CYBER WATCH

YOUR GUIDE TO STAYING SAFE ON THE INTERNET

Acknowledgement

World is a beautiful place, what makes it even better are people who share the gift of their time to mentor the young generation. With this, I have to start by thanking the team of Public Concern for Governance Trust (PCGT) who believed in me and showered this great opportunity to me, special thanks to Mr. Julio Ribeiro IPS (retd), Mr. V.P. Raja IAS (retd), Mrs. Ana Saldanha, and Advocate Sonali Shelar who were the guiding light for this ebook. They were as important to this book getting done as I was and I would like to thank them.

I would like to express my special gratitude to Mr. Nandkumar Saravade without whose expertise this booklet could have not been a reality. From reading early drafts, to suggesting edits, to advising on the design, and last but not the least, his prompt replies and kind suggestions kept me motivated.

Foreword

It has been my pleasure to be able to communicate with the new interns of PCGT during the pandemic which has limited my movement. It has been possible because of the internet technology. Less than a decade ago the possibility of needing the internet for all kinds of work did not even occur to us and now it is an indispensable part of our lives. It is important that this space is kept safe for everyone to use, which is why I am happy that the issue of cyber safety was taken up by Ms. Amisha Upadhyay and Ms. Urja Joshi, our former interns from July 2020, which was PCGT's first batch of online internship programme.

Since then Ms. Upadhyay has continued working on the issue through research and campaigns with support from our staff and experts like Mr. Nandkumar Saravade. I am confident that project Cyber Watch and this booklet has the potential to educate many so they can make use of the internet while protecting their identity and data from harassment, fraud, etc.

My thanks and good wishes to the team!

-J. F. Ribeiro

(Founder Trustee) - PCGT

Contributors

- Ms. Amisha Upadhyay, (Third-year law student, NMIMS, Navi Mumbai)

Author and designer

- Mr. Nandkumar Saravade, (CEO, ReBIT May'21, ex-IPS)

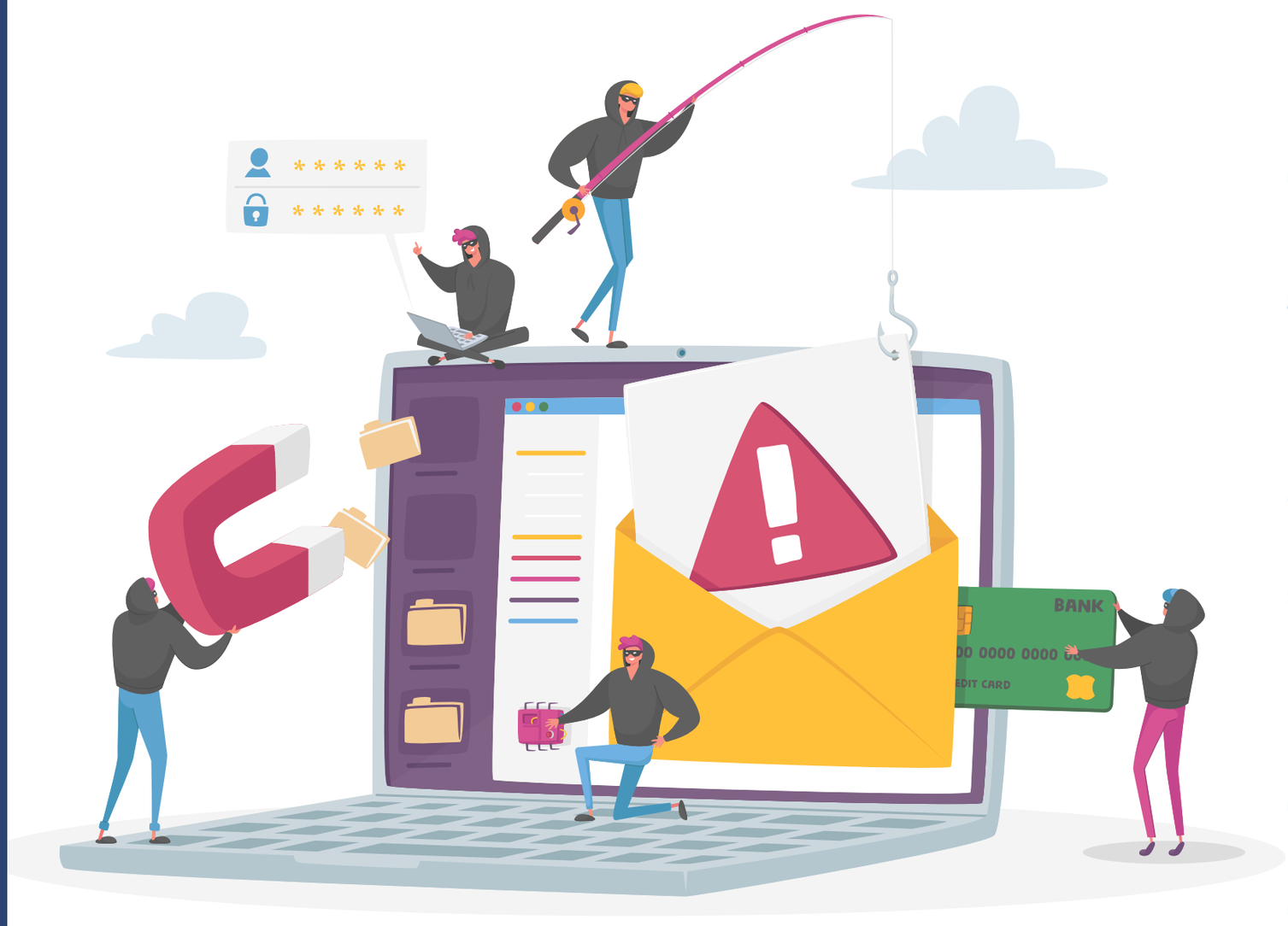
Expert Contributor

<u>Mentors</u>

- Mr. Julio Ribeiro IPS (retd.)
- Mr. V.P. Raja IAS (retd.)
- Advocate Sonali Shelar
- Advocate Ruchi Bhagat

CONTENTS

INTRODUCTION



The disruption caused by the pandemic has given rise to big socio-political and economic issues and has also opened doors to opportunities for digitisation.

As the entire country leapfrogs into digital universe, we go along with it. Necessity, as they say, is the mother of all invention, we could not study or work in the conventional way, so we figured out how to do it online. We no longer have the option of moving towards digitisation, it has become a necessity. Online presence is a must for everyone.

This gives rise to many questions, are we safe on this digital space? How do we protect ourselves? What from? Do laws protect us or are we on our own? The answer is this e-book that seeks to act as a guide to staying safe on the Internet.

Reading Instruction for the ebook

- This e-book acts as a handy reference on staying safe on the Internet

- All the chapters of this e-book are independent of each other

- They can be read all at once, or chapter-wise as well

CYBER SAFTEY ON SOCIAL MEDIA

WHAT IS CYBER ABUSE?

Simply put, it is the use of digital technologies to cause annoyance. It takes place on social media platforms, instant messaging services and mobile phones.

There are many ways through which cyber abuse can take place on social media, we explain you those on the next page

TYPES OF CYBER ABUSE?

Cyber Stalking

Repeated act of chasing someone using electronic media, involves harassment or threatening behaviour.

Flaming

Act of posting or use of obscene language within chat rooms, online discussion forums or any other online community

Cyber Bullying

Attempt to cause embarrassment, humiliation or harm to someone perceived as vulnerable on social media

Impersonation

Making a fake profile of another person with an intention to defame them or to cause emotional stress and/or financial loss

Online Harassment

Posting abusive comments, giving direct or indirect threats of sharing sexual or private messages/images without consent

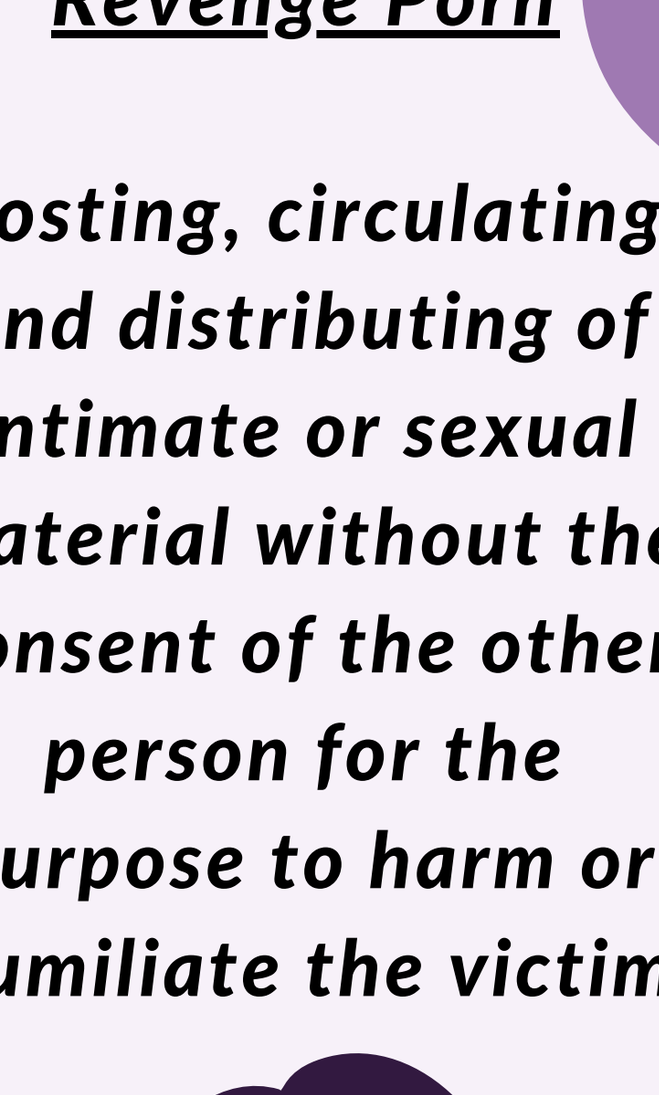
TYPES OF CYBER ABUSE?
POSTING OBSCENE MATERIAL

Act of posting or distributing pornography or any other obscene material on social media.

POSTING OBSCENE MATERIAL

Revenge Porn

Posting, circulating and distributing of intimate or sexual material without the consent of the other person for the purpose to harm or humiliate the victim



Cyber Grooming:

Act of gaining trust and 'befriending' a young child to procure sexual favours, intimate information and photographs

Morphing & Deep Fake

Using technology to change one's image or shape for the purpose to exploit and humiliate and misuse them for online sex chats and other pornographic content

WHAT CONSTITUTES AS CYBER ABUSE ON SOCIAL MEDIA?

Cyber abuse or online harassment has three main components- a severe or inescapable attack on a person or groups of people to cause harm via the means of the Internet.

i. Severe- ***Even small incidences can lead to grave outcomes. For example, publishing someone's personal information such as contact number/residential address can have serious consequences to the safety of the person.***

ii. Inescapable- ***While some incidents of cyber abuse may seem minute, it often becomes an inescapable situation wherein a chain of incidents take place and stays online for everyone to witness endlessly.***

iii. Internet- ***includes email, social media platforms such as Twitter, Facebook, Instagram and TikTok, messaging apps such as Facebook Messenger and WhatsApp.***

IMPACT ON THE VICTIM

Acts of abuse or harassment on social media may have long term impacts such as:

Cyber Abuse on social media causes tremendous emotional and psychological distress to the victim

The feeling of being targeted or laughed at, often prevents people from socialising or talking to friends and family, which may cause isolation in their room etc.

1. ***<u>Mental health</u> – feeling upset, embarrassed, stupid, even angry***

2. <u>Emotionally</u> – feeling ashamed or losing interest in the things you love

3. <u>Physically</u>– tired (loss of sleep), or experiencing symptoms like stomach aches and headaches

There is a need to 'de-normalise' the practice of cyber abuse on social media platforms.

WHY IS REPORTING IMPORTANT?

Cyber abuse extends traditional forms of abuse on the digital platforms, the only difference is that in the former the perpetrator hides behind the screen with anonymity

It's not because of you, but it can change because of you

For cyber abuse to stop, the key is identifying the perpetrator and reporting the abuse. Otherwise the perpetrator may take silence as an acceptance of their behaviour and continue the abuse.

Reporting of cyber abuse helps keep a record of the bad behaviour of perpetrators which can be used by authorities while dealing with similar cases in future.

REPORTING A PERSON ON FACEBOOK

Go to the profile you want to report by clicking its name in your News Feed or searching for it

Click ··· on the right and select the options Find Support or Report Profile

To give feedback, click the option that best describes how this profile goes against our Community Standards , then click Next

Depending on your feedback, you will be able to submit a report to Facebook

To report a profile:

1 Go to the profile you want to report by tapping its name in your News Feed or searching for it.

2 Tap ··· in the top right.

3 Tap **Find Support or Report Profile**.

4 Follow the on-screen instructions.

If someone's bothering you on Facebook, you can also unfriend or block them.

REPORTING A POST ON FACEBOOK

Go to the post you want to report

Click ••• in the top right of the post

Click Find support or report post

To give feedback, click the option that best describes how the concerned post goes against Facebook's Community Standards . Click Next

Depending on your feedback, you will then be able to submit a report to Facebook

To report a post:

1 Go to the post you want to report.

2 Tap ••• in the top right of the post.

3 Tap **Find Support or Report Post**.

4 To give feedback, tap the option that best describes how this post goes against our Community Standards. Tap **Next**.

5 Depending on your feedback, you may then be able to submit a report to Facebook. For some types of content, we don't ask you to submit a report, but we use your feedback to help our systems learn.

REPORTING A MESSAGE ON FACEBOOK

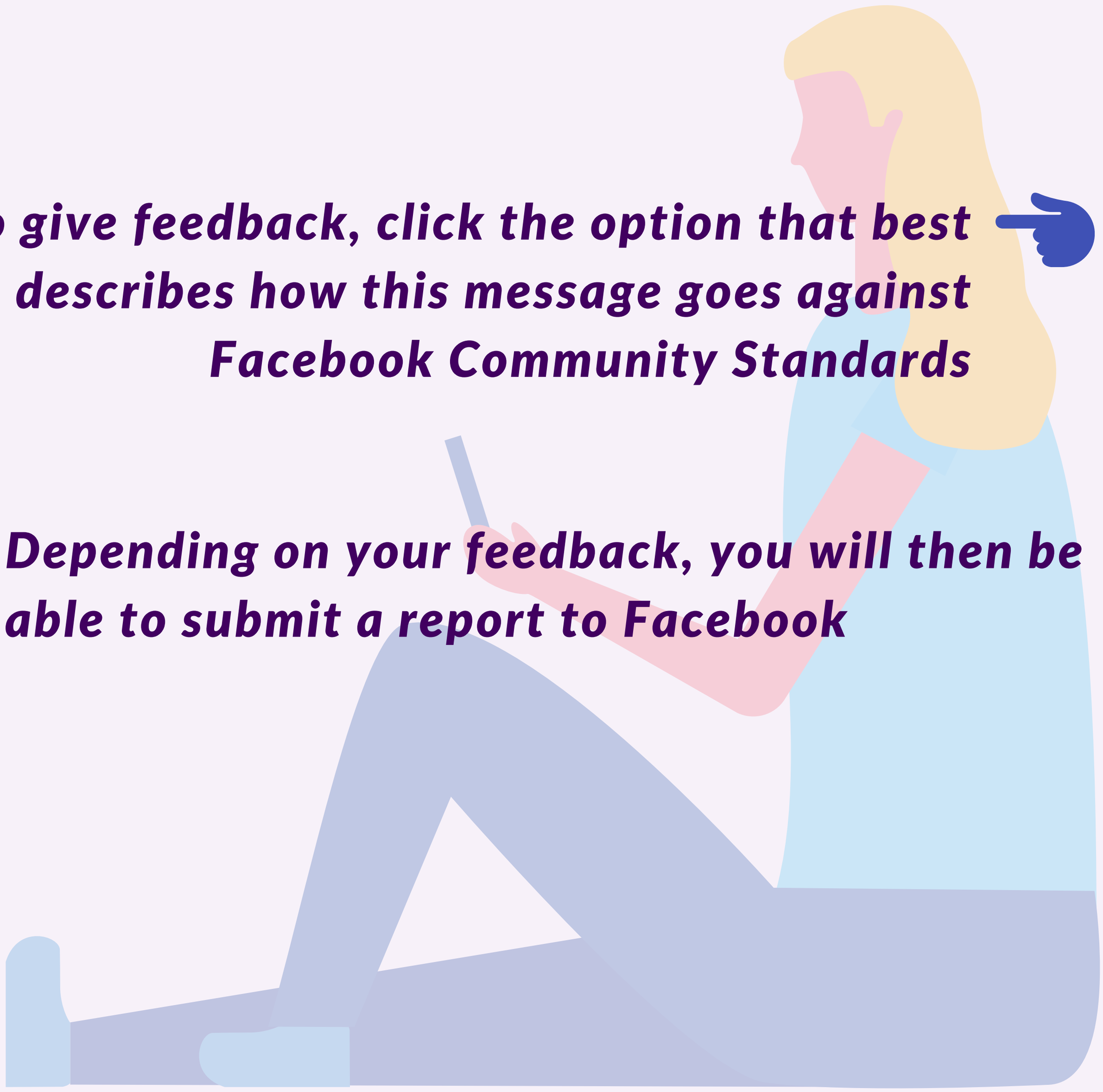
From any page on Facebook, click in the top right

If you opened the message as a pop-up window, click ⚙ If you opened the message in Message view, click ⚙

Click Something's Wrong

To give feedback, click the option that best describes how this message goes against Facebook Community Standards

Depending on your feedback, you will then be able to submit a report to Facebook



REPORT A POST ON INSTAGRAM

Tap ••• above the post

Tap Report

Follow the on-screen instructions

There are multiple ways to report something or someone on the Instagram app for Android and iPhone:

Report a post through Feed

1 Tap ••• (iPhone) or ⋮ (Android) above the post.

2 Tap **Report**.

3 Follow the on-screen instructions.

REPORT SOMEONE THROUGH DIRECT MESSAGE

Tap or in the top right of Feed.

Tap the chat with the person you want to report

Tap the person's name at the top of your chat

Tap Report, then follow the on-screen instructions

Report someone through Direct

To restrict someone through Direct:

1. Tap or in the top right of Feed.
2. Tap the chat with the person you want to report.
3. Tap the person's name at the top of your chat.
4. Tap **Report**, then follow the on-screen instructions.

REPORT SOMEONE THROUGH THEIR PROFILE

Tap their username from their feed or story post, or tap and search their username to go to their profile

Tap ○○○ above the post

Tap Report, then follow the on-screen instructions

Report someone through their profile

1 Tap their username from their Feed or story post, or tap and search their username to go to their profile.

2 Tap ••• (iPhone) or ⋮ (Android) in the top right of the profile.

3 Tap **Report**.

4 Follow the on-screen instructions.

REPORT A TWEET ON TWITTER

Anyone can report abusive behaviour directly from a Tweet, Profile, or Direct Message

Navigate to the Tweet you'd like to report on twitter.com or from the Twitter for iOS or Android app

Select Report and Select It's abusive or harmful

Next, Twitter might ask you to provide more information about the tweet/post you're reporting. Twitter may also ask you to select additional Tweets from the account you're reporting so as to have a better context to evaluate your report

To report a Tweet:

1. Navigate to the Tweet you'd like to report on twitter.com or from the Twitter for iOS or Android app.
2. Click or tap the ••• icon.
3. Select **Report**.
4. Select **It's abusive or harmful**.
5. Next, we'll ask you to provide more information about the issue you're reporting. We may also ask you to select additional Tweets from the account you're reporting so we have better context to evaluate your report.
6. We will include the text of the Tweets you reported in our follow-up emails and notifications to you. To opt-out of receiving this information, please uncheck the box next to **Updates about this report can show these Tweets**.
7. Once you've submitted your report, we'll provide recommendations for additional actions you can take to improve your Twitter experience.

REPORT AN ACCOUNT ON TWITTER

Go to the account profile and click or tap the overflow icon

Select Report and Select It's abusive or harmful

Next, Twitter might ask you to provide more information about the tweet/post you're reporting. Twitter may also ask you to select additional Tweets from the account you're reporting so as to have a better context to evaluate your report

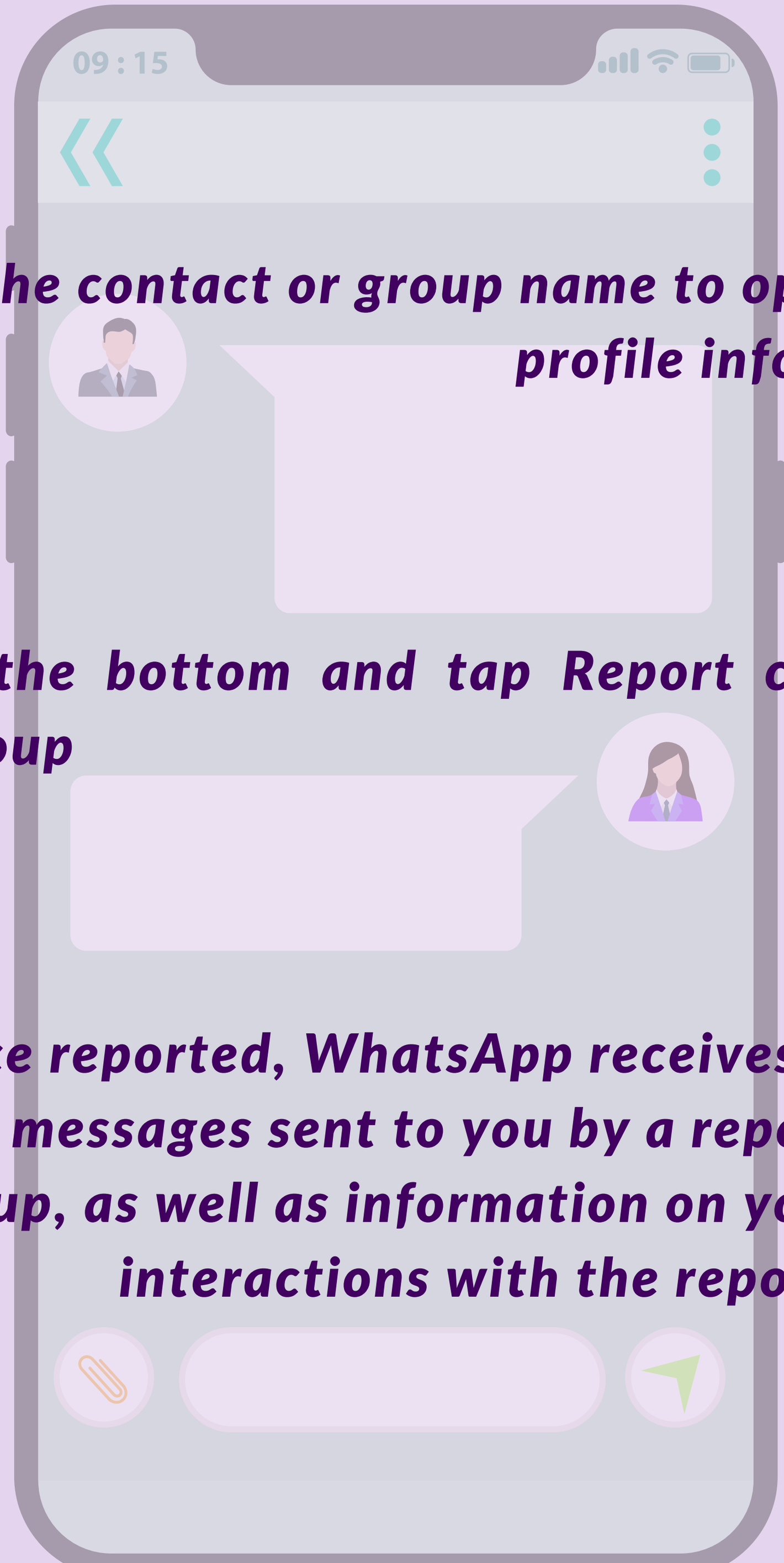
Twitter will include the text of the Tweets you reported in their follow-up emails and notify the same to you

To report an account:

1. Go to the account profile and click or tap the **overflow** icon ···
2. Select **Report**.
3. Select **They're being abusive or harmful**.
4. Next, we'll ask you to provide additional information about the issue you're reporting. We may also ask you to select Tweets from that account so we have better context to evaluate your report.
5. We will include the text of the Tweets you reported in our follow-up emails and notifications to you. To opt-out of receiving this information, please uncheck the box next to **Updates about this report can show these Tweets**.
6. Once you've submitted your report, we'll provide recommendations for additional actions you can take to improve your Twitter experience.

REPORTING A MESSAGE ON WHATSAPP

When you receive a message from an unknown number for the first time, you'll have the option to report the number directly inside the chat



Tap on the contact or group name to open their profile information

Scroll to the bottom and tap Report contact or Report group

Once reported, WhatsApp receives the most recent messages sent to you by a reported user or group, as well as information on your recent interactions with the reported user.

Report Cyber Abuse on National Cyber Crime Reporting Portal

For online reporting of cybercrime, visit the Cybercrime reporting portal URL:(http://www.cybercrime.gov.in)

You can either report a complaint pertaining to online Child Sexual Abuse Material (CSAM)

or sexually explicit content such as Rape/Gang Rape (CP/RGR) content either anonymously or by revealing your identity

Use the "Report and Track" option for reporting the incident and fill in the details

You will receive a tracking number which can be used to track the progress of the complaint by clicking on the "check status" option on the portal

How and where can I report cyber abuse? In Maharashtra

Maharashtra Cyber Cell

You can report online by filling in the requisite information online

URL: https://mumbaipolice.gov.in/OnlineComplaints?ps_id=0

Local Cyber Cell

You can also file an F.I.R.

How and where can I report cyber abuse?

Ministry of Women and Child Development

You can email at: complaint-mwcd@gov.in

The National Commission for Women

You can either make a complaint online, email at: complaintcell-ncw@nic.in; or call the NCW at: +91-11-26944880

How can I report anonymously?

Visit: Central Government Cyber Portal

URL:https://cybercrime.gov.in/

Select "Report Anonymously" option, if you want to report CSAM or sexually explicit content

Select the "Category of Crime" (Mandatory) enter details if known and fill in the details

On submission of the complaint, the complaint would be worked upon by the respective State/UT authorities

What are some Digital Etiquette to be followed?

1. Be mindful of who you accept as a friend/follower. Fake profiles may exist in order to lure you
2. Do not click on links that seem suspicious, even if sent by a friend or colleague
3. Do not post about your whereabouts on social media platforms
4. Keep the privacy settings of your social media profile at the most restricted levels
5. You can report hurtful comments, messages and photos and request them to be removed
6. Remember that information scattered over multiple posts, photographs, status, comments etc. may together reveal enough about you to enable a fraudster to steal your identity and defraud you. So, apply maximum caution while sharing anything online
7. You can decide who can see your profile, send you direct messages or comment on your posts by adjusting your account privacy settings
8. Be careful about posting or sharing anything online – it may stay online forever and could be used to harm you later. Don't give out personal details such as your address, telephone number or the name of your school
9. Besides 'unfriending', you can completely block people from seeing your profile/contacting you

PROTECTION FROM PHISHING SCAMS

What is Phishing?

Phishing is a type of cybercrime wherein you would be contacted by email, call, or text message by someone pretending to be a legitimate institution to extract sensitive data such as debit and credit card details, passwords etc. This is then used for financial gains by the imposter.

PHISHING SCAMS BY SMS/EMAIL/WEBSITE

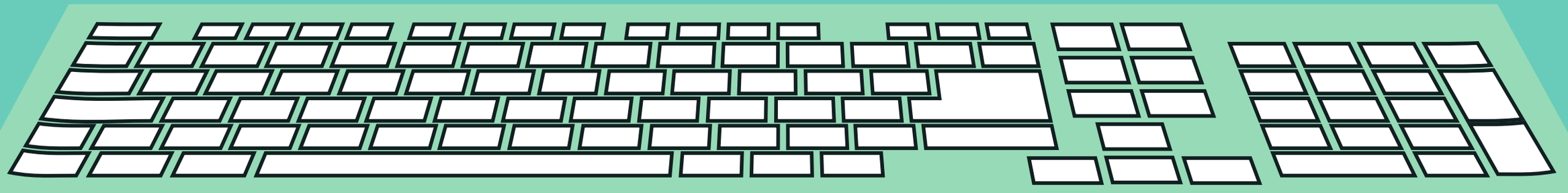
Don’t Be Too Quick To Click!

In this, the fraudster sends you an email or text message inciting you to <u>click on the link provided</u> and to lure you into filling up your personal information which would be later used by the fraudster access your bank account.

MOST COMMON WAYS PHISHING SCAMS TAKE PLACE

Fake Government Schemes:

Usually, a WhatsApp/E-mail/SMS message is circulated claiming to register for some government scheme via a link provided in the text message itself. However, the apparent registration link is designed to extract personal information.



MOST COMMON WAYS PHISHING SCAMS TAKE PLACE

Hacking

Here, an email is sent to you by cyber criminals posing to be from a reputed online platform such as Netflix, Instagram asking you to login into the account via the link provided in the email, when the user does login, the same is being recorded and used to hack your account.

MOST COMMON WAYS PHISHING SCAMS TAKE PLACE

Fake Helpline Number

When you do a Google search for some company's contact information, oftentimes a false search result pops up with a fraudulent number wherein the scamsters are posing as a legitimate institution.

HOW CAN I PROTECT MY PERSONAL EMAIL AND DATA?

<u>Do not click on links or attachments received from an unknown sender.</u> Rather, check upon the website of the company from which you have received the email

Avoid clicking on shortened links, especially on social media

Always check for “https” in the URL to indicate that it is a secure connection

HOW CAN I PROTECT MY PERSONAL EMAIL AND DATA?

Do not enter personal information in pop-up screens. Companies generally do not use pop-up screens to ask for user information

Do not click on any email that you receive from unknown or suspicious email addresses that depict to be government's email Id

KEEPING YOUR PASSWORDS SAFE

1. First and foremost, keep different passwords and pins for different accounts. This will help prevent you from being trampled upon on all your accounts

2. Use a password manager to create strong passwords for multiple accounts

Beware of these Signs of Phishing

Ultimatum

*An urgent warning attempts to intimidate you into responding without thinking. **'Warning!** You will lose your email permanently unless you respond within 7 days'.*

Clickbait

Attention grabbing titles, For example. "You won't believe this video!" on social media, ads etc. may lead to scams.

Incorrect URLs

Scammers may obscure URLs by using hyperlinks that contain a series of numbers or unfamiliar web addresses that appear as a reputable website.

Beware of these Signs of Phishing.

Too good to be true offers

Messages about contests you did not enter or offers for goods or services at an unbelievable price are likely to be fraudulent.

Style inconsistencies

Pop up windows that claim to be from your operating system or other software may have a different style or colours than authentic notifications. Messages that claims to be from a reputable organisation may be missing branding aspects such as a logo.

How and where can I report Phishing Scams?

Phishing scams come under the purview of IT laws and hence can be reported, if you have lost money. Here's how:

Online Complaint:

You can file an online complaint on government portal National Cyber Crime Reporting Portal

(URL: https://cybercrime.gov.in/)

Reporting on National Cyber Portal

Get yourself registered on the portal by using your name and mobile number. An OTP will be sent to you for confirmation. Subsequently, select the appropriate category and sub-category

Collate your complaint with as much evidence as possible, such as, Credit card receipt, bank statement, copy of email, URL of web page etc.

You will receive a tracking number which can be used to keep a track on your complaint.

How and where can I report Phishing Scams in Maharashtra?

<u>Maharashtra Cyber Anti-Phishing Unit:</u>

You can also lodge an online complaint with the <u>Maharashtra Cyber Anti-Phishing Unit</u> by appropriately filling up the information.

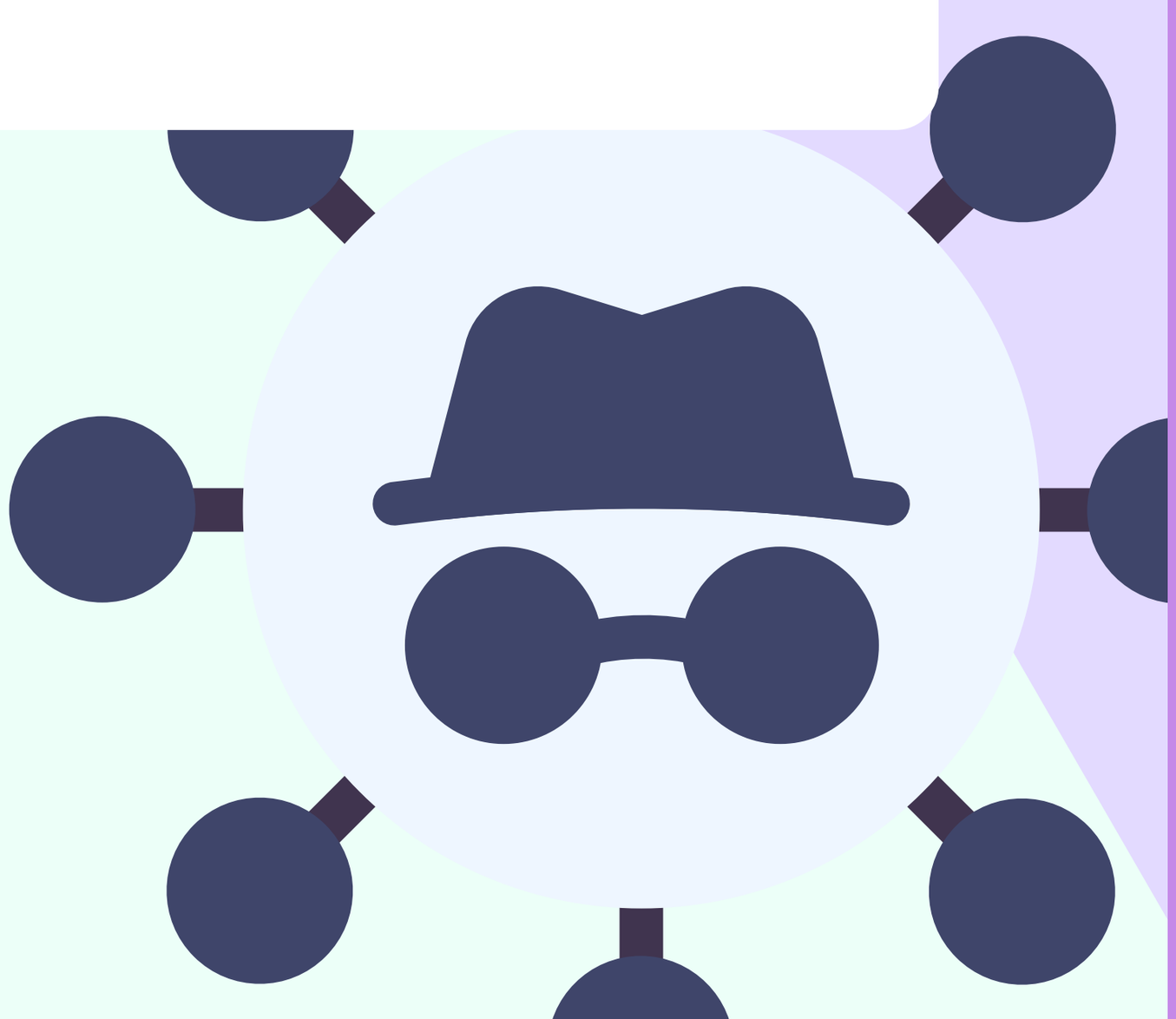
(URL: https://www.reportphishing.in/report-your-incident.php)

FIR:

You can also lodge a physical complaint with your nearest police station or cyber cell

What are some Digital Etiquette to be followed?

1. Be mindful while giving personal information online especially when asked over via emails or pop-ups
2. Keep your software and operating system always updated
3. Do not post about your whereabouts on social media platforms
4. Make sure you do report such incidence. It helps the relevant authorities to pick up on the trends of the perpetrator and helps identify them faster and prevent future cases
5. And lastly, if you have been a victim of a phishing attack it would be mindful of you to block all your cards, change your passwords and pins and notify your bank immediately.



ONLINE PAYMENT FRAUDS

What is UPI?

Unified Payment Interface or UPI, is a digital payment platform that facilitates digital transaction, real-time via smartphones.

What are UPI related online frauds?

The 3 most common ways fraudsters can trick you are as follows-

Here the fraudster will send you an unauthorised link via SMS or email which would be similar to a bank message.

When you click on the link, you will be directed to a UPI Payment page, wherein after putting in your details the same is recorded by the fraudster and money can be easily withdrawn by him from your account.

What are UPI related online frauds?

Fake Verification Attack

The fraudster poses himself as a bank representative who will ask you to download a third-party app (often an unverified app on play store and app store) for "verification purpose."

Once you have downloaded the app, it will give remote access to your phone.

What are UPI related online frauds?

- These fake profiles are either linked to a bank or having a government name attached to it which makes it appear authentic.

- The goal of the fraudster here is to misrepresent themselves as a legitimate site in order to get your account details through the fake UPI handle mentioned on the page.

What is OTP?

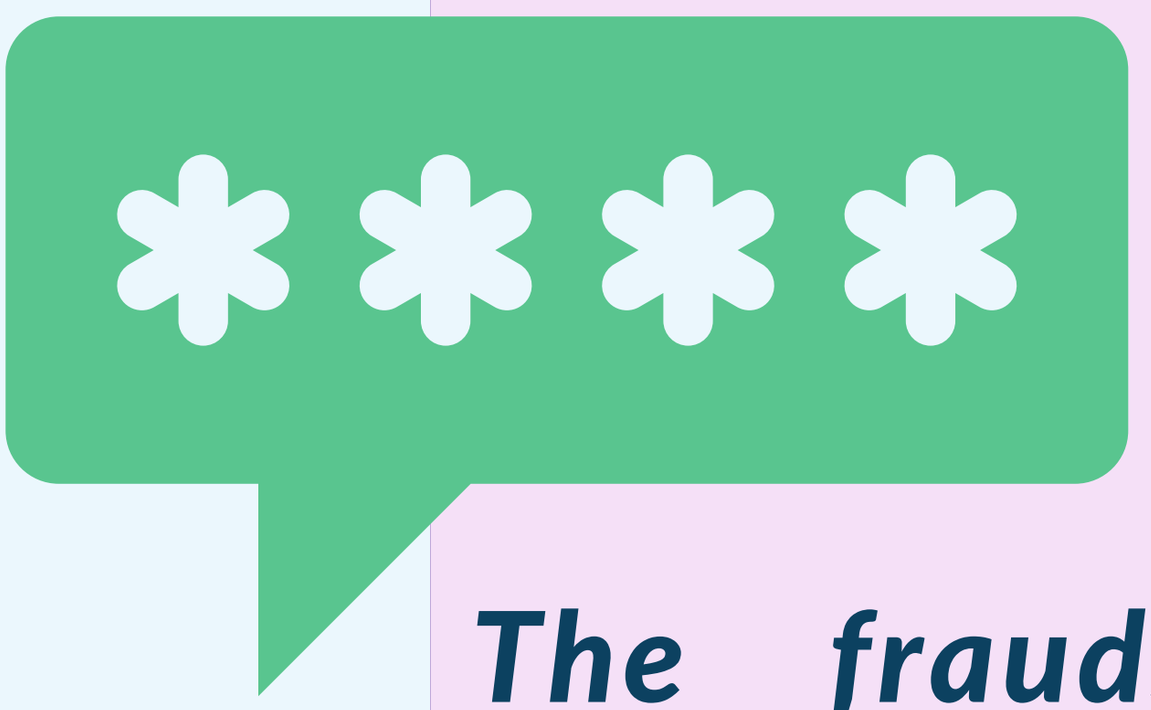
One Time Password or OTP is a password sent to you by your bank for single use and which needs to be kept confidential.

The fraudsters tend to deceive you by asking you to enter your UPI or OTP to complete a monetary transaction.

Never ever disclose your OTP via telephone to anyone, or your UPI even if they ask the same for "confirmation."

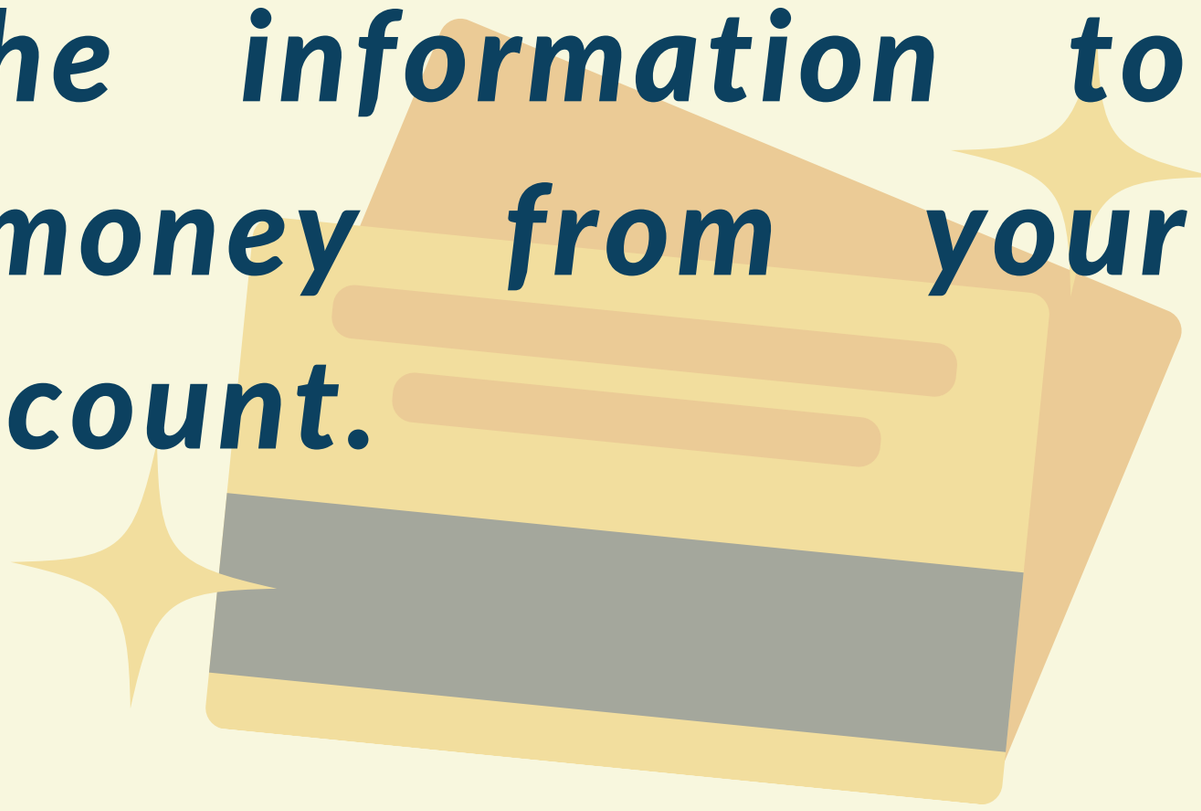
Most common OTP scams

FAKE OFFERS



The fraudsters pose as bank or credit card company providing a free card upgrade.

By asking you, your bank details via telephone such as CVV, the fraudster then uses the information to steal money from your bank account.



Most common OTP scams

Request Money Links

The fraudsters often trick you by sending a "request money link" to lure you into entering your OTP by falsely promising you that you have won a lottery/ lucky-draw and to receive the money, you are required to enter the OTP, in the anticipation of receiving the prize money in your account.

When you enter the OTP, the amount is in fact withdrawn from your account.

Most common OTP scams

Fake KYC

In this, the fraudster contacts you posing as an employee of a bank asking you to immediately complete your KYC, else your account will be locked within 24 hours.

The fraudster then asks you to download an app on your mobile.

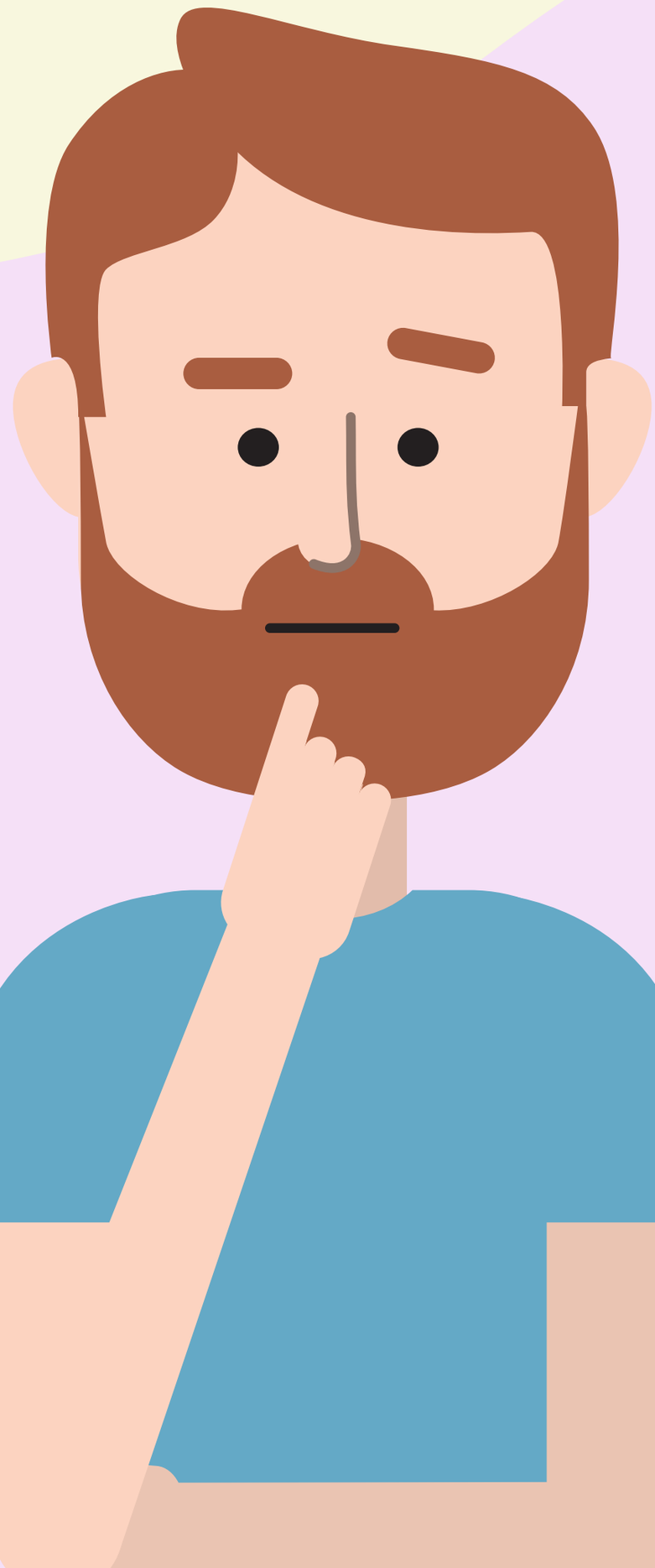
Further, the fraudster asks for your ID and asks you to make a verification payment of rupee one via your digital wallet. As soon as you make the payment, all your details are captured by the fraudster to be later misused.

How can I protect myself while making online transaction?

Do not download an app unnecessarily

Never enter your PIN, CVV or OTP on an unverified payment gateway

Be aware of fake callers

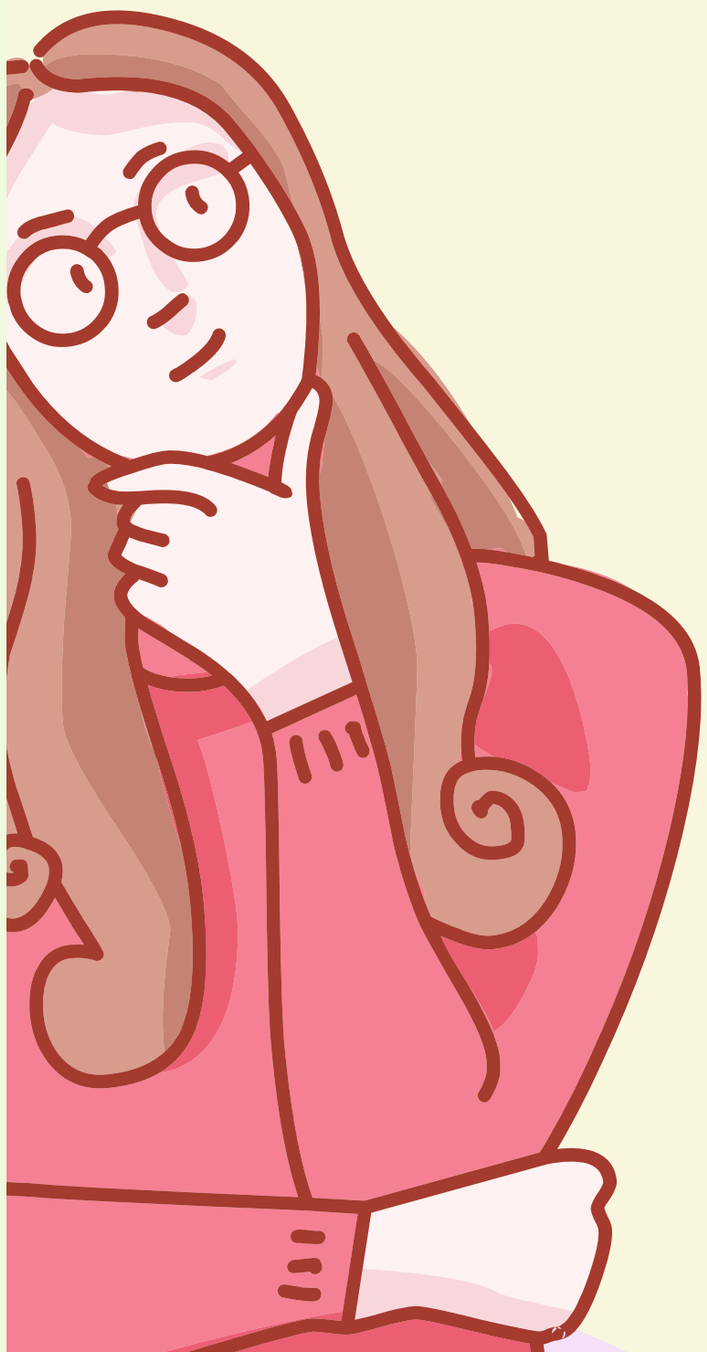


Always talk to banks/ credit card companies on their official helpline number and do not share any details to a caller even if they claim to be an official representative

How and where can I report Online Payment Fraud?

Foremost would be to report such an incident immediately to your bank or e-wallet company to block your account to prevent further loss.

In the case of UPI, you should report the fraud to both their bank and the payment company whether it is Google Pay, Paytm etc.



In case of a payment fraud on an e-commerce website, PoS device or an ATM, customers should file the complaint with the card issuing bank.

How and where can I report Online Payment Fraud?

Online Complaint:
You can file an online complaint on government portal National Cyber Crime Reporting Portal (URL: https://cybercrime.gov.in/)

Reporting on National Cyber Portal

Get yourself registered on the portal by using your name and mobile number. An OTP will be sent to you for confirmation.

Subsequently, select the appropriate category and sub-category

Collate your complaint with as much evidence as possible, such as, Credit card receipt, bank statement, copy of email, URL of web page etc.

You will receive a tracking number which can be used to keep a track on your complaint.

ONLINE SHOPPING

What is Social Commerce?

Social commerce or community commerce is when you buy products via social media platforms such as Instagram, Facebook, Pinterest etc.

Your entire online shopping process that is, from discovering the product to making the final payment is done on a social media platform, (no website is required)

WHY SHOULD YOU BE MINDFUL WHILE SHOPPING FROM SOCIAL MEDIA PAGE?

Often while shopping, especially over social media platforms

we tend to give out more personal information than otherwise would have on a website

which may later on be misused by cybercriminals

On the surface we cannot anticipate the pitfalls of not mindfully shopping on these social media pages

HOW DO CYBERCRIMINALS CHEAT ON SOCIAL COMMERCE PAGES?

The newest way is they hack Instagram pages having more than 10k followers,

change their name, profile, bio etc. to portray as a legitimate online shopping page

Offering huge discounts, they attract a lot of customers, do not accept cash-on-delivery as a mode of payment and insist on making prior payments.

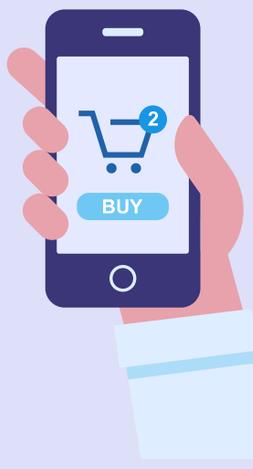
Once the payment is done online the product is never delivered to the customer.

What are some Digital Etiquette to be followed?

1. Be mindful while shopping on any social media platform
2. Do not get fooled by huge discounts and offers. Be very watchful of such low prices of quality products
3. Before you make a purchase, look for authentic reviews of the product as well as the shopping page
4. Prefer cash-on-delivery option over online payment
5. In case you do fall prey to such an incident, make sure to report the incident on the cybercrime reporting portal (URL: https://cybercrime.gov.in) or your state's cyber cell department explaining the incident and attach a few screenshots of your chats and the shopping page as well

FAKE E-COMMERCE WEBSITE SCAMS

The newest form of cybercrime is duping through online e-commerce websites



wherein the fraudsters create fake online shopping websites which are aggressively promoted via digital marketing tools and SEO

These websites offer high discounts on various products and oftentimes do not have a cash-on-delivery option to opt for making payments.

HOW DO FRAUDSTERS CHEAT?

One way is the fraudster creates a fake copy of the website of an existing e-commerce website

or a company offering a high discount on the same products

The trick here is, their website would have only an online payment mode and

once the payment is made, the product is never received by the customer.

HOW DO FRAUDSTERS CHEAT?

The other variant is, when these fake websites have special schemes wherein,

if you purchase beyond a certain amount you would be eligible for an expensive or luxury gift absolutely free of cost.

And as you make a purchase you would receive a call from their customer service asking you to make a refundable payment,

this way the fraudsters trick you to make a payment of thousands of rupees.

HOW DO FRAUDSTERS CHEAT?

The fraudsters create an entirely new website offering huge discounts.

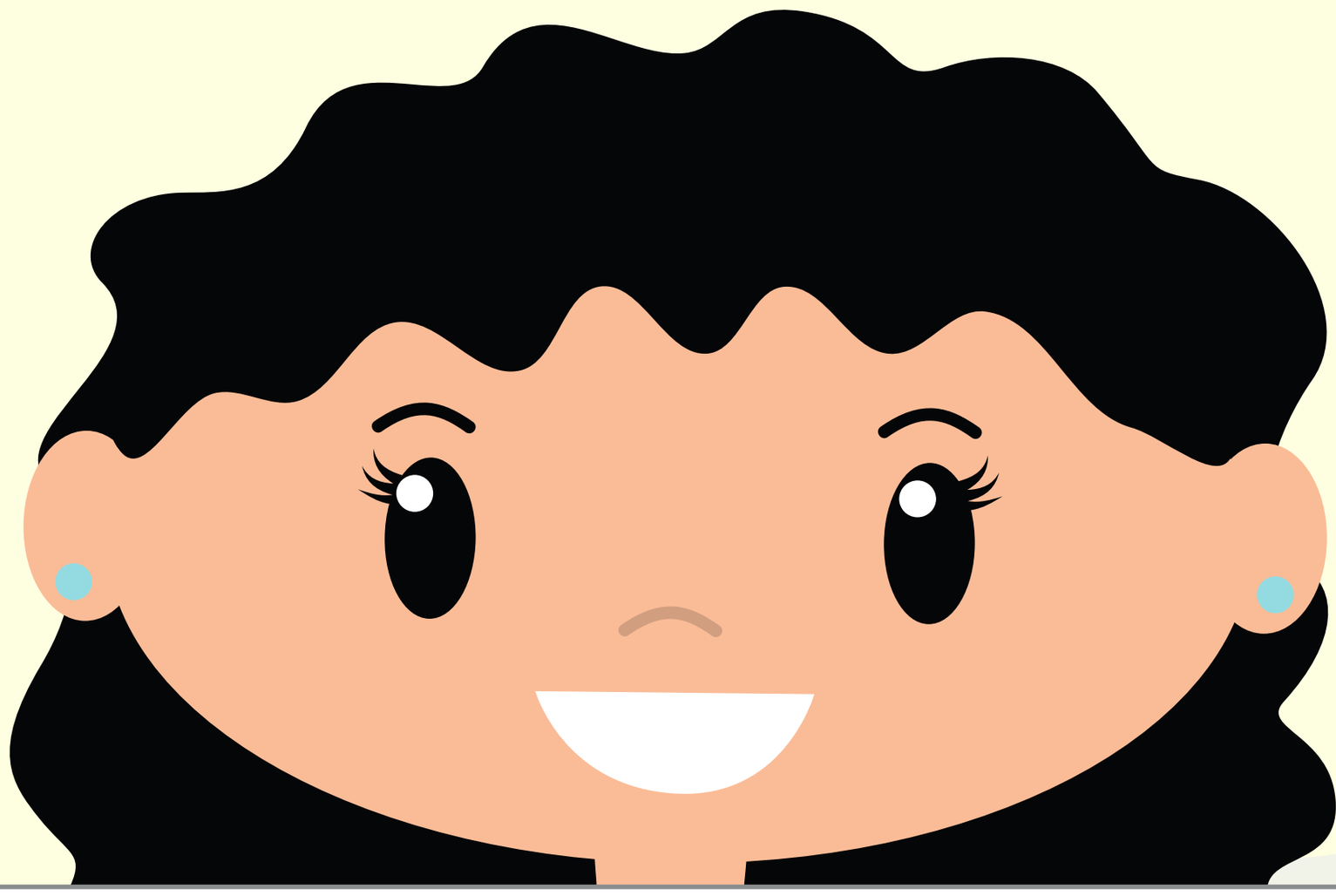
Once the payment is made online, the product is never delivered

or even if delivered, the product is either damaged or a used version

What are some Digital Etiquette to be followed?

1. Always look for reviews on various public forums of the website and their services before making a purchase
2. Check for credentials of the shopping portal online
3. Do not be fooled by huge discounts and flash sales
4. If the sites offer Cash-on-delivery, prefer that. Avoid making online payment on a relatively new shopping website
5. Fraudsters not only steal your money but would, on most occasions, also capture your card credentials. So, prefer a low-balance account while making such payments

THANK YOU



Thank you for taking the time to read through this ebook. If you found the ebook insightful, do share it with your loved ones and also with people in need for cyberspace knowledge.

Help us better ourselves, by giving your valuable feedback. You can fill the form here:
https://bit.ly/3042B4C

ABOUT US

PUBLIC CONCERN FOR GOVERNANCE TRUST

- ***Public Concern For Governance Trust (PCGT)***

PCGT came into existence in the year 2002 by eminent citizens ***Shri J. F. Ribeiro, Dr. R.K. Anand and late Shri B.G. Deshmukh****. We, at PCGT Mumbai, with our primary goal focusing on promoting honesty, transparency and accountability in governance have taken up multiple projects to bridge the gap. We have a vision to strive for good governance, curtail corruption, uphold and inculcate values and enhance Sadbhavna in the citizens.*

- ***Youth For Governance and Cyber Watch***

PCGT undertook the programme of Youth For Governance (YFG) in 2012 and since then has been trying to motivate the youth across Mumbai city colleges to be a part of the movement of promoting good governance.

One such project undertaken by PCGT in the pandemic was ***Cyber Watch*** *with an objective to promote cyber safety. Ever since then, there have been 3 such projects focusing different aspects of Cyber Safety. This ebook is an addition to the project.*

ABOUT US

Mr. NandKumar Saravade

- **Expert Contributor**

He was CEO of Reserve Bank Information Technology Pvt. Ltd (ReBIT) till May'21. He has also led the Data Security Council of India, worked as an independent advisor on fraud risk and cyber security, Ernst&Young, ICICI Bank and CitiBank. As his role in NASSCOM, he headed the Cyber Security & Compliance Dept. as a Director. He has also served in the CBI for 7 years, leading the Bank Securities & Fraud Cell at Mumbai for a year. Currently, he is an advisor/mentor on Security, Technology, Entrepreneurship and Governance.

Amisha Upadhyay

- **Author & Designer**

*Third year law student at Narsee Monjee Institute of Management Studies (NMIMS), Navi Mumbai, she was an intern for the July'20 batch of PCGT wherein the idea to execute a campaign to 'de-normalise cyber abuse on social media'-**Project Cyber Watch** kicked in. After almost a year, gathering much appreciation for the project and examining the dependence on the online world, the conceptualisation of an ebook having the required resources for staying safe on the Internet was born.*

Disclaimer

The references of various tools and apps referred in the ebook belongs to its respective owners. This ebook only aims to educate end users to follow essential steps to take into account for staying safe on the Internet and does not in anyway account for any forum for resolving any grievances.

For any clarification, suggestion or feedback you can reach us at- publicconcern@gmail.com or *amishaupadhyay24@gmail.com*