P.N. DAS COLLEGE

HIGHLIGHTS

- What Security means
- How has Security evolved
- What is Cyber Security
- Why Cyber Security
- Methods of breaching
- Do's & Don'ts
- Questions & Answers

One-Day

State Level Webinar

on

Cyber Security

13 January 2021

11.00 a.m.

Organised by

In collaboration with

IQAC P.N. DAS COLLEGE	IQAC BIJOY KRISHNA GIRLS' COLLEGE	IQAC MURALIDHAR GIRLS' COLLEGE

Resource Person

Mr. Sivamani Sangaranarayanan

Head, Network and Security Division

PC Solutions

CLICK HERE TO REGISTER

The state level webinar on Cyber Security was a collaborative activity between Muralidhar Girls’ College and PN Ds College. It was held on 13 Jan 2021 at 11 am.

16 participants from MGC attended the webinar.

Cyber Security - An Awareness Program

SIVAMANI SANGARANARAYANAN

(SIVA) Sivamani@e-pspl.com

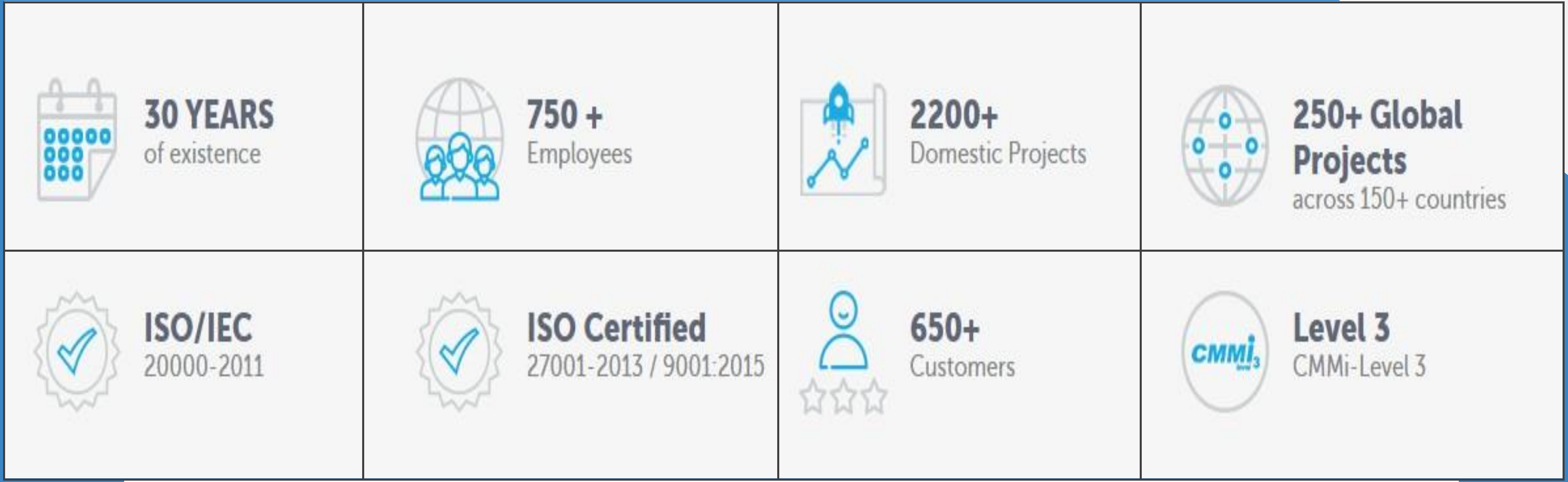
13th January 2021

Disclaimer

This Presentation contains information that are available on internet and sourced from Various sites. I am not the OWNER of this content and I have only collated all the information for creating an awareness among the participants and purely for educational purpose.

About PC Solutions

TECHNOLOGY SOLUTIONS FOR BUSINESS CHALLENGES TO A DIVERSE PORTFOLIO OF DOMESTIC AND GLOBAL CLIENTS FOR 30+ YEARS.



30 YEARS of existence	**750 +** Employees	**2200+** Domestic Projects	**250+ Global Projects** across 150+ countries
ISO/IEC 20000-2011	**ISO Certified** 27001-2013 / 9001:2015	**650+** Customers	**Level 3** CMMi-Level 3

{ One of India's premier system integrators }

What we Intent to do ?

Cyber Security – An Awareness Programme

Inquisitive

5 W’s and 1 H

- What is Security ?
- What is IT / Cyber Security
- Difference IS vs CS
- Why Cyber Security?
- Examples of Breaching Techniques
- Do’s and Don’ts
- Q & A

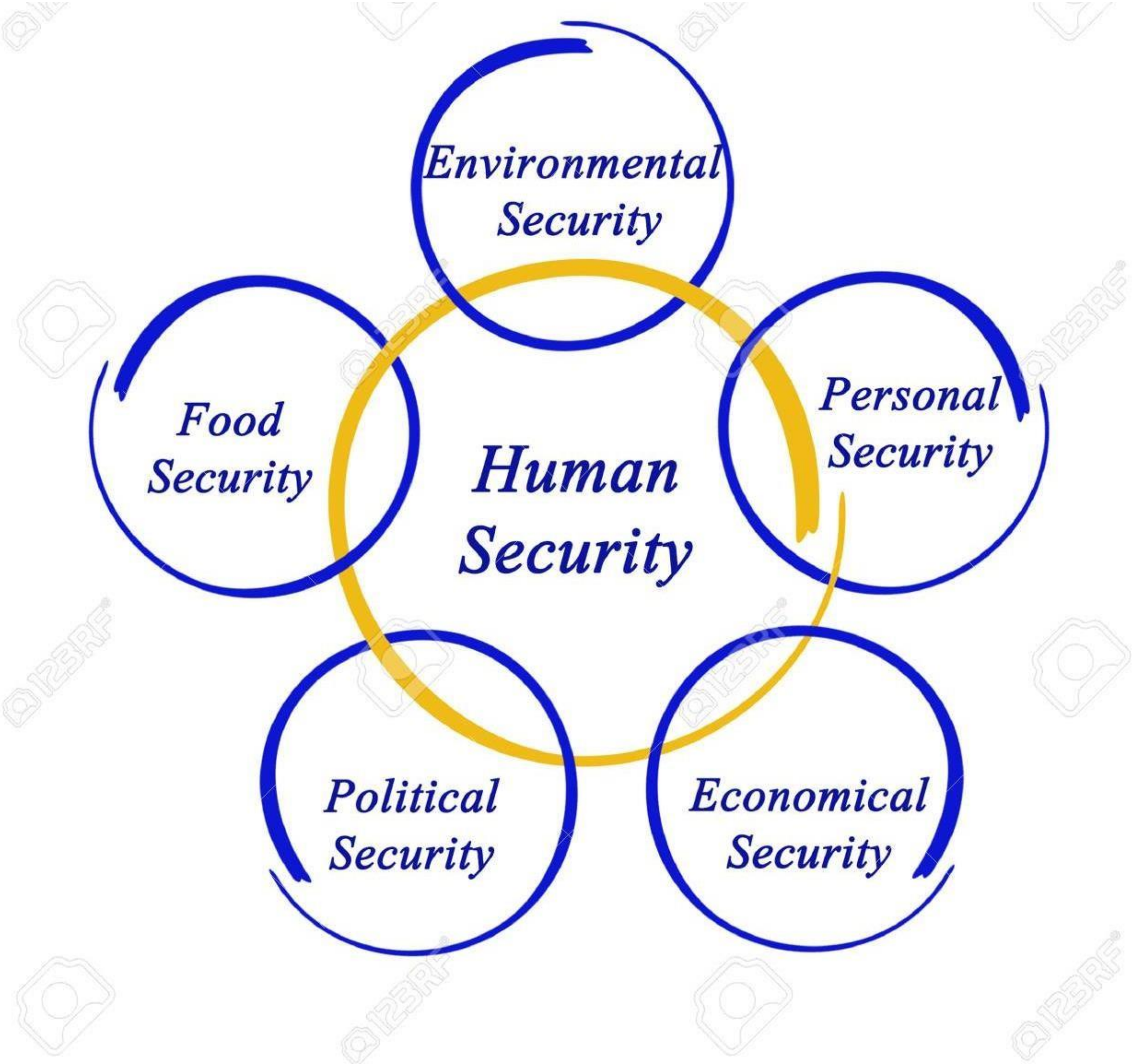
WHAT IS SECURITY

In General Terms

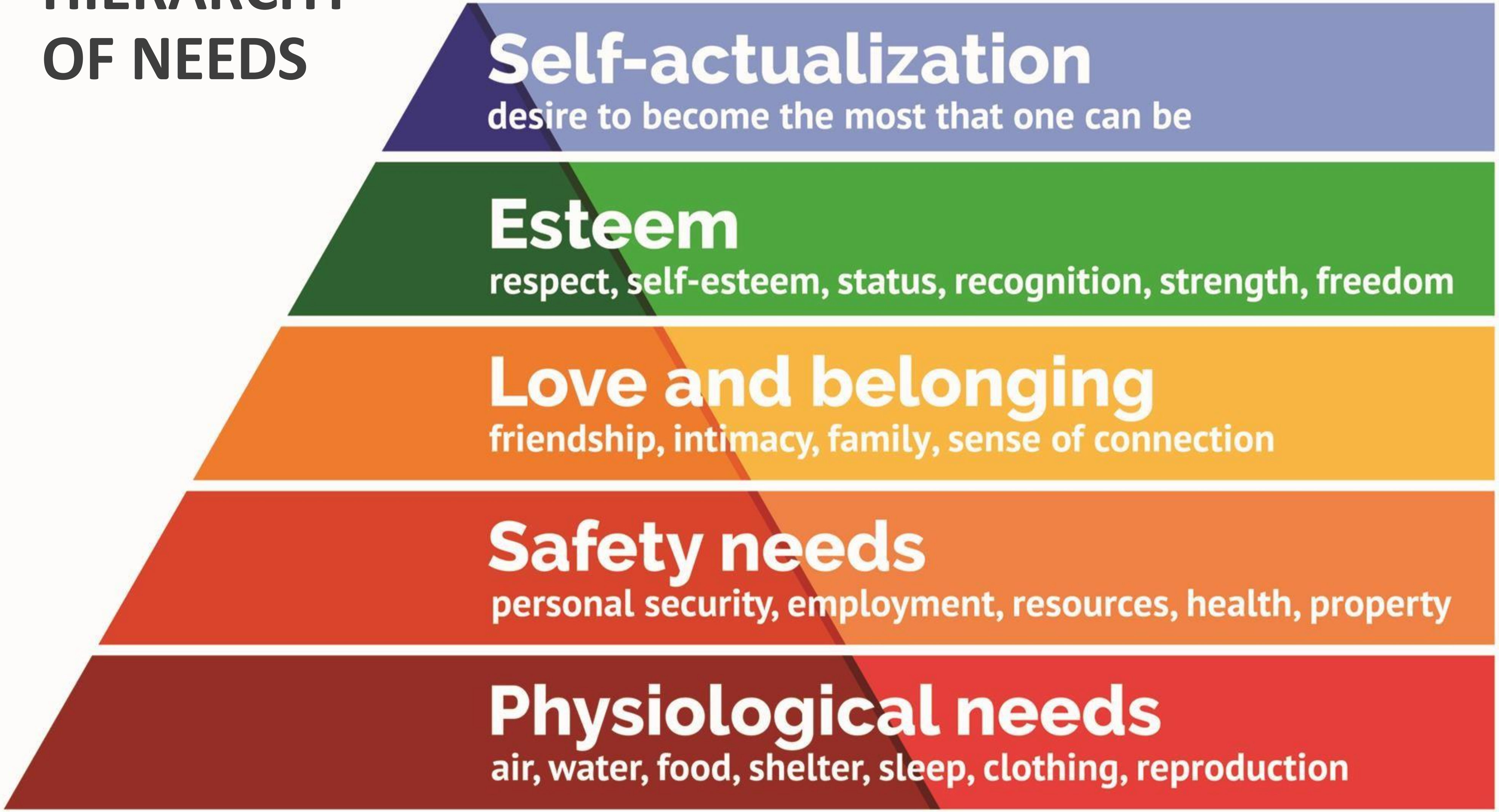
- Freedom from Fear
- Freedom from Danger
- Ability to do what we intent to do

WHERE IT ALL STARTED ?

HUMAN SECURITY



MASLOW's HIERARCHY OF NEEDS



Self-actualization
desire to become the most that one can be

Esteem
respect, self-esteem, status, recognition, strength, freedom

Love and belonging
friendship, intimacy, family, sense of connection

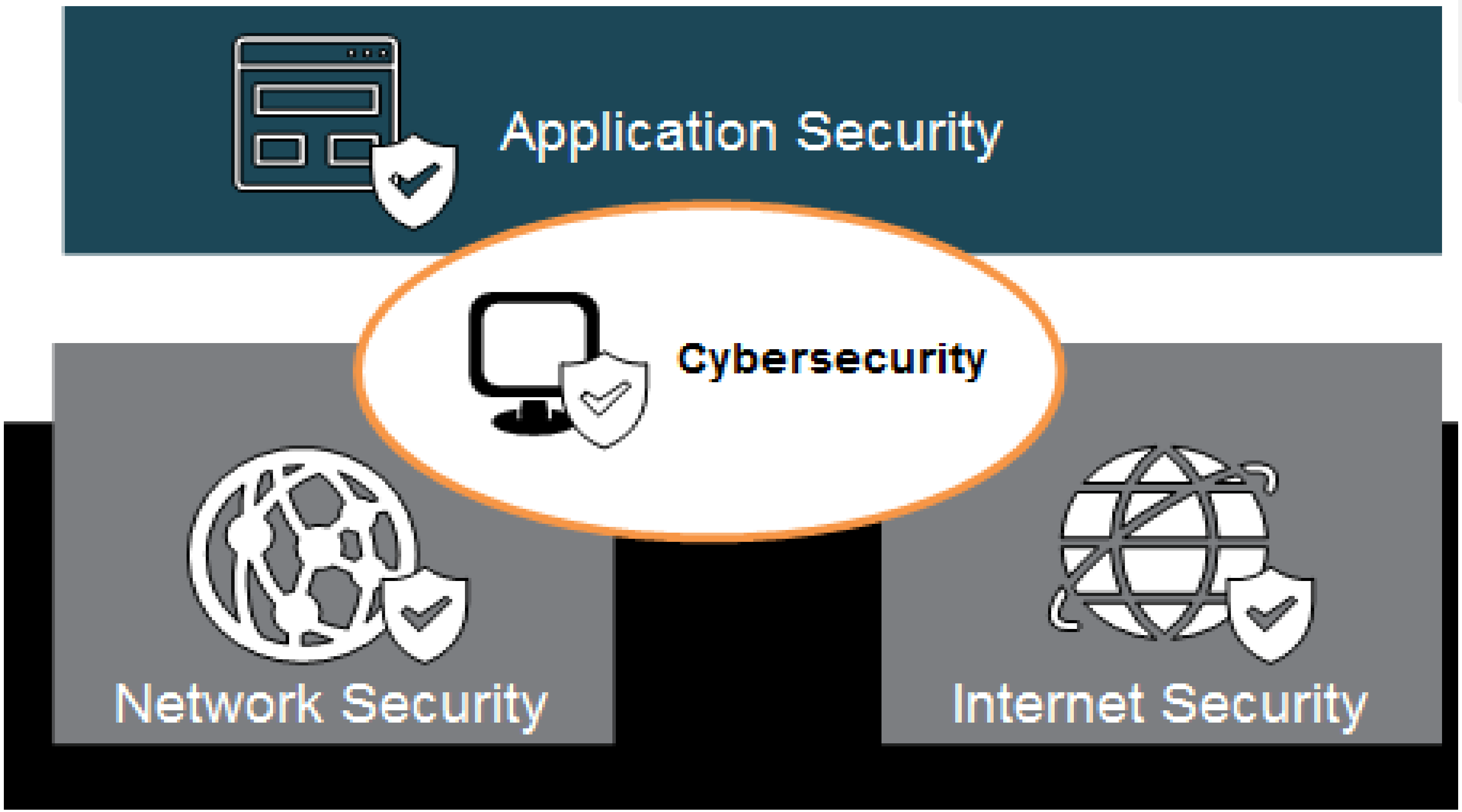
Safety needs
personal security, employment, resources, health, property

Physiological needs
air, water, food, shelter, sleep, clothing, reproduction

What Is Cyber Security ?

- Cyber Security is the process and techniques involved in protecting sensitive data, computer systems, networks and software applications from cyber attacks. The cyber attacks are general terminology which covers a large number of topics, but some of the popular are:
- Tampering systems and data stored within
- Exploitation of resources
- Unauthorized access to the targeted system and accessing sensitive information
- Disrupting normal functioning of the business and its processes
- Using ransomware attacks to encrypt data and extort money from victims
- The attacks are now becoming more innovative and sophisticated that is capable of disrupting the security and hacking the systems. So it's very challenging for every business and security analyst to overcome this challenge and fight back with these attacks.
- To understand the need for Cyber Security measures and its practices, let's have a quick look at the types of threats and attacks.

Information Security



Application Security

Cybersecurity

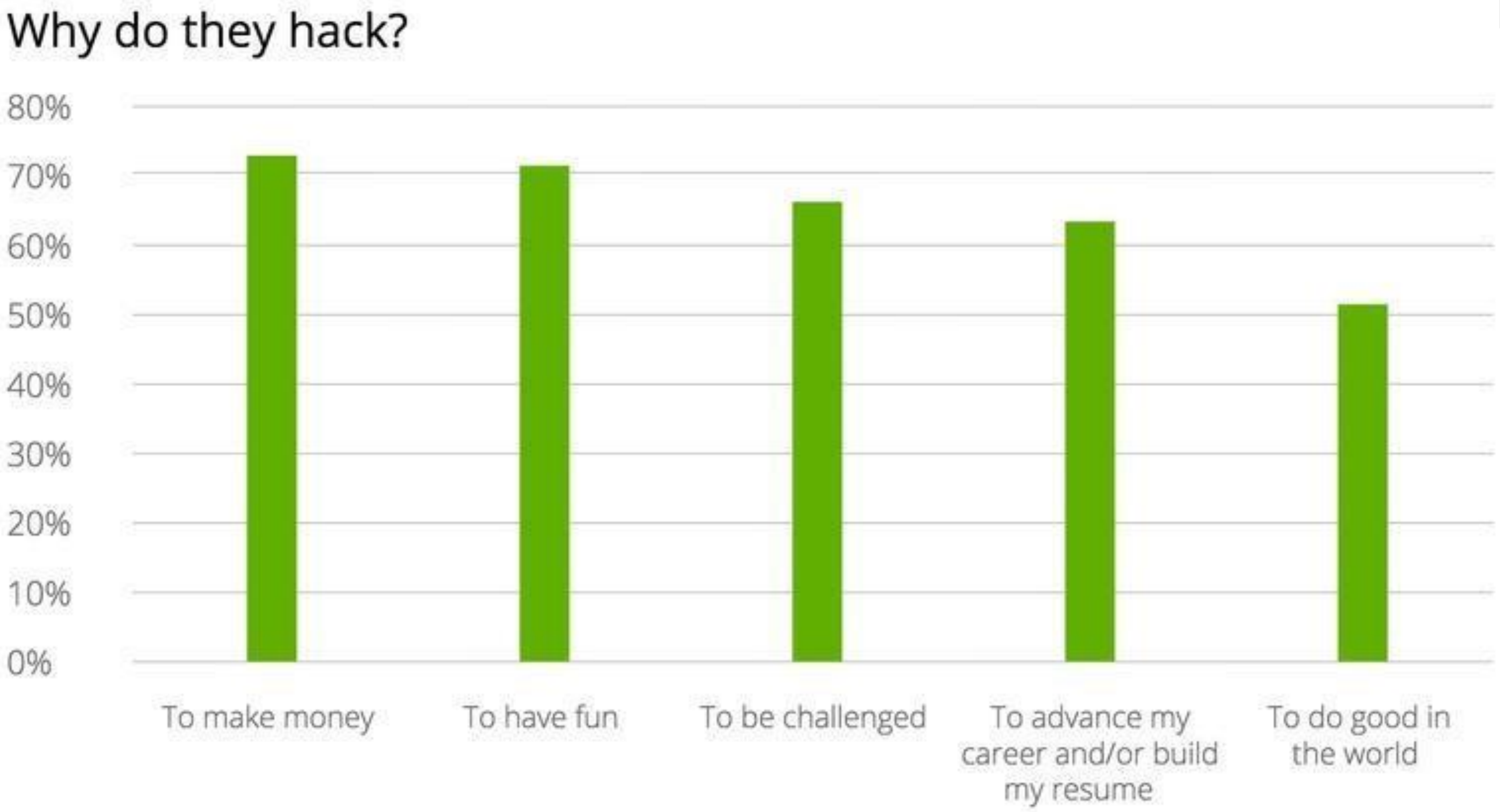
Network Security

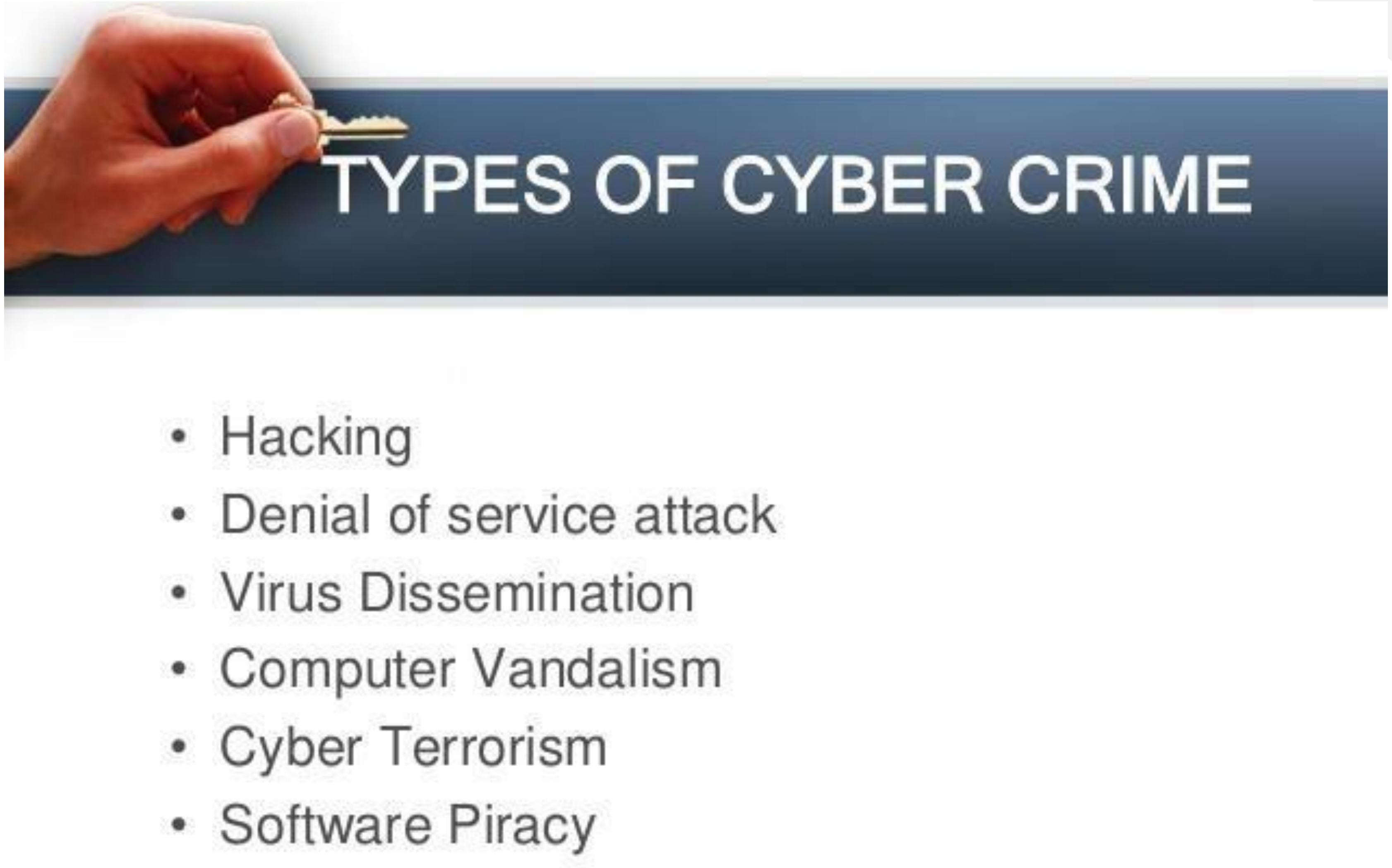
Internet Security

Information Security vs. Cybersecurity

- Information Security
  - Focus: Protection of information, regardless of format, including:
  - Paper documents
  - Digital and intellectual property
  - Verbal or visual communications
- Cybersecurity
  - Focus: Protection of digital assets, including:
  - Network hardware
  - Software
  - Information processed and stored in isolated or networked systems

WHY DO THEY DO IT ?





TYPES OF CYBER CRIME

- Hacking
- Denial of service attack
- Virus Dissemination
- Computer Vandalism
- Cyber Terrorism
- Software Piracy

Protecting yourself and workplace

STAYING SAFE ONLINE

Digital technology provides boundless opportunities to deliver simpler and more convenient experiences to customers and stakeholders. It also presents new and evolving risks to manage.

Some sobering statistics:

Almost one Billion Personal Records have been Stolen in multiple breach's as of 2018

Email Payment Fraud has net attackers in excess of US$10 billion over the last two years.

Ransomware is now a US$5 billion a year industry

Cyber crime and payment fraud cost businesses an estimated $6 trillion in 2019

Cyber crime is big business.

Why do we care about cybersecurity?

Why is Cyber Security Awareness Important?

Advanced technologies have changed the modern way of life. The internet provides us with many benefits. Be it communicating with friends, searching for information, doing banking transactions, availing online services, finding job, finding life partner or even running entire businesses. The internet touches almost all aspects of our lives. However, it also makes us vulnerable to a wide range of threats.

New and powerful cyber-attacks are striking the internet regularly. A minor lapse in managing our digital lives can open the door to cyber criminals. Cyber criminals can steal our money or damage our reputation.

According to a study by a leading industry research organization, 90% of all cyberattacks are caused by human negligence. Therefore, cyber security awareness is important for everyone today.

We must be vigilant while making use of technology to reduce the risk of cyber threats.

costs Delhi man Rs

India's of

duraf

Gadgets Now Bureau / 31 Dec, 2020, 10:39AM IST

Be ga ru loses Rs akh
bo kin fligh cket

he Ti s Of India
pdate hours ago

TNN BENC URU

BE GA RU: 8-year-old man from
W efi d los s 7 la h to cybercrimi nals on
De em er 30 ile trying to book a fl ght to
Th uva anth uram Rajendra (nam
ch ge) said booked the ticket fo January
18 rou gh an p. H e received a text message
sa g t e payment hadn't been recei ved but

Top 6 Cyber Crimes Vectors of Attacking

- Phishing Scams
- MiTM Attacks
- Ransomware and Malware Attacks
- Social Engineering Attacks
- IOT Hacking
- DDoS

Types of Cybercrime

- Identity Theft
- Psychological Tricks
- Social Media related Attacks
- Digital Banking Frauds
- Attacks through Mobile Applications
- Virus Attacks on Personal Computer

IDENTITY THEFT

IDENTITY THEFT

Hacking or gaining access to Social Media Accounts

The attacker hacks or gains access to the social media account of the victim. The attacker can then harm the victim by misusing their personal information and photographs. The attacker can also post offensive content on victim's profile or defame the victim.

Misuse of photocopies of identity proofs

The attacker misuses the photocopies of identity proofs of the victim. These can be PAN Card, Aadhaar Card or any other identity proof of the victim. The attacker can use these photocopies to steal money or cause harm to the victim.

Credit/Debit Card Skimming

Credit/Debit card skimming is done using a small device called skimmer. The magnetic stripe of the card stores details such as name, credit/debit card number and expiration date. First, the credit/ debit card is swiped through a skimmer. Then, the skimmer captures all these details. Thieves use this stolen data to make online transactions. They also use this data to create duplicate credit/debit cards and withdraw money from ATM.

IDENTITY THEFT

Story 1: Hacking or gaining access to Social Media Accounts

Sameera visits a cybercafé to take print out of her work related documents, from her e-mail.

While the print out is processing, she accesses her social media profile and checks other e-mails.

(After 2 hours)

Sameera receives a notification that the password of her social media account has been reset.

She tries to check her social media account from mobile but is unable to access it now.

As soon as the print outs are ready, she rushes to collect it.

She closes the browser window without logging out of the account and leaves the cybercafé.

Sameera gets a call from her Boss stating that the confidential project documents were leaked on the Internet by her.

She again receives a call from her friend saying that her social media page shows obscene images and videos.

IDENTITY THEFT

Sameera loses her job due to leaking of the project documents.

Moreover, she is ashamed that her photoshopped obscene images are posted on social media.

She regrets that she did not log out of her social media account.

Sameera decides to report the incident in the Police Station.

The Inspector investigates the matter and arrests the culprit.

TIPS

- Do not close the browser window without logging out of the account.
- Use 2-step verification such as one-time password (OTP) while using someone else’s computer.
- Do not save your username and password in the web browser.
- Register your mobile number with social networking sites to get alerts in the event of un-authorized access.
- Permanently delete all documents downloaded on computers in cybercafé.

IDENTITY THEFT

Story 2: Misuse of photocopies of identity proofs

Suresh applies for home loan at a non-reputed loan agency giving loan at very low interest rates.

He submits photocopies of documents (PAN Card, IT Returns, etc.) at the counter.

HOME LOAN
DGEV
LOAN AGENCY

MANAGER
BANK OF WSAC

(After 4 months)

Suresh receives a call from a bank.

Bank manager : Sir, have you applied for an auto loan?

Suresh : No, I did not apply for any loan from your bank.

Suresh visits the bank.

He is surprised to know that his documents are present with that bank.

He understands that someone wanted to commit a crime.

MANAGER
BANK OF WSAC

POLICE
CYBER CELL

He visits Police Station where the Inspector explains that it is a case of identity theft.

Someone used his PAN card number and two years of IT returns by changing photograph, signature, address and phone number in his identity proofs.

IDENTITY THEFT

Story 2: Misuse of photocopies of identity proofs

The fraudster had applied for 7 auto and personal loans from other major banks using the same documents.

Suresh regrets sharing his personal documents with the un-trusted agency.

TIPS

- Never provide details or copy of identity proofs (e.g. PAN Card, Aadhaar Card, Voter Card, Driving License, Address Proof) to unknown person/organization.
- Be careful while using identity proofs at suspicious places.
- Do not share sensitive personal information (like Date of Birth, Birth Place, Family Details, Address, Phone Number) on public platforms.
- Always strike out the photo copy of the identity proof; write the purpose of its usage overlapping the photo copy. This way, it becomes difficult to reuse the photo copy.
- Do not leave your credit, debit or ATM card receipts behind, in places such as a bank/ATM or a store; never throw them away in public.

IDENTITY THEFT

Story 3: Credit/Debit Card Skimming

Sachin and his friends are having dinner at a restaurant. The waiter gives the bill to Sachin.

Sachin : Do you accept card payment?

Waiter : Yes Sir.

Sachin hands over the debit card to the waiter for payment.

The waiter brings the card payment machine over to Sachin for him to enter the PIN. Sachin enters the PIN carelessly without hiding it from the people around him.

The waiter makes a note of the PIN.

COUNTER
Skimmer

The waiter takes it to the billing counter where he secretly swipes the card in a skimming machine to capture card information.

The skimming machine looks just like a normal payment machine (usually seen in restaurants, shops etc.)

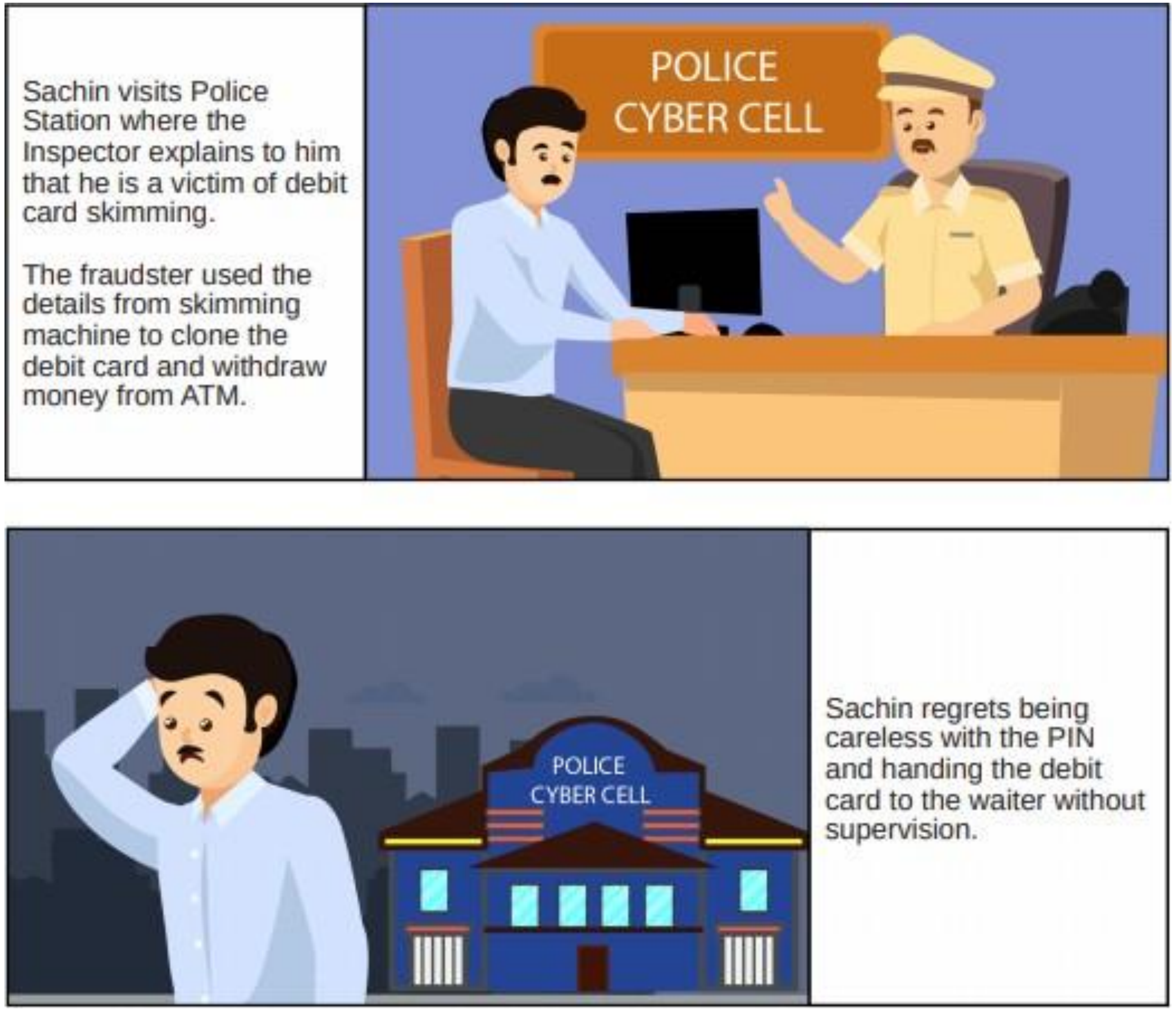
The waiter now has all the required details like account holder's name, account number, debit card number, CVV and PIN.

(After a few days)

Sachin receives an SMS stating ₹ 25,000 are withdrawn from ATM.

IDENTITY THEFT

Story 3: Credit/Debit Card Skimming



Sachin visits Police Station where the Inspector explains to him that he is a victim of debit card skimming.

The fraudster used the details from skimming machine to clone the debit card and withdraw money from ATM.

Sachin regrets being careless with the PIN and handing the debit card to the waiter without supervision.

TIPS

- Always ensure that credit/debit card swipes at shopping malls, petrol pumps, etc. are done in your presence. Do not allow the salesperson to take your card away to swipe for the transaction.
- Look out for credit/debit card skimmers anywhere you swipe your card, especially at petrol pumps, ATMs etc.
- If you notice a credit/debit card reader that protrudes outside the face of the rest of the machine, it may be a skimmer.
- Never share your PIN with anybody, however close they might be.

PSYCHOLOGICAL

TRICKS

PSYCHOLOGICAL TRICKS

Phishing, Vishing, Smishing

Lottery Fraud

The fraudster congratulates the victim for winning a handsome lottery via e-mail/call/SMS. The victim is delighted and is eager to get the lottery money. The fraudster asks the victim to transfer a token amount and share vital personal information to get the lottery money. The victim loses his/her money and does not get anything in return.

Credit/Debit Card Fraud

The attacker tries to scare the victim by informing them that their credit/debit card has been blocked. The victim becomes worried and starts panicking. The attacker takes advantage of this situation and asks victim to provide sensitive personal information to re-activate the card. This information is then misused to steal money or cause harm to the victim.

Job Related Fraud

The attacker sends a fake e-mail to the victim offering a job with an attractive salary. The victim, unfortunately, believes it and follows the instructions. The attacker then steals the money or harms the victim physically

PSYCHOLOGICAL TRICKS

Story 1: Lottery Fraud

Hemant : I have been purchasing lottery tickets since past two years, but I did not win even once! I hope I win this time.

Ravi : Don't waste your money on lottery tickets. Leave this and concentrate on your work.

Hemant follows the instructions given in the e-mail to provide his personal details and transfer a token amount to get the lottery money.

He transfers ₹ 30,000 to an unknown bank account using the given link.

Hemant receives an e-mail stating that he has won the lottery worth ₹ 25 lakhs. Hemant gets excited and readily believes that his long awaited good news has finally arrived.

Hemant : Ravi, my wait is finally over, I won the lottery worth ₹ 25 lakhs. Check this e-mail.

Ravi : This is a fake e-mail. This is not the website from where you purchased the lottery ticket. Don't transfer any money to them.

PSYCHOLOGICAL TRICKS

Hemant (shocked) : I already transferred ₹ 30,000!

Ravi : Report to the nearest police station immediately.

Hemant regrets that he lost his money as he did not think rationally and believed the e-mail without verifying its authenticity.

TIPS

- Do not respond to messages from unknown source requesting personal or financial details even if it assures credit of money into your bank account.
- Do not respond to suspicious e-mails or click on suspicious links.
- Do not transfer money to any un-trusted unknown account.
- Remember you can never win a lottery if you have not participated in it.
- Always verify the correctness of the domain of the e-mail ID, for example, all government websites have ".gov.in" or ".nic.in" as part of their web address.
- Have proper spam filters enabled in your e-mail account.

PSYCHOLOGICAL TRICKS

Story 2: Credit/Debit Card Fraud

Caller : Hello, am I speaking to Ms. Manisha? I'm calling from your bank. Your debit card has been blocked due to suspicious activities. I need to verify your details to re-activate your card. Please provide your debit card number and PIN.

Caller : We already have your details Ma'am, we just need to verify them. Please provide your debit card number and PIN.

(Manisha provides the details asked by the caller)

Manisha : Please re-activate my debit card soon.

Manisha : But, how do I believe whether it's really blocked?

Caller : Is this Manisha living in Sunflower Society in Delhi, having savings account in the bank?

Manisha : Yes, the information you gave is correct.

(After three hours)

Manisha receives SMS notification that ₹ 10,000 have been debited from her account for an online transaction. She realizes that the call was a fake call and the attacker used that information to steal money.

PSYCHOLOGICAL TRICKS

Story 2: Credit/Debit Card Fraud

She visits the Police Station, where Inspector tells her that she is a victim of Vishing crime. The inspector then starts the investigation.

TIPS

- Do not get petrified if you receive a call stating that your card is blocked. Bank will never convey such information on call.
- Do not share your PIN, password, card number, CVV number, OTP etc. with any stranger, even if he/she claims to be bank employee. Bank will never ask for any vital information.
- Keep your bank's customer care number handy so that you can report any suspicious or un-authorized transactions on your account immediately.

SOCIAL MEDIA FRAUDS

SOCIAL MEDIA FRAUDS

Cyber Stalking

Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail, instant messaging (IM), messages posted on a website or a discussion group. A cyber stalker relies upon the fact that his/her true identity is not known in the digital world. A cyber stalker targets the victim with threatening/abusive messages and follows them/their activities in the real world.

Cyber Bullying

Cyber bullying is bullying that takes place over digital devices. Cyber bullying can occur through SMS, social media, forums or gaming apps where people can view, participate or share content. Cyber bullying includes sending, posting or sharing negative, harmful, false content about someone else. The intention is to cause embarrassment or humiliation. At times, it can also cross the line into unlawful criminal behavior.

SOCIAL MEDIA FRAUDS

Story 1: Cyber Stalking

Preeti is a beautiful and popular girl in the college.

She is active on multiple social media platforms.

She is an adventurous girl who likes travelling in different cities.

Rishi keeps stalking Preeti on social media.

One day, Preeti decides to go on a solo trekking trip. Excitedly, she updates her plan on social media with itinerary. Rishi now knows her entire plan and decides to follow her on the trip.

She always uses the Check-In feature of her social media profile to tag the places she has been to.

Rishi follows her near the mountain where he finds her alone and molests her.

SOCIAL MEDIA FRAUDS

Story 3: Cyber Stalking

Preeti cries and shouts for help. Rishi runs away before anyone arrives there for help.

Preeti visits Police Station where the Inspector investigates the case. The Inspector tracks the whereabouts of Rishi and arrests him.

Preeti regrets sharing her trip itinerary publicly on social media.

TIPS

- Restrict access to your profile. Social media sites offer privacy settings for you to manage who can view your posts, photos, send you friend request etc.
- Ensure your personal information, photos and videos are accessible only to your trusted ones.
- Be careful while uploading your photos on social media which show your location or places you frequently visit as cyber stalkers may keep tabs on your daily life.

SOCIAL MEDIA FRAUDS

Story 2: Cyber Bullying

Sameer is an innocent and very shy boy. He does not feel confident to talk with people face to face, hence he talks to people on social media.

Himesh later creates a troll page in the name of Sameer on social media. He irritates and defames Sameer by posting adult jokes about him.

He also posts several memes and funny videos which go viral and everyone starts to make fun of Sameer and abuse him.

One day, Himesh along with his gang of friends in school harass Sameer by calling him a coward. Sameer ignores them as he is not looking for an argument.

After ignoring for a long time, Sameer is depressed and finally decides to tell his parents.

SOCIAL MEDIA FRAUDS

Story 2: Cyber Bullying

His parents later complain to the school authorities and to the Police Station. The Inspector from Cyber Cell deletes the viral posts.

Sameer regrets for not informing school authorities regarding the matter at an earlier stage.

TIPS

- Be careful :
  - If your child's behavior is changing and he/she is more aggressive than before.
  - If suddenly your child stops talking with you or his/her friends.
  - If he/she stops using digital devices or is scared.
- Make your children aware that cyber bullying is a punishable crime so that neither do they indulge themselves in cyber bullying nor do they let anyone tease them.
- Discuss safe internet practices with your friends and family regularly.
- Monitor your kid's activity on internet/social media. Enable parental controls on computer/mobile devices.
- Even if the children or students know about any friend who is a victim of cyber bullying, they should help the victim. Report the matter to parents or teachers immediately.
- Do not delete offensive messages as it will help the police in investigation.

MOBILE APPLICATION FRAUDS

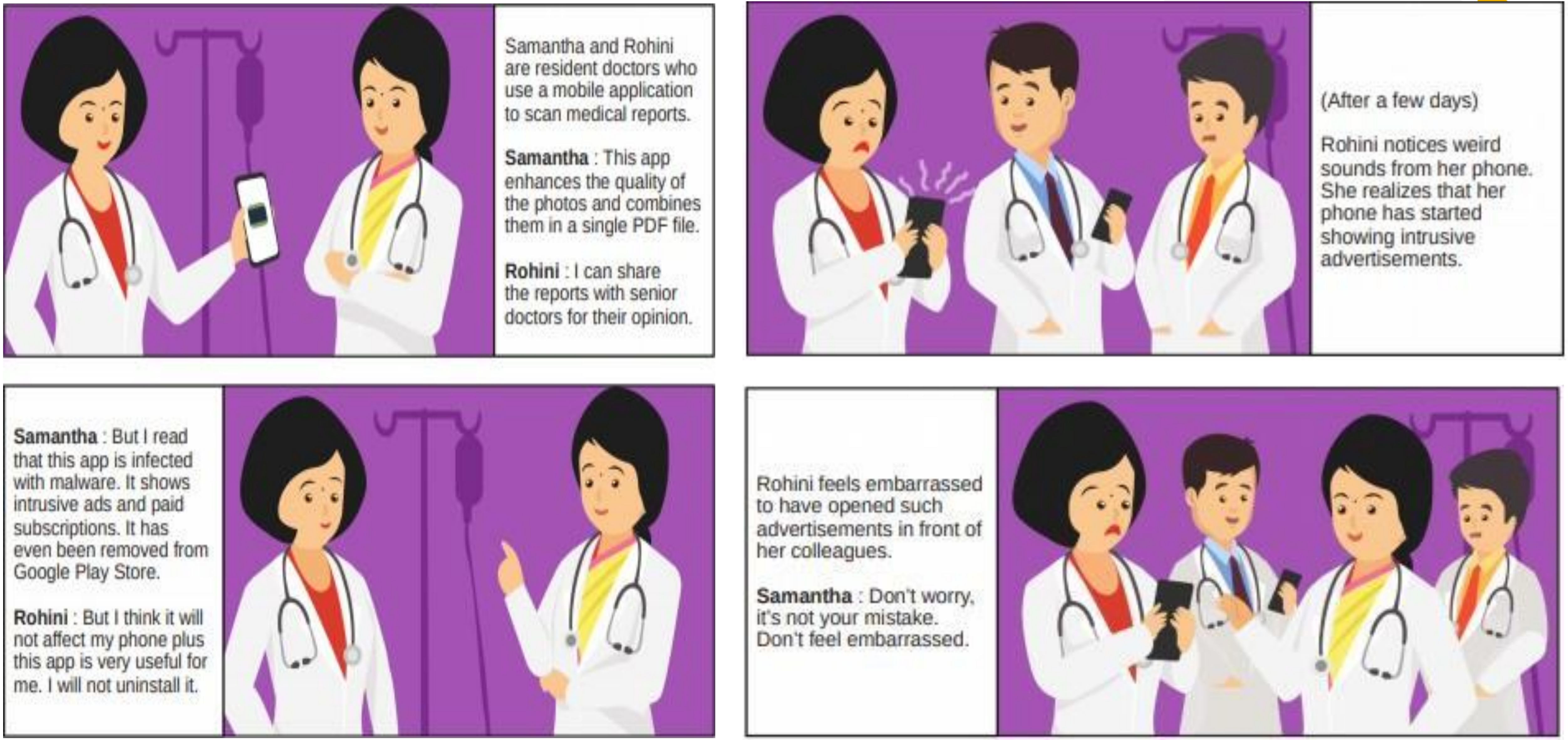
MOBILE APPLICATION FRAUDS

Cyber-attacks using Infected Mobile Applications

People become habitual users of certain mobile applications. As a result, they ignore security warnings. Fraudsters use this to attack the victim by infiltrating through such popular mobile applications. They infect the applications with malicious software, called Trojan. This Trojan can get access to your messages, OTP, camera, contacts, e-mails, photos etc. for malicious activities.

It can also show obscene advertisements, sign users up for paid subscriptions or steal personal sensitive information from the mobile etc.

MOBILE APPLICATION FRAUDS



Samantha and Rohini are resident doctors who use a mobile application to scan medical reports.

Samantha : This app enhances the quality of the photos and combines them in a single PDF file.

Rohini : I can share the reports with senior doctors for their opinion.

(After a few days)

Rohini notices weird sounds from her phone. She realizes that her phone has started showing intrusive advertisements.

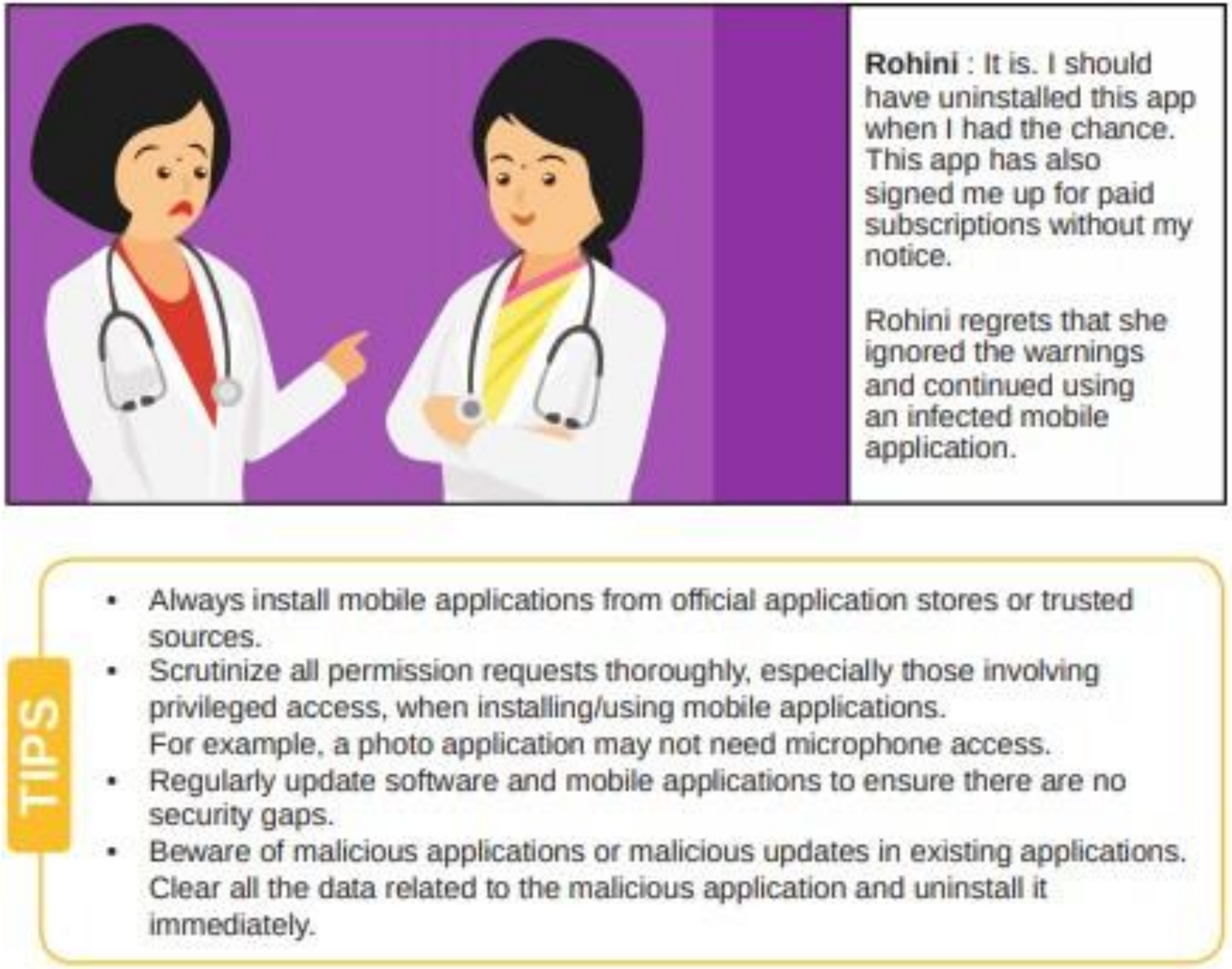
Samantha : But I read that this app is infected with malware. It shows intrusive ads and paid subscriptions. It has even been removed from Google Play Store.

Rohini : But I think it will not affect my phone plus this app is very useful for me. I will not uninstall it.

Rohini feels embarrassed to have opened such advertisements in front of her colleagues.

Samantha : Don't worry, it's not your mistake. Don't feel embarrassed.

MOBILE APPLICATION FRAUDS



Rohini : It is. I should have uninstalled this app when I had the chance. This app has also signed me up for paid subscriptions without my notice.

Rohini regrets that she ignored the warnings and continued using an infected mobile application.

TIPS

- Always install mobile applications from official application stores or trusted sources.
- Scrutinize all permission requests thoroughly, especially those involving privileged access, when installing/using mobile applications.
  For example, a photo application may not need microphone access.
- Regularly update software and mobile applications to ensure there are no security gaps.
- Beware of malicious applications or malicious updates in existing applications. Clear all the data related to the malicious application and uninstall it immediately.

ONLINE BANKING FRAUDS

ONLINE BANKING FRAUDS

Digital Payments Applications related attacks

Digital payments have become very common in today's life. However, they do pose a threat if the account is hacked.

Hacking of Bank Account due to Weak Password

In this type of attack, the attacker hacks into the victim's account by using a program to guess commonly used passwords. Once the account is hacked, the attacker can steal money or perform an illegal transaction in order to defame or frame the victim.

Hacking of Multiple Accounts due to same password

If same password is used for multiple accounts, then hacking of one account may also lead to hacking of other accounts.

PC Solutions

ONLINE BANKING FRAUDS

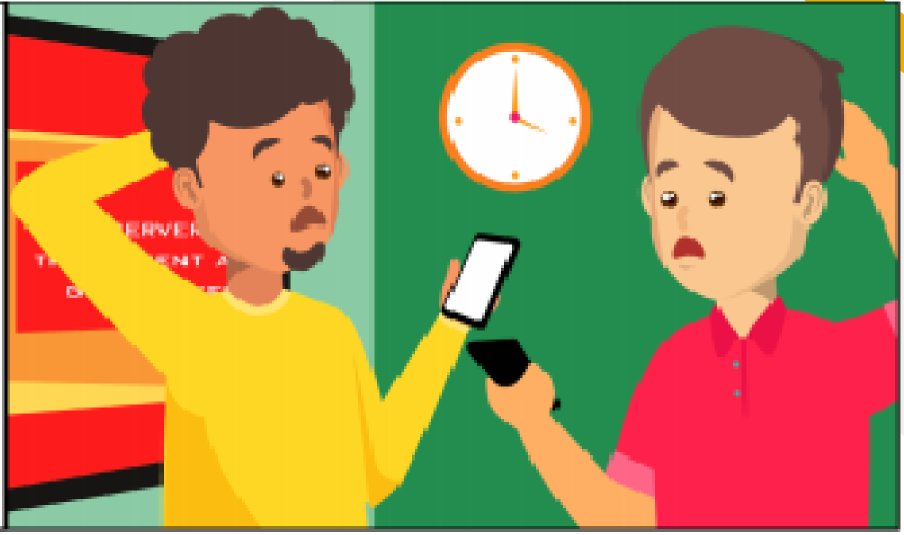
Story 1: Digital Payments Applications Related Attacks

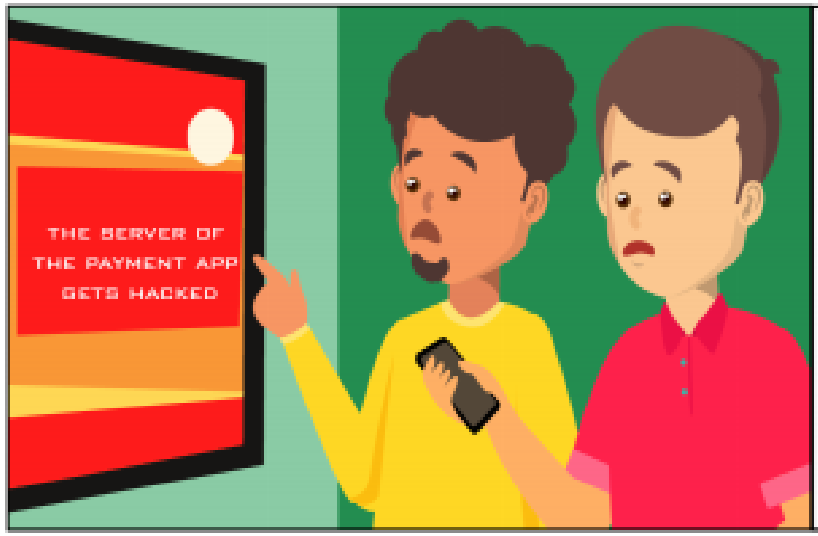
John and Sahil always use digital payments applications in their day-to-day lives for convenience.

They pay house bills, grocery expenses and any other expenditure using digital payments applications.

John losses all the money in his account.

However, Sahil losses only ₹ 5,000 from his account.



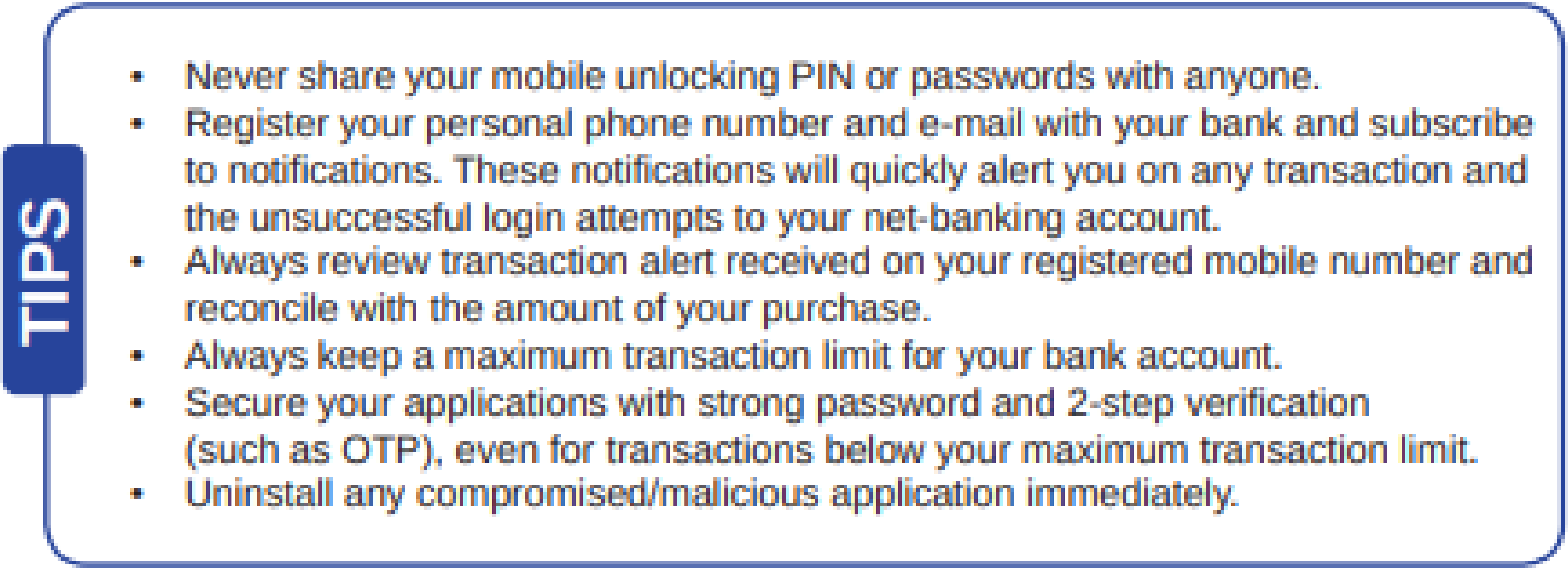


They read news on TV that the server of the payment applications is hacked.

Multiple accounts are affected and many users face financial loss due to this.

Sahil later explains John that he had only kept ₹ 5000 as his maximum transaction limit in his bank account as well as digital payment application. As a result, the attacker could only extract that much amount from his account.

ONLINE BANKING FRAUDS



TIPS

- Never share your mobile unlocking PIN or passwords with anyone.
- Register your personal phone number and e-mail with your bank and subscribe to notifications. These notifications will quickly alert you on any transaction and the unsuccessful login attempts to your net-banking account.
- Always review transaction alert received on your registered mobile number and reconcile with the amount of your purchase.
- Always keep a maximum transaction limit for your bank account.
- Secure your applications with strong password and 2-step verification (such as OTP), even for transactions below your maximum transaction limit.
- Uninstall any compromised/malicious application immediately.

ONLINE BANKING FRAUDS

Story 2: Hacking of Bank Account due to Weak Password

Seema : The contribution for the party is ₹ 1,500. You are coming to the party, right?

Reena : Yes, I'm coming. I'll transfer money using net-banking.

Seema : I'll do it from your phone. What's your password?

Reena : You know it, don't you! It's my birth date.

Ramesh is eavesdropping. He listens to the entire conversation.

Ramesh finds out the birth date of Reena and hacks into her account. Later, he steals money from her account.

Reena visits Police Station. The Inspector investigates the case and finds out Ramesh was the culprit.

Ramesh confesses to his crime and says he heard Reena give up the password.

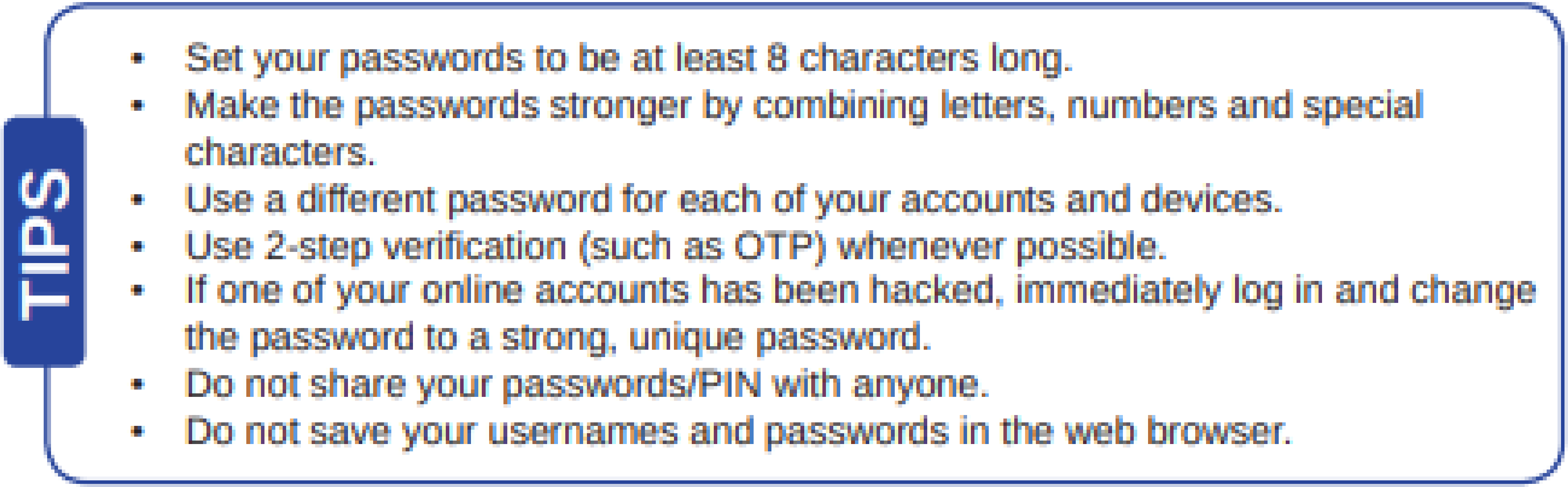
ONLINE BANKING FRAUDS

Reena regrets that she kept a weak password and shared it openly with her friend Seema.

Techniques for strong password which are easy to remember:

- For making unique passwords, create as many pass-phrases and words as possible (different passwords for different accounts) For example:
- shopping – $h0pp!n9 (S =$, i=!, g=9, o=0)
- october – 0cT0b3r9!
  (one more alphabet/number '9' is added as "october" is a 7 letter word)
- Social Network – $0c!alNetw0rK
- Windows – w!nD0W$9
- NULinux – 9NuL!NuX
  (one more alphabet/number '9' is added as "NULinux" is a 7 letter word)

ONLINE BANKING FRAUDS

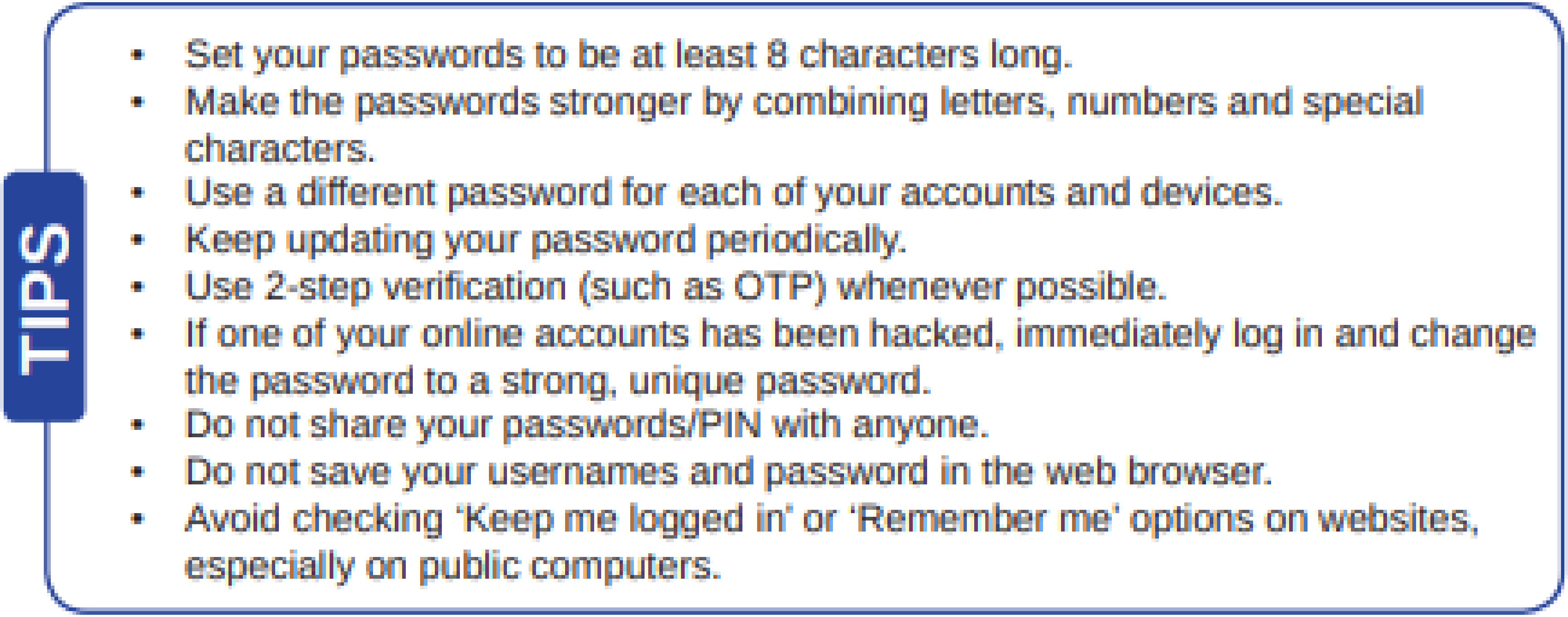


TIPS

- Set your passwords to be at least 8 characters long.
- Make the passwords stronger by combining letters, numbers and special characters.
- Use a different password for each of your accounts and devices.
- Use 2-step verification (such as OTP) whenever possible.
- If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique password.
- Do not share your passwords/PIN with anyone.
- Do not save your usernames and passwords in the web browser.

ONLINE BANKING FRAUDS

Story 3: Hacking of Multiple Accounts due to same password



TIPS

- Set your passwords to be at least 8 characters long.
- Make the passwords stronger by combining letters, numbers and special characters.
- Use a different password for each of your accounts and devices.
- Keep updating your password periodically.
- Use 2-step verification (such as OTP) whenever possible.
- If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique password.
- Do not share your passwords/PIN with anyone.
- Do not save your usernames and password in the web browser.
- Avoid checking 'Keep me logged in' or 'Remember me' options on websites, especially on public computers.

VIRUS ATTACK ON PERSONAL COMPUTER

VIRUS ATTACK ON PERSONAL COMPUTER

Virus Attack through external devices

A virus can enter the computer through external devices like pen drive or hard disk etc. This virus can spread across all the computer files.

Virus Attack by downloading files from un-trusted websites

The virus can enter the computer by download of files from un-trusted websites. The virus can be hidden in the form of music files, video files or any attractive advertisement. This virus can spread across all the computer files.

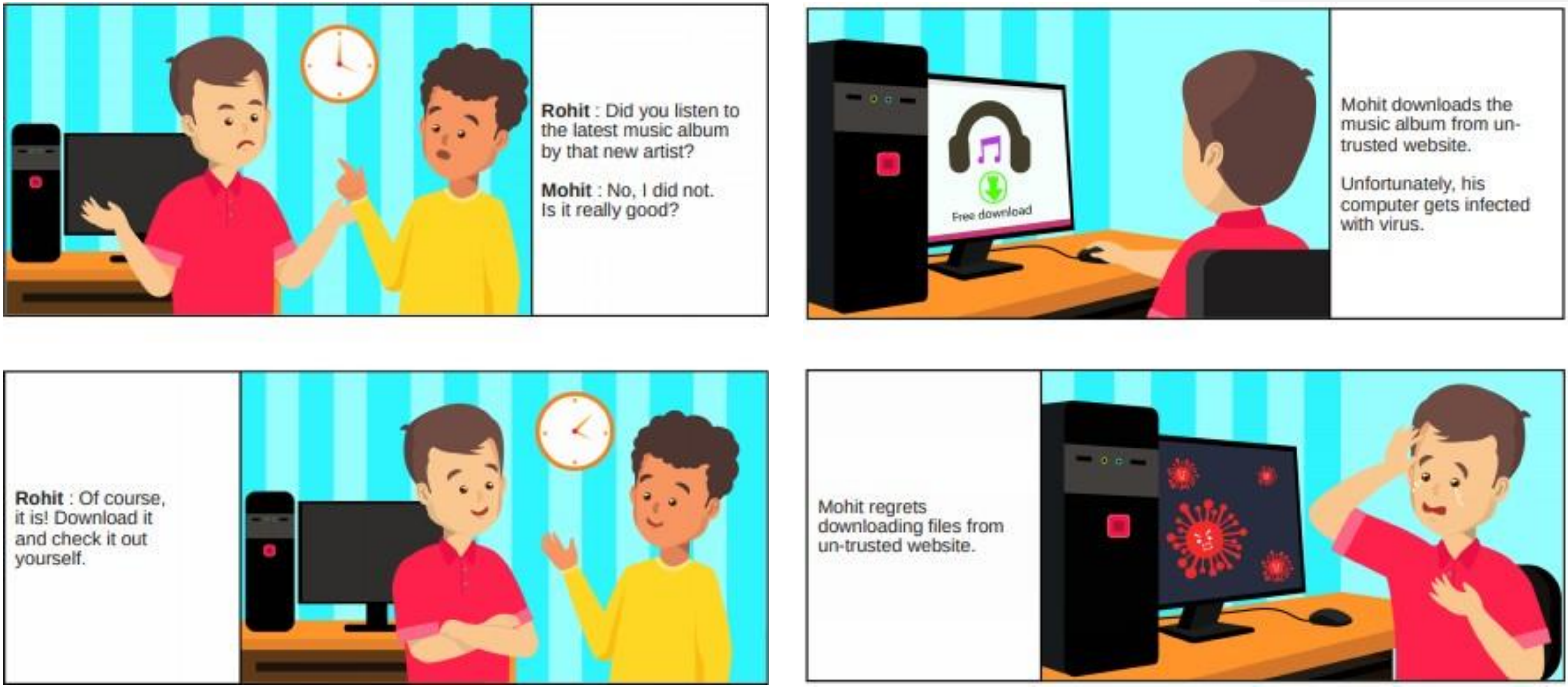
Virus Attack by installation of malicious software

The virus can enter into the computer by installing software from un-trusted sources. The virus can be an additional software hidden inside unknown game files or any unknown software. This virus can spread across all the computer files.

A Virus/Malicious application can cause various harms such as slowing down the computer, lead to data corruption/deletion or data loss

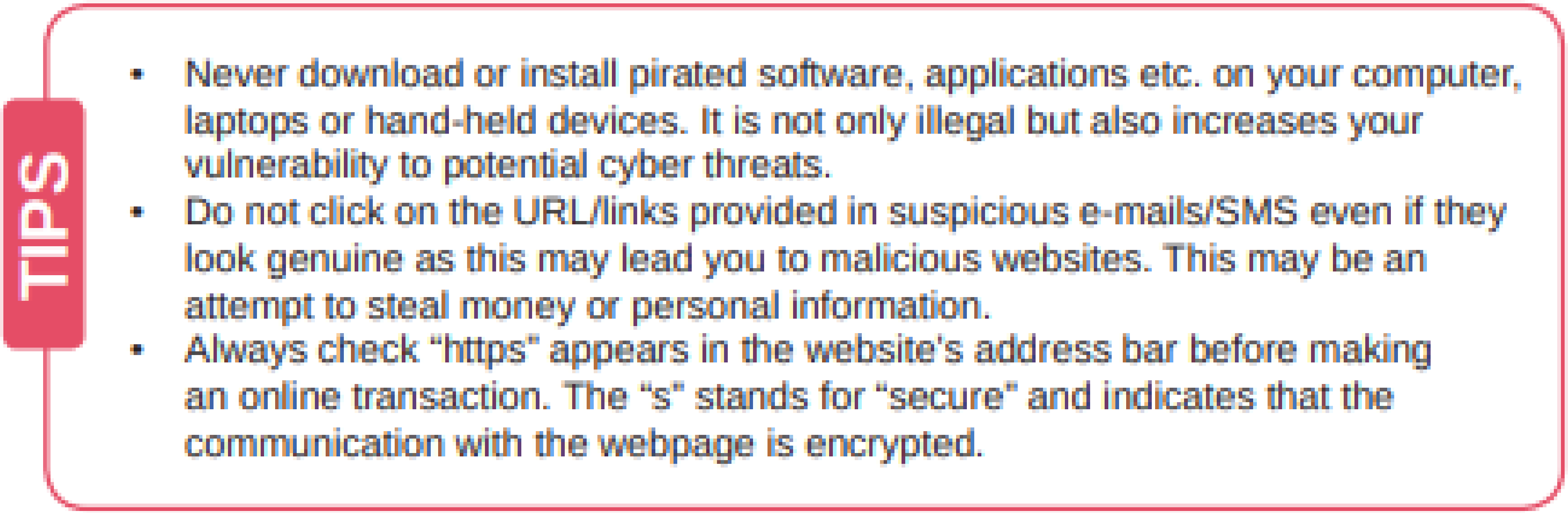
VIRUS ATTACK ON PERSONAL COMPUTER

Story 1: Virus Attack by downloading files from un-trusted websites


Rohit : Did you listen to the latest music album by that new artist?
Mohit : No, I did not. Is it really good?
Free download
Mohit downloads the music album from un-trusted website.
Unfortunately, his computer gets infected with virus.
Rohit : Of course, it is! Download it and check it out yourself.
Mohit regrets downloading files from un-trusted website.

VIRUS ATTACK ON PERSONAL COMPUTER

Story 2: Virus Attack by downloading files from un-trusted websites

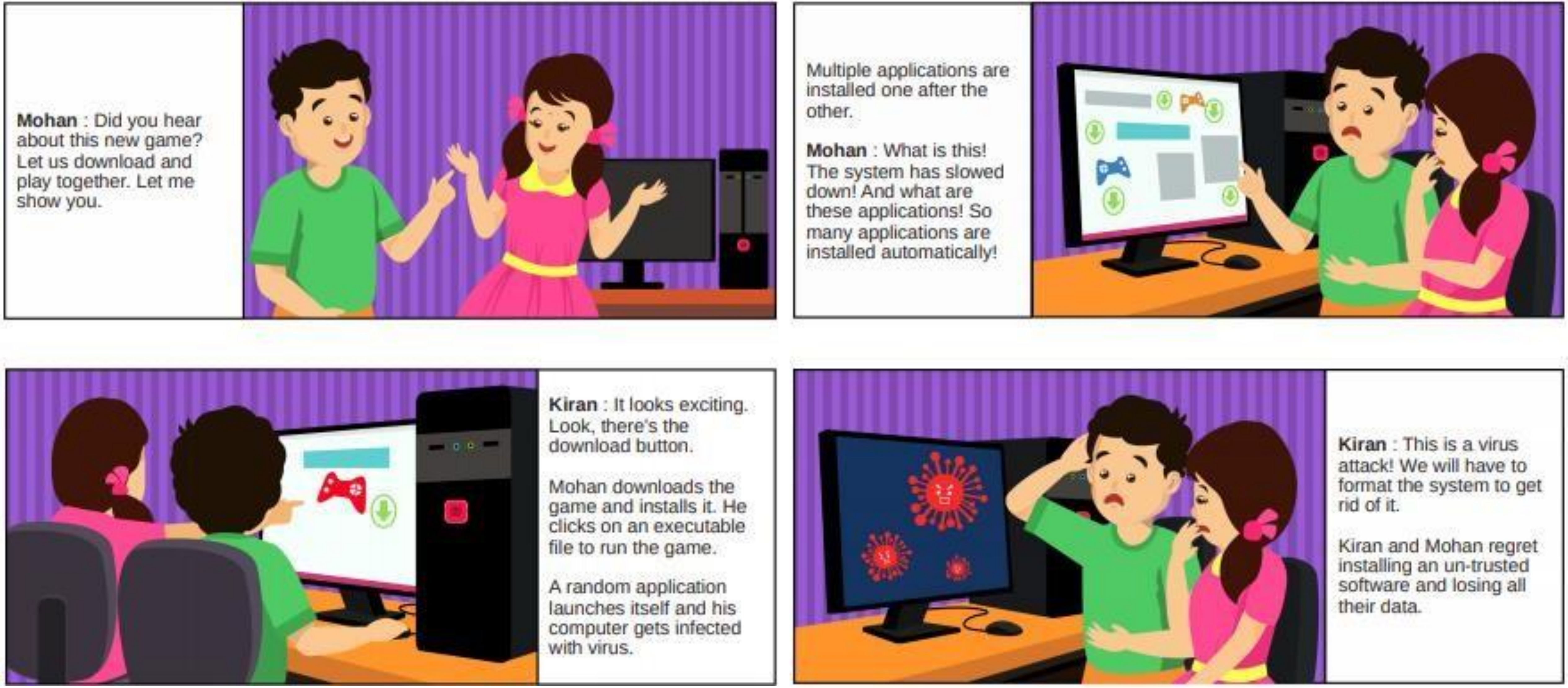


TIPS

- Never download or install pirated software, applications etc. on your computer, laptops or hand-held devices. It is not only illegal but also increases your vulnerability to potential cyber threats.
- Do not click on the URL/links provided in suspicious e-mails/SMS even if they look genuine as this may lead you to malicious websites. This may be an attempt to steal money or personal information.
- Always check "https" appears in the website's address bar before making an online transaction. The "s" stands for "secure" and indicates that the communication with the webpage is encrypted.

VIRUS ATTACK ON PERSONAL COMPUTER

Story 2: Virus Attack by installation of malicious software



Mohan : Did you hear about this new game? Let us download and play together. Let me show you.

Kiran : It looks exciting. Look, there's the download button.

Mohan downloads the game and installs it. He clicks on an executable file to run the game.

A random application launches itself and his computer gets infected with virus.

Multiple applications are installed one after the other.

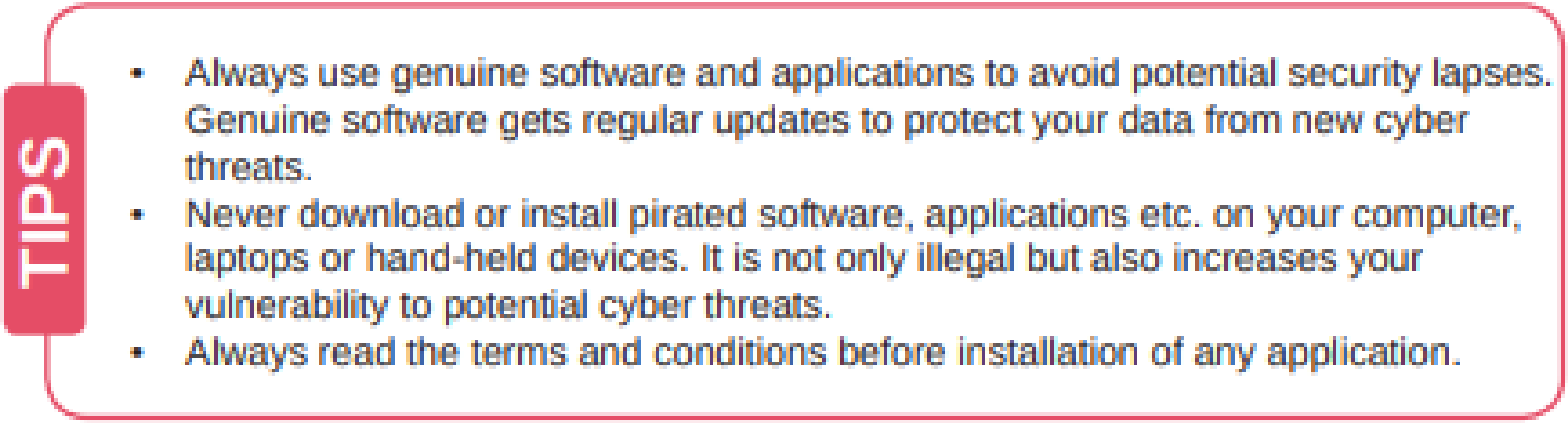
Mohan : What is this! The system has slowed down! And what are these applications! So many applications are installed automatically!

Kiran : This is a virus attack! We will have to format the system to get rid of it.

Kiran and Mohan regret installing an un-trusted software and losing all their data.

VIRUS ATTACK ON PERSONAL COMPUTER

Story 2: Virus Attack by installation of malicious software



TIPS

- Always use genuine software and applications to avoid potential security lapses. Genuine software gets regular updates to protect your data from new cyber threats.
- Never download or install pirated software, applications etc. on your computer, laptops or hand-held devices. It is not only illegal but also increases your vulnerability to potential cyber threats.
- Always read the terms and conditions before installation of any application.

WHAT IS YOUR ROLE ?

- End-users are the last line of Défense.

  As an end-user, you;

- 1.Create and maintain password and passphrase
- 2.Manage your account and password
- 3.Secure your computer
- 4.Protect the data you are handling
- 5.Assess risky behaviour online
- 6.Equip yourself with the knowledge of security guidelines, policies, and procedures

GENERAL TIPS TO KEEP YOU SAFE

GENERAL TIPS TO KEEP YOU SAFE

1. Always keep your systems/devices (desktop, laptop, mobile) updated with latest patches.
2. Protect systems/devices through security software such as anti-virus with the latest version.
3. Always download software or applications from known trusted sources only. Never use pirated software on your systems/devices.
4. Ensure all devices/accounts are protected by a strong PIN or passcode. Never share your PIN or password with anyone.
5. Do not share your net-banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. with any person even if he/she claims to be an employee or a representative of the bank and report such instances to your bank.
6. Always change the default admin password on your Wi-Fi router to a strong password known only to you. In addition, always configure your wireless network to use the latest encryption (contact your network service provider, in case of any doubt).
7. Be cautions while browsing through a public Wi-Fi and avoid logging in to personal & professional accounts such as e-mail or banking on these networks.

GENERAL TIPS TO KEEP YOU SAFE

8. Always use virtual keyboard to access net-banking facility from public computers; and logout from banking portal/website after completion of online transaction. Also ensure to delete browsing history from web browser (Internet Explorer, Chrome, Firefox etc.) after completion of online banking activity.
9. Do scan all e-mail attachments for viruses before opening them. Avoid downloading e-mail attachments received in e-mails from unknown or un-trusted sources.
10. Be careful while sharing identity proof documents especially if you cannot verify the authenticity of the company/person with whom you are sharing information.
11. Note the IMEI code of your cell phone and keep it in a safe place. The operator can blacklist/ block/trace a phone using the IMEI code, in case the cell phone is stolen.
12. Observe your surroundings for skimmers or people observing your PIN before using an ATM.
13. Discuss safe internet practices and netiquettes with your friends and family regularly! Motivate them to learn more about cybercrimes and safe cyber practices.
14. Do not save your card or bank account details in your e-wallet as it increases the risk of theft or fraudulent transactions in case of a security breach.
15. If you think you are compromised, inform authorities immediately.

be

Cyber Smart

be

Cyber Safe

Thank You

For Your Attention