सत्यमेव जयते
TELANGANA STATE
POLICE
Duty
Honour
Compassion

CYBER AWARENESS

SERIES 1.0

FOR CYBER WARRIORS

CYBER CRIME AND CYBER SECURITY AWARENESS FOR CYBER WARRIORS

TELANGANA STATE POLICE
2021

Special thanks to Sri M. H. Noble, MD, Zoom Technologies Pvt. Ltd. Hyderabad for his support in preparing this material.

AUTHORS:

1. **K. Srinath Reddy,** MA (PPM), MA (Philosophy), B.Ed, CJDA (IIT Kanpur)
   DSP, IT Cell, Telangana

2. **K. Nagendar Rao**, M.Tech (CS), CHFI, ISO ISMS LA
   Inspector, IT Cell, Telangana

DESIGN & LAYOUT BY:

1. Y. Ram Reddy, PC, TSP IT Cell,
2. K. Venkata Ratnam, AAO

FIRST EDITION: February, 2021 (2500 Copies)

Disclaimer: The information contained herein has been obtained from several sources believed to be reliable. While compiling the contents of this book care has been taken to provide the material in a lucid way. It would be happy to hear any suggestions, corrections, modifications and further topics to be addressed so that the same will be taken care in the future.

Distribution:

Restricted to Law Enforcement and Investigation Agencies.

M. MAHENDAR REDDY, IPS.,
DIRECTOR GENERAL OF POLICE
Telangana State, Hyderabad.

Ph. Off : 040-23235170
040-23232831
Fax : 040-23296565
e-mail : dgp@tspolice.gov.in

FOREWORD

In Today's World of Digital Life, offenders have been always in the forefront in taking advantage of every latest technology and committing crimes in the cyberspace. Therefore, there is a need for Telangana Police to acquire and upgrade knowledge and skills relentlessly on ever changing and ever increasing threats of Cybercrime, so as to be ahead of offenders in the cyber world. To confront the challenge of cyber threats in all aspects effectively, Telangana State Police declared the year 2021 as the Year of Cyber Safety and decided to build a cadre of cyber warriors in Telangana Police all over the State in all Police Stations. As a part of this strategy , police personnel @ 2 police officers in each Police Station in Districts, 5 police officers each in Police Stations of four Commissionerates of Hyderabad, Cyberabad, Rachakonda , and Warangal and 3 police officers each in Police Stations in Other Commissionerates as Cyber Warriors.

Telangana State Police will focus, on training and capacity building of police personnel at each police station to become Cyber Warriors at the Police Station level to combat cybercrime. This book thus provides knowledge and skills about the emerging trends of cybercrimes, will help support cyber-related investigation processes, help victims of Cybercrimes at Police Station level itself by redressing their grievances in addition to spreading awareness among the public at large so as to protect themselves from cyber offenders.

This book also describes about the on-going cyber threats, how cybercrimes take place, and how the public shall defend themselves from the cyber-attacks. Further, this book explains - various categories/ concepts of cybercrimes, secure digital payments, stay safe on social media, stay away from online frauds, women & children safety, stay anonymous etc. Everyone should be aware of these cybercrimes growing around us. This content has been narrated in such a way that anyone can understand how Cybercrimes are committed and how to overcome them.

This book is informative for anyone looking forward to learn more about the emerging threats of cybercrime; it can give necessary awareness to the staff of concerned vertical on cybercrime and cybersecurity. Therefore, I strongly recommend each reader goes through this book repeatedly for dealing with the menace of cybercrimes more effectively.

I deeply appreciate the invaluable efforts of the contributors in compiling this study material.

Mahender 20/2/21

(M. Mahendar Reddy)

CONTENTS

1.OVERVIEW OF CYBERCRIME

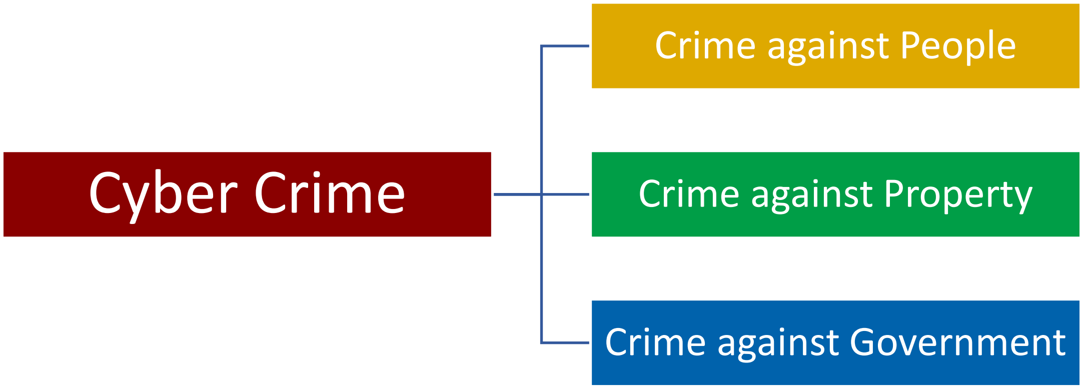
In today’s world it is hard to imagine a crime without a digital device. A wide range of offenders are using computers, Laptops and mobile phones and network servers for committing cyber offenses like cyber bullying, cyber stalking, sending phishing and threatening emails, to transmit content of child pornography, mobile application-based frauds, banking frauds, identity theft, etc. As technology evolves so does the types of crimes. The user must always be careful while sharing any personal or financial information to any stranger as no Bank/Government Organisation will ask for it. Also, we must keep a check on our social media account’s security and privacy policies for better protection. The user should understand that hundred percent privacy is a myth in digital platform. But, one can protect oneself by implementing certain do’s and don’ts.

What is Cybercrime?

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.

This includes a wide range of activities, from illegally downloading music files to stealing money from online bank accounts. Cybercrimes are broadly classified as:

- Crimes against People
- Crimes against Property
- Crimes against Government


Cyber Crime

Crime against People

Crime against Property

Crime against Government

- **Crimes against People**

  These crimes include cyber harassment and stalking, distribution of child pornography, credit card fraud, human trafficking, spoofing, identity theft, and online defaming.

- **Crimes against Property**

  These crimes occur against property, such as a computer or server. They include DDoS attacks, hacking, virus transmission, computer vandalism, copyright infringement, and IPR violations.

- **Crimes Against Government**

  When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty. Cybercrimes against the government mainly include hacking, accessing confidential information, cyber warfare, and cyber terrorism,

  Cybercrimes are further classified mainly into following types:

  - Identity Theft
  - Psychological tricks
  - Social media related attacks
  - Attacks through mobile applications
  - Digital banking frauds
  - Virus attacks on personal computers

2.IDENTITY THEFT

Identity theft is one of the most frequently happening crimes. It means obtaining the personal or financial information of another person to commit fraud by using their identity.

2.1 Social Media based pretention as legitimate user

It is a type of identity theft where a Criminal wrongfully gains someone's personal and financial details by pretending as original user to commit a crime such as creation of fake social media accounts and posting offensive/abusive content.

Modus Operandi

- Criminals gathers personal information and pictures of a victims by different means.
- Using the information, Criminals can create fake social media IDs.
- Criminals then send a friend request or offensive post / messages to all contact list of the victims.

How to protect yourself from crime

- Enable the option of notifications with social media accounts to receive alerts to know if someone else is trying to login.
- Use 2 Factor Authentication or One Time Password

2.2 Misuse of photo copies of identity proofs

The Criminal can misuse the photocopies of identity proofs. He can use PAN card, Aadhar card or any identity proof to purchase a SIM card, steal money and can misuse the proofs to harm others.

Modus Operandi

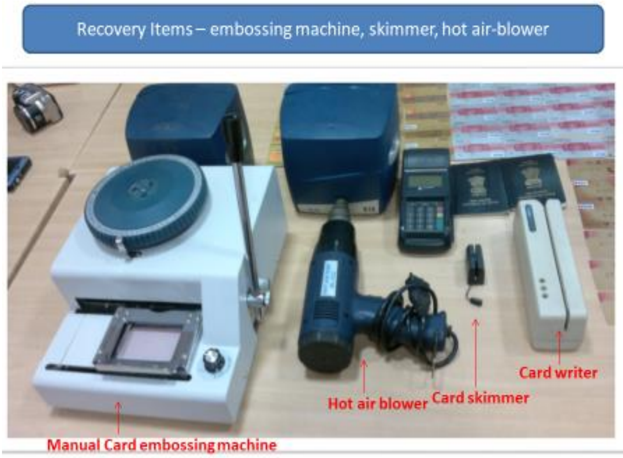
- Criminals can collect proofs from different sources where ID proof copies are submitted.
- Criminals can use the photocopy of identity proof to purchase a new SIM card or apply loans on victim’s name.
- Criminals can apply for a loan or credit card.
- Criminals can commit a crime that results in financial damage to the victim.

How to protect yourself from crime

- Never share identity proofs to any stranger.
- Mention the purpose of usage and date overlapping the photo copy towards the right side.
- Do not throw or leave photo copies in public places.

2.3 Credit/Debit Card Skimming

It is a method where a small device called skimmer is used to clone credit or debit cards and a pinhole camera is used to capture the PIN. It can also capture card details from the magnetic stripe on the card as it stores details of cardholder, these details can further be used for online transaction.


Recovery Items – embossing machine, skimmer, hot air-blower
Card writer
Hot air blower
Card skimmer
Manual Card embossing machine

- Skimming - copying the data from the magnetic strip / Chip of a credit or debit card.
- Card-reader placed over the real card slot on an ATM / merchant’s Electronic Data Capture (EDC) machine. Customer’s card is illegally copied by a syndicate gang / Network.
- Card gets misused at Merchant Establishments (Jewellery, electronic shops), ATMs and online sites.
- Transaction can occur either in India or abroad. Mostly identified “Place of compromise” **Petrol bunks, Hotels and Restaurants.**

Modus Operandi?

- Criminals install a small device called skimmer which captures details of card including CVV on to the ATM machine.
- Pin hole camera is installed to capture the PIN typed.
- Criminals then make a clone of the card and uses it to withdraw money.
- Details captured can be used for online transactions also.

How to protect yourself from crime:

- Before swiping the card always look for skimmer devices.
- Cover with one hand when typing the PIN
- When swiping, never allow sales person to take your card from your sight. Ask him to swipe it in your presence only.

2.4 Lost/Stolen Card

- Customer's card gets stolen and misused by third person.
- As most of the customers write the PIN number behind the card, fraudsters misuse it at ATMs.
- Review of ATM footages revealed that culprits could be a relative, friend, neighbor, colleague or someone unknown.

2.5 Never received Card

- Customer's card is never received and intercepted by a third party.
- Card gets misused by fraudster mostly at ATMs and Merchant Establishments.

Here, Culprits could range from relatives, Courier Executive, friend, neighbor, colleague or someone unknown belongs to an organized gang.

3.PSYCHOLOGICAL TRICKS

Psychological tricks are nothing but playing with the mind of victim and lure them with un-deniable offers. In this case, the victim receives an email or text message stating that he has won a lottery, got selected for a job with attractive packages, IT returns and loan has been approved on victim's name etc. There are some incidents where we receive a phone call asking for approval of personal loans and those calls can be of vishing fraud. For example, in recent times most of the vishing calls were traced to a particular location in Jamtara, Jharkhand. Sometimes, even educated people got convinced and fall prey for psychological tricks of the criminals.

3.1 Phishing

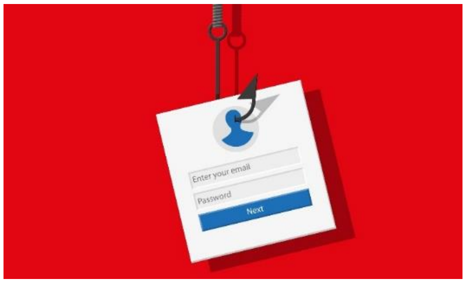
Phishing is an act of receiving malicious links through email which looks exactly like a genuine banking website or recruitment site or a travel agency site etc., this is done to collect personal and financial information to rob the victim.

Modus Operandi

- Criminals does a basic survey on victim needs also called as social engineering attack.
- Once criminal gains knowledge basing on the survey, criminal can send an email to the victim with an attractive offer, which contains malicious link. Which looks exactly similar to the original one.
- If the victim enters his details, all such details are being captured in the background by the criminals.

How to protect yourself from crime

- Do not respond to unknown source emails.
- Do not click on suspicious links attached in the email.
- Do not open spam mails and delete unwanted mails regularly.



3.2 Vishing

Vishing is similar to phishing but instead of receiving malicious links through email the criminal uses telephone to call the victim acting as a bank employee, customer care executive or a travel agent etc., and gains sensitive information from the victim.

Modus Operandi

- Criminal makes a call pretending to be a bank officer or from any legitimate source.
- Criminal tricks saying account will be blocked or Bank card will be blocked if details are not updated.
- Criminal tricks and obtains personal and financial information.

How to protect yourself from crime

- Do not share personal information to any stranger on call.
- Do not get panic when you receive such calls as no bank will ask for such details.
- Do not share your account information or card details to anyone.
- Reach customer care in case of any suspicious or unauthorized transactions.

3.3 Smishing

Smishing is similar to phishing but instead of receiving malicious links through email the criminal uses SMS to send fraudulent text messages. The messages may contain fake bank website links or a phone number to call, upon calling victim is being tricked to share sensitive information.

Modus Operandi

- Fake SMS are sent luring the victim
- Criminal can attach fake website links and phone numbers in the message.
- Upon receiving any call from victim criminal tricks and obtains personal and financial information.

How to protect yourself from crime

- Do not believe in messages from unknown sources.
- Do not click on the links received from unknown numbers.
- Do not give a call back on the numbers received from unknown people.

3.4 Helpline Fraud

It happens when customer/consumer looking for a solution to a problem on google search and calls on the first listed number. Criminal replaces the actual number with fake number and the calls placed goes to him directly.

Modus Operandi

- Criminal replaces the original number of customer care with fake numbers.
- Criminal sends fake links to the victim and tricks them to enter the banking details along with OTP.

How to protect yourself from crime

- To know the customer care number, please visit organisation's official website.
- Do not click on the links received from unknown sources.
- Do not share banking details on any websites that doesn't look genuine.

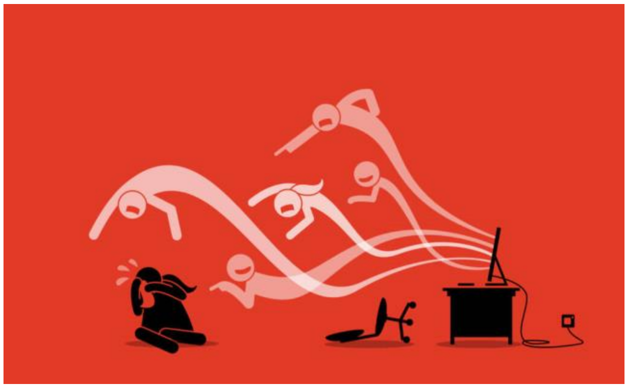
4.SOCIAL MEDIA RELATED ATTACKS

One can understand the entire history of an individual through their social media profile and can even predict future events based on patterns of postings 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.

4.1 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. Stalker believes that his true identity is hidden in the digital world.



Modus Operandi

- Criminal usually observe the daily activities of a person.
- Criminal sometimes also monitors activities of victim in real world.
- Criminal then starts sending threating/abusive messages or mails to the victim.

How to protect yourself from crime

- Restrict access to your profile and check on security and privacy settings on social media sites.
- Make sure your posts are only visible to your trusted once
- Be careful while uploading any of your photos which may show your location and places you frequently visit
- Be cautious while accepting any friend request of unknown person.

4.2 Cyber Bullying

Cyber bullying is an abuse that takes place over cyber space using 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 behaviour.

Modus Operandi

- Criminals usually observe the daily activities of a victim.
- Criminal then starts sending threatening / abusive messages or mails to the victim or posting negative, harmful false content in social media platforms.
- Criminal aims to embarrass or humiliate the victim.

How to protect yourself from crime

- Never share any intimate pictures with anyone on social media platforms.
- Monitor your kid's activity on social media, enable parental controls on computer / mobile devices.
- Make sure your children know that cyber bullying is a punishable crime so that they don't involve in them nor they let anyone harm them.

4.3 Micro Finance Applications

There are some mobile applications which offer small amount of finance with attractive benefits by taking Aadhar and Pan card details during registration process and these apps also access the phone contacts.

Modus Operandi

- Criminals send messages of instant loans approvals for which one need to download the loan apps
- They take your personal information like Aadhar card details and pan card details as a part of registration.
- They also attract by saying they have easy instalment options
- If payment is not paid on time, they even suggest to take another loan from different apps to repay back this existing loan and they make you fall in this trap.

How to protect yourself from crime

- Do not believe in such applications and lucrative offers.
- Do not install the app and give access to your contact list.

4.4 QR-Code SCAM

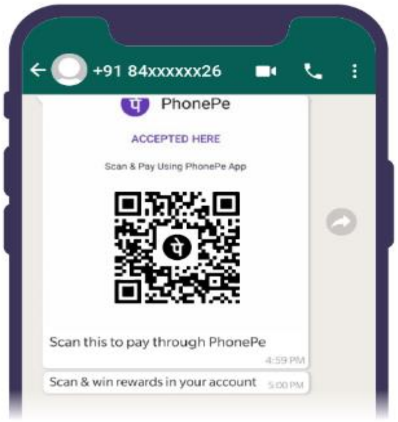
The criminal will reach out to you when you put something on sale on any digital platform. He engages you in a conversation as a buyer and will share a Quick Response (QR) code with a higher amount to pay advance/token amount via WhatsApp or email. Paytm, Phone Pay, Google Pay, Bhim App, Mobikwik, MI Pay, Pay Zaap, Razor Pay Application use QR code scanning for money transfers.

Modus Operandi

- The Criminal will create a QR code with a high amount and will share it with you through WhatsApp, Email or other platforms.
- After sharing the QR code, the user will ask you to select "Scan QR code" option on the app and select QR code from photo gallery
- After scanning the QR code from photo gallery, you will be asked to **Proceed** with the **payment**
- After clicking on "Proceed", you will be asked to enter your UPI PIN and money will be deducted from your account instantly.

How to protect yourself from crime

- Verify the buyer/seller before sending/receiving the payment
- NEVER scan any QR code or enter UPI PIN for payments.



+91 84xxxxxx26

PhonePe
ACCEPTED HERE
Scan & Pay Using PhonePe App

Scan this to pay through PhonePe 4:59 PM

Scan & win rewards in your account 5:00 PM

5.ATTACKS THROUGH MOBILE APPLICATIONS

5.1 Cyber-attacks using Infected Mobile Applications

Mobile apps are widely used for various activities like entertainment, social networking, messaging, 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.

5.2 Cyber-attacks using Infected Mobile Applications

Cyber criminals attack the victim by infiltrating through popular mobile applications. They infect the applications with malicious software and can get access to your messages, OTP, camera, contacts, e-mails, photos.

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

Modus Operandi

- Criminals create clone apps for most popular apps with similar names and icons and upload them to play store or websites.
- Criminals can distribute popular paid apps as free apps through various websites.
- Once the victim downloads and installs the fraudulent app, criminal gains access to the victim's mobile device and can monitor user activities, steal passwords, credit card/debit card information, etc.

How to protect yourself from crime

- Never download apps from unknown sources.
- Always download apps from play store/app store after verifying the app name, app developer information and app ratings.
- Always be careful while giving permissions to the app, think twice before permitting something on the app.

6. DIGITAL BANKING FRAUDS

Digital banking frauds are those related to online payments, internet banking, account compromise because of weak passwords.

6.1 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 compromised or if the user is not cautious about how they are using the payment app.

Modus Operandi

- Criminals pose as if they are a prospective buyer for a product that you have advertised.
- Sometimes they are even ready to do the payment for the product without bargaining or without even looking at the product.
- Once the victim accepts the payment offer, the criminal sends a QR code to the victim.
- Unsuspecting victim scans the QR code and types the UPI PIN assuming they are receiving the money, whereas they are sending money to the cybercriminal.

How to protect yourself from crime

- Always be very careful when doing transaction using any digital payment app.
- Read the message displayed on the app screen very carefully. Do not be in a hurry to complete the transaction.
- Always remember that you only need to enter the UPI PIN while sending the money (payment) not for receiving the money.

6.2 Hacking of Bank Account due to Weak Password

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

Modus Operandi

- Criminals can try to guess one's bank account password by knowing some details about the victim like their full name, date of birth, family and friends, likes & dislikes etc.
- As the criminal has enough information about the victim and knows the pattern of passwords. It can be cracked easily.

How to protect yourself from crime

- Never use an easy to guess word/phrase/number as your password.
- Always choose a strong password with at least 8 characters or more.
- Always make sure that the password includes a combination of lower-case and upper-case alphabets, numbers, and special characters.
- Enable and use One Time Password (OTP) wherever the option is available.

6.3 Hacking of Multiple Accounts due to same password

In this type of attack, the cybercriminal tries to hack other accounts belonging to the victim using the same login credentials that are already compromised.

Modus Operandi

- Criminals can try to access a victim's other accounts using the login credentials that are already compromised through a different attack.

How to protect yourself from crime

- Never use the same password for multiple logins.
- Regularly keep changing the password for every account.
- Always choose a strong password with at least 8 characters or more.
- Always make sure that the password includes a combination of lower-case and upper-case alphabets, numbers, and special characters.
- Enable and use One Time Password (OTP) wherever the option is available.

6.4 SIM Swap

- Under SIM Swap, Criminal manage to get a new SIM card issued against victim's registered mobile number through the mobile service provider. With the help of this new SIM card, they get One Time Password (OTP) and alerts, required for making financial transactions through your bank account.

Modus Operandi

- Criminal gather customer's personal information through Phishing, Vishing, Smising or any other means.

How to protect yourself from crime

- If your mobile no. has stopped working for a longer than usual period, enquire with your mobile operator to make sure you haven't fallen victim to the Scam.

- They then approach the mobile operator and get the SIM blocked. After this, they visit the mobile operator's retail outlet with the fake ID proof posing as the customer.

- The mobile operator deactivates the genuine SIM card and issues a new one to the fraudster.

- Fraudster then generates One Time Password (OTP) required to facilitate transactions using the stolen banking information. This OTP is received on the new SIM held by the fraudster.

- Register for SMS and Email Alerts to stay informed about the activities in your bank account.

- Regularly check your bank statements and transaction history for any irregularities.

7.CRIME AGAINST WOMEN

Women are being subjected to various kinds of cybercrimes. Criminals are using social network sites and instant messengers for this purpose.

The major crimes against woman include-

- Cyber teasing
- Cyber Stalking
- Cyber Defamation
- Trolling
- Doxing
- Revenge Porn
- Cat Fishing

How to protect women from this crime

- Educate every girl/woman to be careful while on internet.
- Never befriend strangers and share too much of personal information.
- If someone starts harassing them, they should report to family and police.

8.CRIME AGAINST CHILDREN

Now-a-days, greater number of Children are exposed to internet and are using social networks for various activities. After befriending them, Criminals are Harassing, Stalking & Bullying children on Social networks and Instant Messengers.

Online Criminals befriending children and youngsters with chatting, likes/shares, positive, comments, coupon offers, free online shopping, taking private photos, live streaming, playing online games, sending videos of interest etc.

How to protect children from this attack/crime

- Educate every child to be careful while on internet.
- Never share too much of personal information to strangers.
- If someone starts harassing them, they should immediately report to family and police.

9.VIRUS ATTACKS ON PERSONAL COMPUTER

Virus is a malware designed to destroy user data or Operating System or dependency files. Cybercriminals are using this malware to damage user data.

9.1 Virus Attack through external devices

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

Modus Operandi

- Criminals can purposefully infect a user's external storage like a pen drive

How to protect yourself from crime

- Install a good anti-malware software on Personal Computer (PC) and make sure or a hard drive with virus to damage the user's data on system.

it is up to date with all malware signatures.

- Never open files or applications from an external device without performing a malware scan.

9.2 Virus Attack by downloading files from un-trusted websites

A virus can enter the computer while downloading applications, documents, music, video, etc. from an untrusted website.

Modus Operandi

- Criminals purposefully post malware infused software, games, audio and video files on to various websites to infect user's PC and either damage data or steal data or gain control over the user's PC.

How to protect yourself from crime

- Install a good anti-malware software on PC and make sure it is upto date with all malware signatures.
- Never open files or applications from an unknown website without performing a malware scan.

10. Cyber Crimes – Category: Major, Minor & Sub-Heads

Sl No	Category of Offences			Sec of Law – Applicability	Description of the Offence
	Major Head	**Minor Head**	**Sub - Head**		
1.	**Identify Theft** **Sec. 66 (C), 66 (D) IT Act, 420 IPC.**	Bank Related Frauds: Vishing (Call) Fraud Smishing (SMS) Fraud Phishing (e-mail) Fraud	Aadhaar Linkage PAN Card Linkage KYC updation Blocking of card Card limit - enhancement Reward Points	66 (C) IT Act and 420 IPC	A. Calling over phone pretending as bank representatives, collection of bank A/c credentials like Card details, OTP and misusing the same. B. Sending SMS/e-mail to the victim, collection of credentials of bank A/c, Card details, OTP and misuse of the same.

Sl No	Category of Offences			Sec of Law – Applicability	Description of the Offence
	Major Head	**Minor Head**	**Sub - Head**		
			Replacement of card - with photo/Chip Any Others		
		Skimming / Cloning of Cards etc.,	ATM Center Merchant Place	66 (C) IT Act and 420 IPC	Placing Skimmers at ATM Centers / collecting data at Merchant Places. Withdrawal of amounts with cloned cards from ATM's and from Merchant Places.
		Fake Customer Care Service Fraud	Google Just Dial Any Others	66 (C), 66 (D) IT Act and 420 IPC	Posting fake customer care service Ads in Google, Just Dial etc., in the name of original firms/companies and deceiving the victims in the name of fake Customer Care Services etc., and taking huge amounts.
		Income Tax Fraud		66 (C) IT Act and 420 IPC	Personating as if from Income Tax department and cheating the victims on the pretext of better return of tax paid amount etc.,
		SIM SWAP Fraud		66 (C) & (D) IT Act and 420 IPC	Submitting forged documents and collecting replace SIM cards from stores of TSP's for committing bank Frauds.
2.	**Online Frauds** **Sec. 66 (D) IT Act, 420 IPC.**	Job Fraud, Visa Fraud	Naukri Shine Monster Any Other	66 (D) IT Act and 420 IPC	Calls / Messages / e-mails are made / sent to the victims on the pretext of arranging Job / Visa etc., and deceiving them by parting with money towards Registration fee, advance fee etc.,
		Loan Fraud		66 (D) IT Act and 420 IPC	Personating as financial institutions and deceiving the victims on the pretext of arranging loans at low rate of interest etc.,
		Insurance Fraud		66 (D) IT Act and 420 IPC	Personating as insurance company representatives and deceiving the victims on the pretext of better insurance plans etc.,
		Lottery Fraud		66 (D) IT Act and 420 IPC	Either calling or sent SMS / e-mails to victims by

Sl No	Category of Offences			Sec of Law – Applicability	Description of the Offence
	Major Head	Minor Head	Sub - Head		
					mentioning that they have won prize over lotteries organized by popular organizations and thus deceiving victims to part with money on the pretext of paying for advance fee, getting no objection certificates etc.,
		Advertisement Portal Fraud	OLX Quikr CarDekho Facebook Instagram Any Other	66 (D) IT Act and 420 IPC	Posting fictitious / fake Ads in classifieds of Social Media Platforms and deceiving the victims.
		Gift Fraud (By using the name of e-Commerce platform)	Snapdeal Shopclues Amazon Flipkart Clubfactory Naaptol Home Shop 18 Any Other	66 (D) IT Act and 420 IPC	Securing customer data of e-commerce platforms and deceiving the customers on the pretext of winning Gift.
		Trading Fraud	Share Trade Forex Trade Commodity Trade Investment Advisors	66 (D) IT Act and 420 IPC	Cheating the victims on the pretext of fetching huge amounts on investing amounts in Share / Forex / Commodity Trade / by paying amounts towards Share market Tips (IA's).
		Delivery of duplicate / Sub-standard products Fraud		66 (D) IT Act and 420 IPC	Cheating the victims by sending duplicate / Sub-standard articles to the victims instead of sending the original products shown in online.
		Mobile Fancy Number Fraud		66 (D) IT Act and 420 IPC	Cheating the victim by offering fancy mobile number.
		Cell Tower Installation Fraud		66 (D) IT Act and 420 IPC	Personating cell companies and cheating the victims in the name of agreement with TSPs & victims and thereby parting with amounts in the

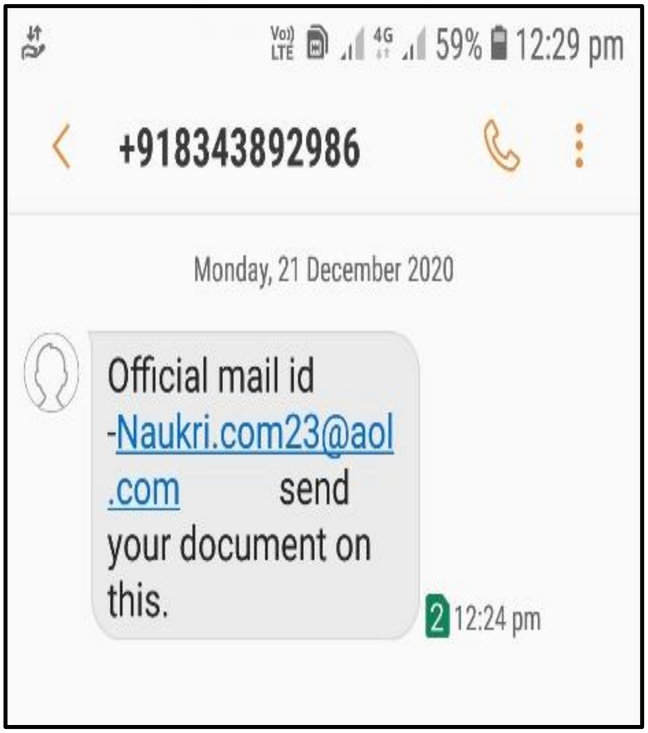
Sl No	Category of Offences			Sec of Law – Applicability	Description of the Offence
	Major Head	Minor Head	Sub - Head		
					name if advance fee, security deposit etc.,
		Online relationship Fraud	Friendship through A). Matrimonial – Websites B). Social Media Platforms	66 (D) IT Act and 420 IPC	Posting attractive fake profiles over matrimonial websites / Social Media platforms once victims get attracted to such posts and after gaining faith collecting money on false pretexts.
		Dating / Female escort Fraud		66 (D) IT Act and 420 IPC	Cheating the victims in the name of dating / female escorts collecting amounts on the pretext of Registration fee, membership fee, character verification fee etc., for sexual favours.
		Business and Investment Fraud		66 (D) IT Act and 420 IPC	Cheating in the pretext of supply of raw materials, better returns in short term etc.,
3	**Cyber Stalking** **Sec. 354 (D), 509, 506, 507 IPC and Sec.67 of IT Act.**	Stalking over 1. Social Media, 2. Classified Websites and 3. Pornographic Websites.	Facebook Instagram Dating Websites Porn Websites Any Other	354 (D), 509 IPC, if the content is obscene Sec. 67 of IT Act is also applicable.	Creating fake profile in the name and identities of victim / sending add friend requests to victim friends, posting the mobile numbers of victim in Classified / Pornographic Websites etc.,
		Stalking over 1. SMS 2. e-mails 3. WhatsApp (VOIP etc.,)		354 (D), 509 IPC, if the content is obscene Sec. 67 of IT Act is also applicable.	Sending un-solicited e-mails and messages with abusive or objectionable contents.
		Stalking by fake Social Media Profiles.		354 (D), 509 IPC, if the content is obscene Sec. 67 of IT Act is also applicable.	Creation of fake profile over Social Media.
		Blackmailing, Intimidation, Sextortion.		354 (D), 506 / 507, 509 IPC and 384 IPC, if	Creating fake profile in the name and identities of victim / sending add friend

Sl No	Category of Offences			Sec of Law – Applicability	Description of the Offence
	Major Head	Minor Head	Sub - Head		
				the content is obscene Sec.67 of IT Act is also applicable.	requests to the victim friends coupled with demand for ransom.
		Cyber Flashing		354 (D) IPC and Sec.67 of IT Act.	Sending unsolicited obscene images / videos to the victims through wireless convention channel.
4.	**Violation of Privacy** **Sec.66(E) IT Act, 354 (C) IPC.**	Taking images through phones.		66-E IT Act, 354 -C IPC (Depending on the case)	Taking images of private parts and activities of people over mobiles phones etc.,
		Taking photos with hidden cameras.		66-E IT Act, 354 -C IPC (Depending on the case)	Keeping hidden cameras and capturing images of private parts at bathrooms, trial rooms etc.,
5	**Cyber Pornography** **Sec.67, 67 (A) IT Act.**	Circulation of obscene images / text.		67 IT Act	Circulation of obscene images or sending obscene text messages over SMS or WhatsApp.
		Circulation of Obscene videos.		67 and 67-A IT Act	Circulation of obscene videos over Social Media, e-mails or WhatsApp.
6	**Child Pornography** **Sec.67, 67 (B) IT Act, POCSO Act.**	Circulation of Obscene child porno		67, 67 (B) IT Act and POCSO Act	Circulation of obscene videos related children over social media, e-mails or WhatsApp or downloading child sexual porno, enticing children for online relationship etc.,
7	**Source Code Tampering** **Sec.65 IT Act**	Stealing, deletion and destruction of source code		65 IT Act	Stealing of computer programme / application/ code and making use of self or for others.
8.	**General Computer Offences** **Sec. 66 r/w.43 IT Act, 384 IPC.**	Hacking		66 r/w. 43 IT Act	E-mail Id, FB Profile Hacking and misuse, Server computer hacking by changing password etc.,
		Business e-mail ID compromise Fraud		66 r/w. 43 IT Act	Compromising business e-mail IDs, interception of data, sending deceptive e-mail for committing Fraud etc.,
		Ransom Ware		66 r/w. 43 IT Act and 384 IPC	Taking control of a computer system or server by sending malware and demanding money to release.

Sl No	Category of Offences			Sec of Law – Applicability	Description of the Offence
	Major Head	**Minor Head**	**Sub - Head**		
9.	**Online IPR Offences Sec.66 (B), 65 IT Act.**	Copy Rights violation over Internet		66-B, 65 IT Act and Copy Right Act	Movie uploads, copy right contents uploads.
10.	**Communal content over Social Media** **Sec. 153 (A), 505 IPC.**	153-A (Depending on the nature of offence), 505 IPC relevant Sub-Sections		Morphing images of gods and goddesses and items of religious importance, and circulation over social media and/or making communal sensitive statements over social media.	Communal content over social media

11. SAMPLE FRAUD MESSAGES / EMAIL

Job Fraud Messages

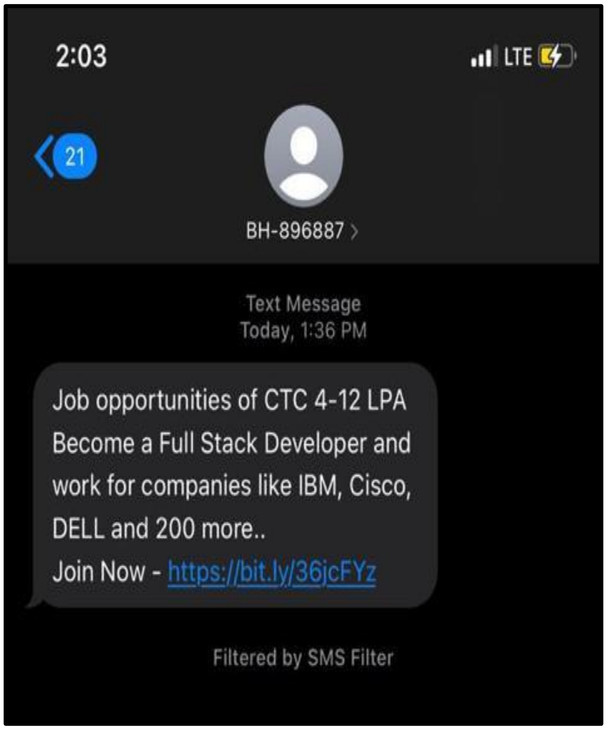


+918343892986

Monday, 21 December 2020

Official mail id -Naukri.com23@aol.com send your document on this.

12:24 pm

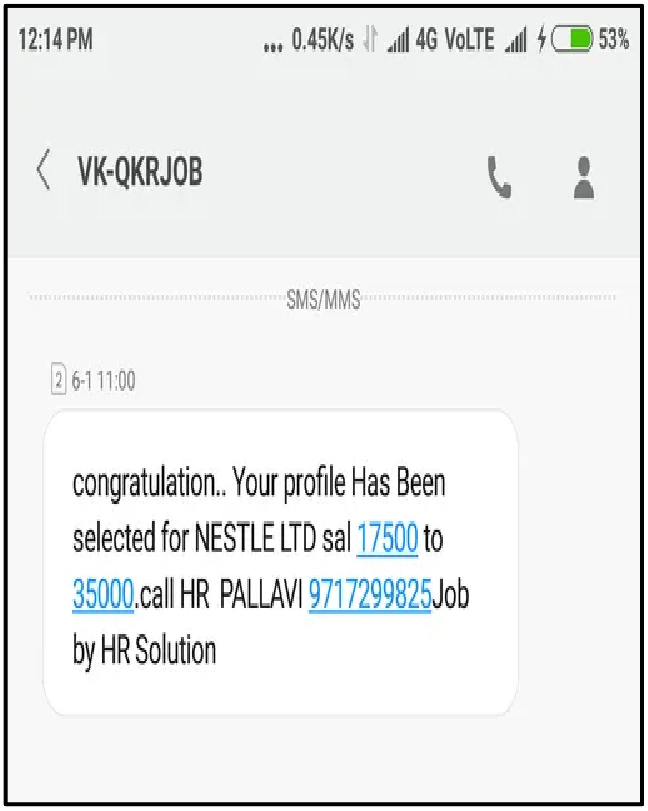


BH-896887

Text Message
Today, 1:36 PM

Job opportunities of CTC 4-12 LPA Become a Full Stack Developer and work for companies like IBM, Cisco, DELL and 200 more..
Join Now - https://bit.ly/36jcFYz

Filtered by SMS Filter

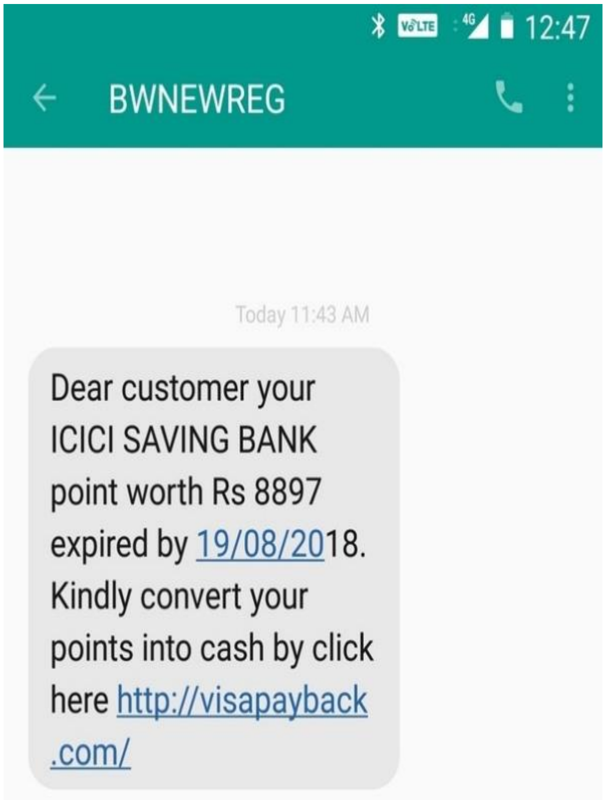


VK-QKRJOB

SMS/MMS

6-1 11:00

congratulation.. Your profile Has Been selected for NESTLE LTD sal 17500 to 35000.call HR PALLAVI 9717299825Job by HR Solution

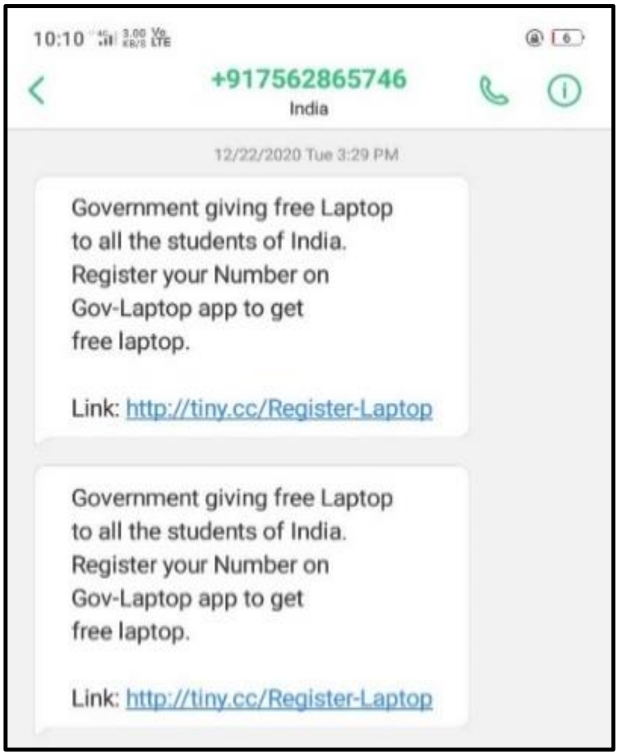


BWNEWREG

Today 11:43 AM

Dear customer your ICICI SAVING BANK point worth Rs 8897 expired by 19/08/2018. Kindly convert your points into cash by click here http://visapayback.com/

Free Gift Messages

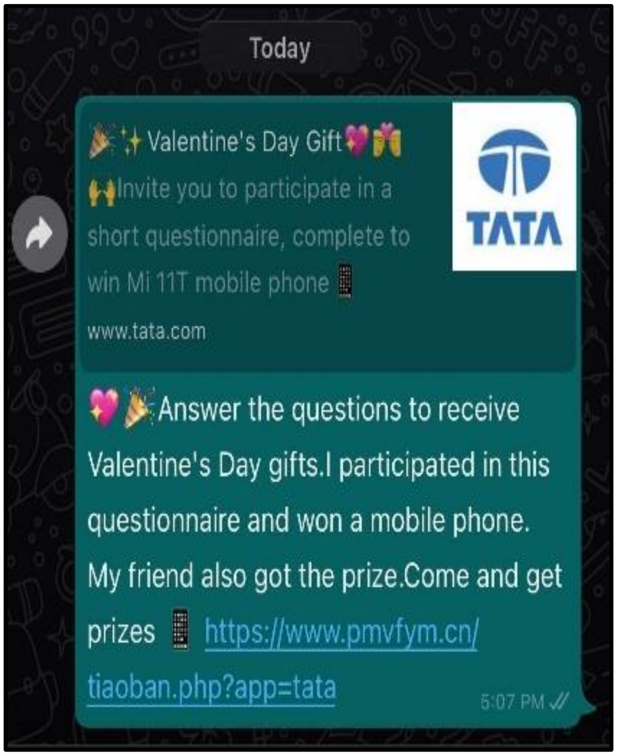


Government giving free Laptop to all the students of India. Register your Number on Gov-Laptop app to get free laptop.

Link: http://tiny.cc/Register-Laptop

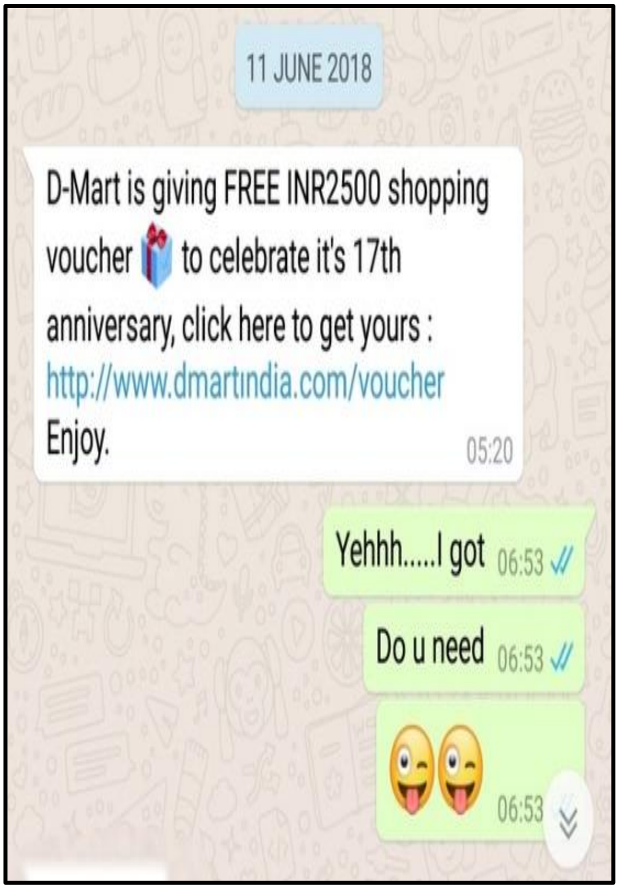
Government giving free Laptop to all the students of India. Register your Number on Gov-Laptop app to get free laptop.

Link: http://tiny.cc/Register-Laptop



🎉✨Valentine's Day Gift💖🥂
🙌Invite you to participate in a short questionnaire, complete to win Mi 11T mobile phone📱
www.tata.com

💖🎉Answer the questions to receive Valentine's Day gifts.I participated in this questionnaire and won a mobile phone. My friend also got the prize.Come and get prizes 📱 https://www.pmvfym.cn/tiaoban.php?app=tata

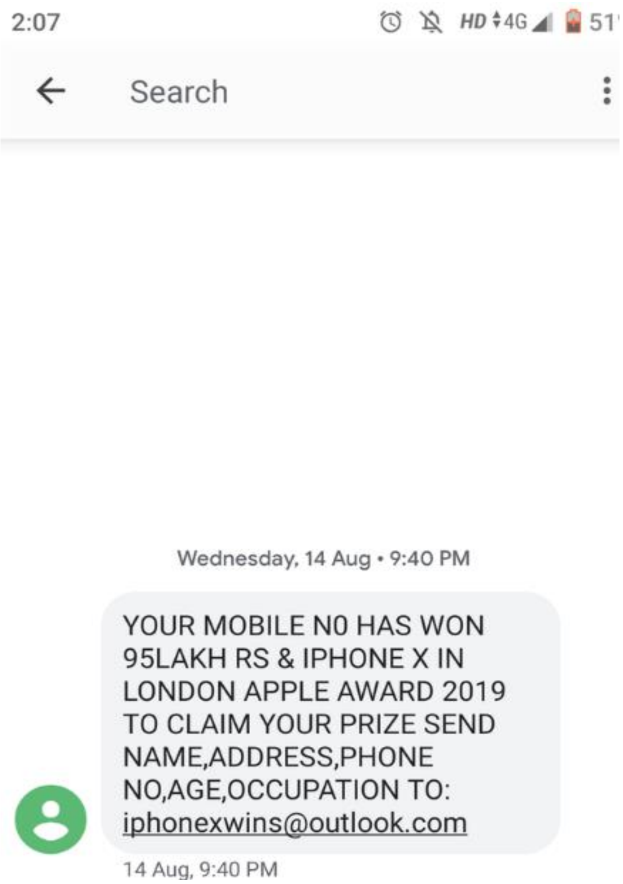


D-Mart is giving FREE INR2500 shopping voucher 🎁 to celebrate it's 17th anniversary, click here to get yours : http://www.dmartındia.com/voucher Enjoy.

Yehhh.....I got

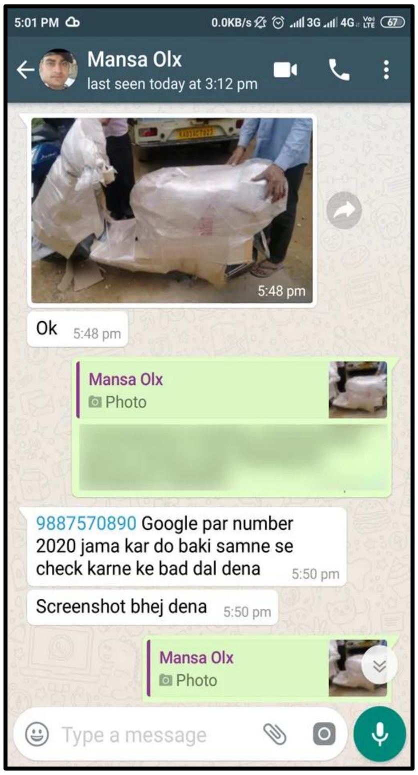
Do u need

😜😜



YOUR MOBILE N0 HAS WON 95LAKH RS & IPHONE X IN LONDON APPLE AWARD 2019 TO CLAIM YOUR PRIZE SEND NAME,ADDRESS,PHONE NO,AGE,OCCUPATION TO: iphonexwins@outlook.com

QR Code Scam Messages



5:01 PM

Mansa Olx
last seen today at 3:12 pm

5:48 pm

Ok 5:48 pm

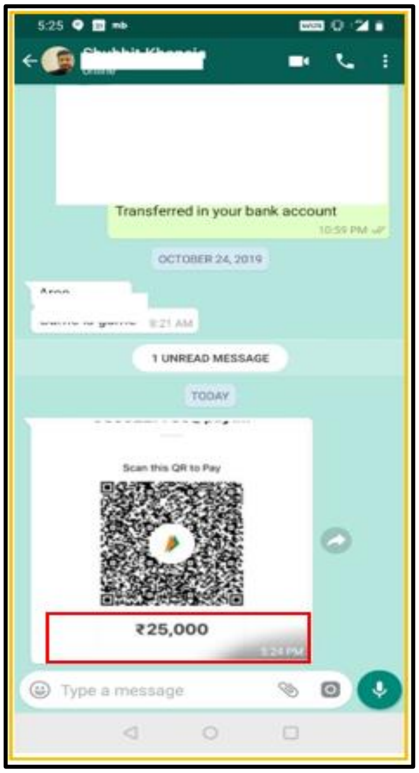
Mansa Olx
Photo

9887570890 Google par number 2020 jama kar do baki samne se check karne ke bad dal dena 5:50 pm

Screenshot bhej dena 5:50 pm

Mansa Olx
Photo

Type a message



5:25

[redacted]

[redacted]

Transferred in your bank account 10:59 PM

OCTOBER 24, 2019

[redacted]

9:21 AM

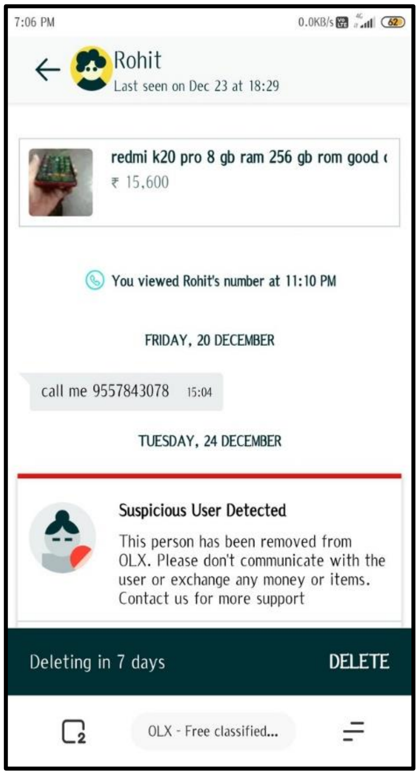
1 UNREAD MESSAGE

TODAY

Scan this QR to Pay

₹25,000

Type a message



7:06 PM

Rohit
Last seen on Dec 23 at 18:29

redmi k20 pro 8 gb ram 256 gb rom good
₹ 15,600

You viewed Rohit's number at 11:10 PM

FRIDAY, 20 DECEMBER

call me 9557843078 15:04

TUESDAY, 24 DECEMBER

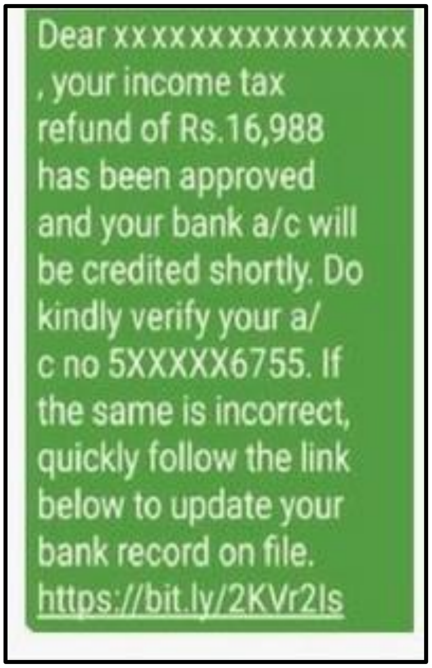
Suspicious User Detected

This person has been removed from OLX. Please don't communicate with the user or exchange any money or items. Contact us for more support

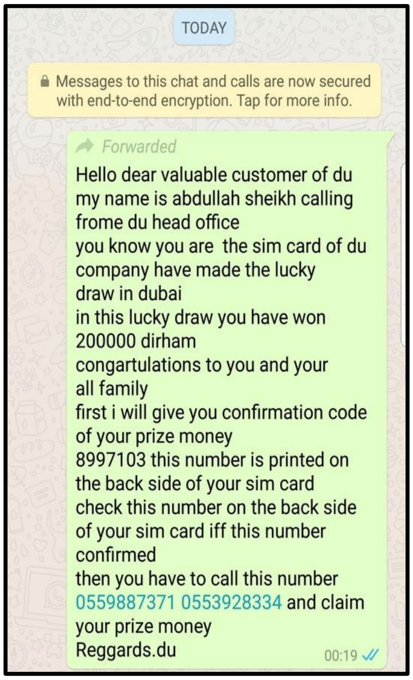
Deleting in 7 days DELETE

OLX - Free classified...

Miscellaneous Messages



Dear xxxxxxxxxxxxxxx , your income tax refund of Rs.16,988 has been approved and your bank a/c will be credited shortly. Do kindly verify your a/c no 5XXXXX6755. If the same is incorrect, quickly follow the link below to update your bank record on file. https://bit.ly/2KVr2Is

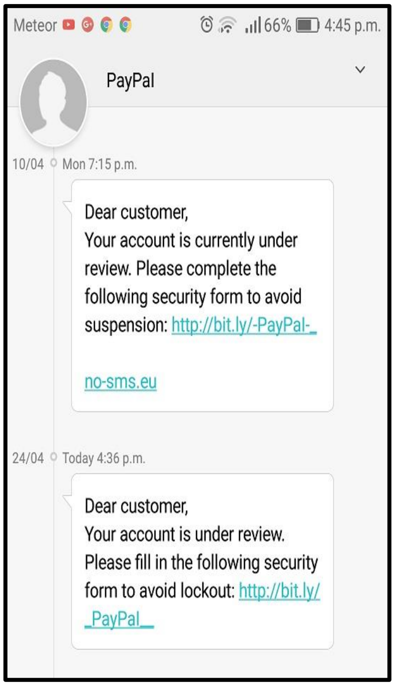


TODAY

Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.

Forwarded

Hello dear valuable customer of du
my name is abdullah sheikh calling
frome du head office
you know you are the sim card of du company have made the lucky draw in dubai
in this lucky draw you have won 200000 dirham
congartulations to you and your all family
first i will give you confirmation code of your prize money
8997103 this number is printed on the back side of your sim card
check this number on the back side of your sim card iff this number confirmed
then you have to call this number 0559887371 0553928334 and claim your prize money
Reggards.du 00:19



Meteor 66% 4:45 p.m.

PayPal

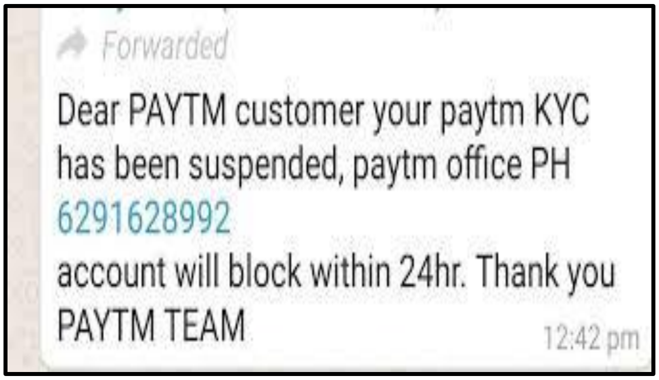
10/04 Mon 7:15 p.m.

Dear customer,
Your account is currently under review. Please complete the following security form to avoid suspension: http://bit.ly/-PayPal-_

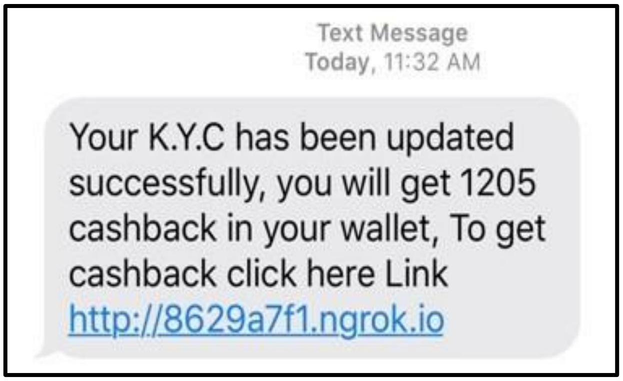
no-sms.eu

24/04 Today 4:36 p.m.

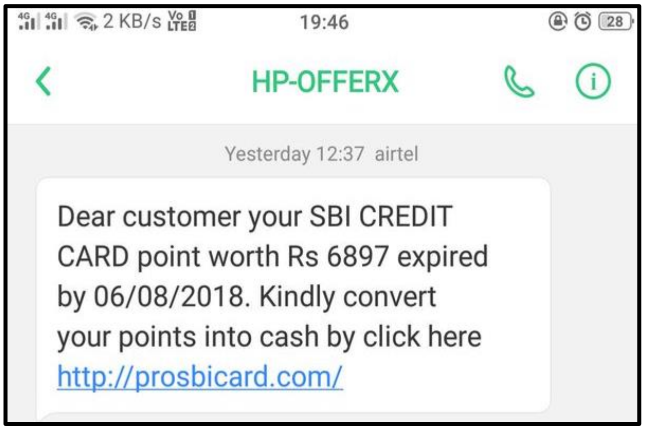
Dear customer,
Your account is under review.
Please fill in the following security form to avoid lockout: http://bit.ly/_PayPal_



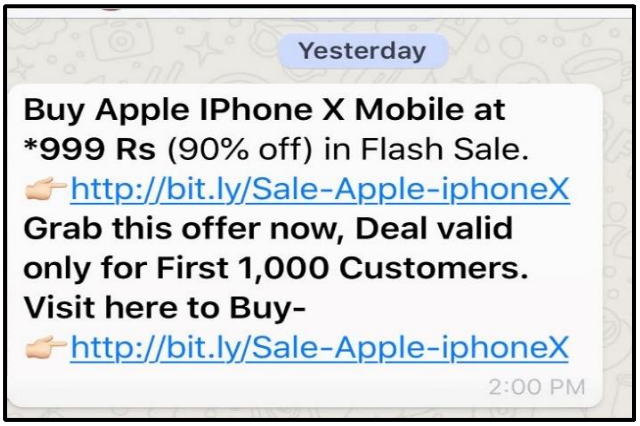
Dear PAYTM customer your paytm KYC has been suspended, paytm office PH 6291628992
account will block within 24hr. Thank you
PAYTM TEAM



Your K.Y.C has been updated successfully, you will get 1205 cashback in your wallet, To get cashback click here Link http://8629a7f1.ngrok.io

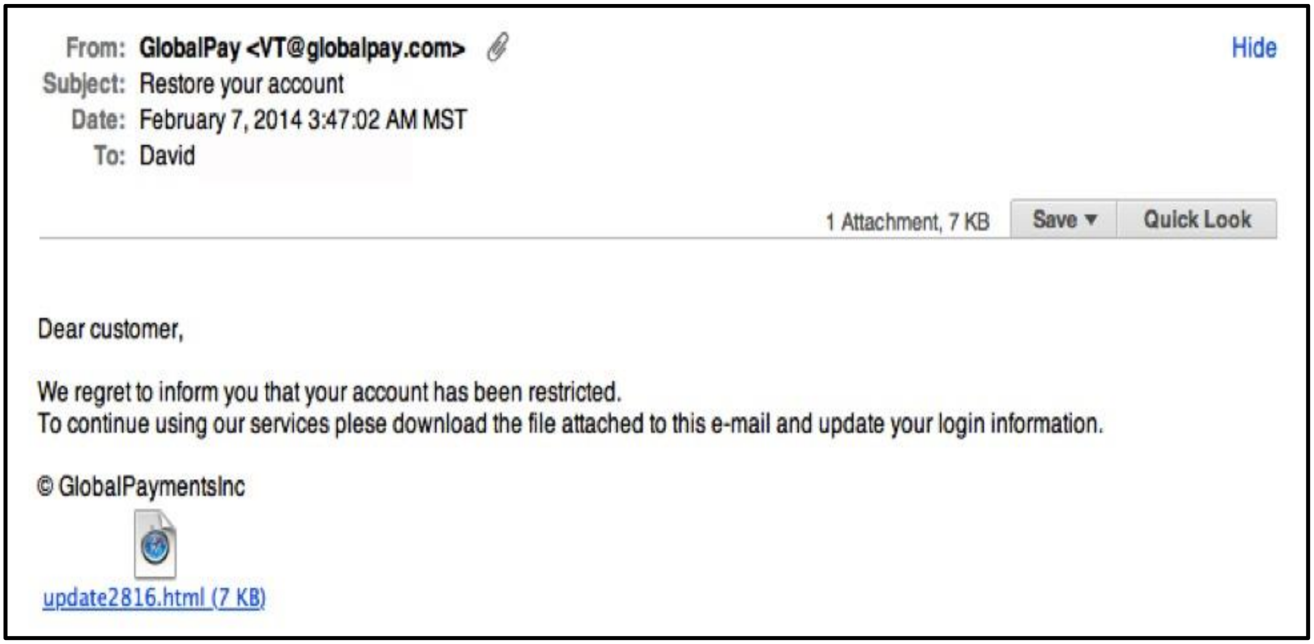


Dear customer your SBI CREDIT CARD point worth Rs 6897 expired by 06/08/2018. Kindly convert your points into cash by click here http://prosbicard.com/



Buy Apple IPhone X Mobile at *999 Rs (90% off) in Flash Sale.
👉http://bit.ly/Sale-Apple-iphoneX
Grab this offer now, Deal valid only for First 1,000 Customers.
Visit here to Buy-
👉http://bit.ly/Sale-Apple-iphoneX

Phishing Emails



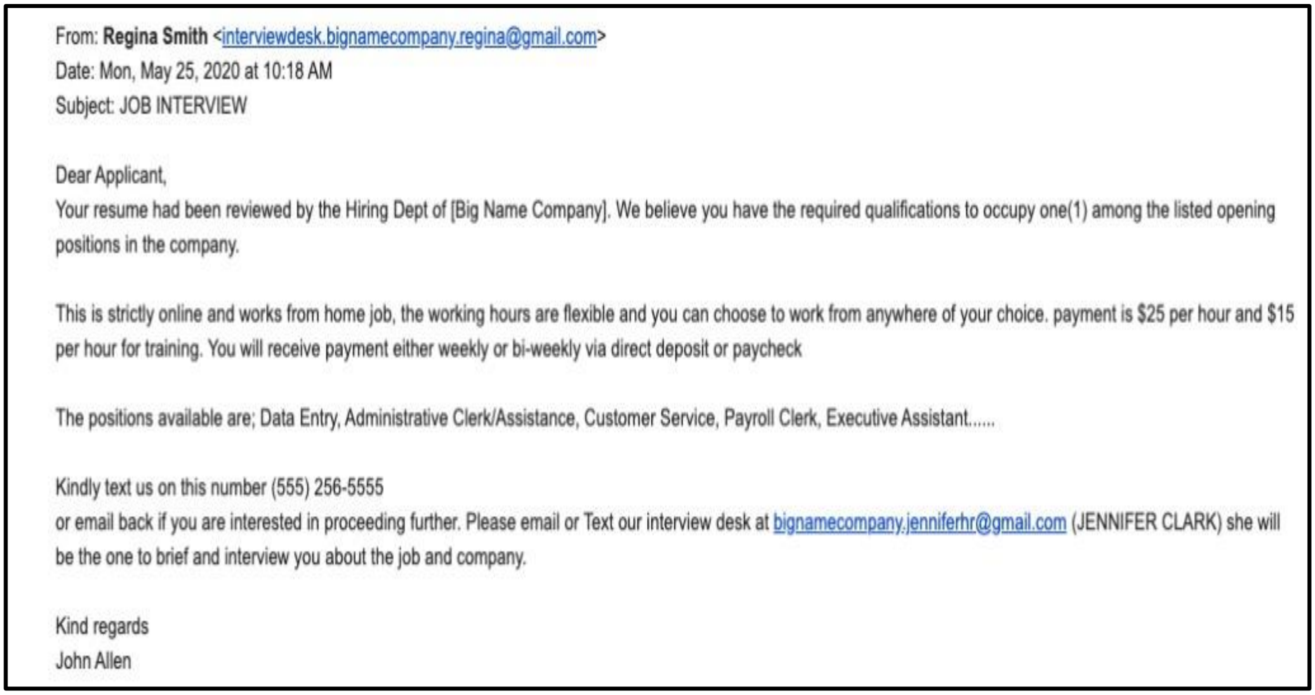
From: GlobalPay <VT@globalpay.com>
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

Dear customer,

We regret to inform you that your account has been restricted.
To continue using our services plese download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc

update2816.html (7 KB)



From: **Regina Smith** <interviewdesk.bignamecompany.regina@gmail.com>
Date: Mon, May 25, 2020 at 10:18 AM
Subject: JOB INTERVIEW

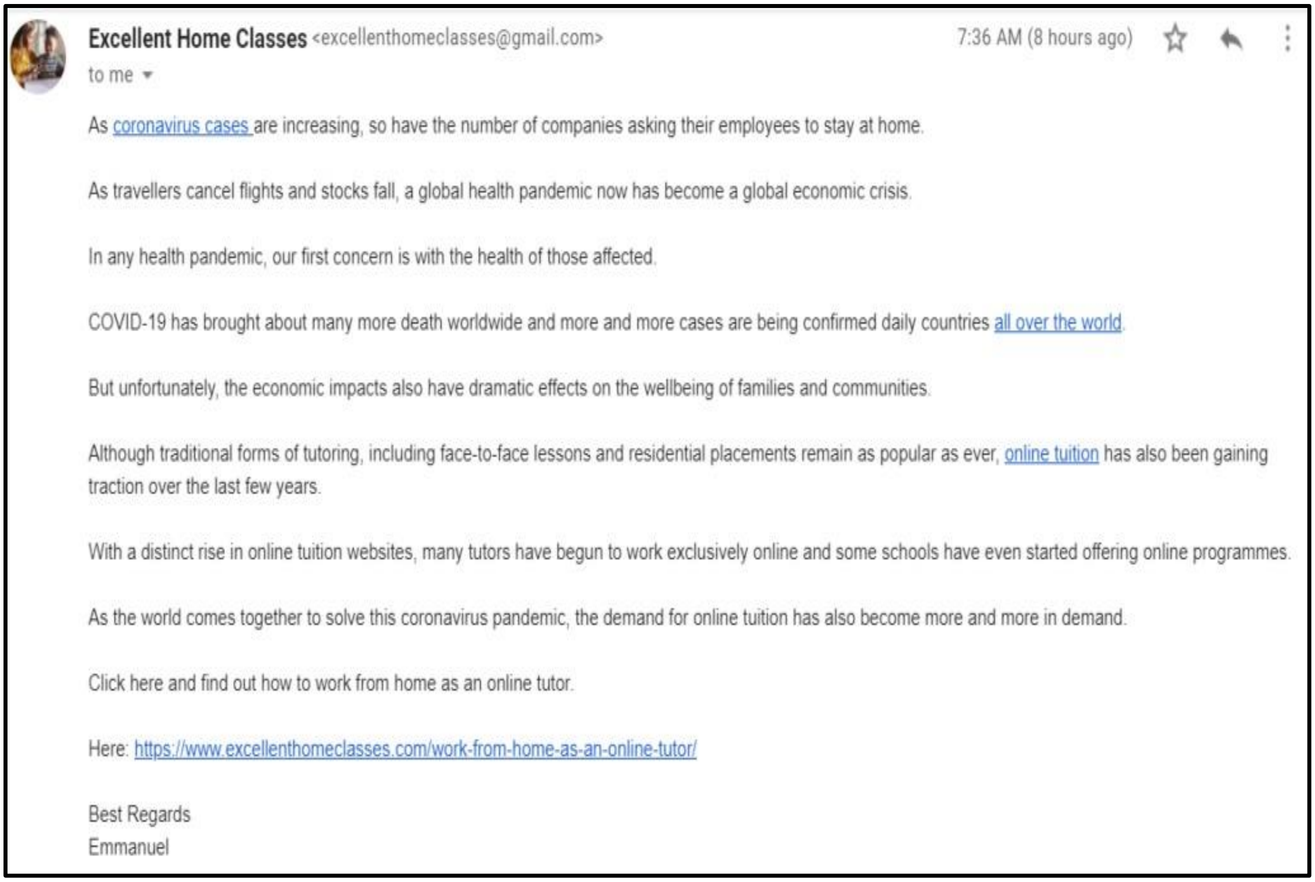
Dear Applicant,
Your resume had been reviewed by the Hiring Dept of [Big Name Company]. We believe you have the required qualifications to occupy one(1) among the listed opening positions in the company.

This is strictly online and works from home job, the working hours are flexible and you can choose to work from anywhere of your choice. payment is $25 per hour and $15 per hour for training. You will receive payment either weekly or bi-weekly via direct deposit or paycheck

The positions available are; Data Entry, Administrative Clerk/Assistance, Customer Service, Payroll Clerk, Executive Assistant......

Kindly text us on this number (555) 256-5555
or email back if you are interested in proceeding further. Please email or Text our interview desk at bignamecompany.jenniferhr@gmail.com (JENNIFER CLARK) she will be the one to brief and interview you about the job and company.

Kind regards
John Allen



Excellent Home Classes <excellenthomeclasses@gmail.com>

As coronavirus cases are increasing, so have the number of companies asking their employees to stay at home.

As travellers cancel flights and stocks fall, a global health pandemic now has become a global economic crisis.

In any health pandemic, our first concern is with the health of those affected.

COVID-19 has brought about many more death worldwide and more and more cases are being confirmed daily countries all over the world.

But unfortunately, the economic impacts also have dramatic effects on the wellbeing of families and communities.

Although traditional forms of tutoring, including face-to-face lessons and residential placements remain as popular as ever, online tuition has also been gaining traction over the last few years.

With a distinct rise in online tuition websites, many tutors have begun to work exclusively online and some schools have even started offering online programmes.

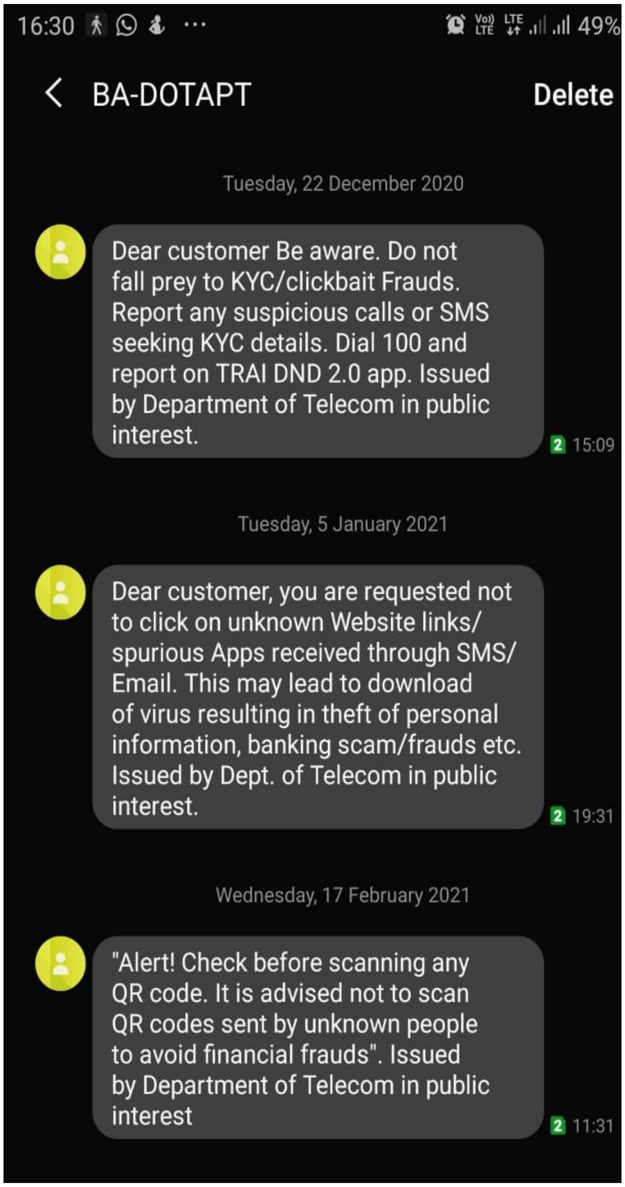
As the world comes together to solve this coronavirus pandemic, the demand for online tuition has also become more and more in demand.

Click here and find out how to work from home as an online tutor.

Here: https://www.excellenthomeclasses.com/work-from-home-as-an-online-tutor/

Best Regards
Emmanuel

12. GENUINE MESSAGES



Tuesday, 22 December 2020

Dear customer Be aware. Do not fall prey to KYC/clickbait Frauds. Report any suspicious calls or SMS seeking KYC details. Dial 100 and report on TRAI DND 2.0 app. Issued by Department of Telecom in public interest.

2 15:09

Tuesday, 5 January 2021

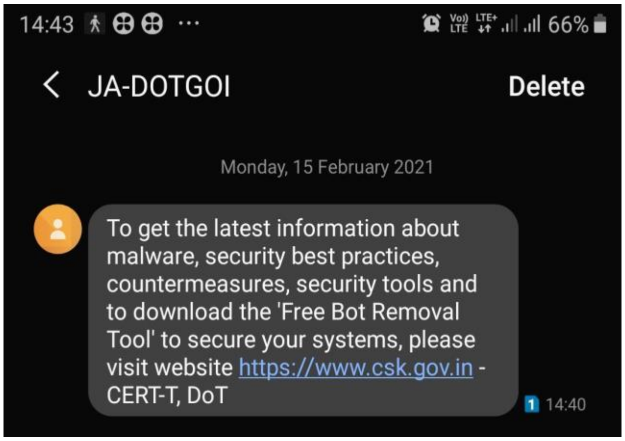
Dear customer, you are requested not to click on unknown Website links/ spurious Apps received through SMS/ Email. This may lead to download of virus resulting in theft of personal information, banking scam/frauds etc. Issued by Dept. of Telecom in public interest.

2 19:31

Wednesday, 17 February 2021

"Alert! Check before scanning any QR code. It is advised not to scan QR codes sent by unknown people to avoid financial frauds". Issued by Department of Telecom in public interest

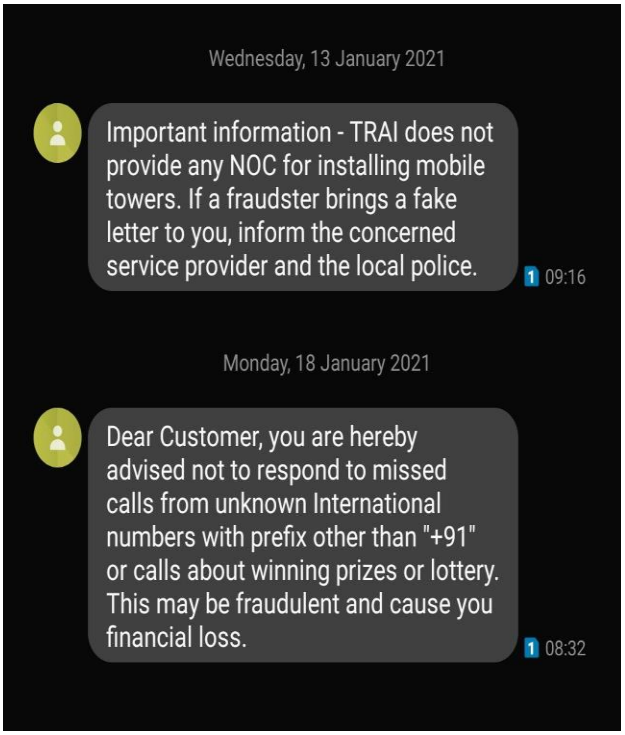
2 11:31



Monday, 15 February 2021

To get the latest information about malware, security best practices, countermeasures, security tools and to download the 'Free Bot Removal Tool' to secure your systems, please visit website https://www.csk.gov.in - CERT-T, DoT

1 14:40



Wednesday, 13 January 2021

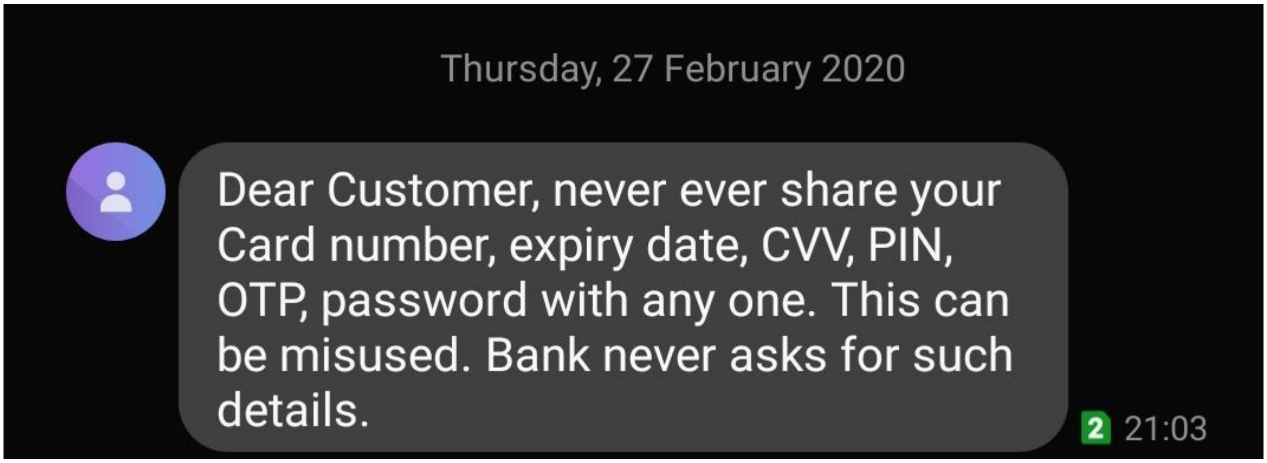
Important information - TRAI does not provide any NOC for installing mobile towers. If a fraudster brings a fake letter to you, inform the concerned service provider and the local police.

1 09:16

Monday, 18 January 2021

Dear Customer, you are hereby advised not to respond to missed calls from unknown International numbers with prefix other than "+91" or calls about winning prizes or lottery. This may be fraudulent and cause you financial loss.

1 08:32



Thursday, 27 February 2020

Dear Customer, never ever share your Card number, expiry date, CVV, PIN, OTP, password with any one. This can be misused. Bank never asks for such details.

2 21:03

SBI

SHARE HAPPINESS, SMILES, JOY...
BUT NEVER SHARE
PASSWORD, OTP, CVV.

SBI never asks for bank account details over a phone call.

Never share:

Account details	Debit Card number	Password or OTP
CVV and other details over phone/SMS		

#SafeBanking

ICICI Bank

Never share your ATM pin, CVV or OTP with anyone, as this may lead to unauthorized transactions. Also, never write down these sensitive banking details on a notepad or don't store them on your phone.

13. AWARENESS

Safety Tips – Payment Cards

NEVER write your PIN in a place where it can be seen by someone who you do not intend to show it to.

Always secure your debit card physically by storing it at a safe place.

NEVER let the person at the counter take your card out of your sight. Ideally there should not be any need for him/her to do so.

If you do not receive your debit card or PIN from the Bank within a reasonable amount of time after requesting for one, check with the Bank when it was dispatched and when you may expect to receive it. It may have been intercepted by someone else in transit.

Check your account statements carefully for transactions that you may not have made. Monthly email statements are free of cost these days for almost all banks - do make full use of the same.

ALWAYS shred or destroy the receipts/ charge-slips from merchants that are no longer required, especially when you have paid for using your debit card.

Safety Tips – ATM Usage

Safeguard your Credit & Debit cards at all times.

When you key in your PIN at an ATM, make sure that you sufficiently obscure the keypad from being viewed by onlookers.

While entering any personal identification numbers, use your discretion to shield the keypad so that your hand movements are not very visible to others.

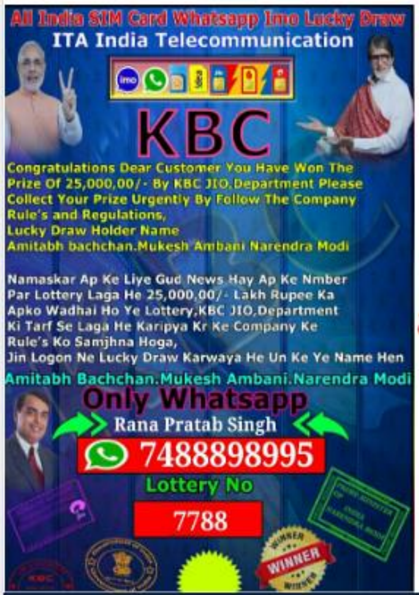
Beware of your surroundings while withdrawing money at ATMs. Do not crumple and throw away the transaction slips or credit card memos - read them, make a mental note of the details and then either tear them or shred them.

When your card gets jammed in the ATM, immediately call up the Bank's helpline for hot-listing and a new card will be issued to you.

If you notice something suspicious about the card slot on an ATM (like an attached device), do not use it and report it to the responsible authorities.

Avoid using ATMs which appear to be physically tampered, or damaged as they may have been manipulated by fraudsters.

మీ వాట్సాప్ నెంబర్ కి 25 లక్షల లాటరీ అంటే నమ్మవద్దు.



All India SIM Card Whatsapp Imo Lucky Draw
ITA India Telecommunication

KBC

Congratulations Dear Customer You Have Won The Prize Of 25,000,00/- By KBC JIO,Department Please Collect Your Prize Urgently By Follow The Company Rule's and Regulations,
Lucky Draw Holder Name
Amitabh bachchan.Mukesh Ambani Narendra Modi

Namaskar Ap Ke Liye Gud News Hay Ap Ke Nmber Par Lottery Laga He 25,000,00/- Lakh Rupee Ka Apko Wadhai Ho Ye Lottery,KBC JIO,Department Ki Tarf Se Laga He Karipya Kr Ke Company Ke Rule's Ko Samjhna Hoga,
Jin Logon Ne Lucky Draw Karwaya He Un Ke Ye Name Hen
Amitabh Bachchan.Mukesh Ambani.Narendra Modi

Only Whatsapp
Rana Pratab Singh
7488898995
Lottery No
7788

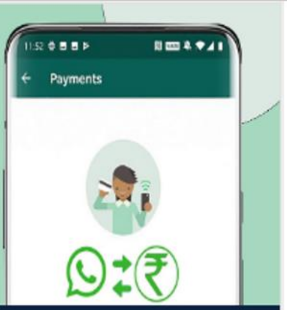
ఒక్క క్షణం ఆగండి.

ఇది మోసం అని గ్రహించండి.

వీటికి స్పందించవద్దు

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

WhatsApp Payments



Important Notice

Until now Google Pay, PhonePe, Paytm wallet services were used but now "WhatsApp Pay" is going to come.

You may receive unkonwn calls or messages or dubious links or OTP for whatsapp KYC but you do not respond and disclose your bank account details to anyone.

Know about "WhatsApp Pay" services well before use it.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

If you receive any message like "You won a lottery on your whatsapp number". Do not believe, It's Fake.

Remember!
If you believe it, then you will be cheated.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to repor t crime, for helpline call 155260 between 9am to 6pm//

Be Aware!

If you receive any calls, messages and dubious links for registration of 'COVID-19 Vaccine', do not believe such calls and messages and do not share Aadhar and its registered phone number with anyone.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

TELANGANA STATE
POLICE
Duty
Honour
Compassion

VOLUNTEERS NEEDED

If you want to help and curb the cyber crimes, join as a "Cyber Volunteer" and Join hands with the Telangana Police.

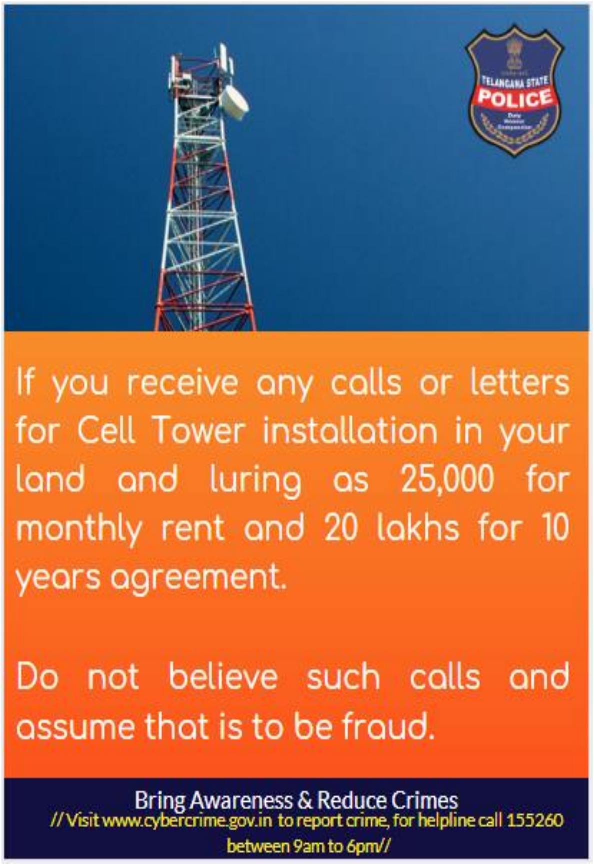
Please register your name as a Cyber Volunteer by visiting www.cybercrime.gov.in

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

+1, +92, +968, +44 starting phone calls are dubious calls. Remember! If you receive such calls, it means cyber criminals are trying to cheat you.

You may receive a whatsapp call with these numbers by displaying with your friend's photo also. So, don't believe such calls.

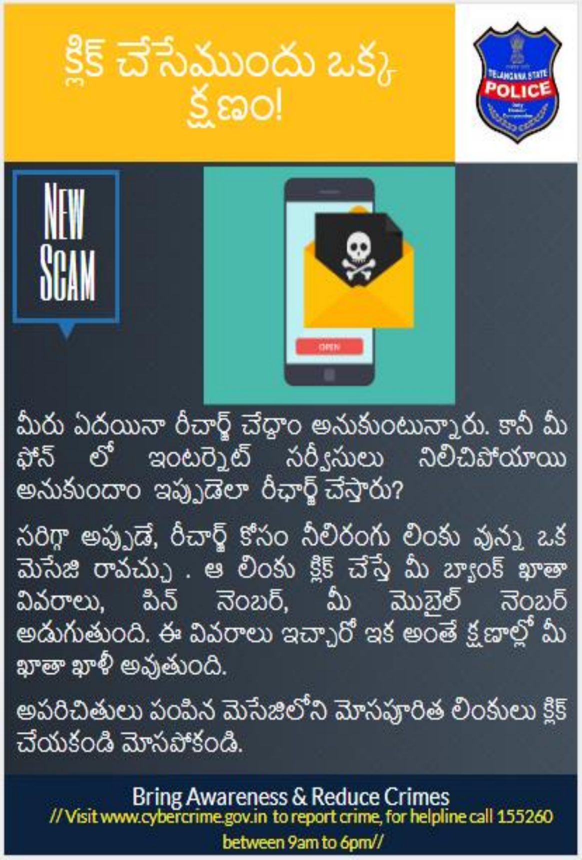
Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



If you receive any calls or letters for Cell Tower installation in your land and luring as 25,000 for monthly rent and 20 lakhs for 10 years agreement.

Do not believe such calls and assume that is to be fraud.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



క్లిక్ చేసేముందు ఒక్క క్షణం!

మీరు ఏదయినా రీచార్జ్ చేద్ధాం అనుకుంటున్నారు. కానీ మీ ఫోన్ లో ఇంటర్నెట్ సర్వీసులు నిలిచిపోయాయి అనుకుందాం ఇప్పుడెలా రీఛార్జ్ చేస్తారు?

సరిగ్గా అప్పుడే, రీచార్జ్ కోసం నీలిరంగు లింకు వున్న ఒక మెసేజి రావచ్చు . ఆ లింకు క్లిక్ చేస్తే మీ బ్యాంక్ ఖాతా వివరాలు, పిన్ నెంబర్, మీ మొబైల్ నెంబర్ అడుగుతుంది. ఈ వివరాలు ఇచ్చారో ఇక అంతే క్షణాల్లో మీ ఖాతా ఖాళీ అవుతుంది.

అపరిచితులు పంపిన మెసేజిలోని మోసపూరిత లింకులు క్లిక్ చేయకండి మోసపోకండి.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

Just lock your mouth and save your money present in your account.

Do not reveal OTP to Unknown.

Bring Awareness & Reduce Crimes
// Visit www.cybercrime.gov.in to repor t crime, for helpline call 155260 between 9am to 6pm//

FRAUD SMS
BH-PayTM
TELANGANA STATE POLICE
AnyDesk
Quick Support
Team Viewer

DO NOT download any app for Paytm KYC

Dear Paytm User, Your Paytm A/C KYC has expired. Download App Immediately for Verification or A/C will be blocked in 24hr. Download App Click here

Do not download AnyDesk, QuickSupport and TeamViewer apps. These remote apps make empty your bank accounts.

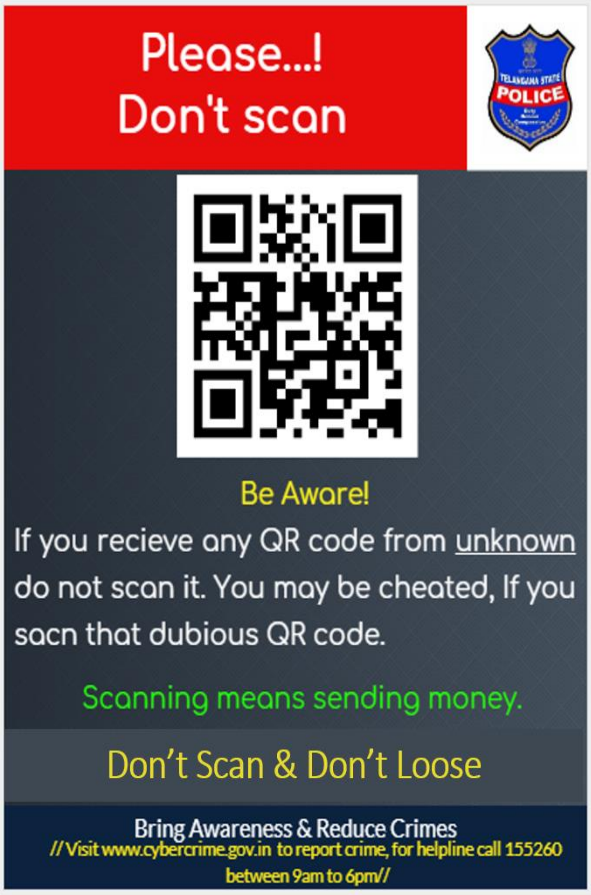
Bring Awareness & Reduce Crimes
// Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

హెచ్చరిక.

Paytm KYC పూర్తిచేయడానికి అపరిచిత వ్యక్తులు ఎవ్వరు చెప్పినా AnyDesk, QuickSupport, SMS to Phone వంటి రిమోట్ ఆప్ లను డౌన్లోడ్ చేయకండి.

ఈ ఆప్ లతో సైబర్ నేరగాళ్లు మీ బ్యాంక్ ఖాతాను క్షణాల్లో ఖాళీ చేస్తారు. జాగ్రత్త.

Bring Awareness & Reduce Crimes
// Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



Please...!
Don't scan

Be Aware!

If you recieve any QR code from unknown do not scan it. You may be cheated, If you sacn that dubious QR code.

Scanning means sending money.

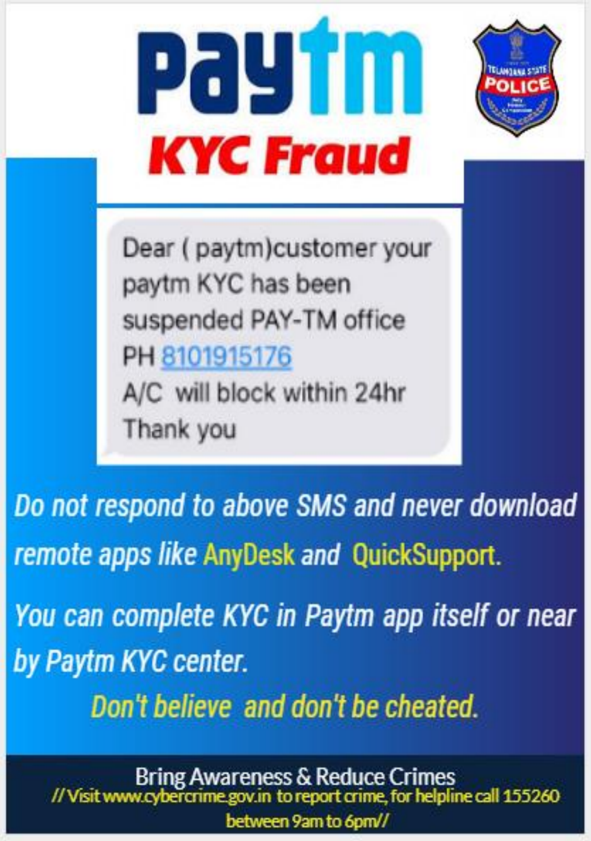
Don't Scan & Don't Loose

Bring Awareness & Reduce Crimes
// Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

TELANGANA STATE
POLICE

Cyber criminals are watching your Facebook profile and creating fake profile with your photos and sending messages to your friends behalf of you and asking money. Your friends may belive that message was sent by you and might be cheated. If you are in Facebook just " LOCK " your profile to see you and your friends only. Then why late LOCK your profile immediately.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



KYC Fraud

Dear (paytm)customer your paytm KYC has been suspended PAY-TM office PH 8101915176
A/C will block within 24hr
Thank you

Do not respond to above SMS and never download remote apps like AnyDesk and QuickSupport.

You can complete KYC in Paytm app itself or near by Paytm KYC center.

Don't believe and don't be cheated.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

TELANGANA STATE
POLICE

అపరిచితులకు OTP చెప్తే అంతే మరి.

బ్యాంకు ఖాతాలో లక్ష రూపాయలు ఉన్నప్పుడు.

ఒక అపరిచిత వ్యక్తి OTP అడిగితే చెప్పేసాడు.
లక్ష పోయాయి.

ఏంటి. ఇలా కూడా చేస్తారా?
ఖాతాలో ఒక్క రూపాయి కూడా ఉంచరా!

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

TELANGANA STATE
POLICE
I never share my OTP with anyone but you?

Please...!
Don't share it.

Be Aware!

Cyber Criminals are creatinkg fake whatsapp with your number. If you receive any OTP don't share it with anyone.

Don't share & don't be cheated

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

OLX

In OLX, If the seller pretending as a ARMY person do not believe and do not pay any amount to deliver the goods .

TELANGANA STATE POLICE

Bring Awareness & Reduce Crimes

// Visit www.cybercrime.gov.in to repor t crime, for helpline call 155260 between 9am to 6pm//

TELANGANA STATE POLICE

DISCOUNT UPTO 45%

ఫేస్బుక్, వాట్సాప్, ట్విట్టర్ మరియు ఇంస్టాగ్రామ్ లలో వచ్చే మోసపూరిత డిస్కౌంట్ ఆఫర్ ప్రకటనలను క్లిక్ చేయకండి. నేరుగా ఫ్లిప్ కార్ట్, అమెజాన్, మింత్రా వంటి 'అధికారిక' వెబ్సైట్ల లోనే ఆఫర్లు ఉన్నాయేమో చూసుకోండి.

సైబర్ నేరగాళ్లు పండగ ఆఫర్ల పేరుతో ఇంటర్నెట్లో అబద్ధపు ప్రకటనలు ఉంచారు. కేవలం మీ క్లిక్ కోసం ఎదురుచూస్తున్నారు అంతే.

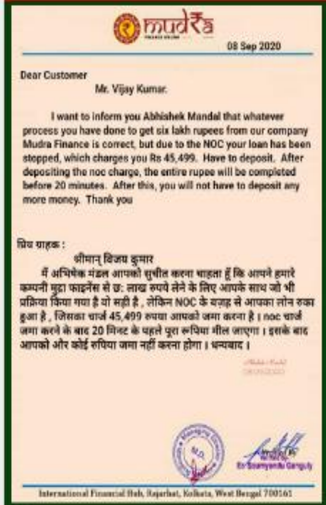
డిస్కౌంట్ ఆఫర్లకు పోయి పండగ పూట మోసపోకండి.

Bring Awareness & Reduce Crimes

// Visit www.cybercrime.gov.in to repor t crime, for helpline call 155260 between 9am to 6pm//

Don't believe Fake Loan Offers

TELANGANA STATE POLICE



mudra

08 Sep 2020

Dear Customer

Mr. Vijay Kumar.

I want to inform you Abhishek Mandal that whatever process you have done to get six lakh rupees from our company Mudra Finance is correct, but due to the NOC your loan has been stopped, which charges you Rs 45,499. Have to deposit. After depositing the noc charge, the entire rupee will be completed before 20 minutes. After this, you will not have to deposit any more money. Thank you

प्रिय ग्राहक :

श्रीमान् विजय कुमार

मैं अभिषेक मंडल आपको सूचीत करना चाहता हूं कि आपने हमारे कम्पनी मुद्रा फाइनेंस से छः लाख रुपये लेने के लिए आपके साथ जो भी प्रक्रिया किया गया है यो सही है , लेकिन NOC के वजह से आपका लोन रुका हुआ है , जिसका चार्ज 45,499 रुपया आपको जमा करना है । noc चार्ज जमा करने के बाद 20 मिनट के पहले पुरा रूपिया मील जाएगा । इसके बाद आपको और कोई रुपिया जमा नहीं करना होगा । धन्यवाद ।

Er Soumyendu Ganguly

International Financial Hub, Rajarhat, Kolkata, West Bengal 700161

Be aware. Cyber Criminals are misusing the Government Mudra Loan Policy.

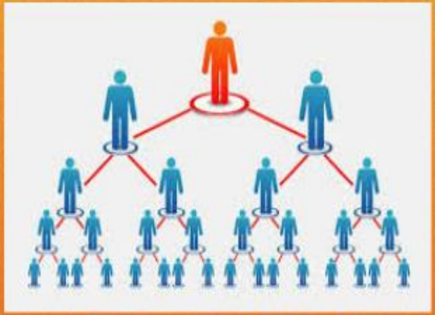
If you recieve any message or mail with loan offer, don't respond and pay any charges for loan approval.

Bring Awareness & Reduce Crimes

// Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

Be Aware of Fake Multi Level Marketing Schemes

TELANGANA STATE POLICE



ముందుగా కొన్ని డబ్బులు కట్టి ఒకరు ఇద్దరినీ, ఇద్దరు మరో ఇద్దరినీ చేర్పించడం వంటి ఆన్లైన్ మార్కెటింగ్ స్కీముల వైపు ఆకర్షితులు అవకండి.

డబ్బుల కోసం డబ్బులు కట్టడమంటే మోసం జరగదంటారా?

ఇవి స్కీములు కాదు మిమ్మల్ని మోసం చేసే స్కాములు. జాగ్రత్త పడాల్సింది మీరే.

Bring Awareness & Reduce Crimes

// Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

ఇవి చేయకండి చాలు.

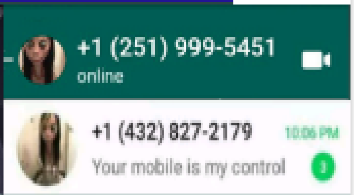
1. అపరిచితులకు OTP చెప్పకండి.
2. మీ కార్డు వివరాలు చెప్పకండి.
3. AnyDesk, Quick Support ఆప్ లను డౌన్లోడ్ చేయకండి.
4. అనుమానిత నీలిరంగు లింకులను క్లిక్ చేయకండి
5. అపరిచితులు పంపిన QR కోడ్ స్కాన్ చేయకండి.

లేదంటే మీ ఖాతాలు ఖాళీ అవుతాయి జాగ్రత్త.

మీకు అర్థం అవుతుందా...

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260
between 9am to 6pm//

ఎవరు ఈ అపరిచితులు???



+1 (251) 999-5451
online

+1 (432) 827-2179 10:06 PM
Your mobile is my control 3

- వాట్సాప్ లో మీకు తెలిసిన వ్యక్తి ఫోటో వుండి, వాట్సాప్ నెంబర్ +1 , +968 , +44 లతో మెసేజి గాని, కాల్ గాని వచ్చిందా? తస్మాత్ జాగ్రత్త.
- మీ స్నేహితుల, బంధువుల ఫోటోలను వాట్సాప్ DP గాపెట్టి అత్యవసరంగా డబ్బులు అవసరమని మిమ్మల్ని మోసం చేయవచ్చు.
- గుర్తుంచుకోండి. ఆ అపరిచితులు సైబర్ నేరగాళ్లు మీ బంధువులు కాదు.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260
between 9am to 6pm//

అపరిచిత వ్యక్తులకు OTP, UPI పిన్ నెంబర్,
బ్యాంకు ఖాతా వివరాలు చెప్పవద్దు.
ఎవరైనా అడిగితే

మీరు నోరు మూసుకోండి అంతే.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to repor t crime, for helpline call 155260
between 9am to 6pm//

ఎవరో తెలుసుకోండి.

ఒంటరి మహిళలకు విజ్ఞప్తి.

మ్యాట్రిమోనీ వెబ్సైట్లలో పరిచయం అయిన వ్యక్తులు
విలువైన బహుమతులు పంపిస్తున్నాను అంటే
మోసమని గ్రహించండి.

ఫేస్బుక్, వాట్సాప్ లో ఫోటోలు చూసి నమ్మకండి.
కళ్ళు తెరవండి, ఎవరో తెలుసుకోండి.

అపరిచితులు చెప్పే కథలు నమ్మకండి
వారి ఖాతాల్లో డబ్బులు వేసి మోసపోకండి.

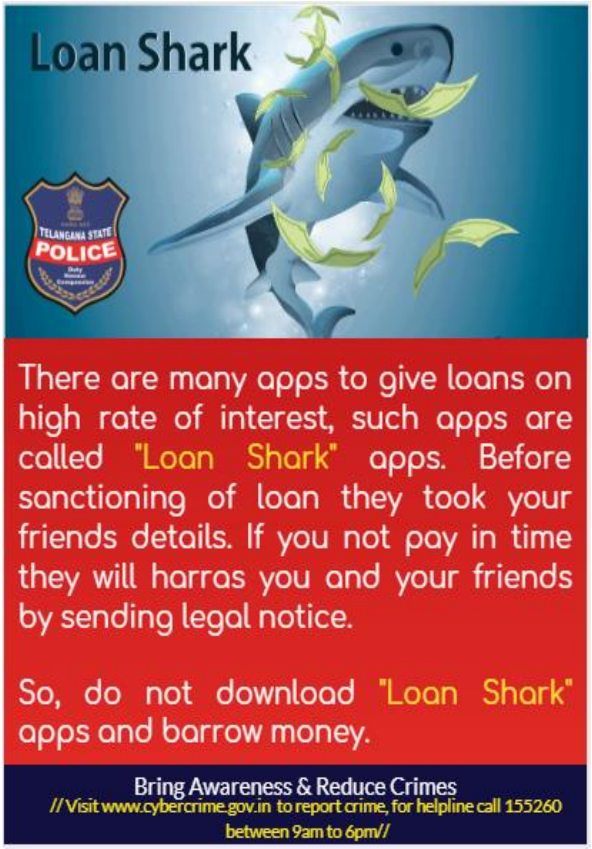
Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260
between 9am to 6pm//

It's Danger

DO NOT DOWNLOAD LOAN APPLICATIONS AND TAKE LOANS FROM THEM.

YOU WILL BE CHEATED AND HARRASSED BY THE MONEY LENDERS.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



Loan Shark

There are many apps to give loans on high rate of interest, such apps are called "Loan Shark" apps. Before sanctioning of loan they took your friends details. If you not pay in time they will harras you and your friends by sending legal notice.

So, do not download "Loan Shark" apps and barrow money.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

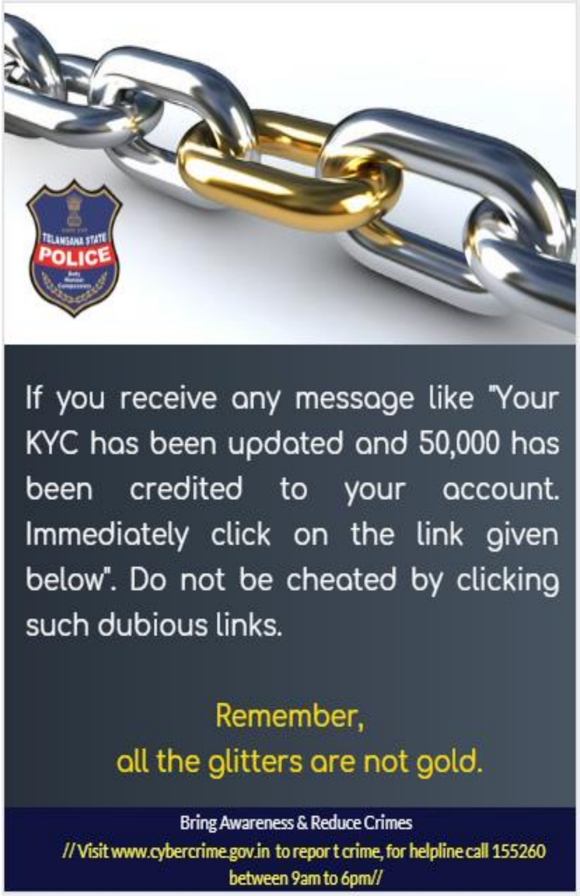
Do not download and get instant loan from Loan aaps.

If you want to take a loan from Loan apps, Remember, you must give follwing details.

Personal details
Permanant Address
Bank details
All your phone contacts
and agreement.

If you could not pay in time, you and your friends will be harrassed and received a legal notice also. Beware of it.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



If you receive any message like "Your KYC has been updated and 50,000 has been credited to your account. Immediately click on the link given below". Do not be cheated by clicking such dubious links.

Remember,
all the glitters are not gold.

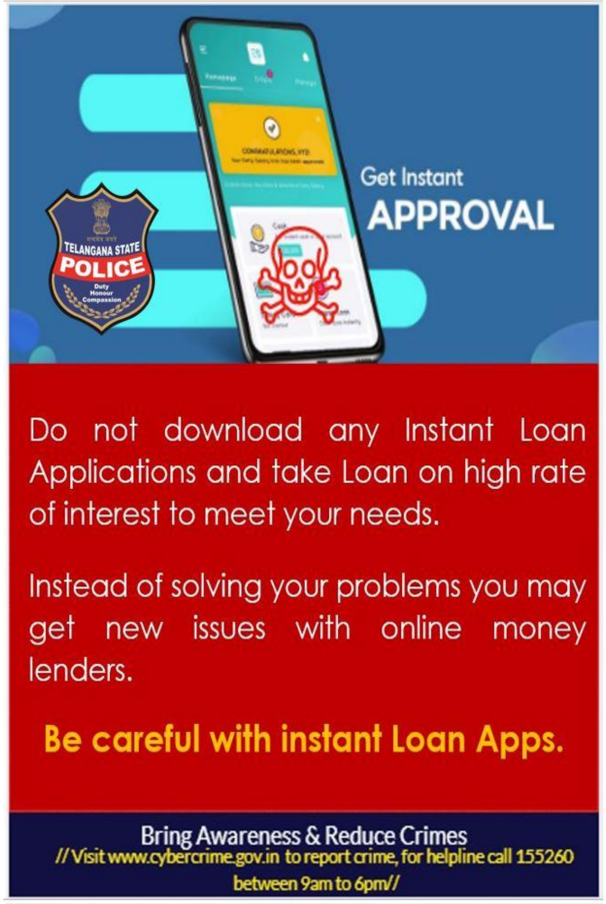
Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to repor t crime, for helpline call 155260 between 9am to 6pm//

Be Alert !

If you receive unknown calls regarding your insurance policy do not respond and pay any amounts.

Always verify with your policy authority but not with unknown.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



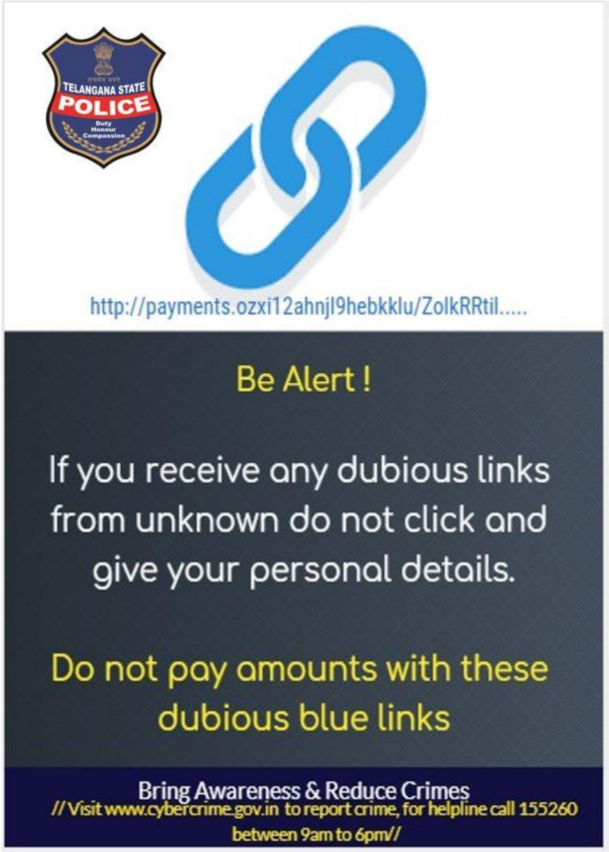
Get Instant
APPROVAL

Do not download any Instant Loan Applications and take Loan on high rate of interest to meet your needs.

Instead of solving your problems you may get new issues with online money lenders.

Be careful with instant Loan Apps.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



http://payments.ozxi12ahnjl9hebkklu/ZolkRRtil.....

Be Alert !

If you receive any dubious links from unknown do not click and give your personal details.

Do not pay amounts with these dubious blue links

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

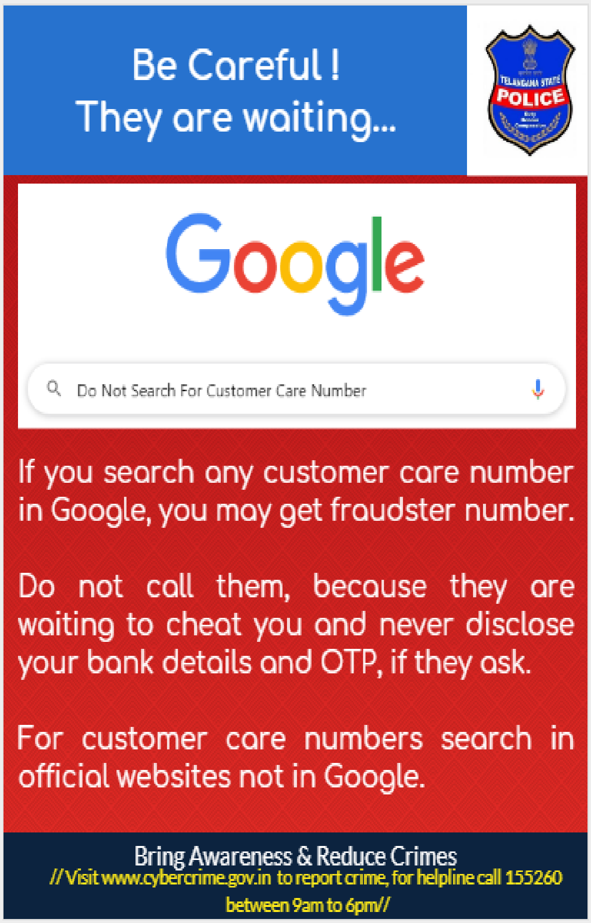
BEWARE OF
FAKE JOB OFFERS!

Have you applied for a job online?

The employer will not ask you for money. to give job.

Your unemployment should not be a lucrative job for cyber criminals.
Be careful.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



Be Careful ! They are waiting...

Google

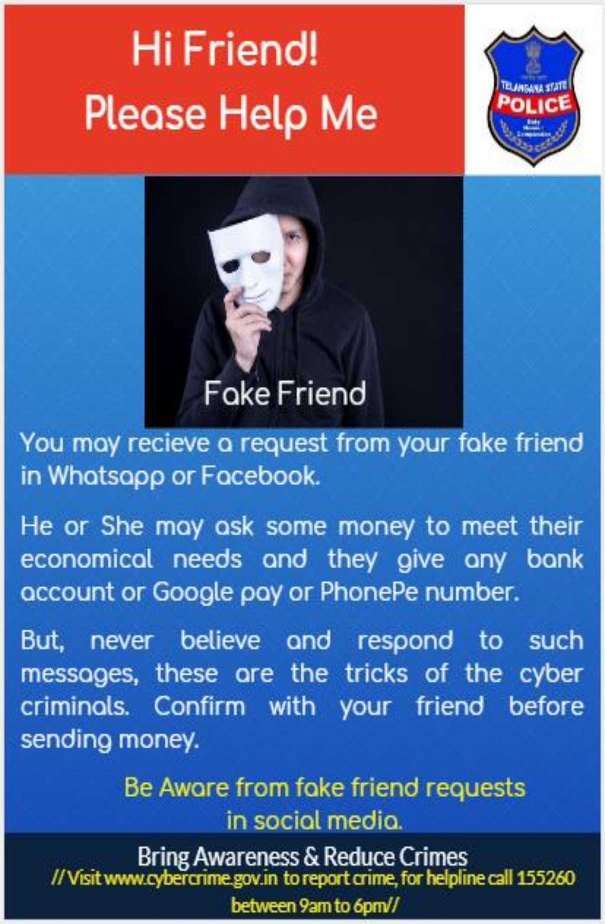
Do Not Search For Customer Care Number

If you search any customer care number in Google, you may get fraudster number.

Do not call them, because they are waiting to cheat you and never disclose your bank details and OTP, if they ask.

For customer care numbers search in official websites not in Google.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



Hi Friend! Please Help Me

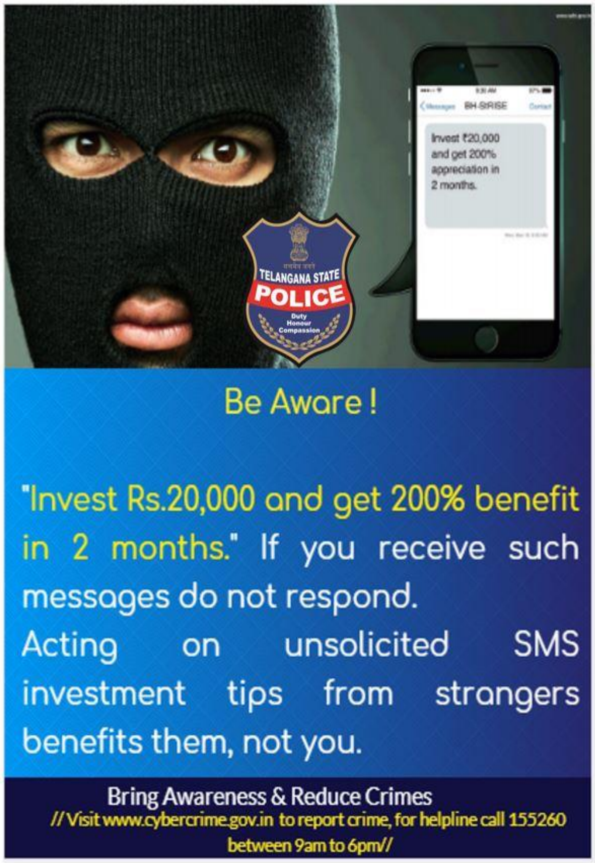
You may recieve a request from your fake friend in Whatsapp or Facebook.

He or She may ask some money to meet their economical needs and they give any bank account or Google pay or PhonePe number.

But, never believe and respond to such messages, these are the tricks of the cyber criminals. Confirm with your friend before sending money.

Be Aware from fake friend requests in social media.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



Be Aware !

"Invest Rs.20,000 and get 200% benefit in 2 months." If you receive such messages do not respond.
Acting on unsolicited SMS investment tips from strangers benefits them, not you.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

ONLY FOR MEN

Half naked video call from strange woman, you also want to make a half naked video call. But, threatening to put your video on Whatsapp, Facebook is the present trend of Cyber Criminals.
So, Be Careful.

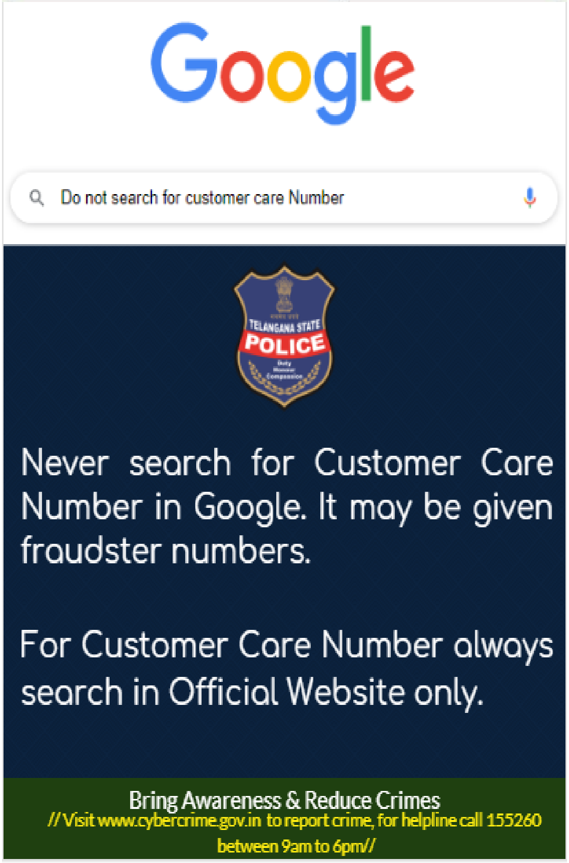
Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

Dear
This is for you

Never believe and suspect on valuable gift offers from strangers who met on social media platforms like Facebook, Instagram and Twitter. They might be cyber criminals.

If you believe them, you will be cheated.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

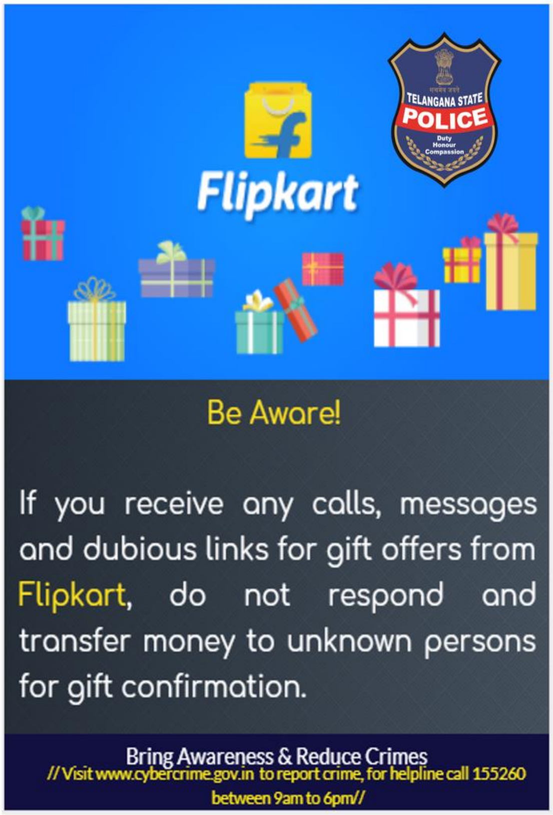


Do not search for customer care Number

Never search for Customer Care Number in Google. It may be given fraudster numbers.

For Customer Care Number always search in Official Website only.

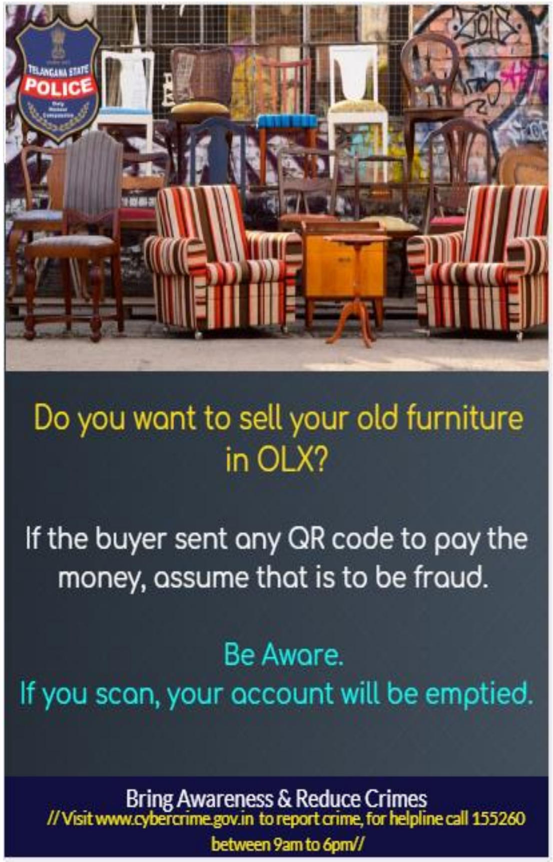
Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



Be Aware!

If you receive any calls, messages and dubious links for gift offers from Flipkart, do not respond and transfer money to unknown persons for gift confirmation.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



Do you want to sell your old furniture in OLX?

If the buyer sent any QR code to pay the money, assume that is to be fraud.

Be Aware.
If you scan, your account will be emptied.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

లోన్ ఆప్ ల ద్వారా మీరు అప్పు తీసుకుంటే మీకు
అప్పు ఇచ్చినవారి నుండి వేధింపులే కాదు మీరు
మనోవేదనకు కూడా గురికావచ్చు.
లోన్ ఆప్ లను డౌన్లోడ్ చేయవద్దు, లోన్ తీసుకోవద్దు.

ఈ అప్పు మీ ప్రాణాలకు ముప్పు. జాగ్రత్త.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260
between 9am to 6pm//

Report Cyber Crime only in official website. Do not believe FAKE wesites and pay any charges.

☑ Official website:
www.cybercrime.gov.in

☒ Fake website:
www.jancybersurakshakendra.com

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260
between 9am to 6pm//

How to Delete
Fake Facebook Accounts

Any Fake Facebook profile was created with your Name and Photo by anyone?

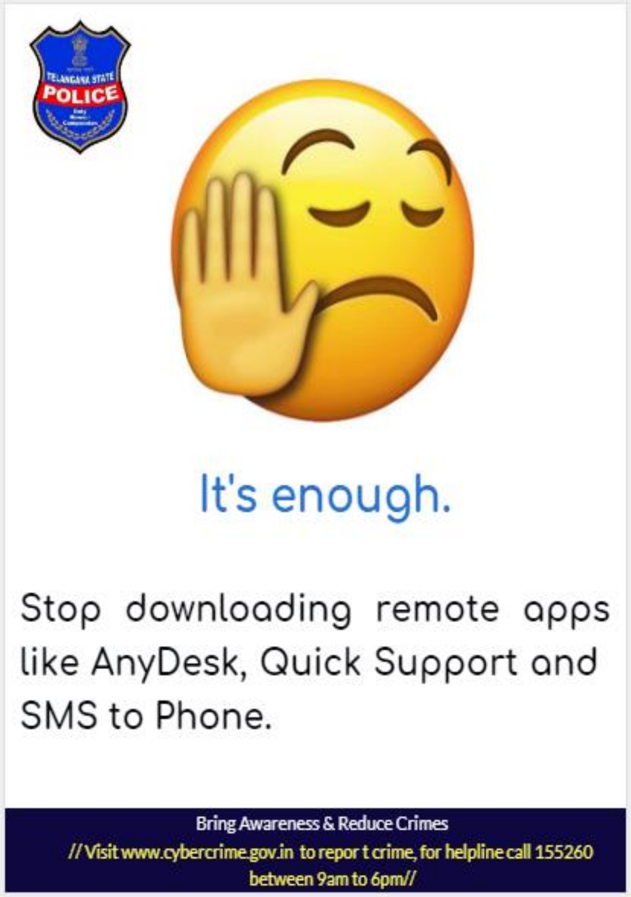
Please inform to your 20 friends as below.

Click three dots on top right corner of the Fake profile and choose report option and click "Delete Account". Facebook removes that fake account immediately.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260
between 9am to 6pm//

Don't waste time report cyber crime as early as possible in www.cybercrime.gov.in

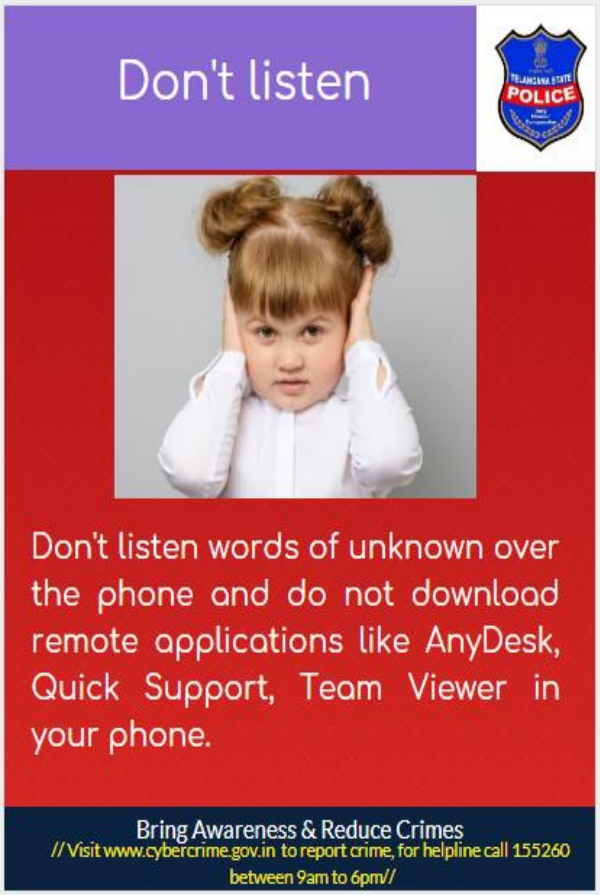
Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to repor t crime, for helpline call 155260
between 9am to 6pm//



It's enough.

Stop downloading remote apps like AnyDesk, Quick Support and SMS to Phone.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to repor t crime, for helpline call 155260
between 9am to 6pm//



Don't listen

Don't listen words of unknown over the phone and do not download remote applications like AnyDesk, Quick Support, Team Viewer in your phone.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260
between 9am to 6pm//

Don't be late

Report Cyber Crime as early as possible on www.cybercrime.gov.in before it's too late.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260
between 9am to 6pm//

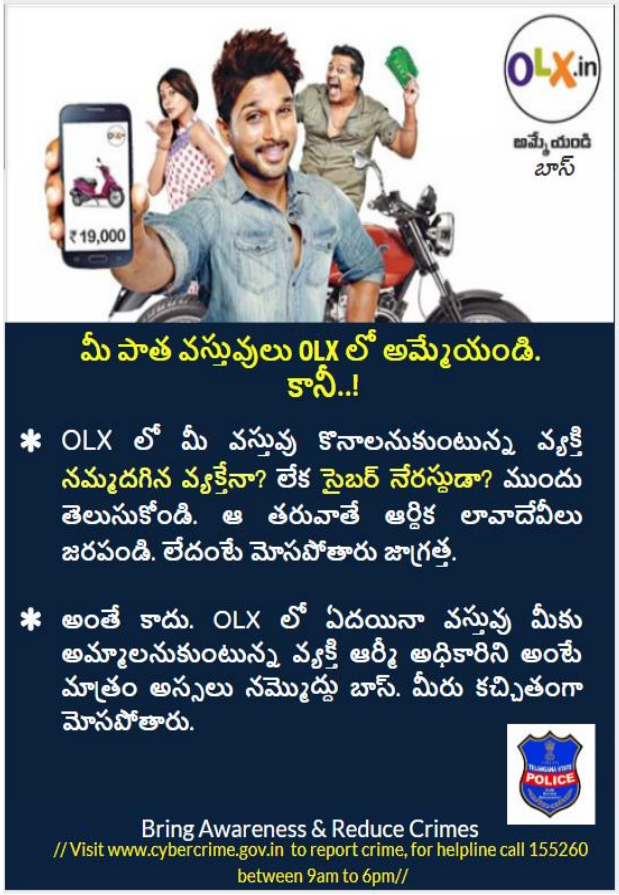
Your dating aap is playground for fraudsters

Be careful, if you use dating apps like Tinder, Mingle, OKCupid, Hinge, and Bumble.

Never share your personal information, photos and your vulnerabilities with unknown persons on dating aaps. Because, the other side are cyber criminals.

If you beleive them. You may be cheated emotionally and economically. Be aware!

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260
between 9am to 6pm//

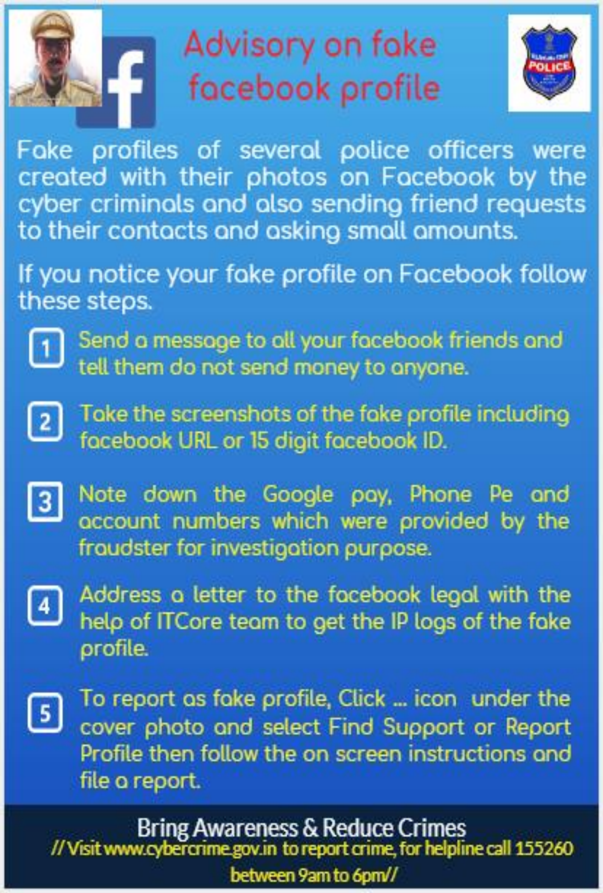


మీ పాత వస్తువులు OLX లో అమ్మేయండి.
కానీ..!

✱ OLX లో మీ వస్తువు కొనాలనుకుంటున్న వ్యక్తి నమ్మదగిన వ్యక్తేనా? లేక సైబర్ నేరస్థుడా? ముందు తెలుసుకోండి. ఆ తరువాతే ఆర్థిక లావాదేవీలు జరపండి. లేదంటే మోసపోతారు జాగ్రత్త.

✱ అంతే కాదు. OLX లో ఏదయినా వస్తువు మీకు అమ్మాలనుకుంటున్న వ్యక్తి ఆర్మీ అధికారిని అంటే మాత్రం అస్సలు నమ్మొద్దు బాస్. మీరు కచ్చితంగా మోసపోతారు.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



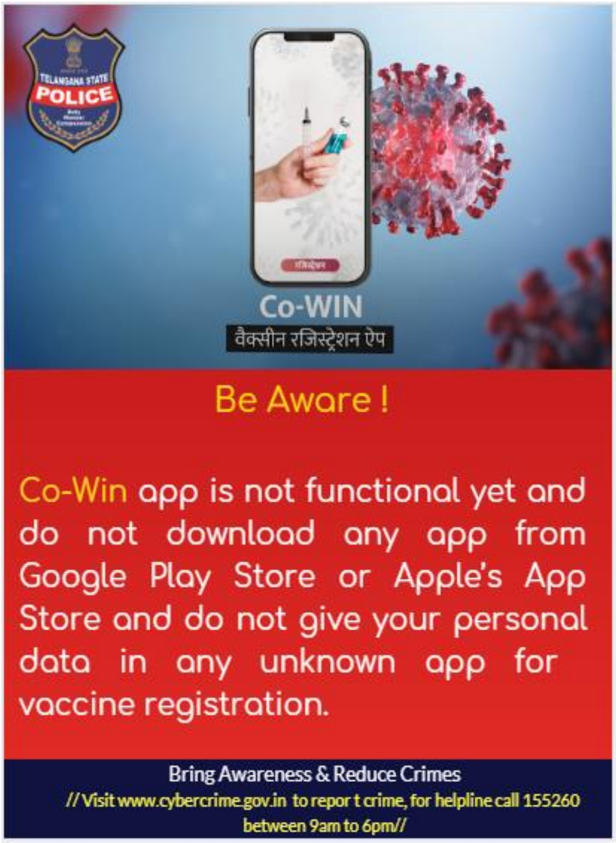
Advisory on fake facebook profile

Fake profiles of several police officers were created with their photos on Facebook by the cyber criminals and also sending friend requests to their contacts and asking small amounts.

If you notice your fake profile on Facebook follow these steps.

1. Send a message to all your facebook friends and tell them do not send money to anyone.
2. Take the screenshots of the fake profile including facebook URL or 15 digit facebook ID.
3. Note down the Google pay, Phone Pe and account numbers which were provided by the fraudster for investigation purpose.
4. Address a letter to the facebook legal with the help of ITCore team to get the IP logs of the fake profile.
5. To report as fake profile, Click ... icon under the cover photo and select Find Support or Report Profile then follow the on screen instructions and file a report.

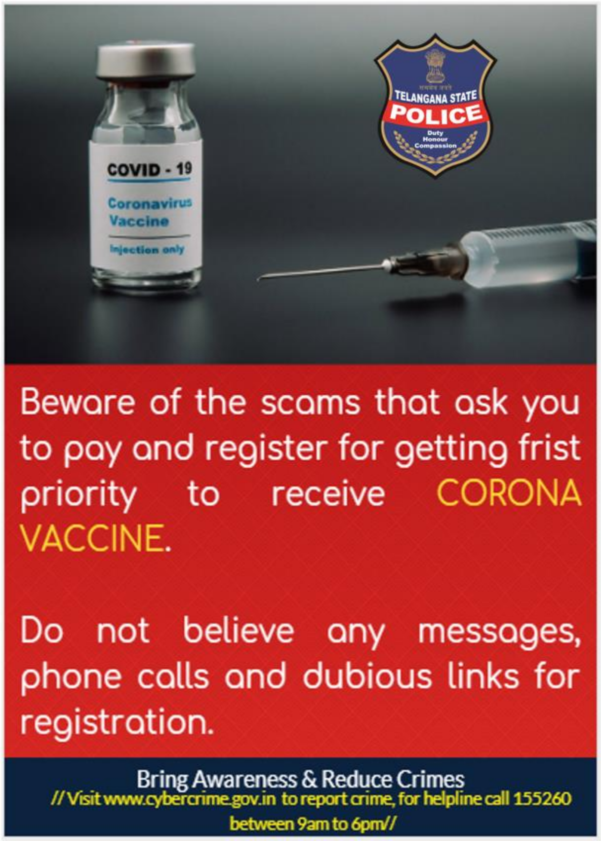
Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



Be Aware !

Co-Win app is not functional yet and do not download any app from Google Play Store or Apple's App Store and do not give your personal data in any unknown app for vaccine registration.

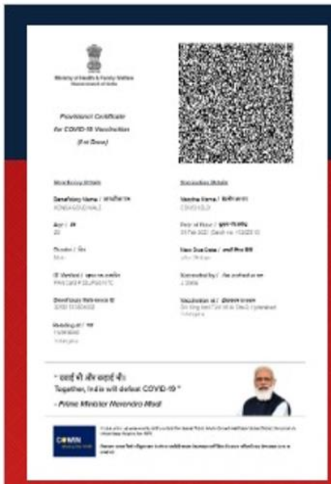
Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to repor t crime, for helpline call 155260 between 9am to 6pm//



Beware of the scams that ask you to pay and register for getting frist priority to receive CORONA VACCINE.

Do not believe any messages, phone calls and dubious links for registration.

Bring Awareness & Reduce Crimes
//Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//



Provisional Certificate for COVID-19 Vaccination

" Together, India will defeat COVID-19 "

- Prime Minister Narendra Modi

Be Alert

Do not share your Co-win Provissional Certificate in Social Media and do not put as profile picture in Whatsapp. This certificate contains your Name & PAN number, it is enough to the cyber criminals to cheat you.

Bring Awareness & Reduce Crimes
// Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

Be Aware !

If you receive any investment tips in unknown Telegram and Whatsapp groups on BITCOINS, do not beleive them.

Cyber Criminals are luring the innocent people to invest on BITCOINS to cheat.

Bring Awareness & Reduce Crimes
// Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

చిక్కుకుంటారేమో!
జాగ్రత్త.

లోన్ ఇస్తామని వచ్చే ఫోన్ కాల్, మెసేజ్ మరియు ఈ - మెయిల్ ని నమ్మవద్దు.

తక్కువ వడ్డీ అని మీకు ఎర వేసినా వారి గాలానికి చిక్కుకోవద్దు, చిక్కుల్లో పడవద్దు.

సైబర్ నేరం మీరు మోసపోయేంతవరకూ తెలియదు.
ఆశపడవద్దు, మోసపోవద్దు.

Bring Awareness & Reduce Crimes
// Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

అమెజాన్ నుండి మీకు విలువైన బహుమతి లేదా లక్షల రూపాయల లాటరీ వచ్చిందని మెసేజిలు వస్తే స్పందించకండి అవి మోసపూరిత ప్రకటనలని గ్రహించండి.

అపరిచితుల ఖాతాల్లోకి నగదు బదిలీ చేయకండి, మోసపోకండి.

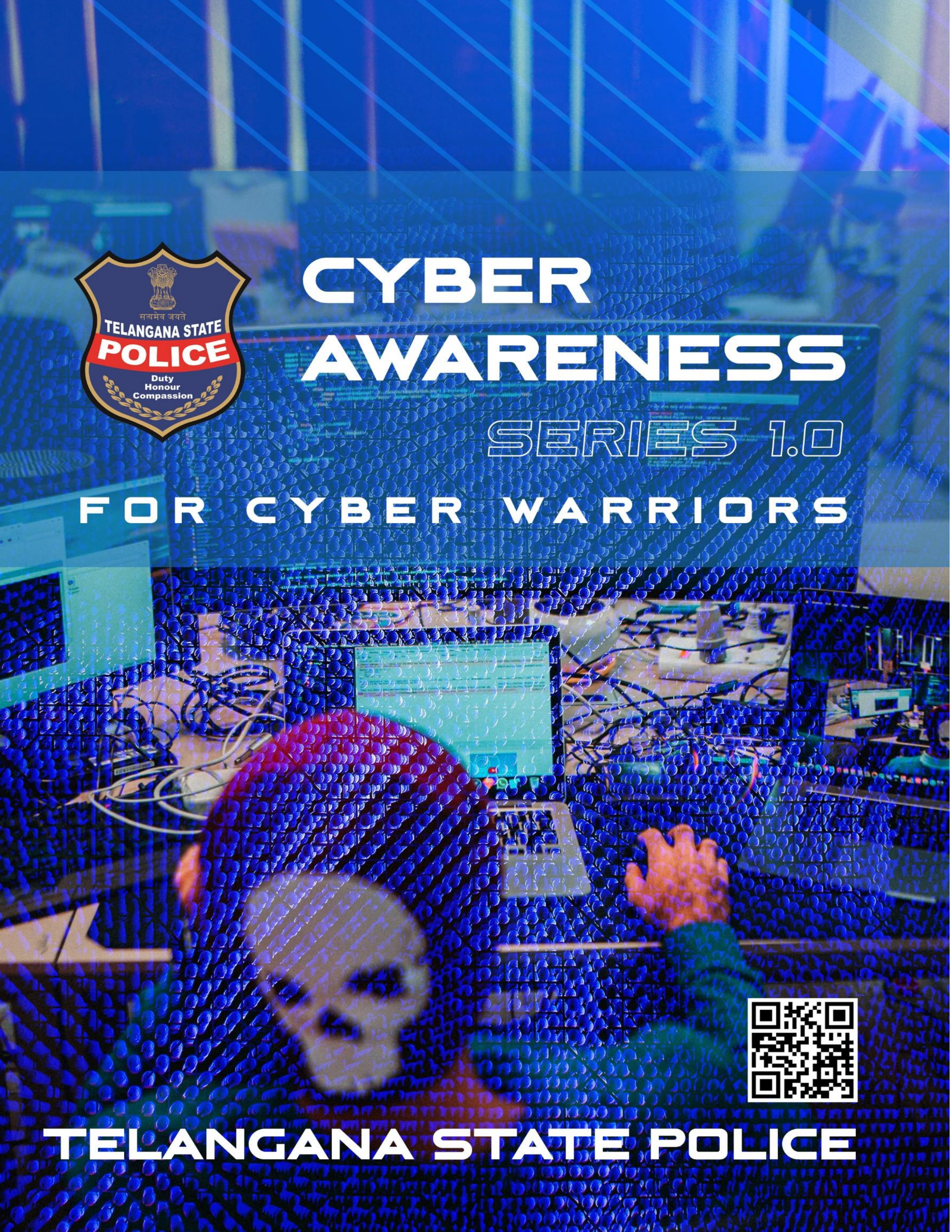
Bring Awareness & Reduce Crimes
// Visit www.cybercrime.gov.in to report crime, for helpline call 155260 between 9am to 6pm//

14. GENERAL PREVENTIVE MEASURES

- Make sure all your devices are PIN/Password protected, and must not save passwords in the browsers and passwords of different IDs should be unique.
- Do not download from unauthorized websites or untrusted sources.
- Must use recent anti-virus with latest versions.
- Update the devices with recent patches.
- Do not share your personal banking details, passwords and PIN to anyone, do not reveal passwords to anyone on phone calls.
- Always change the default passwords given by bank, or of your Wi-Fi router. Always use strong password that is 8 digit or more combination of alphanumeric symbols, special characters.
- Be aware when using public Wi-Fi and avoid logging into email or banking networks using public Wi-Fi networks.
- Do not open spam emails, and do not respond to strangers on emails,
- Do not open the links present in the mails and do not download the attachments of the mail.
- Be very careful while providing the personal documents like identity proofs and address proofs to any organizations.
- If any SIM card or mobile phone is lost make sure to block the SIM card and inform the nearest police station about the loss of mobile device.
- At ATM machines, look for skimmers or any devices installed before entering your PIN.
- Learn and discuss safe internet practices with children, women, family and friends.
- If you are trapped in a fraud inform the concerned authorities immediately.
- Prevent anonymous users from viewing your profile online
- Never open web links in email
- Never click links in email starting with IP address
- Do not use PIN numbers that match your personal information like date of birth, vehicle number etc.,
- Do not believe everything which you read online
- Do not keep sensitive documents on desktop
- Disable auto play option while using pen drive
- Use separate passwords for separate accounts

15. IMPORTANT RESOURCES FOR CYBERCRIME AND CYBERSECURITY

1. https://cybercrime.gov.in/
2. https://www.infosecawareness.in/
3. http://www.isea.gov.in/
4. https://www.cert-in.org.in/
5. https://staysafeonline.org
6. https://cytrain.ncrb.gov.in/
7. http://www.cybercelldelhi.in/
8. http://www.cyberabadpolice.gov.in/other-services/cyber-crime-cell.html
9. https://www.facebook.com/cybercrimepolice.gov.in/



सत्यमेव जयते
TELANGANA STATE
POLICE
Duty
Honour
Compassion

CYBER AWARENESS

SERIES 1.0

FOR CYBER WARRIORS

TELANGANA STATE POLICE