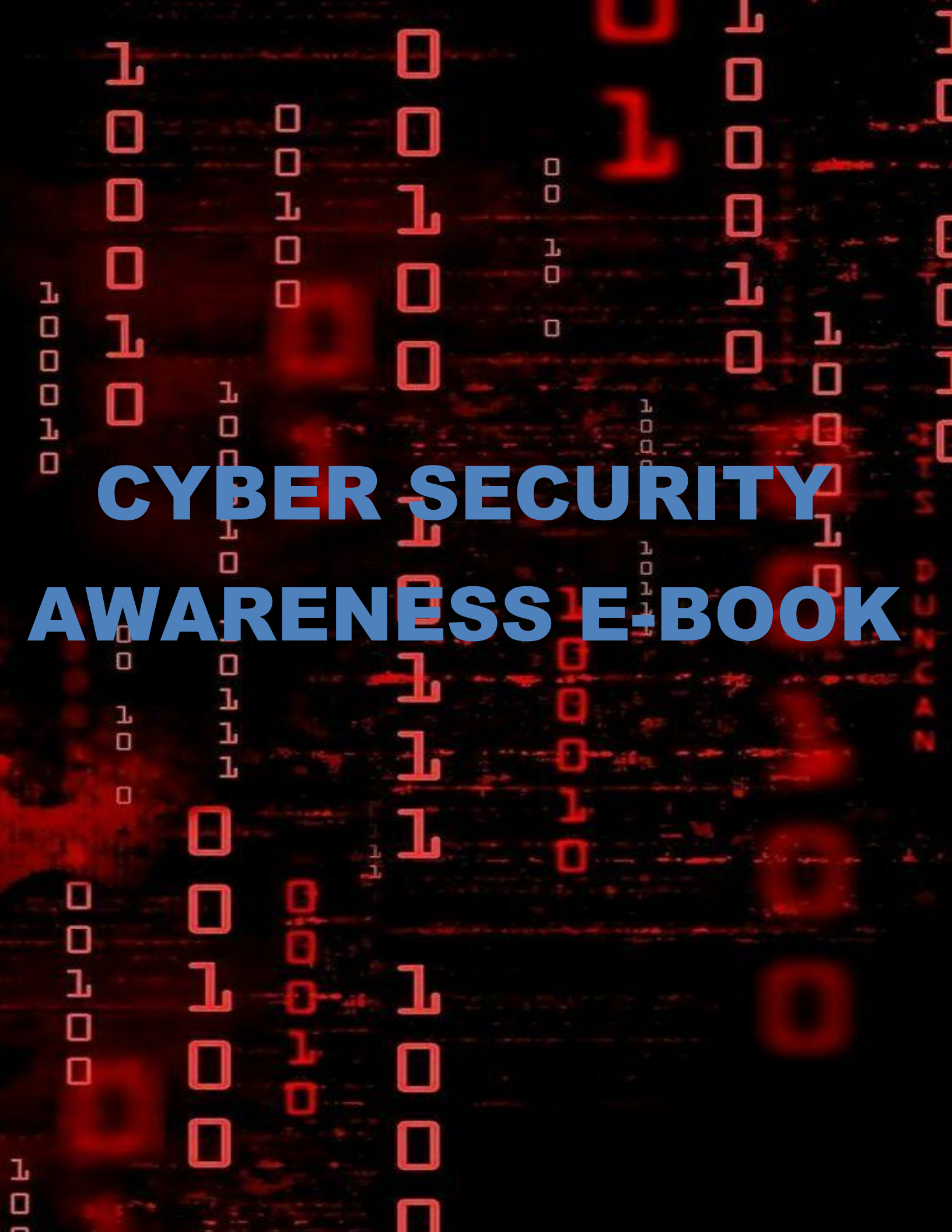

CYBER SECURITY
AWARENESS E-BOOK

# ABOUT THE E-BOOK

Information & Communication Technology has become an integral part of our day to day life. It has changed the way we connect with friends, find jobs, find matches for marrying, run businesses, play games, do shopping and so on. With the cheap availability of broadband and smart-phones, almost everyone has access to the cyber space, connecting virtually to millions of online users across the globe. Increasing use of cyber space has also made us vulnerable to cybercrime threats. A minor lapse/negligence in managing our digital life can open the doors for cybercrimes and hence can lead to financial loss, damage to reputation, harassment etc. So, we must be vigilant and careful while connecting digitally to the outside world whether for financial transactions, social networking, playing games or searching things on the internet etc.

The information provided in this handbook is intended to create awareness among citizens about various cyber threats that can impact them and provide some tips to safeguard themselves against cybercrimes.

The initial part of the booklet depicts the different types of cybercrimes being reported these days, categorized as per their *modus operandi.* For cybercrime of each *modus operandi*, we have given its brief description in the box at the top. Below that, is a pictorial representation of how cyber criminals commit that particular cybercrime on the victim. We have tried to keep it simple so that even a common man can understand it. At the bottom of the page are the tips/possible ways by which one can avoid the particular cybercrime/fraud.

There might be certain overlapping tricks found in the various types of cybercrimes explained in the handbook. Still they have been discussed separately because cyber criminals apply some common tricks with very subtle differences because of which many people become victims.

# TABLE OF CONTENTS


| Sr No. | Topic | Page No. |
|---|---|---|
| 1. | **Importance of Cyber Security** | 4 |
| 2. | **Social Engineering Frauds** | 5-14 |
| | • CVV/OTP Sharing Fraud | 5 |
| | • UPI Phishing Fraud | 6 |
| | • Fraud by Request Money QR Code/Link on Google Pay/PhonePe/Paytm | 7 |
| | • Fraud During Covid-19 Pandemic | 8-9 |
| | • Fraud through Google Docs App | 10 |
| | • Fraud using Olx/E-commerce Platforms | 11 |
| | • Fraud through Fake Cashback Offers | 12 |
| | • Fraud through Screen Sharing Apps | 13 |
| | • SIM Card Swapping Fraud | 14 |
| 3. | **Financial Frauds using Social Media Platforms** | 15-16 |
| | • Fraud using Fake Social Media Account | 15 |
| | • Sextortion on Facebook | 16 |
| 4. | **Other Cyber Crimes using Social Media Platforms** | 17-19 |
| | • Harassment through Fake Social Media Profiles | 17 |
| | • Cyber Bullying | 18 |
| | • Cyber Stalking | 19 |
| 5. | **Other Cyber Crimes/Frauds** | 20-29 |
| | • ATM/Debit Card Cloning | 20 |
| | • Edited Google Customer Care number Fraud | 21 |
| | • Ransomware Attacks | 22 |
| | • Juice Jacking | 23 |
| | • Lottery Fraud/ Nigerian Fraud | 24 |
| | • Online Job Fraud | 25 |
| | • Computer or Device Hacking | 26 |
| | • Mobile Application Fraud | 27 |
| | • Remote Access Application Fraud | 28 |
| | • Matrimonial Frauds | 29 |
| 6. | **Cyber Safety Tips for Children, Parents and Women** | 30-35 |
| 7. | **General Cyber Safety Tips** | 36-39 |
| 8. | **How to make a Complaint to Police** | 40 |

# 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.

# SOCIAL ENGINEERING FRAUDS

## CVV/OTP SHARING FRAUD

Cyber criminals posing themselves as bank /RBI officials call people and tell them that their ATM card has been blocked or their KYC (Know Your Customer) is not updated or their Aadhaar is not linked to their bank account & hence their account will be blocked. Then on the pretext of updating the KYC/linking bank account to Aadhaar or for resuming the services of ATM card/activation of new ATM card asks for details related to victim's bank account like ATM card number, CVV number, OTP etc. After these details are shared by victim, money is siphoned off from the victim's bank account.

**TIPS**

- Remember bank never asks for card number/CVV number/OTP.
- Never share the ATM card number, CVV, OTP or any other confidential banking credentials with anyone over a phone call/SMS/WhatsApp.
- E-mail should not be shared as this may lead to activation of Internet banking by cyber criminals, leading to siphoning off of one's money.

# UPI PHISHING FRAUD

On the pretext of helping in banking related issues, fraudsters ask victims to forward an alphanumeric link to a particular number (depending upon the bank associated with the victim) from their registered mobile number. Once it is done, cyber criminals install the UPI wallet of the victim (using Wi-Fi) bypassing the SIM binding process onto their own mobile phone, thus gaining access to the victim's bank accounts linked to the registered mobile number.

*Fraudsters call people on the pretext of updating KYC/Aadhaar & link his account to UPI by convincing him to share the alphanumeric link & OTP to a particular number associated to the bank of the victim*

*Victim shares link & OTP*

*Fraudsters get access to the UPI wallet which is linked to victim's bank account. Fraudsters set MPIN also*

*Fraudsters use the victim's account as their own*

*Victim duped of money in his bank account until he gets his account blocked*

**TIPS**

- Never share any OTP or link to any number given by someone calling oneself as bank /RBI officials.
- People calling to customer care number of airlines/e-commerce entities obtained from Google search for rescheduling flights/getting refunds etc. have become victims of such frauds following their instructions. Never do that.

## FRAUD BY REQUEST MONEY QR CODE/LINK ON GOOGLE PAY/PHONEPE/PAYTM

Cyber fraudsters send debit links or QR codes to victims to scan and receive money in their bank accounts through Google Pay/PhonePe/Paytm. But instead of receiving money, it actually gets debited from the victim's account as fraudsters actually send a request money QR code/link.

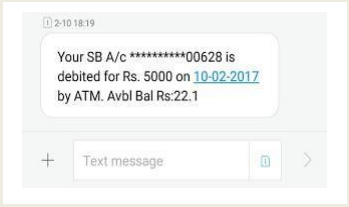
*Fraudster calls the vendors or any shopkeeper or businessman & requests for Google Pay or PhonePe registered mobile number for making payment*

*Victim shares registered mobile number & receives a request money link or QR code*

http://8629a7f1.ngrok.io

OR

*The QR code is tampered with to make it look like as if it is for credit though actually it is for debit*



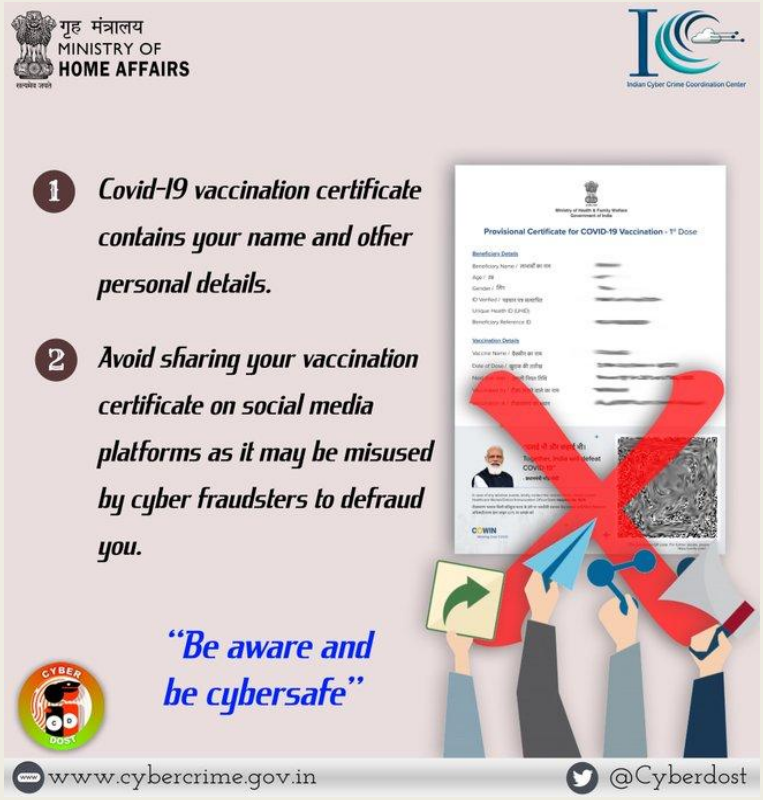

*Victim ignores the text message received on the registered phone number with one's bank account*

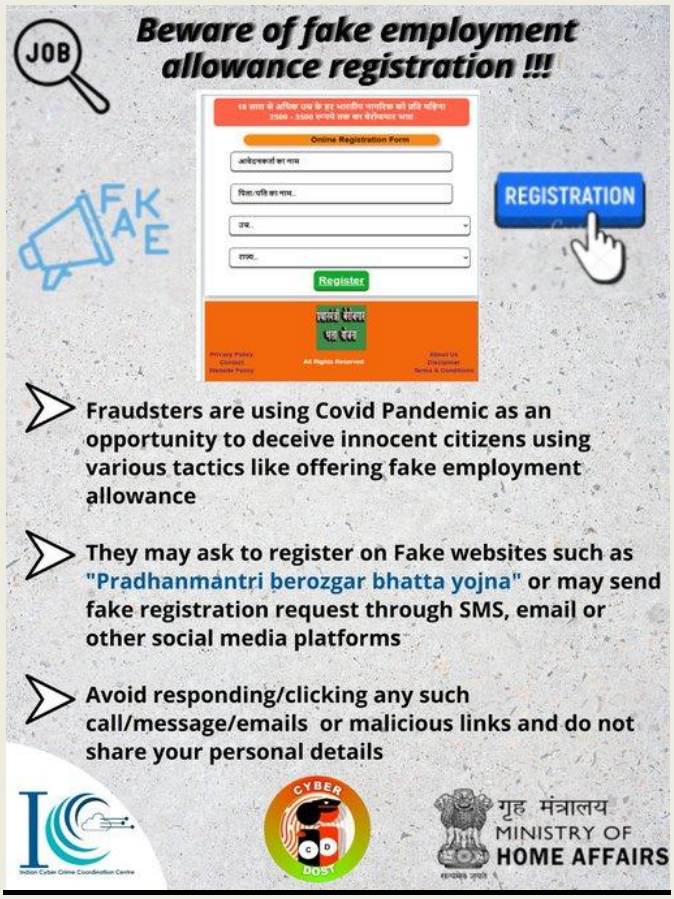
*Instead of recieving money, victim ends up paying to the fraudster via request money QR code or link*

**TIPS**

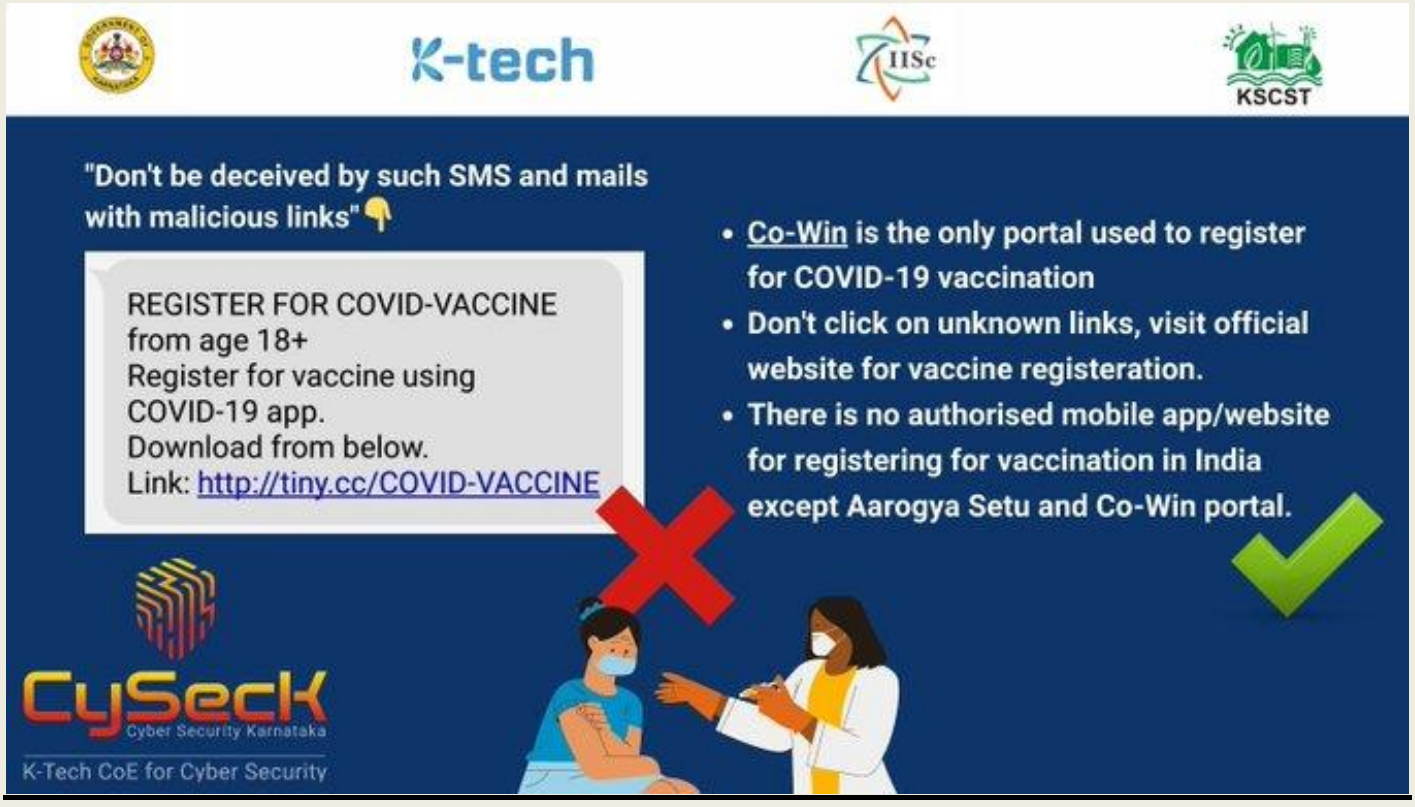
- Never accept/click on any link or scan any QR code from unverified sources as they may send you a manipulated one.
- For receiving money, there is no need to enter MPIN or UPI PIN.

# FRAUD DURING COVID-19 PANDEMIC



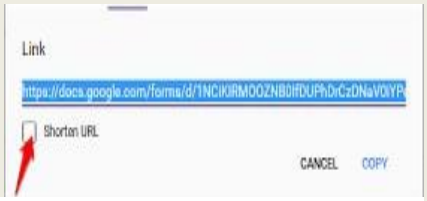

Beware of fake employment allowance registration !!!
JOB
FAKE
REGISTRATION
Online Registration Form
Register
Fraudsters are using Covid Pandemic as an opportunity to deceive innocent citizens using various tactics like offering fake employment allowance
They may ask to register on Fake websites such as "Pradhanmantri berozgar bhatta yojna" or may send fake registration request through SMS, email or other social media platforms
Avoid responding/clicking any such call/message/emails or malicious links and do not share your personal details
CYBER DOST
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

बेरोजगारी भत्ता योजना" धोखाधड़ी
JOB
FAKE
REGISTRATION
Online Registration Form
Register
साइबर अपराधी इस महामारी का इस्तेमाल, मासूम/अनभिज्ञ लोगों को फर्जी रोजगार भत्ता की पेशकश कर, ठगने के अवसर के रूप में कर रहे है ।
वे लोगों को "प्रधानमंत्री बेरोजगारी भत्ता योजना" जैसी नकली वेबसाइटों में पंजीकरण करने के लिए कह सकते हैं या एसएमएस, ईमेल या अन्य सोशल मीडिया प्लेटफॉर्म के माध्यम से फर्जी पंजीकरण अनुरोध भेज सकते हैं।
इन नकली वेबसाइटों से सतर्क रहें और किसी भी कारण से संदिग्ध होने पर अनजान कॉल/संदेश/ईमेल आदि का जवाब न दें और अपनी व्यक्तिगत जानकारी साझा न करें।
CYBER DOST
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

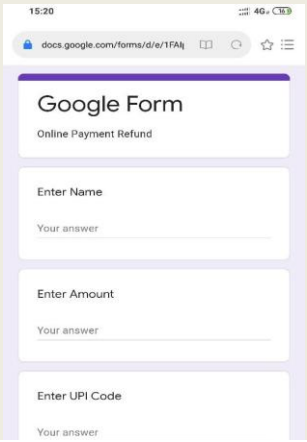

K-tech
IISc
KSCST
"Don't be deceived by such SMS and mails with malicious links"
REGISTER FOR COVID-VACCINE
from age 18+
Register for vaccine using
COVID-19 app.
Download from below.
Link: http://tiny.cc/COVID-VACCINE
Co-Win is the only portal used to register for COVID-19 vaccination
Don't click on unknown links, visit official website for vaccine registeration.
There is no authorised mobile app/website for registering for vaccination in India except Aarogya Setu and Co-Win portal.
CySecK
Cyber Security Karnataka
K-Tech CoE for Cyber Security

# FRAUD USING GOOGLE DOCS APP

Apps for online forms like Google Docs etc. are widely used to collect data. Fraudsters take advantage of such applications and misguide the victim to fill or submit his/her confidential bank related data like ATM number, UPI PIN, password etc. As soon as they fill up the form and submit their data, it is directly transferred to the creator of the form.




*Cyber criminals send a link for Google Docs form. They mislead you by writing it is for money refund*




*Cyber criminals misguide the victim to fill or submit his/her confidential bank related data like ATM number, UPI PIN, passwords etc.*

*As soon as the victim submits the form, confidential data is received by the cyber fraudster*

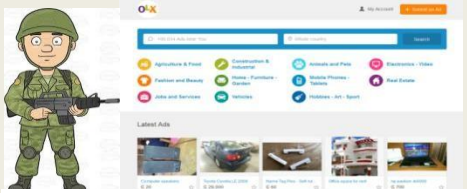
*Cyber fraudster then siphons off money from the victim's bank account using the credentials*

**TIPS**

- You are advised to never share confidential banking details in online forms like Google Docs.
- Bank never asks their customers to fill such forms.

# FRAUD USING OLX/E-COMMERCE PLATFORMS

Cyber fraudster uses the e-commerce platforms like Olx/Quikr/Facebook for giving fake advertisements to sell commodity at lucrative prices. When someone intends to buy, cyber fraudster asks for advance payment in the form of packaging/transportation/registration charges etc. Buyer pays the money believing him/her to be a real seller and the fraudster disappears with the money. Frauds are also committed by cyber criminals posing themselves as buyers to real sellers. In this *modus operandi*, cyber criminals get the seller's account debited on the pretext of paying advance money by sending request money link/QR code instead of the credit link/QR code.

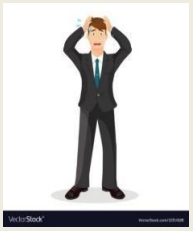


*Army/para-military force personnel upload commodity (vehicle/fridge /mobile phone etc.) to be sold on Olx /Quikr/Facebook etc.*

*Cyber criminals contact these personnel & get their id proof, canteen smart card and other documents on the pretext of buying the advertised item*

*Fraudsters then use the id proof & other documents of army/para-military force personnel as their own & post fake adv for sale on Olx /Quikr/Facebook etc.*

*Buyer seeing attractive price himself contacts the fraudster assuming him as army/para-military force personnel*



*On the pretext of GST/transportation charge/packaging charge/registration charge /other advances, fraudster keeps duping the victim of his/her money until the victim realizes the fraud*

**TIPS**

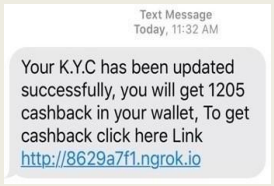
- Never pay advance money without seeing the article physically and meeting the seller in person.
- For receiving any type of payment via link or QR code, there is no need to enter MPIN or UPI PIN.
- Always remember entering MPIN or UPI PIN is required only for paying money.

# FRAUD THROUGH FAKE CASHBACK OFFERS

Fraudsters lure victims by offering cashback offers from PhonePe/Google Pay etc. and request the victims to click on a request money link or scan a QR code to avail the same. Once the link is clicked or QR code is scanned, money is debited from the victim's bank account instead of being credited as he enters MPIN or UPI PIN. Link can be of type http://8629a7f1.ngrok.io or SMS 1533c608933b85f448a7428b4365a042ae6

*Fraudsters lure victims by offering cashback offers*

OR




OR

OR

*Do not get confused by what is displayed here*

*Fraudsters mislead by editing the QR code by writing "payment refund", "money receive" etc. instead of "pay"*

*Victims don't pay attention to what is written here*

*Instead of receiving money, victim himself/herself pays to the fraudster via a request money link or QR code after entering MPIN/UPI PIN*

**TIPS**

- Never forward /click on any suspicious link from unverified sources.
- Remember the thumb rule: You need to enter MPIN or UPI PIN only for debiting money from your account; it is never required for receiving money.

# FRAUD USING SCREEN SHARING APPS

Cyber fraudsters on the pretext of aiding or citing the policy of a company guide the victim to install screen sharing apps like Quick Support/TeamViewer/AnyDesk etc. and thus get control of the victim's phone, thereby getting access to banking credentials like OTP/MPIN/username/password for internet banking etc. The fraudster then siphons off money from the victim's account using those credentials. By the time the victim realizes it, a lot of money is already siphoned off.

*People contact fake customer care number of bank or e-commerce platforms after searching it from Google search engine*

*AnyDesk*

OR

*Quick Support*

OR

*Victim shares the code with the fraudster*

*Fraudster gets access to the victim's phone & steals banking credentials*

*Fraudster, posing as a customer care operator, asks the victim to install any of the above screen sharing apps and share the code to allow victim's screen access to help him*

*Fraudster transfers money to his account without the need of sharing the OTP by the victim*

**TIPS**

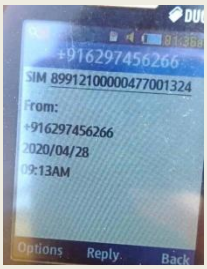
- Never install any screen sharing app when asked to do so over a phone call by customer care/help desk representative of any entity.
- Banks/E-commerce entities etc. never ask to install third party application for screen sharing.

## SIM CARD SWAPPING FRAUD

It is a type of identity theft where cyber criminals manage to get a new SIM card issued for your registered mobile number through the Telecom Service Provider. With the help of the new SIM card, fraudsters get OTP & other confidential details required for financial transaction from your bank account.

*Cyber criminals get a blank SIM card from retailer, who is also a gang member*

*Cyber criminals call the victim pretending as customer care executive of a TSP, to initiate 4G SIM upgradation by themselves otherwise services of their SIM will get blocked*




*In furtherance of their fraud, cyber criminals provide one SIM no. & ask the victim to send that SIM no. through SMS to customer care number to avail the services*

*Victim forwards the SIM no. from his mobile phone considering the fraudster as genuine customer care operator of the TSP*

*The TSP closes the services of victim's old SIM and issues the victim's mobile number to the blank SIM card*

*Now, the cyber criminal is able to access all the bank account details linked to the victim's mobile number and withdraws the money*

**TIPS**

- Never share any information related to your account and SIM over a phone call. The 20-digit SIM number mentioned on the back of the SIM is a very sensitive data.
- If your mobile number is inactive/out of range for a few hours, enquire from your mobile operator immediately.
- Register for regular SMS as well as e-mail alerts for your banking transactions (this way, even if your SIM is de-activated, you shall continue to receive the alerts via your email).

# FINANCIAL FRAUDS USING SOCIAL MEDIA PLATFORMS

## FRAUD USING FAKE SOCIAL MEDIA ACCOUNT

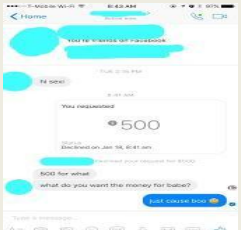
Fraudsters target accounts on popular social media platforms like Facebook and Instagram. They commit fraud by creating a similar fake account of the target profile and requesting his/her friends for instant money transfer citing some medical emergency etc. Target profile's friends transfer the money considering him/her as his/her friend. By the time the target profile comes to know of it, many of his friends become victims of the fraud. Similar fraud is also committed by hacking the target account.

*A similar profile of target social media account is created by a fraudster*

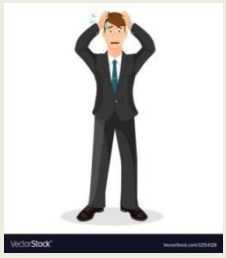
*Original Facebook profile*

*Fake Facebook profile created using the same display picture*

*Sends request to those who are in the friend list of the impersonated account*




*Imposter contacts those in the friend list of impersonated account via Messenger & then requests for money on the pretext of some medical emergency. He provides PhonePe/Google Pay/Paytm account or a bank account for making payment*



*If anyone sends money without verifying from one's friend, he/she becomes a victim of the fraud*

**TIPS**

- Keep the privacy setting as "My friends" only.
- Before transferring the money requested via Facebook, WhatsApp or other social media account, verify the authenticity of the message by meeting the concerned person or calling him.
- Turn on 2-step verification for all your social media accounts.
- Keep your password strong and maintain the privacy of the password.

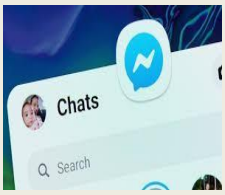
# SEXTORTION ON FACEBOOK

Live video chat is done on Facebook via Messenger by cyber criminals posing as female. Cyber criminals convince the victim for video call in compromising positions, following which fraudsters take screenshots of the same or do screen recording of the video call. Cyber criminals then threaten the victim to circulate the photographs/videos in compromising positions on various online platforms, if the demanded money is not paid.

Or

*Cyber criminal sends friend request on Facebook based on the videos and posts liked by you*

*Many a times cyber criminals advise the victim to download several types of video chat applications*




*After several chats, cyber criminal convinces the victim to come for video calling*

*Cyber criminal seduces the victim to go naked and then saves the screenshot or screen recording of ongoing video call in which the victim is nude*

*Cyber criminal starts blackmailing victim & extorts money or else threatens to upload naked photo on porn websites, YouTube etc.*

*Person sends money in fear and becomes a victim of blackmailing & extortion*

**TIPS**

- Avoid friendship with unknown people on social media platforms.
- Never make video calls to unknown people on Facebook or any other social media platform.

# OTHER CYBER CRIMES USING SOCIAL MEDIA PLATFORMS

## HARASSMENT THROUGH FAKE SOCIAL MEDIA PROFILES

Cyber criminals morph the photographs of the victim which they get from social media and upload it on social media platforms. After that they demand money to remove the morphed pictures from social media. Victim falls prey to the trap and transfers the money.

*Victim usually accepts all the friend requests without knowing the person sending it.*

*OR*

*Because of poor privacy settings of the victim's account, everyone has access to his/her photographs or posts on social media platforms which cyber criminals take advantage of*

*Cyber criminals download photographs and create a fake account impersonating the victim and upload the morphed obscene photographs etc. harassing the victim*

**TIPS**

- Social media sites offer privacy settings to manage who can view your posts, photos, or send you friend request etc. Restrict access to your profile.
- Ensure your personal information, photos and videos are accessible only to your friends.
- Refrain from making friendship with unknown persons over social media platforms.

## CYBER BULLYING ON SOCIAL MEDIA

Cyber bullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms etc. It is a sort of repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Examples include: spreading lies about or posting embarrassing photos of someone on social media, sending hurtful messages or threats via messaging platforms, impersonating someone and sending mean messages to others on his/her behalf.

*Perpetrators of cyber bullying (usually known to the victim) get the personal photographs and details of the victim from various social media sites*

*Perpetrators of cyber bullying create a fake account either in the name of the victim or a random name & post several memes and videos making fun of the victim, which goes viral*

**TIPS**

- Learn about the privacy settings of the social media apps being used by you.
- Ensure your personal information, photos and videos are accessible only to your trusted ones.
- Think twice before posting or sharing anything online – it may stay online forever and could be used to harm you later.
- Make your children aware that cyber bullying is a punishable crime so that neither do they indulge in cyber bullying nor do they let anyone bully them.
- Report hurtful comments, messages and photos and request to the concerned Social Media Platforms to remove them. Besides 'unfriending', you can completely block people to stop them from seeing your profile or contacting you.

## CYBER STALKING

Cyber stalking is online stalking. It involves the repeated use of the internet or other electronic means to harass, intimidate or frighten a person or group. Common characteristics of cyber stalking may include false accusations or posting derogatory statements, monitoring someone's online activity or physical location. Cyber stalkers may use email, instant messages, phone calls, and other communication modes to stalk you. Cyber stalking can take the form of sexual harassment, inappropriate contact or an unwelcome attention in your life and your family's activities.

*Victim uses check in feature of social media to inform one's friends and followers about his/her whereabouts (locations, places) and also about one's future plans on social media platforms*

*Stalker keeps a watch on the posts of the victim*

*Stalker takes advantage of the future whereabouts of the victim and intimidates or frightens him/her when the opportunity is ripe*

**TIPS**

- Be careful while uploading your personal information, photos and videos on social media. Ensure that these are accessible only to your trusted ones.
- Never add unknown people to your friend list.
- Review all the privacy and security settings of social media and restrict them to "my friends only''.

# OTHER CYBER CRIMES/FRAUDS

## ATM/DEBIT CARD CLONING FRAUD

Each ATM/debit card has a magnetic strip in it containing confidential data. Cyber criminals use a skimmer machine to read this strip and capture the confidential data related to the card. Then they copy the data onto a blank card, which is used for fraudulent transactions. They use overlay devices/pin-hole camera/ spy camera or peep from behind in the queue to read ATM/Debit card PIN while it is being entered by the user on the ATM keypad/POS machines.

*Data of ATM card skimmed while withdrawing money from ATM kiosk & Cyber Criminal stealing the PIN by peeping from behind*

*Cyber criminals rewrite the ATM card data on a blank ATM card, thus cloning. Nowadays, they are also cloning ATM/debit card data by guessing the card number & PIN*

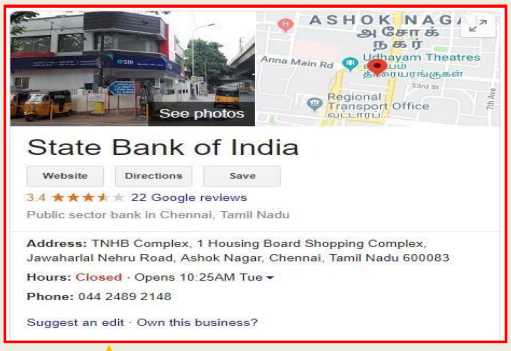
*Withdraws money using cloned card and peeped PIN from far off ATM kiosks*

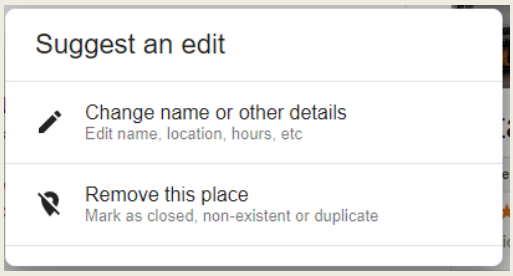
**TIPS**

- Enter the PIN yourself taking due care to hide the PIN (as in image 1).
- Check for hidden cameras/skimmer devices while withdrawing cash (as in image 2).
- Physically check the keypad to ensure it does not have an overlay device.
- Do not allow anyone to stand beside or behind you while carrying out transaction with ATM/Debit card/Credit card.
- Do not keep a PIN which can be guessed easily. Keep changing your PIN.
- Ensure you get transaction receipt or confirmation through SMS.
- Ensure that any part of the ATM machine is open or loosely attached.

## EDITED GOOGLE CUSTOMER CARE NUMBER FRAUD

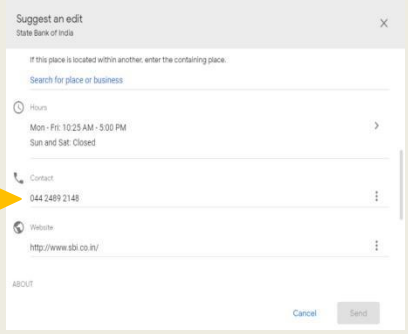
Cyber fraudsters edit the customer care number of banks/airlines/food outlets/e-commerce entities etc. on Google page and customize it in such a manner that whenever someone searches on Google for the customer care number, the edited number of cyber criminals appears on top of the search results for that entity. Victim ends up calling the fraudsters instead of the real helpline numbers. The fraudsters portraying themselves as helpers actually give instructions to dupe the caller victim.




*Fraudsters take benefit of "Suggest an edit" option on the Google page*

*Fraudsters feed their own number as the bank's helpline number. People call on the edited number assuming it as genuine & get defrauded by following their instructions*




**TIPS**

- Always search for customer care number from the official website of the banks/airlines/food or retail outlets/other e-commerce entity and not by searching the entity name on Google search.
- Toll free number for any bank is given on back/flip side of debit/credit card. Call on the given numbers only.
- Always remember that Google does not give verified information on searches.

# RANSOMWARE ATTACKS

Ransomware is a category of malicious software which, when run, disables the functionality of a computer in some way. The ransomware program displays a message that demands payment to restore functionality. The malware, in effect, holds the computer system to ransom. In other words, ransomware is an extortion racket. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.

*Cyber criminals send an email to the victim containing suspicious attachment or phishing links. Victim downloads the attachment and opens the file*

*Once the infected file is opened, victim's system gets locked and all files get encrypted. Alert message on computer screen demands ransom to be paid to unlock the screen or encrypted data*

**TIPS**

- Do not open emails from unknown sources containing suspicious attachment or phishing links.
- Keep your antivirus up-to-date and windows firewall turned on and properly configured.
- Back up your most important files on a regular basis. Keep the important data on a separate hard disk.
- Have proper spam filters enabled in your e-mail account.

# JUICE JACKING

Juice jacking is a kind of cyber fraud where data is copied from a smart phone, tablet or other electronic devices using a USB charging port that is actually used for both data connection and charging. The victim believes it to be a charging port only.

*Hacker uses the same charging point to steal data through USB port using data cable*

*Victim's mobile/device plugged into a charging port at a public place*

*This type of stealing of data from the victim's mobile is called Juice Jacking*

**TIPS**

- Disable data transfer on your phone while charging.
- Switch off your device before charging in public places.
- Carry your own portable power pack/bank.
- Can buy a data disabled charging cable.

## LOTTERY FRAUD/NIGERIAN FRAUD

Cyber fraudsters send e-mails/SMSs informing the recipient (victim) that he/she has won a lottery/prize worth millions of rupees/dollars and the recipient only needs to click on the link sent on their e-mail/mobile phone or to tell how they want to receive the prize money. However, on responding positively, the recipient is asked to pay money in the name of registration/shipment/service charges, GST etc. one after the other for releasing the prize money. This way the recipient keeps on paying the fraudsters until he/she realizes the fraud. The fraudsters were initially mainly from Nigeria and hence the terminology.

*Fraudsters give information through email/SMS/call to the victim about the prize money won by them through lottery*

*If the victim replies positively, fraudsters then ask how they would like to receive the prize money*

*On telling the mode of receiving, they then ask for registration/shipment /service charges, GST etc. for releasing the prize money*

*The person (victim) falls into the trap and sends the money to the fraudster one by one until he/she realizes the fraud*

**TIPS**

- Never respond to calls/SMSs/e-mails related to winning a lottery/prize or seeking personal or financial details.
- Have proper spam filters in your email account to stop receiving unsolicited emails.
- Follow the thumb rule: Never transfer funds to unknown persons or entities in promise of higher returns/winning prizes or lottery.

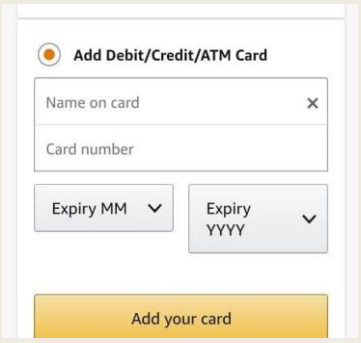
# ONLINE JOB FRAUD

Cyber criminals advertise fake job offers using various platforms either online via fake websites. Victim, in search of a job, goes through these fake job offers and contacts the cyber criminal. Upon contacting cyber criminals, victim is asked to pay registration fee or make an advance payment (which they claim is refundable) to avail their services for getting a job. Victim transfers the money and follows the guidelines of the fraudster for getting a job and falls prey to the cyber crime. In some cases, a fake website phishes financial data through a fake payment channel.

*People share their data on different websites or social media platforms in search of jobs*

*Cyber criminals contact victims using these data and in the name of providing a good job, they demand money such as registration fee, service charge, etc. while never intending to provide a job*

*OR*




*Tech-savvy cyber criminals create fake websites to steal financial details through fake payment channels*

*Victim ends up losing/paying money for a job which didn't exist*

**TIPS**

- To avoid such frauds, it is necessary to submit your application to a registered website only.
- Do not make any advance payments for getting a job.

## COMPUTER OR DEVICE HACKING

Hacking is the act of gaining access to a computer/device without legal authorisation. Cyber criminal uses various methods for hacking a victim's computer/device such as infecting a computer/device by a virus or malware. Hacking may lead to data corruption/deletion or data loss or stealing of data.

*Cyber criminals send malicious attachments to the victim hidden in the form of attractive advertisements*

*Victim downloads the attachment or apps from an un-trusted website after which his /her computer/device gets infected with the virus*

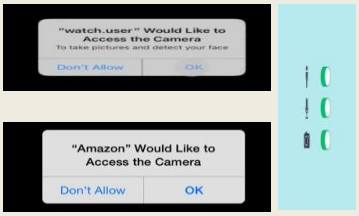
*Victim has not installed any antivirus into his system and ignored the standard security features. Victim's system starts working slowly and later he loses his personal photos, videos and other important document*

**TIPS**

- Computers/laptops should have a firewall and antivirus installed, enabled and updated with latest versions.
- Never download or install pirated software, applications etc. on your computer, laptops or hand- held devices.
- Always scan external devices for viruses, while connecting to the computer.
- Be careful while browsing through a public Wi-Fi and avoid logging in to personal and professional accounts while using public Wi-Fi systems.

## MOBILE APPLICATIONS FRAUD

Mobile applications may be mediums of cyber-attacks, stealing of confidential data or mode of getting access to the controls of your phone/device. People download mobile applications from unknown sources ignoring security warnings. These applications may have viruses which pass sensitive information or give control of your phone/device to some outside agent, who gets access to your contacts, passwords, financial data etc. Several mobile applications from unknown sources ask for unnecessary permissions for access to your phone/device, which one grants without due diligence. Thus, these mobile applications can access a huge amount of personal information, photographs etc. from your phone/device.



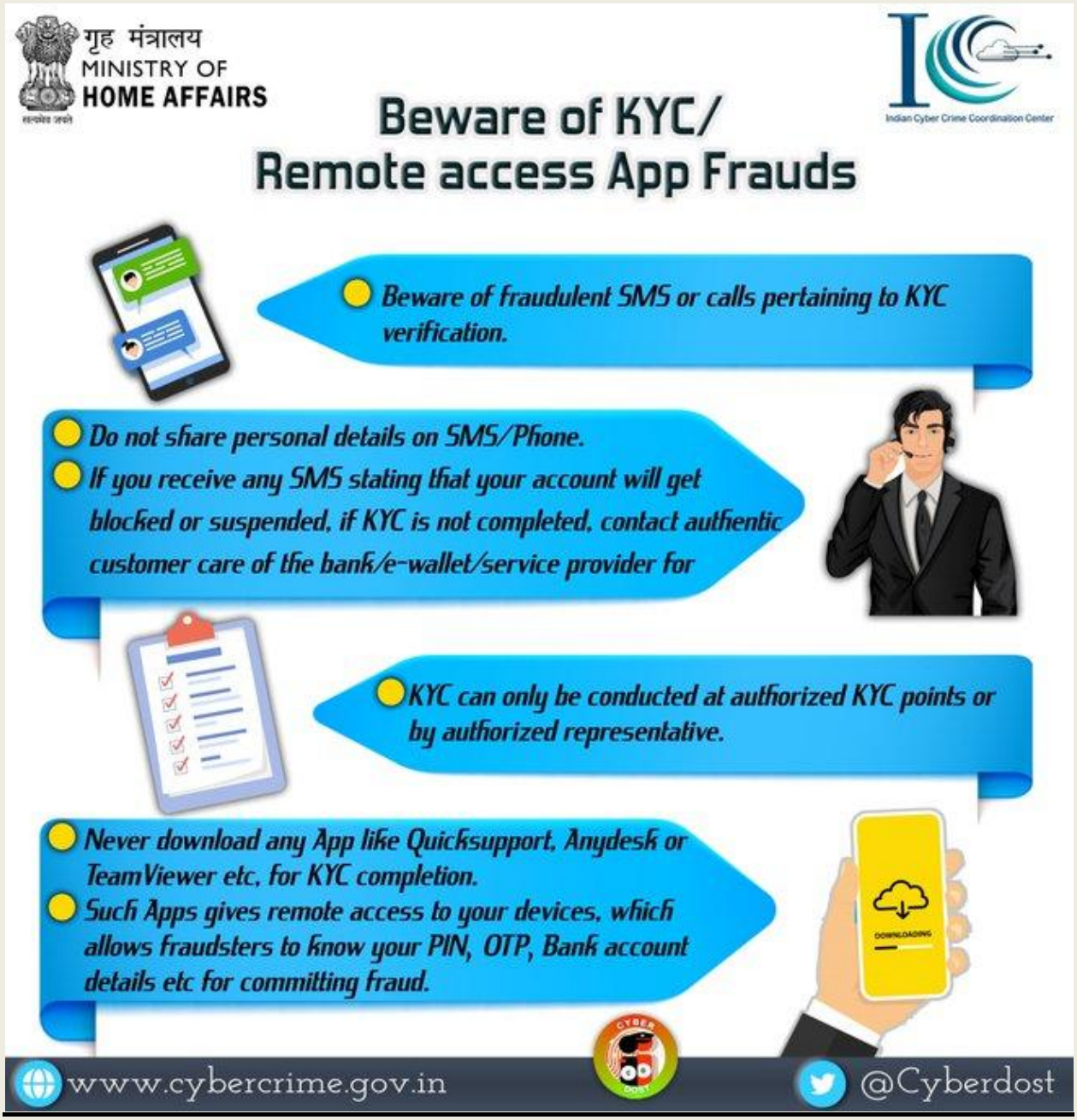

*Victim, a habitual user of certain mobile application downloads the mobile application ignoring security warnings and/or grants unnecessary permissions to the application, which is not required in the functioning of the app*

*Cyber criminals take advantage of this and attack the victim's device by infiltrating into it using the application. They infect the application with malicious software and get access to the victim's messages, cameras, contacts, photos etc. for malicious activities*

**TIPS**

- Always install applications from trusted sources like for Android devices, use Google Play, for Apple devices use App Store. Please ensure that the app is having Play Protect shield.
- It is also important to read reviews about the app. If it has a negative review, read more to see if anybody noted any security concerns like bugs or unencrypted passwords.
- Update your software and mobile applications on a regular basis so that you don't miss on important security patches.
- Be careful while granting app permissions like a document scanning app does not require permission to access your location, call logs etc. Sometimes applications are filled with spyware and other types of malware.

## REMOTE ACCESS APPLICATION FRAUD



# MATRIMONIAL FRAUDS

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

## How to detect fraudsters on matrimonial websites?

In case of any of the following, please be careful:

1. If a person is reluctant to come on video chat or to meet in person, he/she can be a fraudster as the profile picture posted on matrimonial website may not be of his/ her.
2. A fraudster may express his/ her love in just a short span of acquaintance.
3. Fraudsters will usually call from multiple numbers. He/ She usually don't give a number to call back. Even if he/ she give a number, they don't pick up when you call. Later, he/ she calls you back from a new number.
4. If a person enquires about your financial status at initial stage of interaction.
5. A Fraudster may not have a social media profile or have few friends on social media.

# CYBER SAFETY TIPS FOR CHILDREN

## DO's

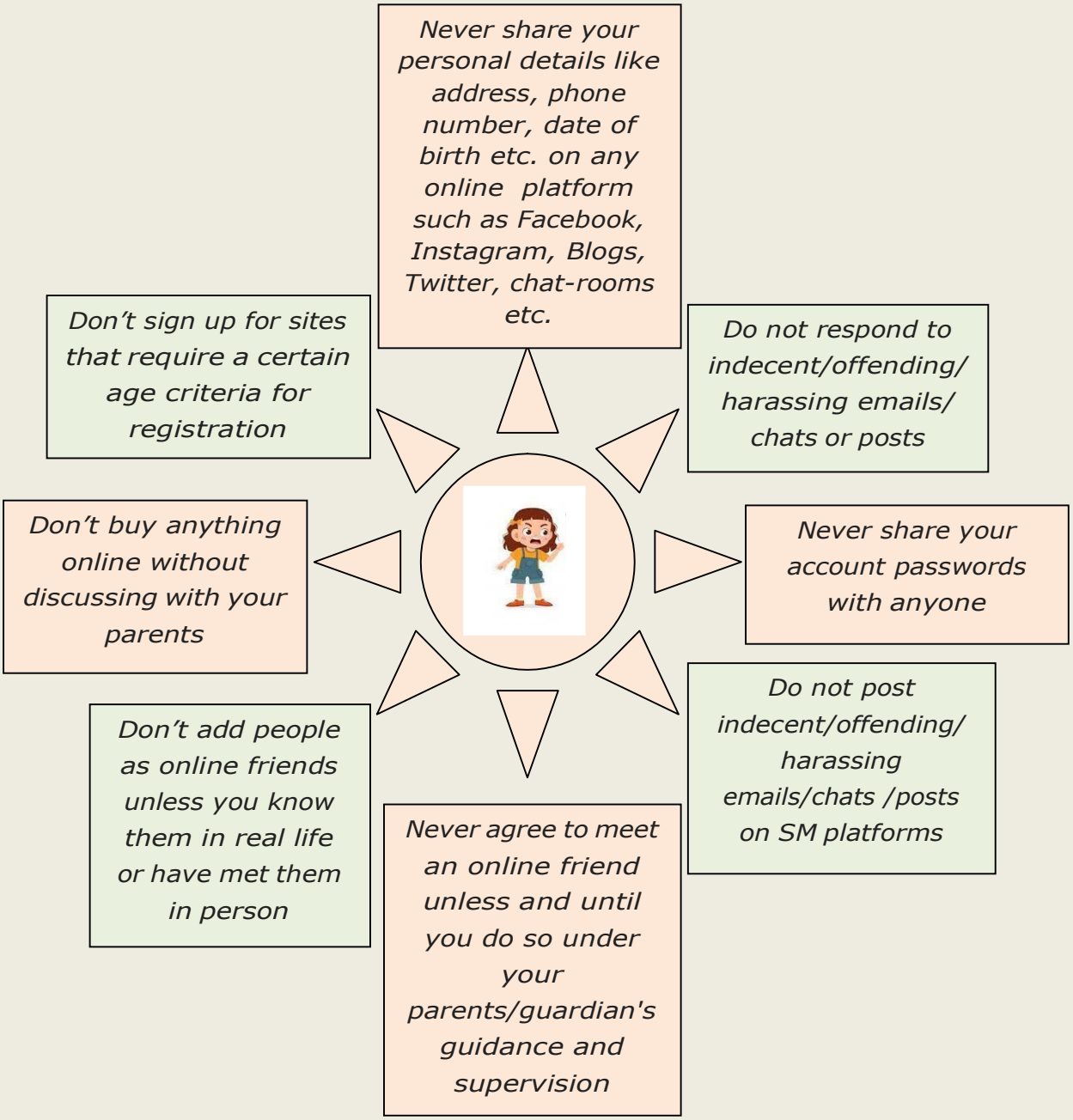
*When you feel uncomfortable with any SM post/mail/chatting, immediately share your concern with your parents or any trustworthy person*

*Password should be strong with alpha-numeric symbols and special characters*

*Real life etiquettes and manners apply equally to the virtual space*

*Always add persons whom you know in real life & with the permission of your parents*

# DON'Ts


Never share your personal details like address, phone number, date of birth etc. on any online platform such as Facebook, Instagram, Blogs, Twitter, chat-rooms etc.
Do not respond to indecent/offending/ harassing emails/ chats or posts
Never share your account passwords with anyone
Do not post indecent/offending/ harassing emails/chats /posts on SM platforms
Never agree to meet an online friend unless and until you do so under your parents/guardian's guidance and supervision
Don't add people as online friends unless you know them in real life or have met them in person
Don't buy anything online without discussing with your parents
Don't sign up for sites that require a certain age criteria for registration

# CYBER SAFETY TIPS FOR PARENTS

## DO's

*Have an open conversation with your kids about safe browsing and computer use*

*Check online activity of your child on Facebook, WhatsApp etc. especially if you notice a sudden change in behaviour*

*Educate yourself also on social media safety and have open discussions with teens*

*If you have found inappropriate content about your child, please contact the nearest PS at the earliest*

*Tell your children to immediately exit any site that makes them feel uncomfortable or worried*

*Keep computer in an open area. Make a rule that doors are always left open when kids are online*

*Explain it to your child that all social networking profiles must be set to private*

*Make sure that your children understand that they will not get into trouble if they tell you about their problem*

## DON'Ts

*Don't allow your child to have SM accounts if there is an age limit for the same*

*Do not let young children browse 'Google' or other search engines unnecessarily without supervision*

*Don't allow your child to use apps like Snapchat that immediately delete the posts*

*Do not replace physical parental supervision of computer use at home with any safe search engine or any other tool*

# CYBER SAFETY TIPS FOR WOMEN

## DO's

*Be selective about what information you make public. Sensitive information includes real name, date of birth, gender, town, e-mail address, school name, place of work, and personal photos*

*Periodically review your internet contacts and online activities*

*Block people you don't want to interact with*

*On social media accounts keep your privacy settings to the most stringent levels. Only share information about yourself on 'need to know' basis*

*On WhatsApp and other messaging apps, ensure that 'media auto-download' is deactivated, especially from senders who are not in your contact list*

*Be extremely cautious while posting photographs and control who can view them*

*Use strong passwords and use different passwords for different accounts*

*Contact the nearest PS immediately if you feel your privacy/safety has been compromised online. You can also report your problems online at* https://cybercrime.gov.in

# DON'Ts

*Never, try to meet a person with whom you've interacted only online without taking somebody else along and such meetings must always be in a public place*

*Don't share your password with anyone or let anybody else handle your account*

*Don't trade personal information for "freebies."*

*Don't accept "friend requests" from people totally unknown to you and from those with whom you don't want to interact with*

*Don't post personal information such as mobile numbers and personal email ids on social networking sites*

*Don't share any OTP or other passwords, even with friends*

*Don't accept a friend request only on the basis that the person is a mutual friend of a friend of yours*

*Don't click on unsolicited links sent over Facebook messenger or other messaging services, even if they are sent from your friend's account*

# GENERAL CYBER SAFETY TIPS

## For Device/Computer Security

- Keep your antivirus and operating system updated at all times.
- Backup your sensitive/important data at regular intervals.
- Be careful while opening suspicious web links/URLs.
- Always scan external storage devices (e.g. USB) for viruses, while connecting to your device.
- To prevent unauthorized access to your device, consider activating your wireless router's MAC address filter to allow authorized devices only.
- Wireless router can screen the MAC addresses of all devices connected to it, and users can set their wireless network to accept connections only from devices with MAC addresses recognized by the router.
- Secure all your wireless access points with a strong password. Hackers usually scan for open access points and may misuse it to carry out unwanted activities. Log records may make you more vulnerable for such misuse.
- Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your device. 'File Shredder Software' should be used to delete sensitive files on computers.
- Delete unwanted files or data from your computer device. It prevents unauthorized access to such data by others.
- Use 'Non-Administrator Account' privileges for login to the computer and avoid accessing with 'Administrator' privileges for day-to-day usage of computers.
- Make sure to install reputed mobile anti-virus protection to protect your mobile from prevalent cyber threats and also keep it updated.
- In case of loss or theft of your mobile device, immediately get your SIM deactivated and change passwords of all your accounts, which were configured on that mobile.
- Do not leave your phone unattended in public places and refrain from sharing your phone password/ pattern lock with anybody.
- Always enable a password on the home screen to restrict unauthorized access to your mobile phone. Configure your device to automatically lock beyond a particular duration.
- Always lock your computer before leaving your workplace to prevent unauthorized access. A user can lock one's computer by pressing 'Ctrl +Alt + Del' and choosing 'Lock this Computer' or "Window button+ L".
- Remove unnecessary programs or services from computer which are not required for day to day operation.

## For Safe Internet Browsing

- Beware of various fraudulent lucrative advertisements regarding discount coupons, cashback and festival coupons offering payments through UPI apps popping up while browsing.
- Some URL links on the internet are advertising to provide fake mobile Oximeter apps to check your oxygen level. Do not download such fake Oximeter apps on your mobile, as these apps may steal your personal or biometric data from your mobile phone.

- Avoid using third-party extensions, plug-ins or add-ons for your web browser as it may track your activity and steal your personal details.
- Always browse/visit the original website for purchasing.
- Always type the information in online forms and not use the auto-fill option on web-browser to fill online forms as these forms may store your personal information such as card number, CVV number, bank account number etc.
- Be careful about the name of a website. A malicious website may look identical to a legitimate one, but the name may use variation in spelling or a different domain (eg.,[dot]com, [dot]net etc.)
- In general all the government websites have [dot]gov[dot]in or [dot]nic[dot]in ending.
- Avoid clicking 'Keep me logged in' or 'Remember me' options on websites, especially on public computers.
- Beware of fraudulent charity activities or non-existent charitable organizations having names identical to government charity funds, requesting money for victims, products or research. Always check the credentials of charity organizations before donation.
- Never allow the browser to store your username/password, especially if you use a shared computer device. Also make it a habit of clearing history from the browser after each use session to protect your privacy.
- Be cautious with tiny or shortened URLs (it appears like http://tiny.cc/ba1j5y). Don't click on it as it may take you to a malware infected website.
- Prior to registering on a job search portal, check the privacy policy of the website to know the type of information collected from the user and how it will be processed by the website.
- Many social networking sites prompt to download a third-party application that lets you access more pages. Do not download unverified third-party applications without ascertaining its safety.
- Beware of e-commerce websites and advertisements selling items at highly discounted prices.

## For safe Internet Banking

- Always use virtual keyboard for accessing net banking facility and log off from banking portal/website after completion of online transaction. Also ensure deletion of browsing history from web browser (internet explorer, chrome etc.) after completion of online banking activity.
- Use multiple factor authentications for login into your bank accounts.
- Avoid writing down or storing in mobile phones the information used to access digital wallets/bank accounts.
- One should not use the same password for internet banking of all accounts.
- One should not keep the same mobile number registered for all bank accounts.
- Always enable getting notification of transactions from the banks via both SMS & e-mail.
- Login and view your bank account activity regularly to make sure that there are no unapproved transactions. Report discrepancies, if any, to your bank immediately.
- It is preferable to have two separate e-mail accounts, one for communicating with people and another for your financial transactions.

## For E-wallet Security

- Enable password/PIN on your mobile phones, tablets & other devices that you use.
- While doing transactions using your e-wallet, you should never save the details of your debit or credit cards.
- Use multiple factor authentications for logging into your e-wallets.
- Avoid writing down information used to access the digital wallets in mobile phones.
- Install e-wallet accounts from sources you trust. Do not install e-wallet apps via links shared over e-mail, SMS or social media. Always verify and install authentic e-wallet apps directly from the app store (Google/ iOS store) on your smart phone. Please check if the app is having the "Play Protect" shield.

## For E-mail Account Security

- Never keep the same password for all your e-mail accounts.
- Use secure network connections.
- Avoid the use of public Wi-Fi networks. More secure Wi-Fi connections require passwords & are easily identified as "WPA or WPA2". Highly insecure Wi-Fi is open for anyone to connect to & may be labelled as a "WEP" (Wired Equivalent Privacy).
- Don't click on the links provided in suspicious e-mails even if they look genuine as this may lead you to malicious websites and this may be an attempt to defraud your hard earned money.

## For Identity Proof Card's Security

- Never leave the discarded photo copy of your identity proof card at shops.
- Never allow the shopkeeper to keep a copy of your identity proof card in their computer.
- Never share your identity proof cards to unknown persons on social media platforms including WhatsApp.
- Never share your property papers or other personal information on social media platforms.

## For Password Security

- Keep a strong password of at least 13 characters with alphanumeric, special character, upper case & lower case combination.
- Keep two factor authentications for all your accounts.
- If you suspect that any of your account has been hacked, immediately change the password and contact the nearest Police Station.

**Social Rumors :**

## HOW TO MAKE A COMPLAINT TO POLICE

You can lodge a complaint at the nearest Police Station or, if specifically notified, the Cyber Police Station in your district. Cyber crimes can also be registered online at https://cybercrime.gov.in .

For proper investigation, please handover the following to the Police Station Officer along with the complaint or as soon as possible after the complaint.

### For Facebook or other Social Media Account related complaints

- If a fake Facebook or Instagram account has been created then take a screenshot of the fake profile along with the URL or mention the URL of the profile in the application.
- Attach self-attested identity card along with the complaint copy.

### For Financial Frauds

- Self-attested passbook/credit card transaction statement copy should be submitted, highlighting the fraudulent transactions along with bank account number, debit card/credit card number & registered mobile number with the bank account or credit card.
- Screenshot of text messages of fraudulent transactions received on the registered mobile phone number should be preserved and attached with the complaint copy.
- Screenshot of any suspicious link or OTP received for fraudulent transactions should also be preserved and attached with the complaint copy.

### For Fake Website related Frauds

- Screenshot of the fake website along with the URL of the website should be taken and submitted along with the complaint copy.
- Self-attested copy of fraudulent transactions, if any, should be attached with complaint copy.

**APPEAL**

Please help us in fighting cybercrime by being aware and not falling into the traps laid by cyber criminals. Also, please report all attempted cyber frauds. It will help us in nabbing the cyber criminals and bringing them to justice before they can defraud someone else.