

QUICK HEAL FOUNDATION'S EBOOK ON CYBER AWARENESS



www.quickhealfoundation.org

HAVE YOU BEEN CHEATED ONLINE?

A GUIDE FOR VICTIMS OF

CYBER CRIME

QUICK HEAL FOUNDATION'S
EBOOK ON **CYBER AWARENESS**

Contents

About Quick heal Foundation..... 01

Introduction..... 02

Loan Application Fraud..... 03

Matrimony Fraud..... 05

Job Fraud..... 08

Sextortion..... 11

Financial Frauds..... 13

Cyber Bullying..... 15

Task Fraud..... 17

Social Media Marketplace Fraud..... 19

New Fraudulent Scheme Alert: Beware of New Tactics Used by Fraudsters..... 21

Stay Vigilant! Protect your future..... 22

ABOUT QUICK HEAL FOUNDATION

Quick Heal Foundation is the CSR arm of Quick Heal Technologies Limited, India's leading cybersecurity products and Solutions Company. We have leveraged over 25 years of experience in simplifying security to chart a brand new course in our journey – towards 'Securing Futures'.

Our initiatives in corporate social responsibility address pressing challenges to development outlined by the United Nations Sustainable Development Goals. Through efforts aimed at promotion of education, and employment enhancement, vocational training & cybersecurity awareness, we seek to provide innovative and technology- based solutions to these global hurdles. Implemented by the Quick Heal Foundation, each of these initiatives go on to help ensure a future with a promise of success and security for all.





Introduction

Cyber Scams are nothing new!

Every day, con artists are looking for the highest “Marks.” And if you think you are a student or not worth being a cybercrime target? Think Again!

Hackers don't care about how much balance you have in your bank accounts. They try to steal and make money out of it. Be it your identity or your financial data, for them, everything is valuable. They're counting on you thinking you're not a target!

They try to get all your information and can also frame you as a target, which can further penalize you for the crimes you haven't committed. So, beware of the cyber threats and don't be a cyber victim. Stay alert!

To keep you safe from all threats, Information Technology Act 2000 was passed which was introduced to recognize, mitigate and prevent cyber threats. So if you have been cheated online or have become a victim of cybercrime, you should be aware of this act to take further needed actions.

Many cybercrimes are frequently reported including cyberstalking, pornography, morphing, online harassment, defamatory or annoying messages, trolling or bullying, blackmailing, threat or intimidation, email spoofing, impersonation, etc.

This booklet is a complete guide for students to understand more about cyber frauds in the cyber world and how to stay safe & secure digitally.



Loan Application Fraud

This kind of fraud is targeted at low-income groups/poor people who need less money and have nothing to mortgage or guarantor to support.

How to identify a fraudulent person/app?

- A loan of small amounts (2000 – 25000) is offered without any guarantor, mortgage, or documentation
- A loan is provided without asking or immediately when you seek the same.
- Sometimes just an inquiry is enough to deposit money in your account
- You will continuously receive lucrative offers through email, phone, text message, WhatsApp message
- No one will meet you in person or share their office address

How to prevent victimization?

- Never trust apps/links shared on social media
- No one offers a loan without documentation, guarantor, or mortgage
- Insist on visiting the office in person
- Do not believe in existing customer's video bytes without meeting the person.
- Check details of the organization offering loans on the internet by visiting their website, local address, contact details, and office bearer's names, contact details etc.

Steps to be taken in case of victimization

Once the victim realizes self-victimization, one should stop responding to the fraudster. A fraudster can pass on your details to other syndicates who can use your morphed photo to extort money.

One must ensure to follow these steps after they fall into the trap.

01

Do not panic if you receive threatening calls/messages & stop paying further

02

Inform your contacts about this fraud and ask them not to pay on your behalf

03

Even your contact list may receive threats along with their morphed photos, but don't panic; instead, report to the police

04

Collect/compile all evidence like call/chat history, payment history, etc.

05

Do not delete any evidence like an app, links shared, or the number of fraudsters helping police to further investigate and act

06

Report to nearest cyber police station / take help from the local police station

07

Do not hide anything from police

08

For reporting, you can call helpline 1930 (By Ministry of home affairs, Government of India) or Report a complaint on the National cybercrime reporting portal <https://cybercrime.gov.in/>

Matrimony Fraud

This fraud can go hand in hand with customs fraud & usually happens with a person looking for life partner through matrimony sites

How to identify a fraudulent person?

- Recent/new lucrative profile (5 –15 days old) highlighting income from job/business

- Photographs show luxurious lifestyle – selfies in front of a bungalow, swimming pool, 5-star hotels, and malls wearing branded outfits, watches, and other accessories.

- No social media details are shared, or if shared, the profile is recent with minimal friends.

- All communication happens on Audio or WhatsApp calls. If you insist on video calls, it happens outside the home/office – mostly in public places with lots of noise.

- They gain trust and convince the victim that no family members stay with them; hence, communication with family members is not possible.



How to prevent victimization?

Never trust a proposal without personal meetings/video calls with family members.

Insist on checking their social media accounts and friend lists. Also, do not forget to check friend list of friends

Never send money even in case of a medical emergency, if you have not met the person

Never accept any gifts without meeting in person

Remember, custom officers never ask for online settlement without the formality of filling out forms.

If the gift is genuine, it will reach your city (the Post office where your address belongs)

You will never receive a call from customs in Delhi, Mumbai, or any such place

A call from the post office will ask you to visit the post office, pay charges and get your gifts

Steps to be taken in case of victimization

Once the victim realizes they have been cheated, the person becomes anxious and starts retaliating by denying paying. Then fraudster starts blackmailing by intimidating morphed images and videos, sharing them with their friends and relatives, lodging complaints for defaulting payment, etc.

The following steps must be taken after victimization:

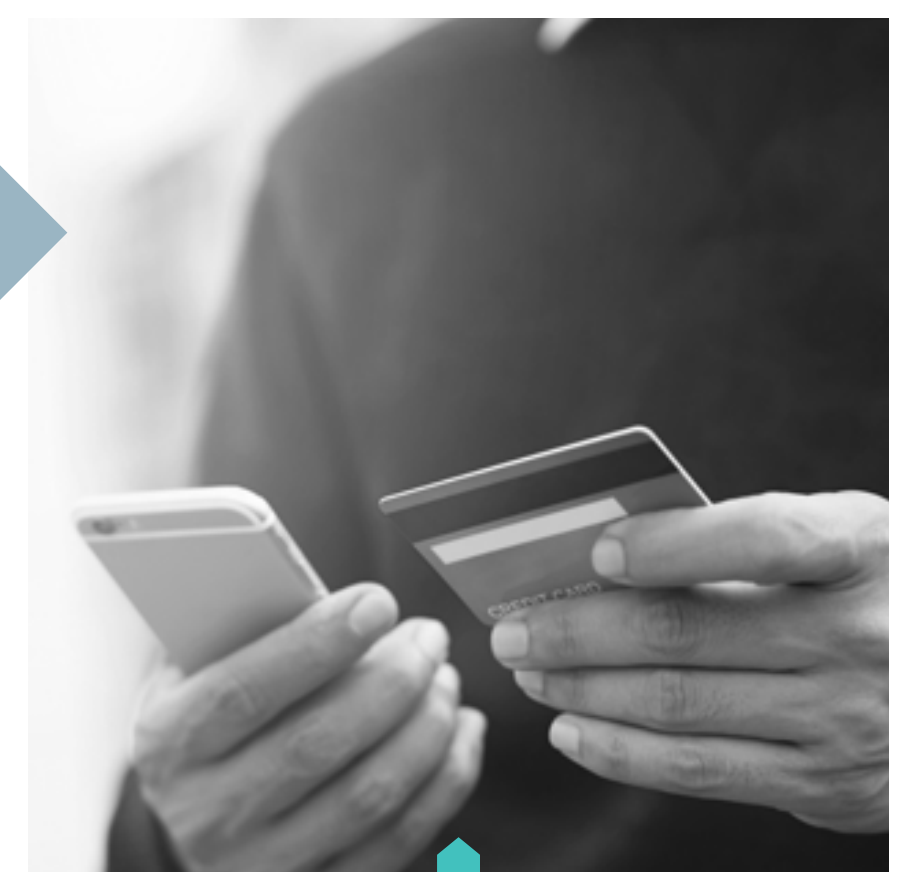
01

Stop responding
to the fraudster



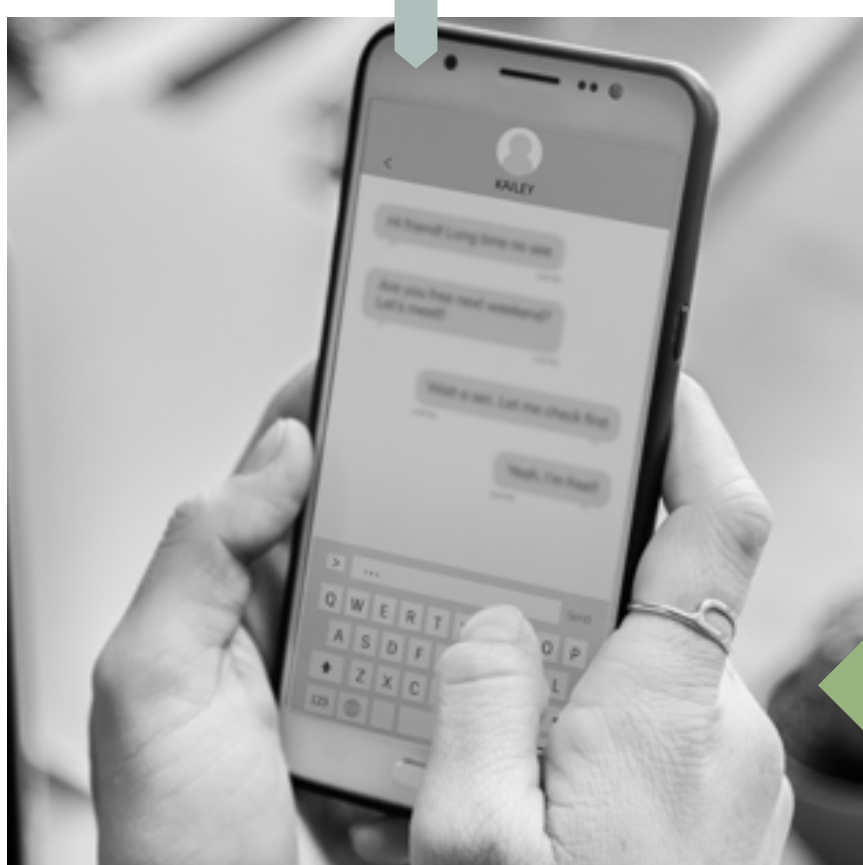
02

Do not
pay further



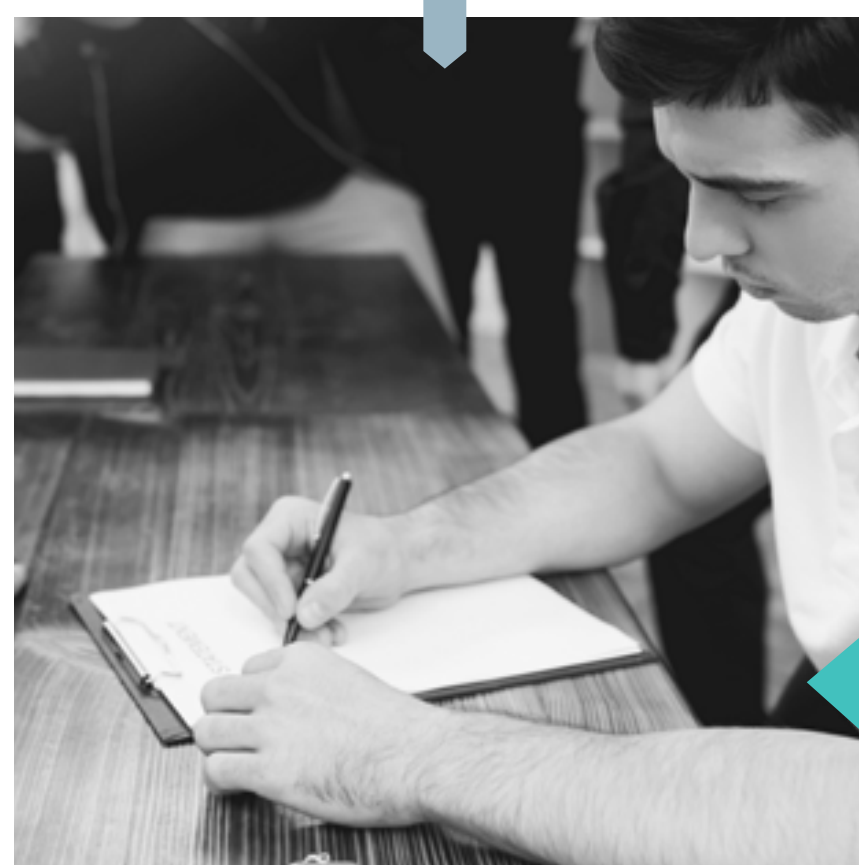
03

Collect/compile
all evidence like
call/chat history,
payment history,
etc.



04

Report to the
nearest cyber
police station and
take help from the
local police station



05

Do not delete evidence like the
app, links shared, or the
number of fraudsters – this
helps police investigate and act

06

Do not hide anything
from police

07

Call helpline 1930 (By Ministry
of home affairs, Government
of India)

08

Report the complaint on
the National cybercrime
reporting portal
<https://cybercrime.gov.in/>

Job Fraud

Victims of these frauds can be fresher or experienced both. In job fraud, the fraudster convinces aspirants that they can get the job if they can pay amounts ranging from Rs.5K onwards after judging their paying capacity.

How to identify fraudsters?

- Receive a call from someone in higher positions like HR Head, Sales Head, etc.
- The interview will be telephonic.
- Straightforward questions would be asked
- You will be praised during the interview for your knowledge, achievements, or for any personal reason
- You will be informed about your selection in the same interview call
- You are offered a salary more than your expectations with lots of perks/facilities



How to prevent victimization?

- Never trust apps/links/websites shared on social media
- Even if you receive an offer letter, visit the company, and confirm about the offer letter
- None of the heads will call and conduct interviews on the same call.
- Never agree to pay for training. No company seeks any training charges separately.
- You may get less salary or no salary during the training period
- In the case of remote /WHF mode of working, never pay.
- Be careful while sharing your account details. Do not share card details – it is not required to transfer salary to your account



Steps to be taken in case of victimization

Once the victim realizes they have been cheated, the person becomes anxious and starts retaliating by denying paying. Then fraudster starts blackmailing by intimidating morphed images and videos, sharing them with their friends and relatives, lodging complaints for defaulting payment, etc.

The following steps must be taken after victimization:

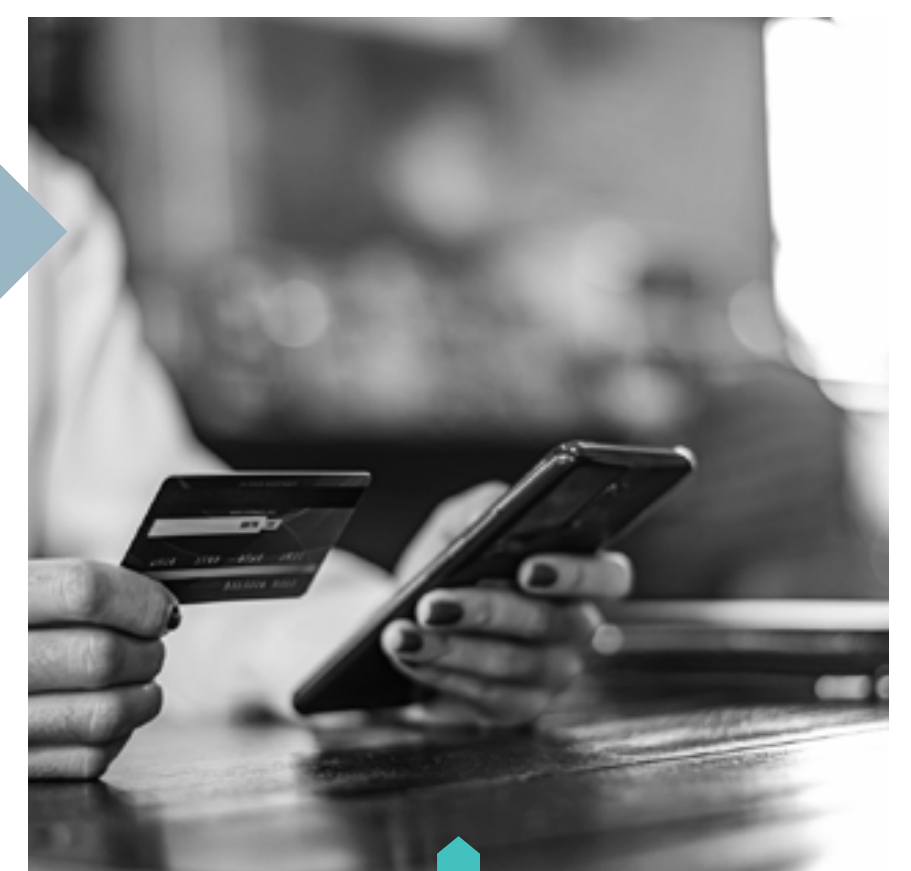
01

Stop responding
to the fraudster



02

Do not
pay further



03

Collect/compile
all evidence like
call/chat history,
payment history,
etc.



04

Report to the
nearest cyber
police station and
take help from the
local police station

05

Do not delete evidence like the
app, links shared, or the
number of fraudsters – this
helps police investigate and act

06

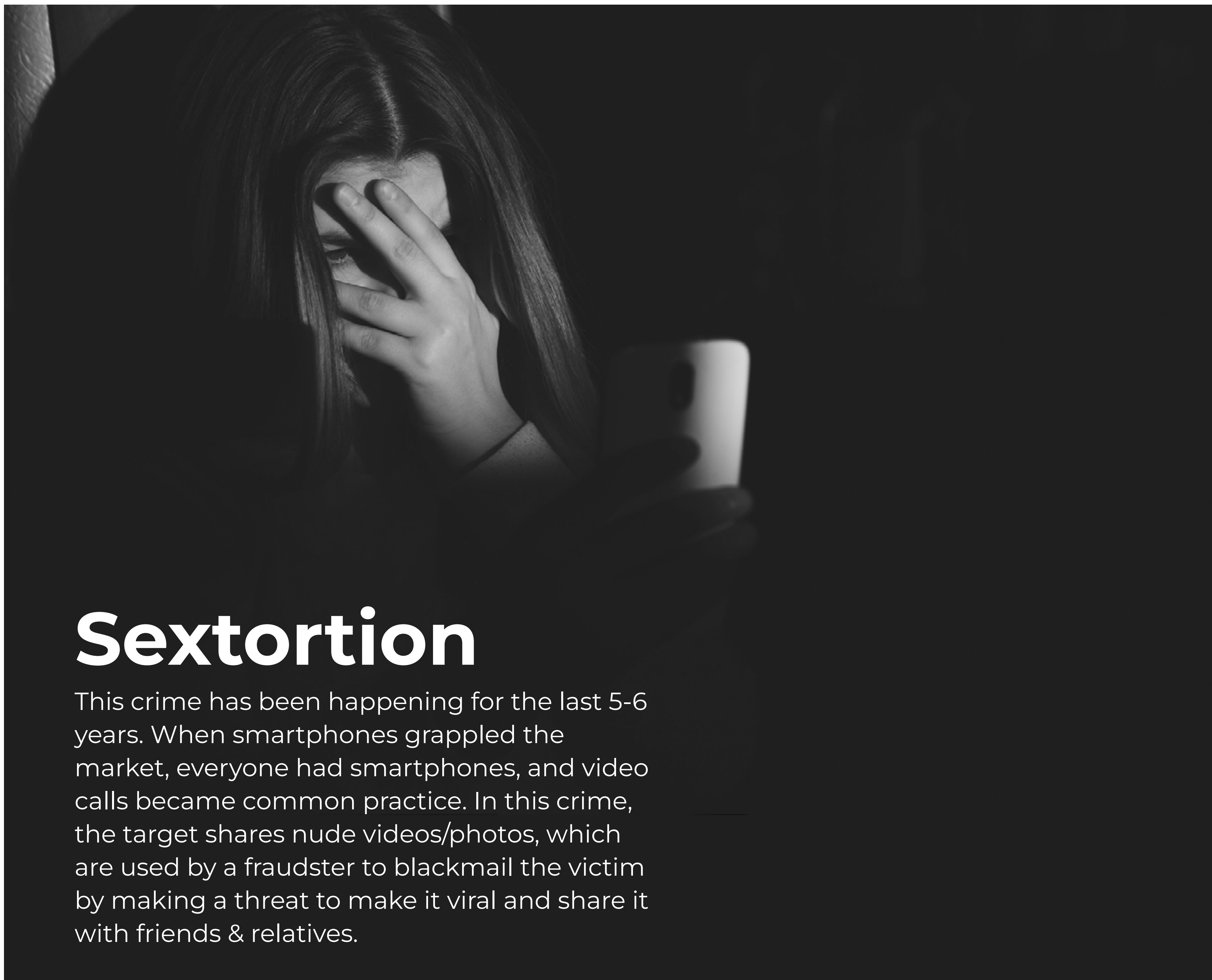
Do not hide anything
from police

07

Call helpline 1930 (By Ministry
of home affairs, Government
of India)

08

Report the complaint on
the National cybercrime
reporting portal
<https://cybercrime.gov.in/>



Sextortion

This crime has been happening for the last 5-6 years. When smartphones grappled the market, everyone had smartphones, and video calls became common practice. In this crime, the target shares nude videos/photos, which are used by a fraudster to blackmail the victim by making a threat to make it viral and share it with friends & relatives.

How to prevent this fraud?

- Never share high-resolution photos or videos on social media
- Never publicize your lonely/single status on social media
- Never use your real name and other details on apps like tinder
- Never respond to video calls from unknown numbers
- Never allow your intimate photos/videos to be captured by anyone
- In case you must attend a video call from an unknown number, ensure to cover the camera


Steps to be taken in case of victimization

Once the victim realizes they have been cheated, the person becomes anxious and starts retaliating by denying paying. Then fraudster starts blackmailing by intimidating morphed images and videos, sharing them with their friends and relatives, lodging complaints for defaulting payment, etc.

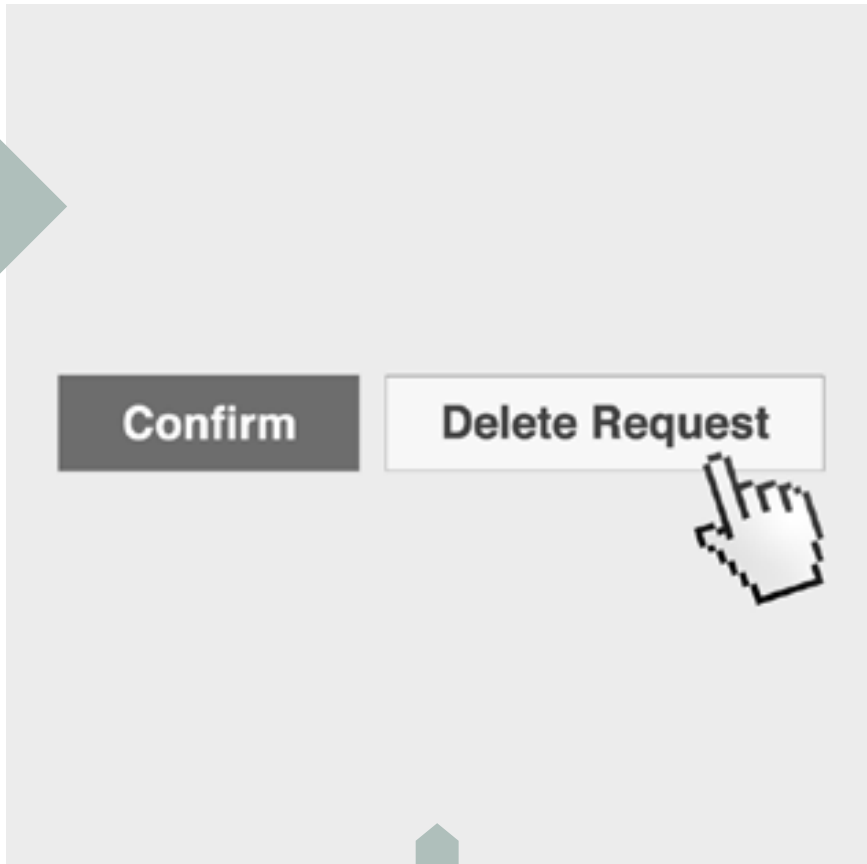
The following steps must be taken after victimization:

- 01 –


Stop responding to the fraudster


- 02 –


Use the report and block option on social media.


- 03 –

In the case of FB, Instagram, or similar media, ask all your social media friends to do the same


- 04 –

Inform all your social media connections about cybercrime and not to respond to any call/message from you unless you call them personally on a regular call.


- 05

Collect/compile all evidence like call/chat history, payment history, etc.
- 06

Do not delete evidence like the app, links shared, or the number of fraudsters – this helps police investigate and act
- 07

Report to nearest cyber police station/take help from the local police station
- 08

Do not hide anything from police
- 09

Call helpline 1930
(By Ministry of home affairs, Government of India)
- 10

Report the complaint on the National cybercrime reporting portal
<https://cybercrime.gov.in/>

Financial Frauds

People lose their money from the accounts without sharing any details. If you receive a message stating your bank balance is zero, visit your bank and inform bank officers about the same. Fill dispute form and do not share OTP or any other details on call.

How to identify?

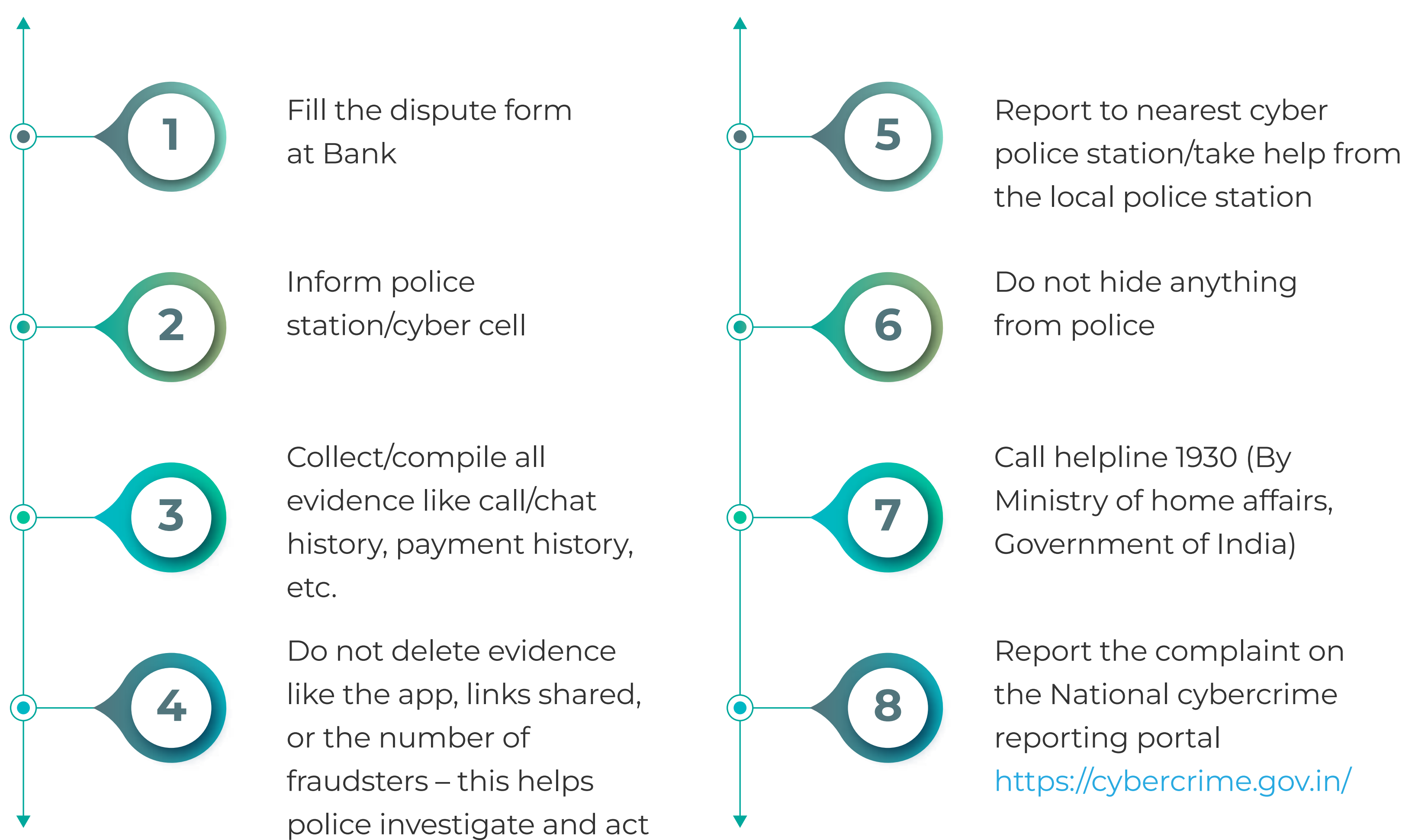
- You will receive a call (sometimes message) creating a sense of urgency for various reasons like ATM card blockage, electricity cut, or bank account deactivation
- You will be asked to pay through the link
- You will be asked to share details like date of birth, mother's name, address etc.
- You will be asked to share details like OTP / PIN /code.
- You will be asked to share your debit/credit card number, CVV (Customer Verification Value), etc.
- You will be asked to download the app / click on the link / provide access to your device by pressing some keys
- For emails, check for the use of English as it may not have proper grammar or have a few spelling mistakes



How to prevent?

- Never believe on phone calls or messages. Bank never asks for your personal details
- Never share OTP (One Time Password) to unknown person. Police or Banks will be helpless if you share your OTP
- Similar to OTP, CVV number, mother's maiden name, birth dates are also used as password or answer to secret questions.

What to do in case of victimization?





It is an act of harassing, threatening, and embarrassing people with the use of technology. Online bullying is harmful as anonymous persons, or a known person usually does it but hides their identity.

Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content.

Symptoms of cyber bullying victim

- Considerable increase or decrease in usage of a mobile, laptop or tablet
- Sudden deactivation of their social media accounts or opening of new ones
- Hiding of the device screen when others are close by
- Display of emotional responses such as sadness, anger, depression, withdrawal symptoms
- The tendency to avoid discussion on online activities

Targeted strata of people

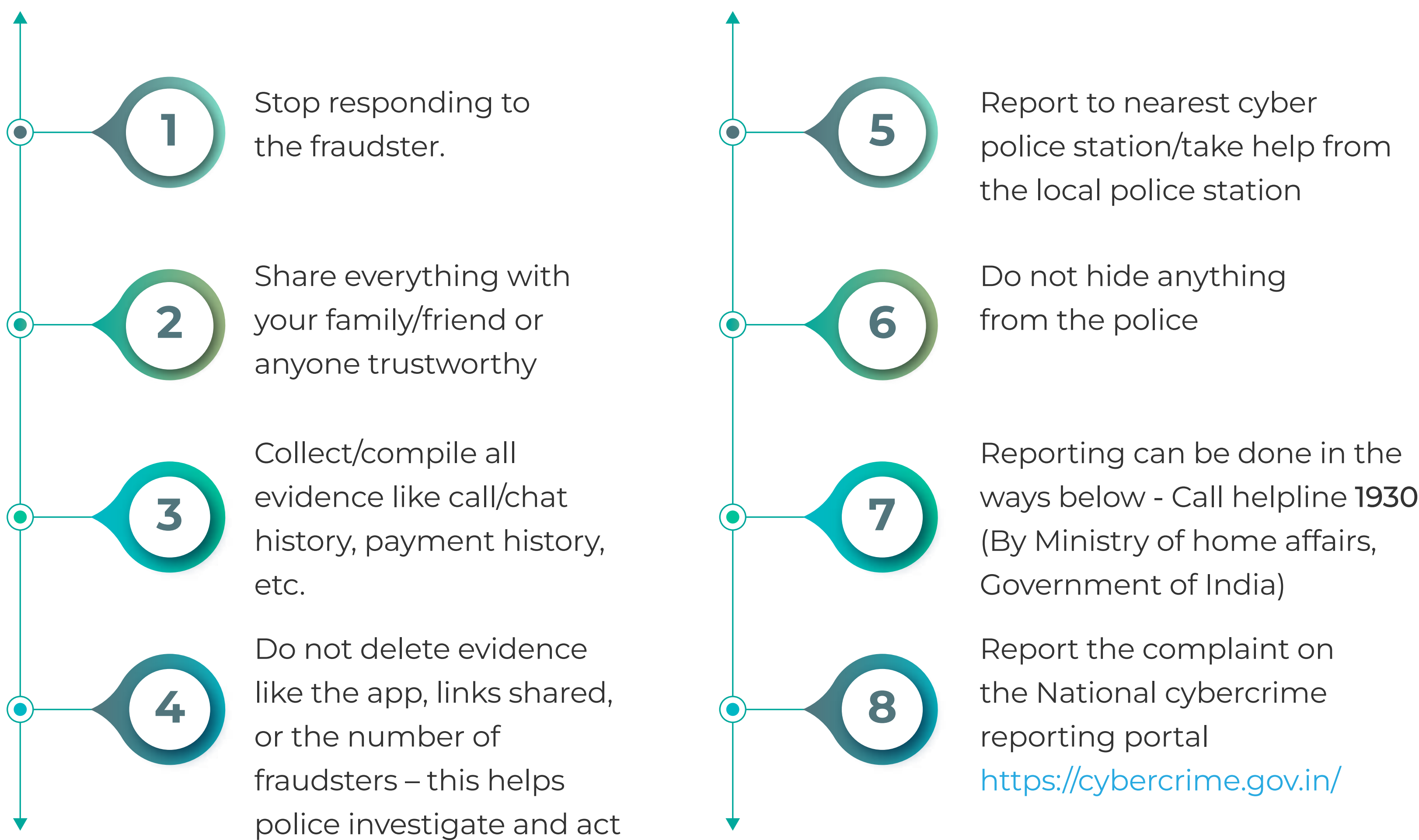
- Mostly children, shy students, intelligent students who are introvert

How prays are identified? & how people get into trap?

Target is identified by sending a friend request on social media and communicating through WhatsApp. Sometimes, the target is identified offline, and cyberbullying is started by forming a group of people.

Bullying is often done by juveniles without knowledge of cybercrime and its consequences. This act is done out of fun or to take revenge.

The following steps must be taken after victimization





Online task fraud typically involves trapping victims by luring those who are looking for work-from-home opportunities or another source of income in their spare time, offering them simple tasks to be performed and promising money in return.

How to Identify Fraudulent Person/App?

- **Unsolicited Messages:** Usually begins with unsolicited messages, mostly on WhatsApp or Telegram.
- **False Promises:** Offers work-from-home opportunities with flexible hours, requiring no experience or specific skill set.
- **Cloned/Phishing Websites:** The message may include a link to a company website, which is a cloned or phishing website of some reputed company.
- **Payment Methods:** Offers payment on a daily or weekly basis, sometimes in cryptocurrency.
- **False Trust Building:** In the initial days, you may receive payment to gain your trust.
- **Requests for Payment:** To earn more money, you will be asked to pay premium charges, usually slightly less than what you have earned to date.
- **Payment Process:** You will be asked to make payments using various methods like scanning multiple QR codes, net banking, etc. Each time, you will be told that the payment was not successful.

How to prevent victimization?

- **Avoid Unsolicited Messages:** Be cautious of unsolicited messages promising high-paying for simple tasks or work-from-home opportunities.
- **Check Website Legitimacy:** Verify the website address and its legitimacy before proceeding.
- **Confirmation Before Payment:** If asked to make a payment, avoid doing so without confirming the legitimacy of the company.

Steps to be taken in case of victimization.

Once the victim realizes they have been cheated, the person becomes anxious and starts retaliating by denying paying. Then fraudster starts blackmailing by intimidating morphed images and videos, sharing them with your friends and relatives, lodging complaints for defaulting payment, etc.

Following steps must be taken after victimization:



Social Media Marketplace Fraud



Marketplace fraud involves making false or misleading claims through a company, such as exaggerating product or service qualities in advertising, selling imitations as genuine products, or concealing negative aspects or side effects. False advertising is a common form of marketplace fraud.

How to Identify Fraud:

- Attractive advertisements with lucrative offers.
- Unusual products not commonly found on popular platforms like Amazon or Flipkart.

How to Prevent Marketplace Fraud:

- Assess the product's quality and value compared to its price.
- Verify the legitimacy of the seller and the authenticity of the product before making a purchase.
- Attempt to communicate with the seller through their official website before placing an order.

Steps to be taken in case of victimization



New Fraudulent Scheme Alert: Beware of New Tactics Used by Fraudsters



Recently, a new method of fraud has emerged, exploiting individuals by falsely claiming that a courier containing drugs has been received in their name or sent by them. Another scam involves informing individuals that their son or daughter has been detained for attending a rave party, demanding money to resolve the situation.

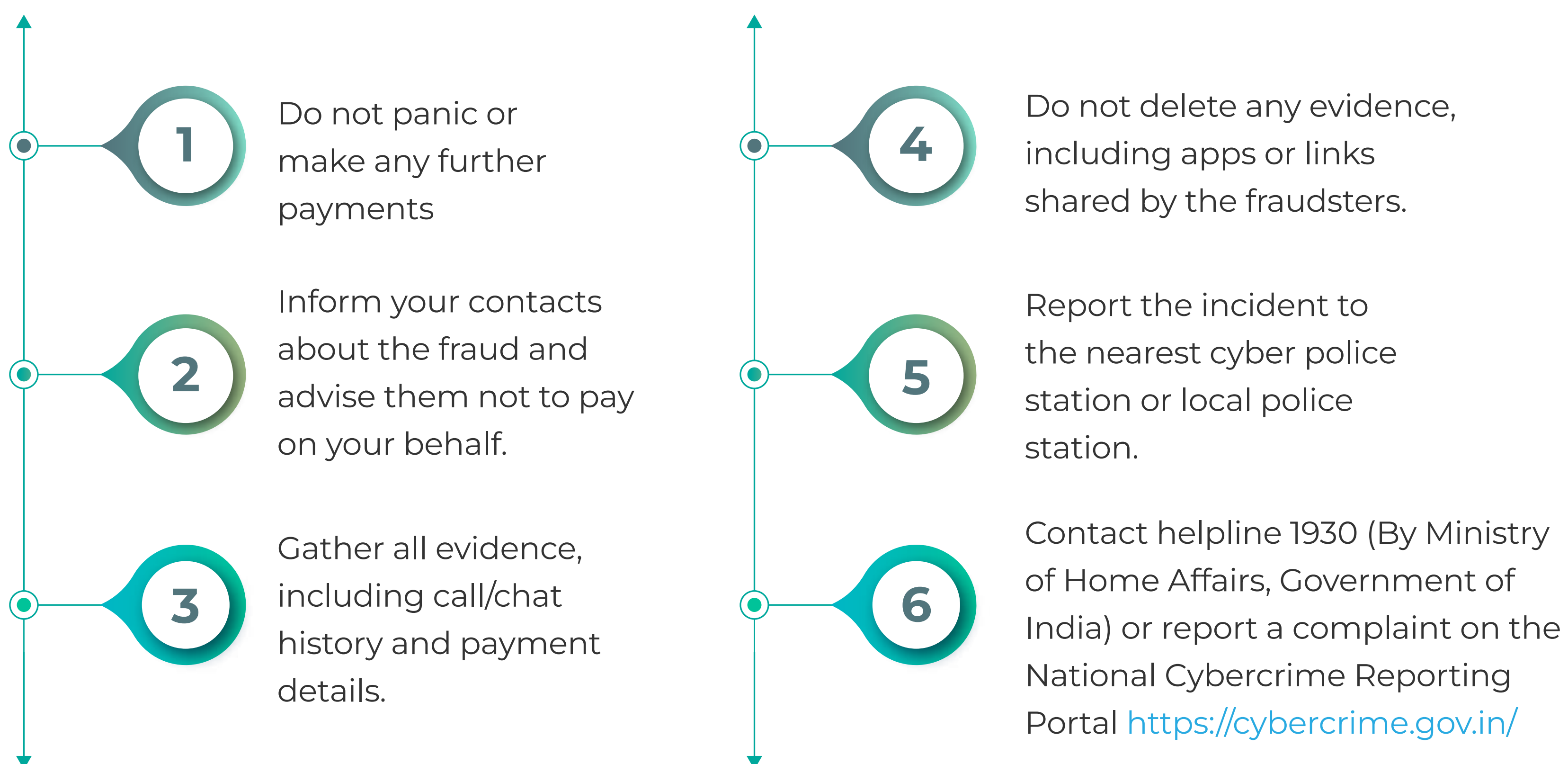
How to identify a fraudulent person/app?

- Unusual claims of receiving a courier containing illegal substances.
- Claims of a family member being detained for attending a rave party.
- Demands for immediate payment to resolve the situation.

How to prevent victimization?

- Never trust unsolicited messages or calls claiming legal trouble.
- Verify claims through official channels before taking any action.
- Refuse to make any payments without verifying the authenticity of the claims.
- Insist on meeting in person at official address, if the situation seems suspicious.

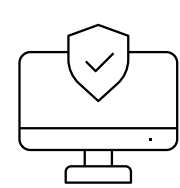
Steps to be taken in case of victimization



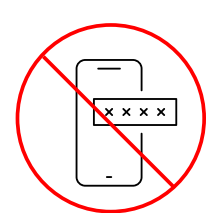
Stay Vigilant! Protect your future



Do not use free wi-fi



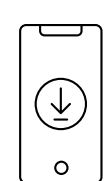
Use licensed and updated antivirus



Do not store passwords on phone



Use strong password and change it frequently



Download apps from trusted app



Don't use torrent sites



Use licensed and updated operating system



Quick Heal Foundation

Regd. Address: S. No. 207/1A, "Solitaire Business Hub", C Building, 7th Floor, Office No 7010 Viman Nagar, Pune - 411014

Contact: +91-20-41467229

E-Mail: contact@quickhealfoundation.org

Website: www.quickhealfoundation.org