Volume 1
10 January 2020

Cyber Security
Awareness for Citizens

Issued by
Office of Special Inspector General of Police
Maharashtra Cyber, Home Department
Government of Maharashtra

Knowledge Partner
PricewaterhouseCoopers Pvt. Ltd.

Concept and Advisors

Shri. Brijesh Singh, Inspector General of Police, Government of Maharashtra

Shri. Harish Baijal, Deputy Inspector General, Government of Maharashtra

Shri. Ajay Ambekar, Director Information, Government of Maharashtra

Dr. Balsing Rajput, Superintendent of Police, Government of Maharashtra

Shri. Sachin Pandkar, Superintendent of Police, Government of Maharashtra

Shri. Vijay Khaire, Deputy Superintendent of Police, Government of Maharashtra

Shri. Laxman Kamble, Police Inspector, Government of Maharashtra

Ms. Deepika Singh, CM Fellow, Government of Maharashtra

Ms. Dhrumi Gada, CM Fellow, Government of Maharashtra

Shri. Raunak Maheshwari, CM Fellow, Government of Maharashtra

Shri. Subodh Patil, Artist & Graphics Designer

Uddhav Balasaheb Thackeray
Chief Minister
Maharashtra

Mantralaya
Mumbai 400 032

8th January, 2020

MESSAGE

In this growing digital age, we have become more dependent on the internet for many of our daily activities. There are both advantages and disadvantages of using internet. Everyday, we see new cyber crimes being reported. Though Government agencies are equipped to deal with cyber crimes, it is our duty to take precautions to remain safe.

It is a proven fact that if we are aware about how various cyber crimes are committed, then it helps us to protect ourselves and our family from such frauds. Preventing crimes and protecting women and children in cyber space is the objective of this initiative.

I am happy to know that Maharashtra Cyber is bringing out the Cyber Security Awareness Booklet. I am sure that the tips given in the Cyber Security Awareness Booklet will help you to avoid everyday cyber frauds.

I wish all the best to the Maharashtra Cyber team in their endeavour to keep the state of Maharashtra cyber safe and secure.

Yours truly,

(Uddhav Balasaheb Thackeray)

Tel. : 022-2202 5151/2202 5222, **Fax :** 022-2202 9214
E-mail : cm@maharashtra.gov.in, **Website :** www.maharashtra.gov.in

Acknowledgement

Maharashtra Cyber is a nodal agency for conceptualization and implementation of all the Cyber initiatives/programs for the State of Maharashtra. The department was established by the Home Department of Government of Maharashtra as the Office of Special Inspector General of Police, Maharashtra Cyber, vide GR No. MISC-2015/CR-119/Spl-3A, dated 5th January 2015. Currently, Shri Brijesh Singh – Special Inspector General of Police is the head of this department.

Maharashtra Cyber works closely with district police personnel, cyber-security experts, law enforcement agencies/public prosecutors, pleaders/judicial officials in digital forensics to proactively thwart the cyber threats arising in the State of Maharashtra. As a nodal agency, the department focuses on spreading awareness to the Government officials, corporates & public at large about cyber security and building capability for Maharashtra Police in combating cybercrime.

Maharashtra Cyber would like to acknowledge the contribution made by **Directorate General of Information and Public Relations (DGIPR)** for providing support in publishing this booklet specially Shri. Ajay Ambekar, Ms. Mayura Deshpande and Ms. Reshma Tamboli; **PricewaterhouseCoopers Pvt. Ltd.** for supporting as the Knowledge Partner for this booklet specially Mr. Rahul Aggarwal, Mr. Krishna Sastry, Mr. Vikas Sood, Ms. Nidhi Khator, Mr. Raj Sawant, Mr. Tanmay Barhale, Mr. Dipankar Tripathy, Mr. Chinmay Vaidya and Mr. Akshat Agarwala who have contributed immensely in drafting the content, designing the graphics and managing the entire project from conceptualization to publication of the booklet.

Maharashtra Cyber would also like to thank **BSE Ltd.** for providing the platform to launch this booklet in the Cyber Security Conference, 2020 specially Shri. Shivkumar Pandey.

TABLE OF CONTENTS

IMPORTANCE OF CYBER SECURITY

IMPORTANCE OF CYBER SECURITY

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 cyber-attacks 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.

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.

In this booklet, we will discuss following common types of cybercrimes prevalent today.

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

IDENTITY THEFT

IDENTITY THEFT

What is 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.

Hence, everyone should be aware about identity theft and should know how to prevent it. Let us look at some examples of 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 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.

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.

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 it now.

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.

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 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.

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 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

What are 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.

Let us look at some 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.

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 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 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 : 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.

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.

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.

PSYCHOLOGICAL TRICKS

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 fraudulant e-mail without verifying the details.

TIPS

- 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 FRAUDS

What are 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.

Let us look at some examples of social media frauds.

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.

SOCIAL MEDIA FRAUDS

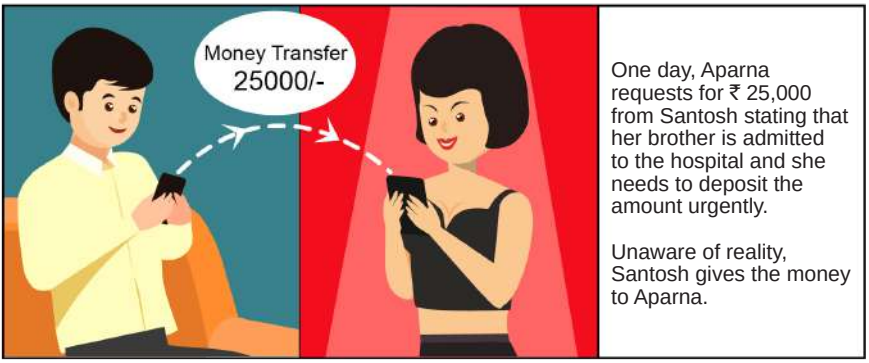
Story 1: Sympathy Fraud

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 woman 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.

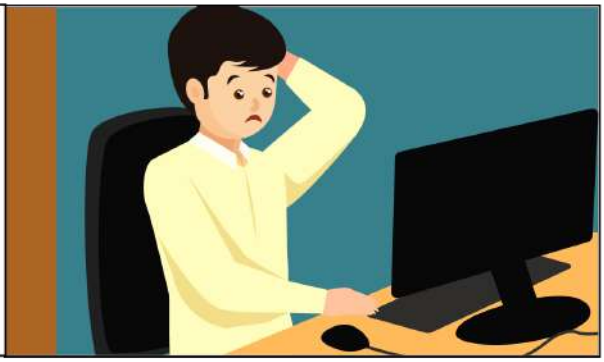


One day, Aparna requests for ₹ 25,000 from Santosh stating that her brother is admitted to the hospital and she needs to deposit the amount urgently.

Unaware of reality, Santosh gives the money to Aparna.

Aparna flees, never to be seen again.

Worried about her whereabouts, 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 money to her.

TIPS

- Be careful while accepting friend request from strangers on social media. Cyber criminals often create fake social media profile to befriend potential victims with an intention to harm them.
- Do not share personal details or get into financial dealings with an unknown person whom you have met on social media platform.
- Keep family/friends informed, in case you plan to meet a social media friend. Always plan such meetings in public places.

SOCIAL MEDIA FRAUDS

Story 2: Romance Fraud

Sadhna likes to surf the internet and has many friends on her social media profile.

One day she receives a friend request from a handsome young man named Vicky. She accepts the friend request as she likes the profile picture.

Sadhna and Vicky start chatting and talking on call all day. Soon, she begins to fall for Vicky and accepts when Vicky proposes to her.

One day, Vicky convinces her into an intimate relationship and takes her to a lodge.

After that day, he breaks up with her. He later blackmails her by demanding money, else he would upload her pictures and videos on social media.

She gets worried and decides to report this in Police Station where the Inspector explains her that she has been a victim of romance fraud.

The Inspector investigates the matter and arrests Vicky.

Sadhna is depressed and regrets befriending a random stranger on social media.

TIPS

- Be cautious while responding to unknown friend requests on social media platforms. Do not respond to unknown friend requests.
- Never share intimate pictures with anyone on online platform as they can be misused later.
- Do not share personal details or get into financial dealings with an unknown person whom you have met on social media platform.

SOCIAL MEDIA FRAUDS

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.

SOCIAL MEDIA FRAUDS

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

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.

Let us look at some day to day example on how mobile applications can be used for cyber 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

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.

ONLINE BANKING FRAUDS

ONLINE BANKING FRAUDS

What are Online Banking Frauds?

Nowadays, all banking services are shifting online. Services like retrieving account statement, funds transfer to other accounts, requesting a cheque book, preparing demand draft etc. can all be done online. Most of these services can be done sitting at home without physically visiting the bank. As the services are shifting towards online platforms, cyber frauds related to banking are also increasing. Just like we protect our locker full of jewelry with a lock and key, we must protect our online bank accounts with strong passwords. If the key is stolen, then the jewelry will be stolen. Similarly, if the password is stolen, then the money in the bank accounts will be stolen. Hence, protection of bank accounts with strong passwords becomes highly essential.

Let us look at some examples of online banking fraud.

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.

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.

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.

John losses all the money in his account.

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

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.

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.

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)

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

Although Ramesh got captured, Reena hadn't recovered from the shock that the money from her bank account was stolen.

(Two days later)

Jayesh : Thank you for leaking the question paper for today's exam. It was really helpful.

Reena : What! I did not leak the question paper!

Jayesh : It is uploaded on your profile on the social media.

Reena reports the incident to the college authorities and Police Station.

The Inspector explains that her social media account was also hacked as she had kept the same password for bank account and social media account.

Reena regrets that she kept the same password for bank account and social media accounts. She then changes credentials of all other accounts.

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 on Personal Computers/Laptops

Personal Computers or laptops play a very important role in our lives. We store our crucial information such as bank account numbers, business documents etc. in the computer. We also store personal files like photos, music, movies etc. in the computer. Therefore, protection of all this data is highly essential. Just as we keep a physical lock on our safe vaults, it is equally important to protect our valuable data from viruses/malicious applications that can damage it.

Let us look at some examples on how our personal computer can get affected by virus.

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 through external devices

I need to take print out of a few documents. Let me put the documents in a USB drive and go to a cybercafé.

Ramesh goes to a cybercafé to take print out of his documents.

Ramesh plugs in the USB drive and takes the print out. He is unaware that the computer in cybercafé is infected with virus.

As a result, the USB drive too is now infected with virus.

Ramesh goes back home.

Oh! I need to take more print outs, let me put more documents in the USB drive.

Ramesh connects USB drive to his computer. The virus gets transferred to his computer.

The computer slows down due to virus infection.

Ramesh loses his personal photos, videos, games, scanned documents, health reports and other important documents.

Ramesh regrets that he did not install an anti-virus software in his computer.

TIPS

- Computers/Laptops should have a firewall and anti-virus installed, enabled and running the latest version.
- Always scan external devices (e.g. USB) for viruses, while connecting to the computer.
- Always keep the “Bluetooth” connection in an invisible mode, unless you need to access file transfers on your mobile phone or laptops.
- Before disposing of computers or mobile devices, be sure they are wiped of any personal information. For mobile devices, this can be done by selecting the option for a secure reset/factory reset of the device.

VIRUS ATTACK ON PERSONAL COMPUTER

Story 2: 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?

Rohit : Of course, it is! Download it and check it out yourself.

Mohit downloads the music album from un-trusted website.

Unfortunately, his computer gets infected with virus.

Mohit regrets downloading files from un-trusted website.

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 3: 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.

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.

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.
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.

INCIDENT REPORTING

INCIDENT REPORTING

Where to Report a Cyber Fraud?

1. Visit the nearest police station immediately.
2. To report cybercrime complaints online, visit the **National Cyber Crime Reporting Portal**. This portal can be accessed at **https://cybercrime.gov.in/.** In this portal, there are two sections. One section is to report crimes related to Women and Children (where reports can be filed anonymously as well). Another section is to report other types of cybercrimes. You can also file a complaint offline by dialing the helpline number **1930** .
3. 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 **Maharashtra Cyber's** web portal by visiting **www.reportphishing.in**
4. Refer to the latest advisories which are issued by **CERT-IN** on **https://www.cert-in.org.in/**
5. 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
6. 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.

NOTES

Disclaimer

This booklet is designed solely to provide helpful information and general guidance on the themes discussed and should not be used as a substitute for any legal or professional advice. The names, characters, entities, places and incidents have been used entirely in a fictitious manner. Any resemblance to real persons, either living or dead, is purely coincidental.
This booklet includes certain material from third party sources and the copyright in such third party content continues to be owned by the respective third parties. While best efforts have been used in preparing this booklet, the publisher makes no representations or warranties of any kind and assumes no liabilities of any kind with respect to the accuracy, completeness of the contents and specifically disclaim any implied warranties of merchantability or fitness of use for a particular purpose or of the results obtained from the use of the information provided herein. In no event shall the publisher nor its associated partners be held liable or responsible to any person or entity with respect to any loss or incidental or consequential damages caused, directly or indirectly to the user or anyone else, by the information contained herein or for any action taken or omitted by placing reliance on the information contained herein.

be
Cyber Smart
be
Cyber Safe

This initiative is supported by
PricewaterhouseCoopers Pvt. Ltd.