimate one. Once the victim scans the malicious QRL, the device gets compromised, allowing the attacker to take over complete control over the device.

Thank you so much for telling me about the this. I will always keep in mind this while scanning any QR Code.



GYAAN KA SAAR



To help you stay safe, here are six tips to protect yourself when using QR codes:

1. **Safety First!** Step up your mobile device security. Just as you would for laptops and desktops, mobile devices should have a reputable antivirus installed as well.
2. **Slow Down.** QR codes that may seem like they have been sent by a co-worker, friend, or even family member can present risks as there is always a chance that the sender's account has been hacked. *Always ask yourself: Do I trust that it is safe?*
3. **Practice Caution.** This is especially true when entering login, personal, or financial information into a site navigated to or from a QR code. Always confirm that the URL is correct. A fraudulent domain name may be similar to the intended URL, but may include typos or a misplaced letter.
4. **Look Before You Scan.** Check for tampered codes, such as a sticker placed on top of the original code. This is a common form of QR code fraud.
5. **Say No To Apps.** Do not download a QR code scanner app. This increases your risk of downloading malware onto your device. Instead, use your device's camera. Also, always go to the official app store for your device's operating system and download your apps from there, never directly from a QR code.
6. **Don't make electronic payments via QR codes.** Always use the native app or visit the official domain and log in there.



**By:
IT Awareness Team**

Digamber Capfin Limited

**J 54-55, "Anand Moti", Himmat Nagar,
Gopalpura, Tonk Road, Jaipur-302018**