NATIONAL INSTITUTE OF ELECTRONICS AND INFORMATION TECHNOLOGY
Sumit Complex, A-1/9, Vibhuti Khand, Gomti Nagar, Lucknow,


# Cyber Security Awareness Program
# 29.08.2022 to 02.09.2022

# Index

# Types of Cybercrime

- A cybercrime is a crime involving computers and networks. This includes a wide range of activities, from illegally downloading music files to stealing money from online bank accounts. Cyber criminals are not always financially motivated. Cybercrimes include non-monetary offenses as well. It can include frauds such as job related frauds, matrimonial frauds; stealing and misusing sensitive personal information (Aadhaar details, credit/debit card details, bank account credentials, etc.); defamation of an individual on social media; distribution of computer viruses etc. Cybercrimes can also lead to physical or sexual abuse.

# IDENTITY THEFT

- Identity theft is the act of wrongfully obtaining someone's personal information (that defines one's identity) without their permission. The personal information may include their name, phone number, address, bank account number, Aadhaar number or credit/debit card number etc.
- Identity theft can have many adverse effects. The fraudster can use stolen personal information and identity proofs to:
  - gain access to your bank accounts
  - apply for loans and credit cards or open insurance accounts
  - file a tax refund in your name and get your refund
  - obtain a driver's license, passport or immigration papers
  - create new utility accounts
  - get medical treatment on your health insurance
  - assume your identity on social media
  - give your name to the police during an arrest etc.

## 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 photo copies of identity proofs

- The attacker misuses the photo copies 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 photo copies 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.

# 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.

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.

(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 now.

Sameera gets a call from her Boss stating thatthe 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.

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 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.
- 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.

# Story 2: Misuse of photo copies 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.

(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.

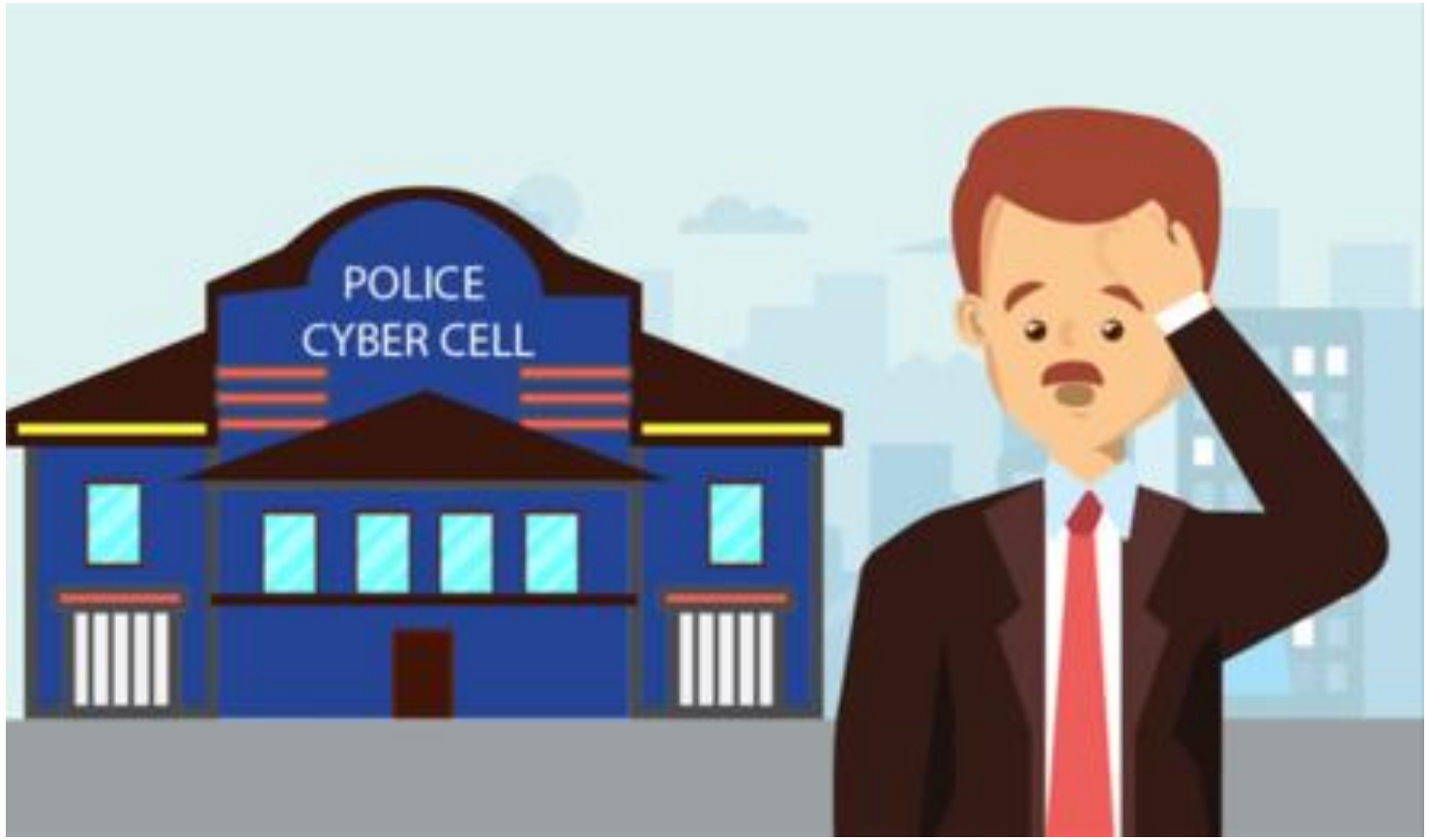
He understands that someone wanted to commit a crime.

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.

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.

# 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 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 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.

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.

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 sales person 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 are where attackers play with the minds of the user to trap them with lucrative offers. Once trapped, the attackers can exploit the victim by either stealing money or stealing sensitive personal information (name, Aadhaar details, bank account details etc.) or harm the victim in any other way. The entire basis of this kind of attack is to make the victim fall into their trap by sending fake e-mails, calls or SMSs.
- **Phishing** is the act of sending fraudulent e-mail that appears to be from a legitimate source, for example, a bank, a recruiter or a credit card company etc. This is done in an attempt to gain sensitive personal information, bank account details etc. from the victim.

- **Vishing** is similar to phishing. But, instead of e-mail, in this type of crime, the fraudster uses telephone to obtain sensitive personal and financial information.
- **Smishing** is the SMS equivalent of phishing. It uses SMS to send fraudulent text messages. The SMS asks the recipient to visit a website/weblink or call a phone number. The victim is then tricked into providing sensitive personal information, debit/credit card details or passwords etc.
- Phishing, Vishing and Smishing are done in an attempt to steal money from the victim or cause any other harm to the victim.

# Examples of Psychological Tricks

**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.

# 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 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 thewebsite from where you purchased the lottery ticket. Don't transfer any money to them.

**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.

# 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.

**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.

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

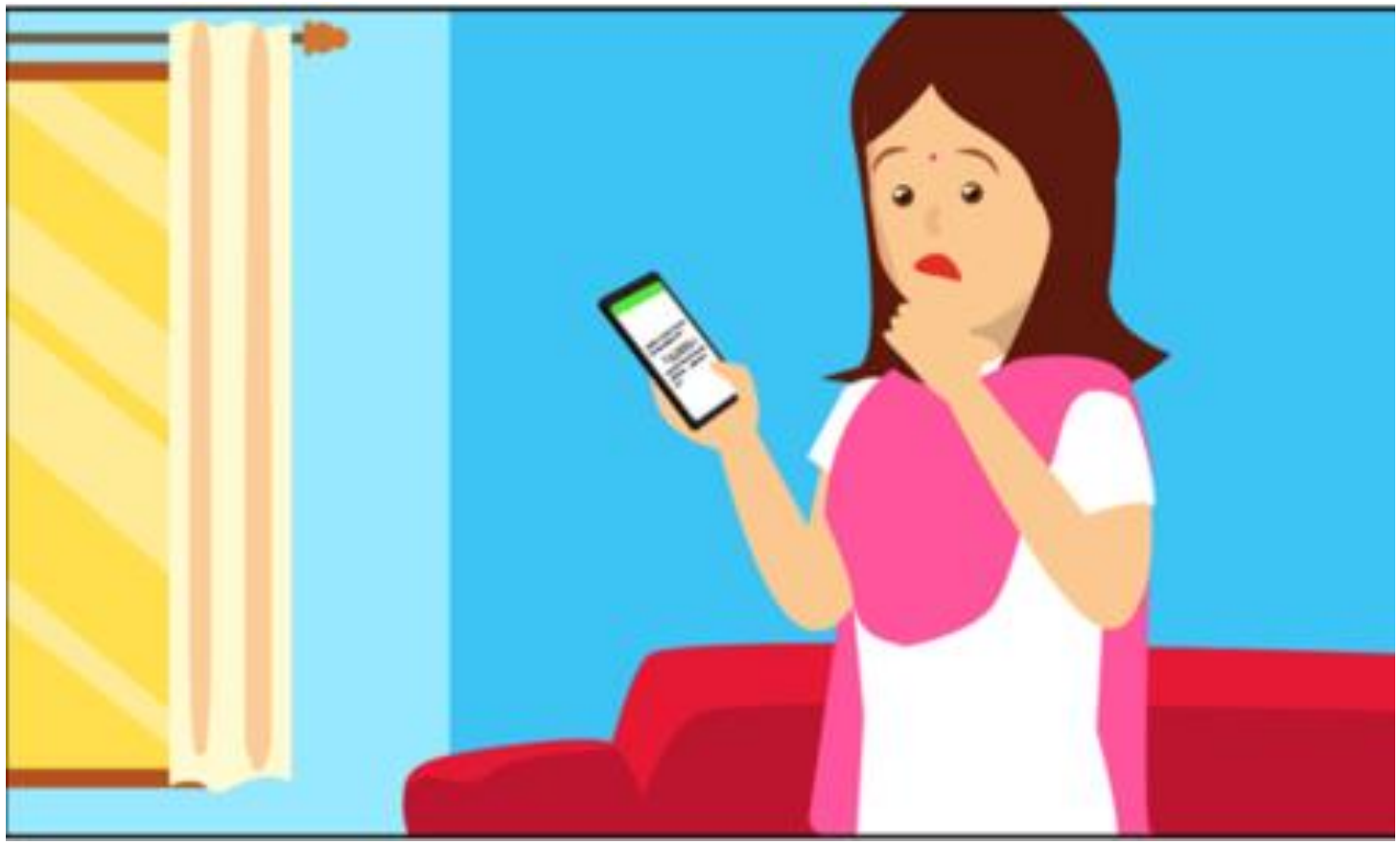
(Manisha provides the details asked by the caller)

**Manisha :** Please re-activate my debit card soon

(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.



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

Manisha regrets believing the attacker and giving away vital information without thinking rationally.

# Tips

Do not get petrified if you receive a call stating that your card is blocked. Bank will never convey such information on call.

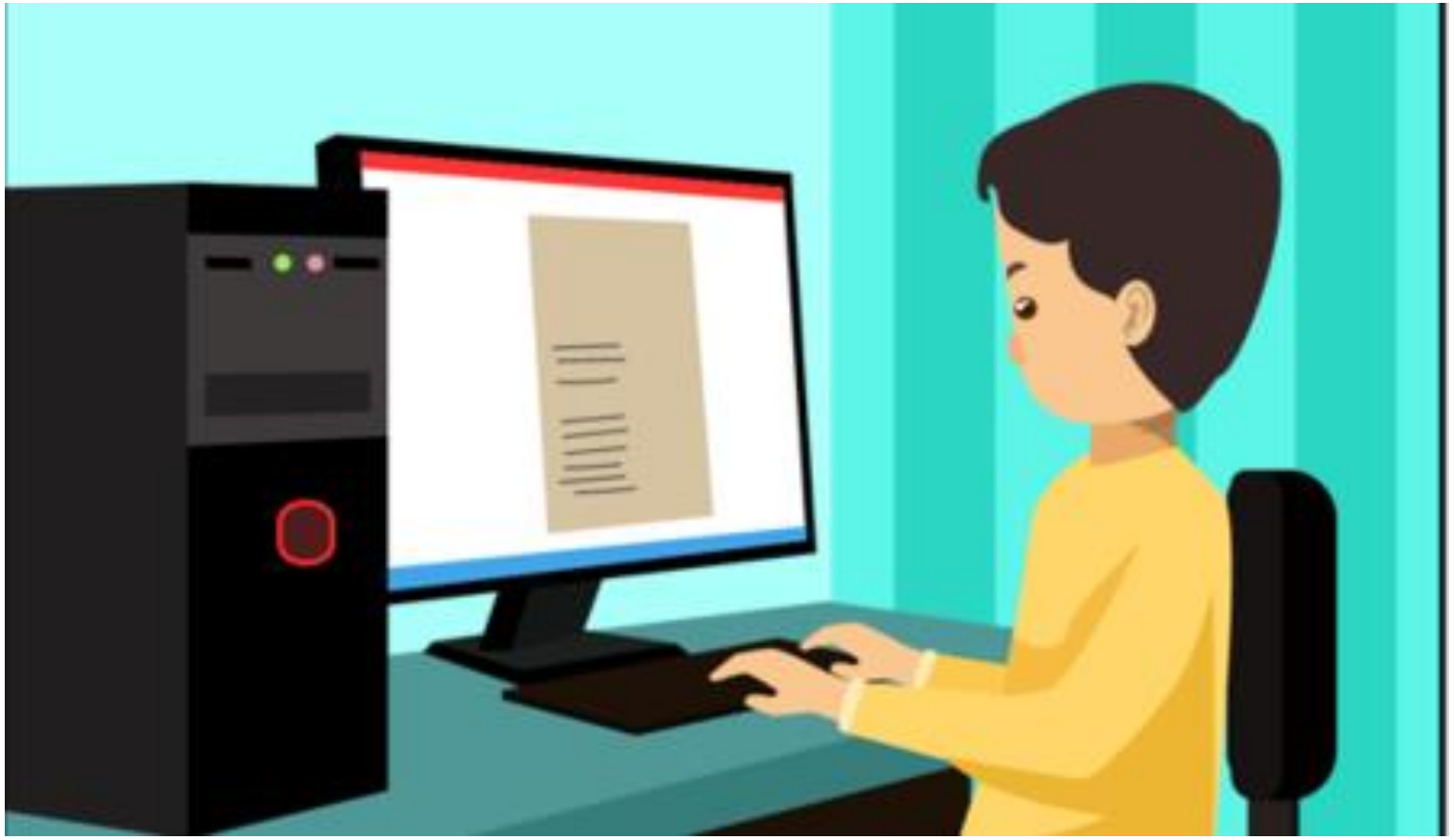
Do not share your PIN, password, card number, CVV number, OTP etc. with any stranger, even if he/she claims to be bank employee. Bank will never ask for any vital information.

Keep your bank's customer care number handy so that you can report any suspicious or un-authorized transactions on your account immediately

# Story 3: Job Related Fraud

Vikrant is a bachelor who stays alone. He receives an e-mail stating that he has been shortlisted for a job in an advertising firm with a very high salary. He gets very excited after reading the e-mail.

Vikrant applies for the job and follows the mentioned procedure. He provides his CV including personal information such as address, mobile number etc. The e-mail also states that he needs to travel to a different city and stay in the mentioned hotel for two days for the interview process.



Vikrant reaches the mentioned venue. He sees other candidates waiting in the same hotel. He is offered a welcome drink by a waiter.

After having the drink, Vikrant starts to feel dizzy.

Once he wakes up, he finds himself lying on the street, all his belongings were gone. He realizes that he was robbed.

He somehow tries to get back to his home. He notices that the door lock is broken and his house was robbed too.

He later reaches the Police Station to report a crime, where the Inspector informs that he got tricked using Phishing e-mail.

Vikrant regrets sharing personal information in a fraudulent e-mail without verifying the details.

Always search and apply for jobs posted on authentic job portals, newspapers etc.

Check if the domain of the e-mail is the same as the one you have applied with. For example, all government websites have “.gov.in” or “.nic.in” as domain.

If an e-mail has spelling, grammatical and punctuation errors, it could be a scam.

Beware of the fake calls/e-mails impersonating themselves as recruiters and requesting for personal information or money.

# Social Media Frauds

- Social Media has become an integral part of our lives. It is the new way of communicating, sharing and informing people about the events in our lives. We share our day to day lives on social media in the form of self and family photographs, updates on our locations/whereabouts, our views/thoughts on prevalent topics etc. One can understand the entire history of an individual through their social media profile and can even predict future events based on patterns in the past.
- This poses a threat to an individual as unwanted access to social media profile can cause loss of information, defamation or even worse consequences such as physical/sexual assault, robbery etc. Hence, protection and appropriate use of social media profile is very important.

**Sympathy Fraud**

- The attacker becomes friends with the victim on social media. The attacker gains trust by frequent interactions. The attacker later extracts money/harms the victim.

**Romance Fraud**

- The attacker becomes friends with the victim on social media. Over a period, the attacker gains victim’s affection. The attacker later exploits the victim physically, financially and/or emotionally.

## 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.

# Story 1: Sympathy Fraud

Santosh likes to surf the internet and has many friends on his social media profile.

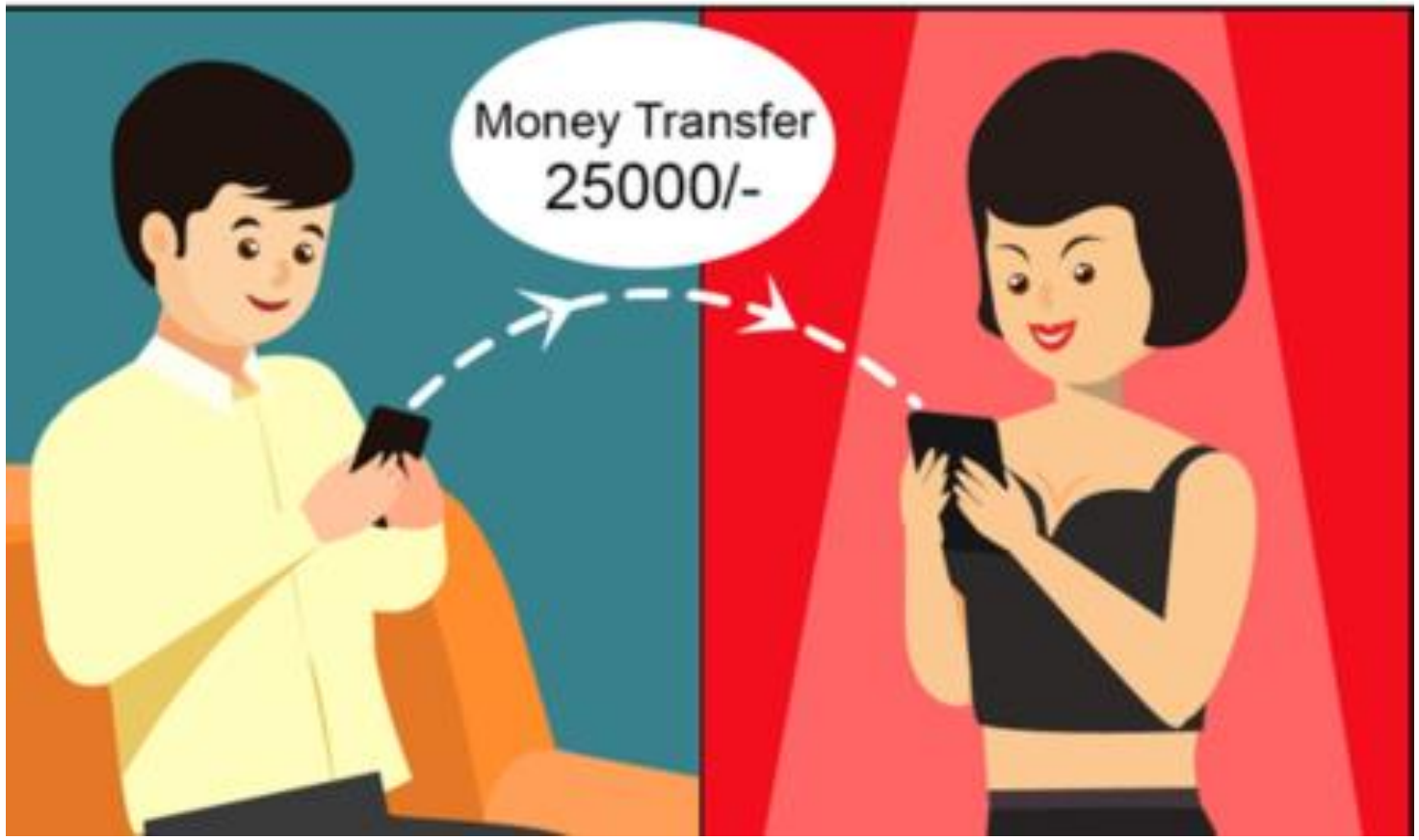
One day he receives a friend request from a beautiful young oman named Aparna. He accepts the friend request as he likes her profile picture.

Santosh and Aparna start chatting and talking on call all day.

Soon, Santosh begins to like spending time with Aparna. He starts to trust her completely.

One day, Aparna requests for ` 25,000 from Santosh stating that her brother is admitted to the hospital and she needs to deposit the amount urgently.

Unaware of reality, Santosh gives the money to Aparna.



Aparna flees, never to be seen again.

Worried about her hereabouts, Santosh decides to report the same to the Police Station.

Santosh files a missing complaint at Police Station.

The Inspector explains that this is a very common crime and he has been a victim of sympathy fraud.

The Inspector investigates the matter and catches Aparna. Santosh realizes that Aparna was a fraud.

He regrets trusting a random stranger on social media and giving such a large amount of moneyto her.

# Story 3: Cyber Stalking

Preeti is a beautiful and popular girl in the college.

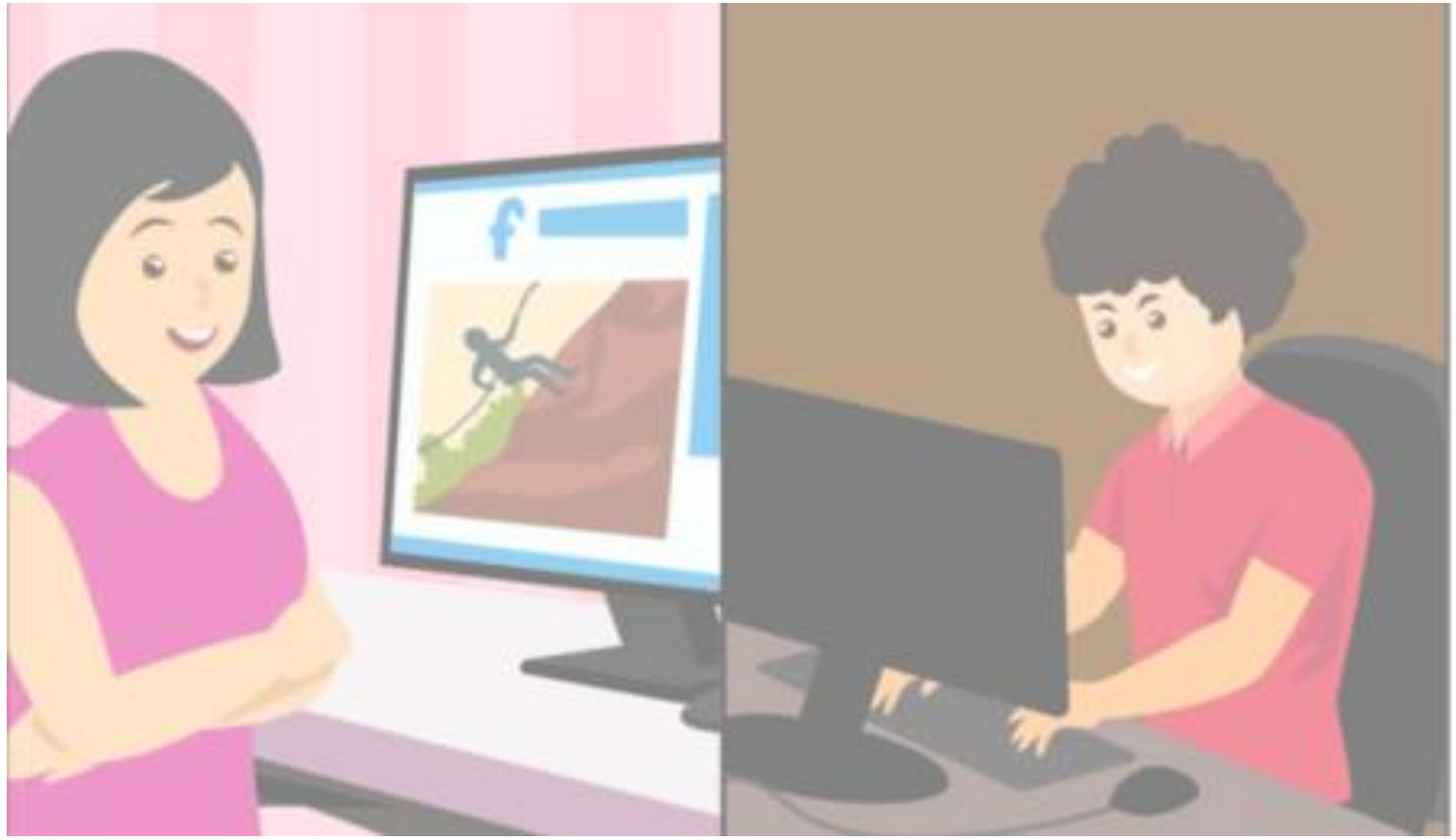
She is active on multiple social media platforms.

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

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

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.



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

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.

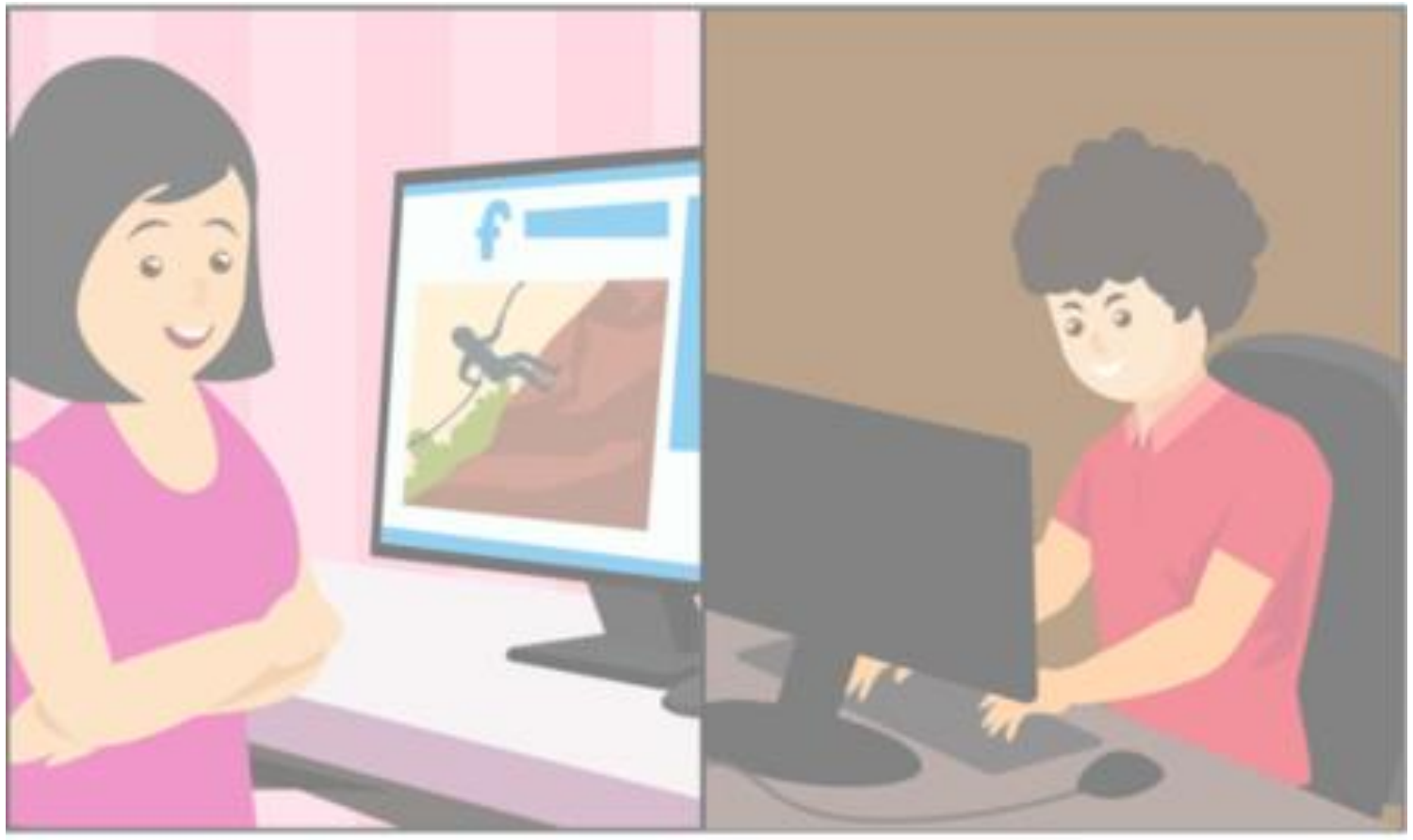
# Story 4: Cyber Bullying

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.

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.

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.



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

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

**How mobile applications can be used for cyber frauds?**

- With the increase in the use of smartphones and the consequent rise in the use of mobile applications, associated security risks have also increased. The number of mobile transactions has increased four times in the last couple of years, and now, cyber criminals are targeting mobile users to extract data and money.
- Mobile applications are widely used not only for entertainment but also for ease and convenience to perform day-to-day tasks such as bill payments, bank accounts management, service delivery etc. As a result, these applications are more prone to cyber-attacks. Users need to be aware of such attacks on commonly used mobile applications such as digital payment applications and gaming applications.

## 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.

# Story 1: Cyber-Attacks using Infected Mobile Applications

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

**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.

(After a few days)

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

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.

**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.

- In case you receive or come across a fraud sms, e-mail, link, phone call asking for your sensitive personal information or bank details, please report it on web portal by visiting **www.reportphishing.in**
- Refer to the latest advisories which are issued by **CERT-IN** on **https://www.cert-in.org.in/**
- Report any adverse activity or unwanted behavior to **CERT-IN** using following channels
- **E-mail :** incident@cert-in.org.in
- **Helpdesk :** +91 1800 11 4949
- Provide following information (as much as possible) while reporting an incident.
  - Time of occurrence of the incident
  - Information regarding affected system/network
  - Symptoms observed

- To report lost or stolen mobile phones, file a First Information Report (FIR) with the police. Post filing the FIR, inform Department of Telecommunications (DoT) through the helpline number **14422** or file an online compliant on **Central Equipment Identity Register (CEIR)** portal by visiting **https://ceir.gov.in**. After verification, DoT will blacklist the phone, blocking it from further use. In addition to this, if anyone tries to use the device using a different SIM card, the service provider will identify the new user and inform the police.

# References


- Wikipedia.org
- Tutorialspoint.com
- TechCrunch.com

# Thank You ! ! !