Safer Internet Day Campaign

Secure way of using Smartphones and Safety on Social Media

Information Security
Education & Awareness
Project Phase - II

M Jagadish Babu ,
Project Manager - ISEA,
C-DAC, Hyderabad

Safer Internet Day Campaign

Organized by

Central Institute of Educational Technology (CIET)
National Council of Educational Research and Training,
Ministry of Education , New Delhi,
in collaboration with
Information Security Education and Awareness(ISEA) ,
a programme by Ministry of Electronics and Information Technology(MeitY), Govt. of India.

Secure way of using Smart Phone

Introduction

- Mobile devices have revolutionized the way we communicate, we surf the internet, we do payments, we do gaming and many more
- They have the capability to perform the functionality of a camera, calculator, barcode reader, credit card scanner, USB thumb drive, eBook reader, audio recorder and many more
- This multi function capability of the device along with the cost and mobility factor has made mobile devices an important part of personal and business life of people and organizations
- This has led to tremendous increase in the usage of mobile devices in the country
- Now a days, mobile devices have become an important part of personal and business life of people and organizations

INDIA 2ND LARGEST AFTER CHINA

227m Rural India

205m Urban India

71m kids aged between 5-11 also go online using adults' devices

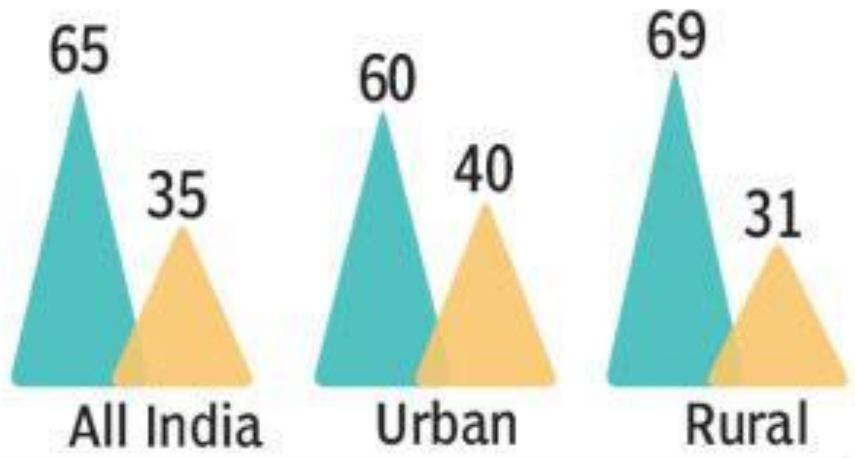
503m India

850m China

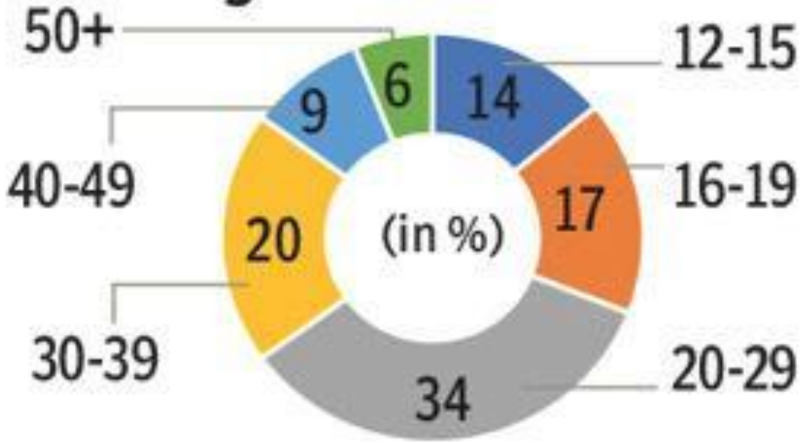
Source: IAMAI/Nielsen

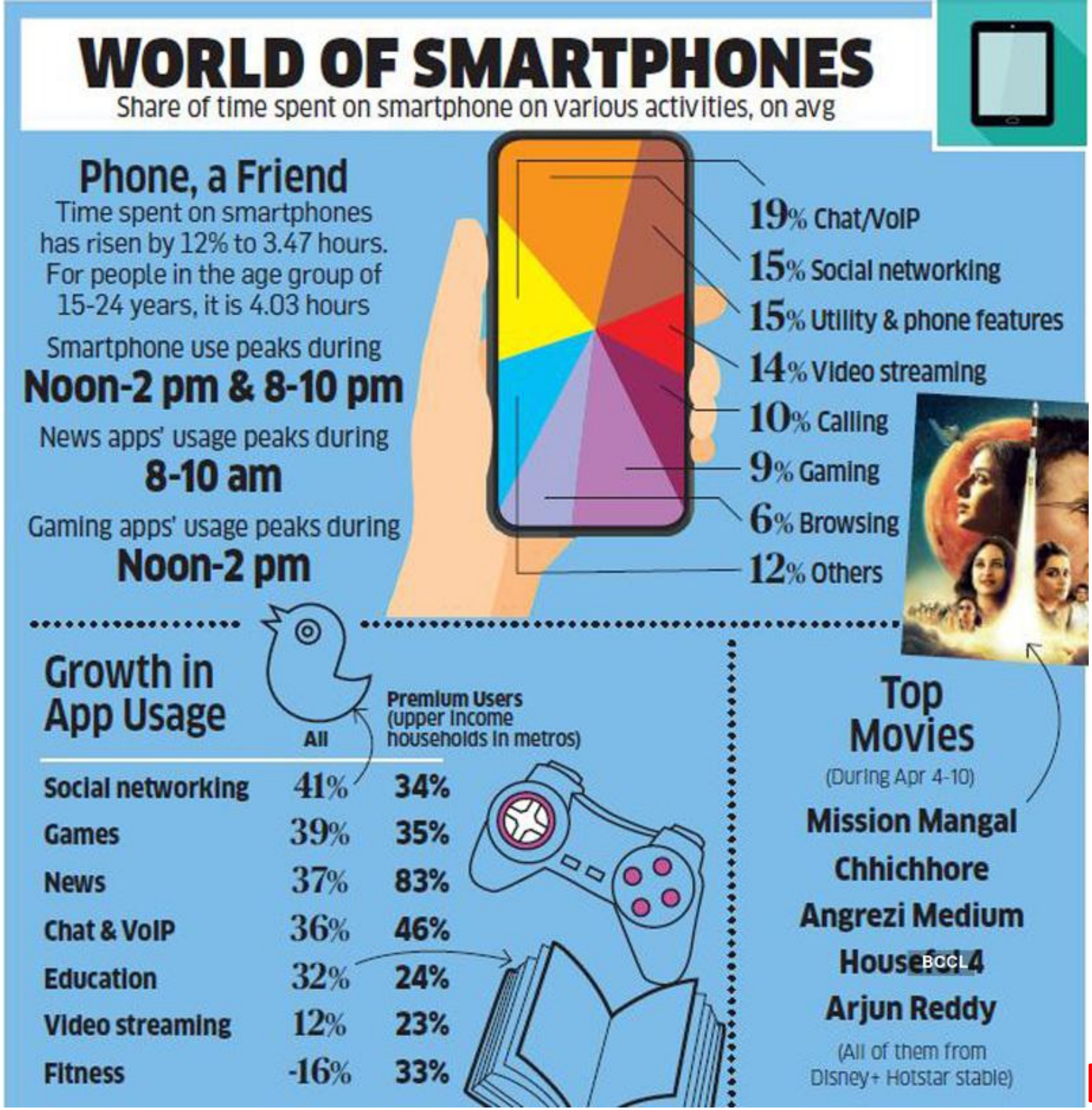
Gender Distribution

(as %)



Age Distribution





WORLD OF SMARTPHONES

Share of time spent on smartphone on various activities, on avg

Phone, a Friend

Time spent on smartphones has risen by 12% to 3.47 hours. For people in the age group of 15-24 years, it is 4.03 hours

Smartphone use peaks during

Noon-2 pm & 8-10 pm

News apps' usage peaks during

8-10 am

Gaming apps' usage peaks during

Noon-2 pm

- 19% Chat/VoIP
- 15% Social networking
- 15% Utility & phone features
- 14% Video streaming
- 10% Calling
- 9% Gaming
- 6% Browsing
- 12% Others

Growth in App Usage

	All	Premium Users (upper income households in metros)
Social networking	41%	34%
Games	39%	35%
News	37%	83%
Chat & VoIP	36%	46%
Education	32%	24%
Video streaming	12%	23%
Fitness	-16%	33%

Top Movies

(During Apr 4-10)

Mission Mangal

Chhichhore

Angrezi Medium

Housefull 4

Arjun Reddy

(All of them from Disney+ Hotstar stable)

Economic Times

Latest phishing and fraud attacks

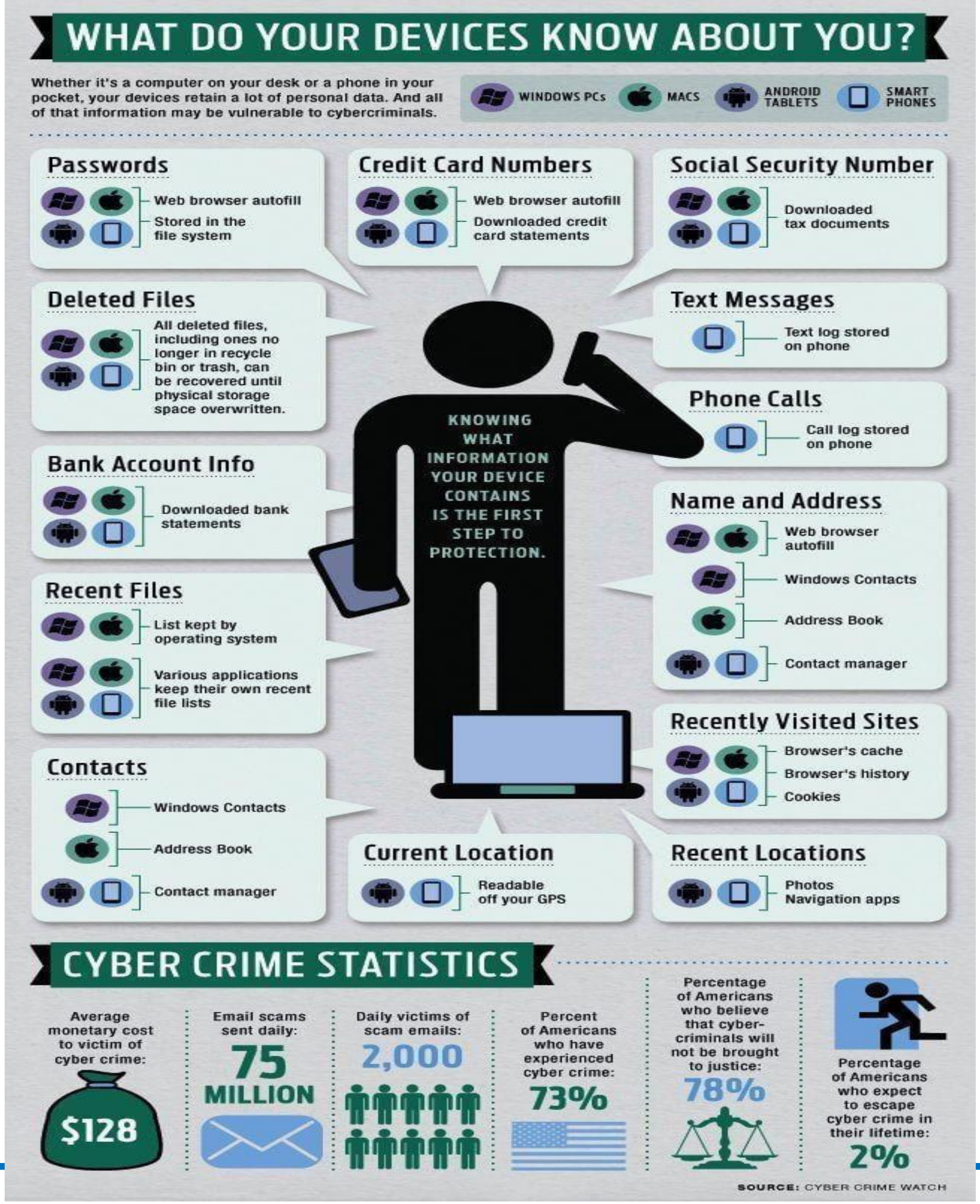
Amazon, Apple, Netflix, Facebook and WhatsApp are top brands leveraged by cybercriminals in phishing and fraud attacks – including a recent strike on a half-million Facebook users.

Facebook has been a top cybercriminal favorite in phishing attacks so far this year, with recent research shedding light on 4.5 million phishing attempts that have leveraged the social media platform between April and September 2020.

Behind Facebook, messenger app WhatsApp is the second-top platform leveraged by attackers (with 3.7 million phishing attempts), followed by Amazon (3.3 million attempts), Apple (3.1 million attempts) and Netflix (2.7 million attempts).

Google's offerings (including YouTube, Gmail and Google Drive) took sixth position, with 1.5 million phishing attempts altogether according to a

by Kaspersky.



WHAT DO YOUR DEVICES KNOW ABOUT YOU?

Whether it's a computer on your desk or a phone in your pocket, your devices retain a lot of personal data. And all of that information may be vulnerable to cybercriminals.

WINDOWS PCs · MACS · ANDROID TABLETS · SMART PHONES

Passwords

- Web browser autofill
- Stored in the file system

Credit Card Numbers

- Web browser autofill
- Downloaded credit card statements

Social Security Number

- Downloaded tax documents

Deleted Files

- All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.

Text Messages

- Text log stored on phone

Phone Calls

- Call log stored on phone

Bank Account Info

- Downloaded bank statements

KNOWING WHAT INFORMATION YOUR DEVICE CONTAINS IS THE FIRST STEP TO PROTECTION.

Name and Address

- Web browser autofill
- Windows Contacts
- Address Book
- Contact manager

Recent Files

- List kept by operating system
- Various applications keep their own recent file lists

Recently Visited Sites

- Browser's cache
- Browser's history
- Cookies

Contacts

- Windows Contacts
- Address Book
- Contact manager

Current Location

- Readable off your GPS

Recent Locations

- Photos
- Navigation apps

CYBER CRIME STATISTICS

Average monetary cost to victim of cyber crime: $128

Email scams sent daily: 75 MILLION

Daily victims of scam emails: 2,000

Percent of Americans who have experienced cyber crime: 73%

Percentage of Americans who believe that cyber-criminals will not be brought to justice: 78%

Percentage of Americans who expect to escape cyber crime in their lifetime: 2%

SOURCE: CYBER CRIME WATCH

Why should we worry ?

- Smartphones
  - Have our credentials are saved
  - Have our banking apps are installed
  - We carry out many financial transactions - UPI, wallets etc.,
  - Messages
  - Photographs and videos

Why should we worry ?

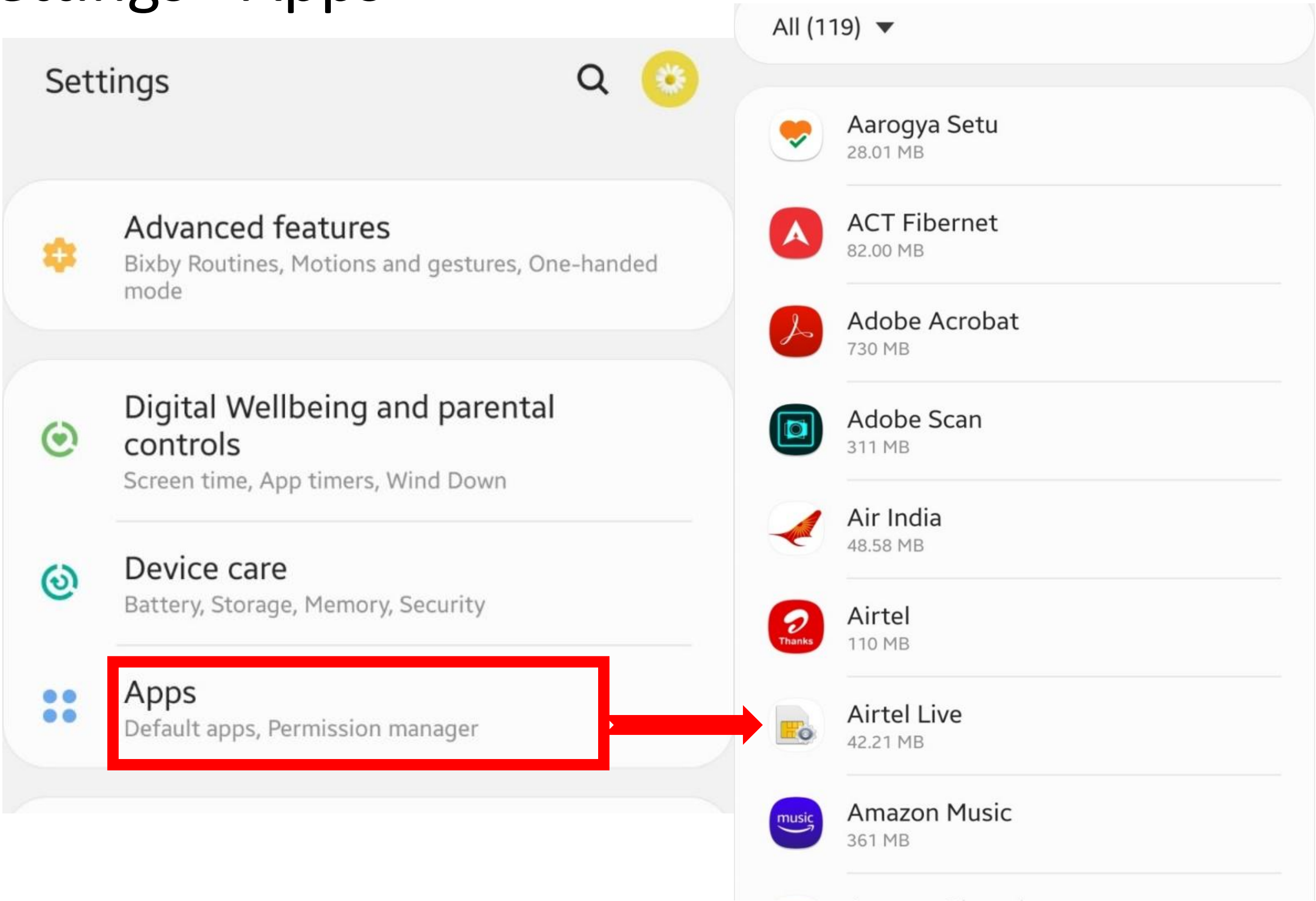
- Our complete Personal Sensitive Information is carried by our smart phones
  - Messaging – OTP , password research codes etc.,
  - Camera
  - Microphone
  - Gallery
  - Contacts
  - Location

QUICK TIP

Regularly Monitor the permissions of critical features in your mobile

Monitor Permissions

- Settings - Apps



Settings

Advanced features
Bixby Routines, Motions and gestures, One-handed mode

Digital Wellbeing and parental controls
Screen time, App timers, Wind Down

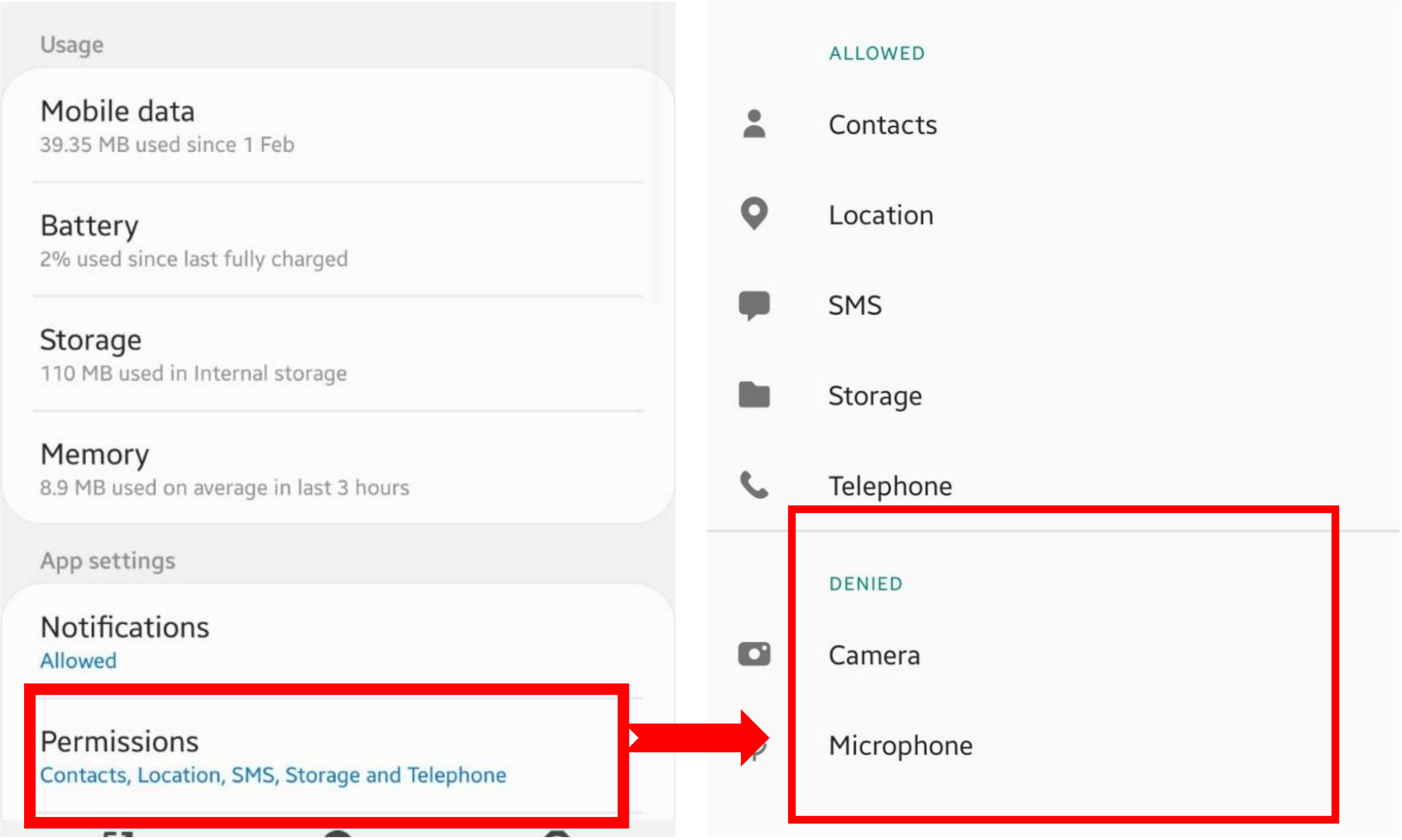
Device care
Battery, Storage, Memory, Security

Apps
Default apps, Permission manager

All (119)

Aarogya Setu	28.01 MB
ACT Fibernet	82.00 MB
Adobe Acrobat	730 MB
Adobe Scan	311 MB
Air India	48.58 MB
Airtel	110 MB
Airtel Live	42.21 MB
Amazon Music	361 MB

Monitor Permissions



Usage

Mobile data
39.35 MB used since 1 Feb

Battery
2% used since last fully charged

Storage
110 MB used in Internal storage

Memory
8.9 MB used on average in last 3 hours

App settings

Notifications
Allowed

Permissions
Contacts, Location, SMS, Storage and Telephone

ALLOWED

Contacts

Location

SMS

Storage

Telephone

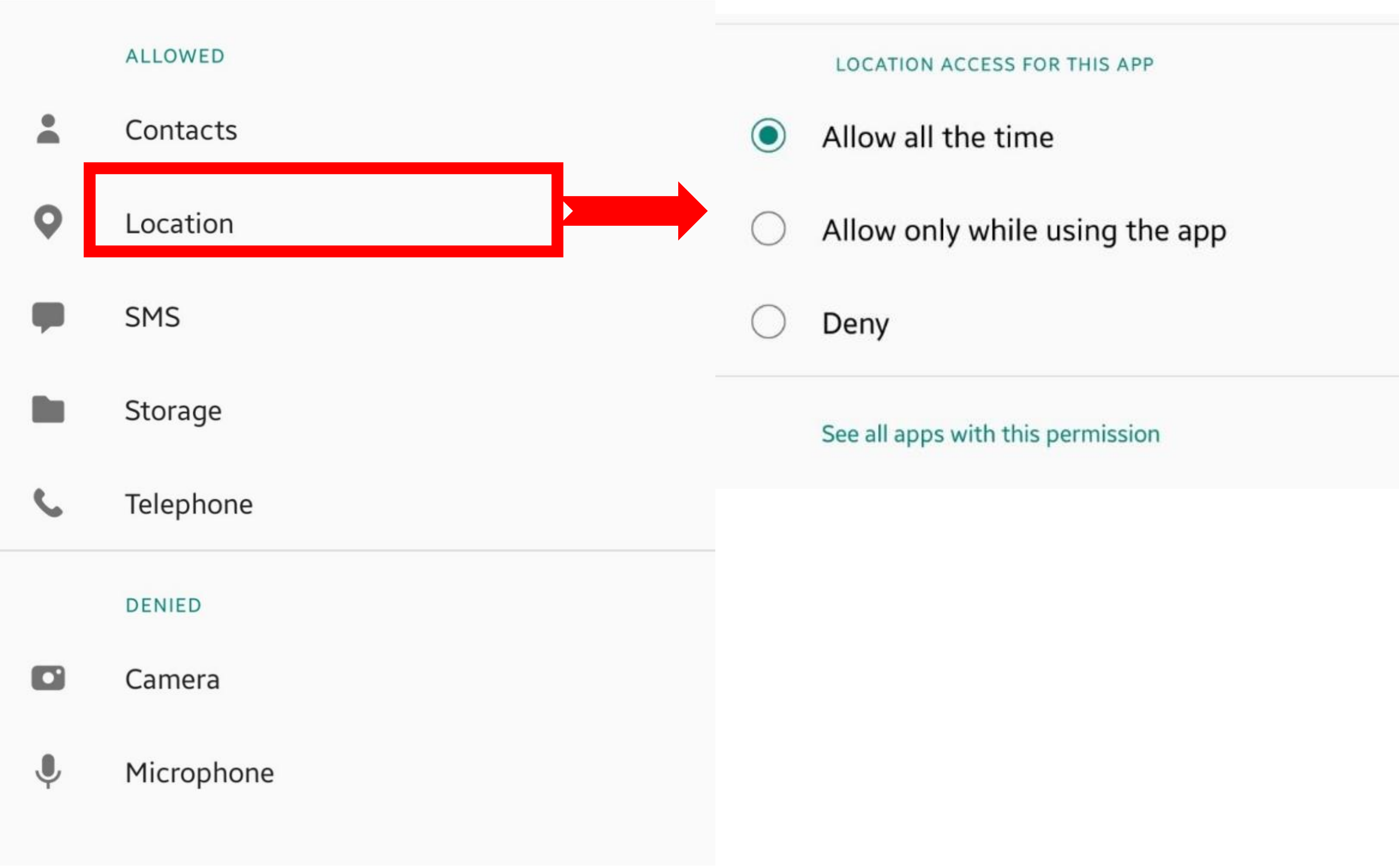
DENIED

Camera

Microphone

Based on App functionality we should be able to analyze if these permissions are necessary for the app or not

Change Permissions



ALLOWED

- Contacts
- Location
- SMS
- Storage
- Telephone

DENIED

- Camera
- Microphone

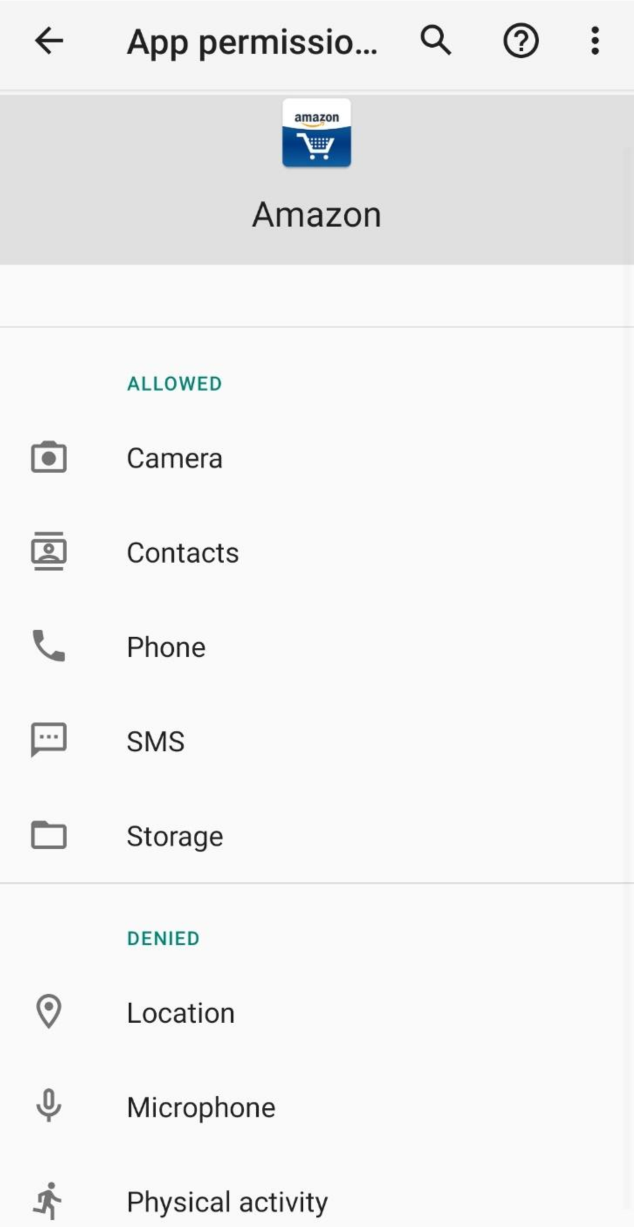
LOCATION ACCESS FOR THIS APP

● Allow all the time

○ Allow only while using the app

○ Deny

See all apps with this permission



App permissio…

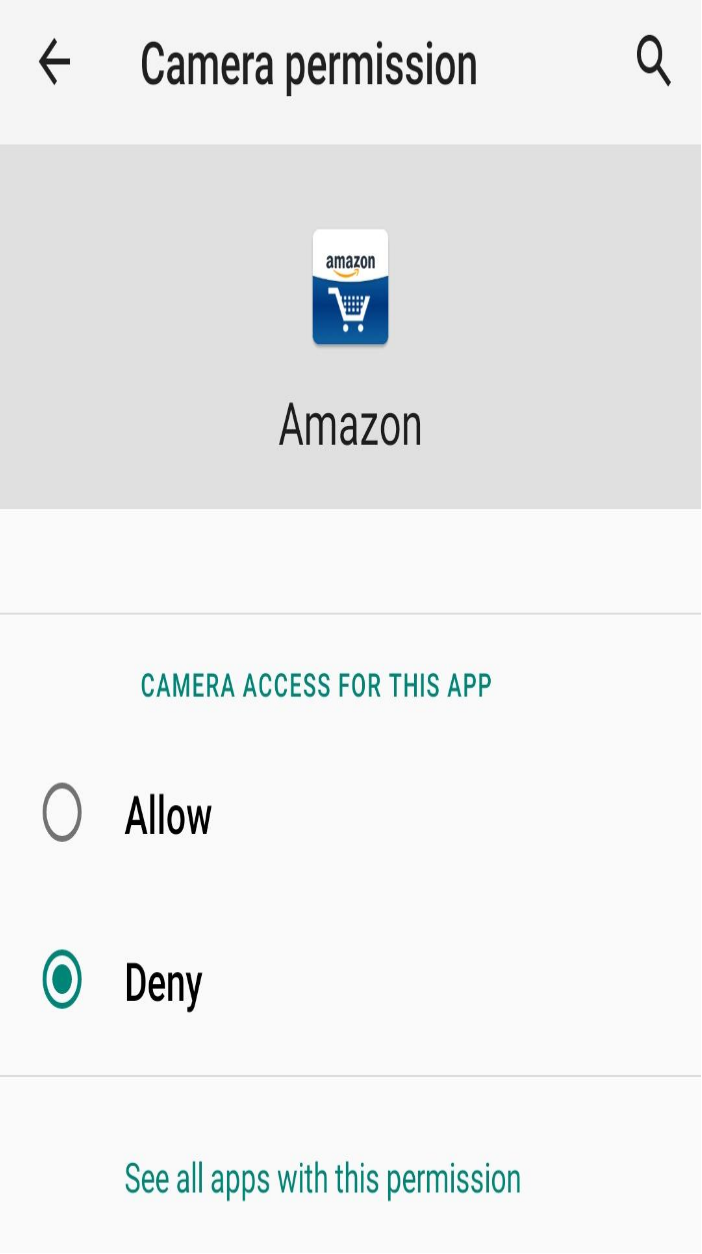
Amazon

ALLOWED

- Camera
- Contacts
- Phone
- SMS
- Storage

DENIED

- Location
- Microphone
- Physical activity



Camera permission

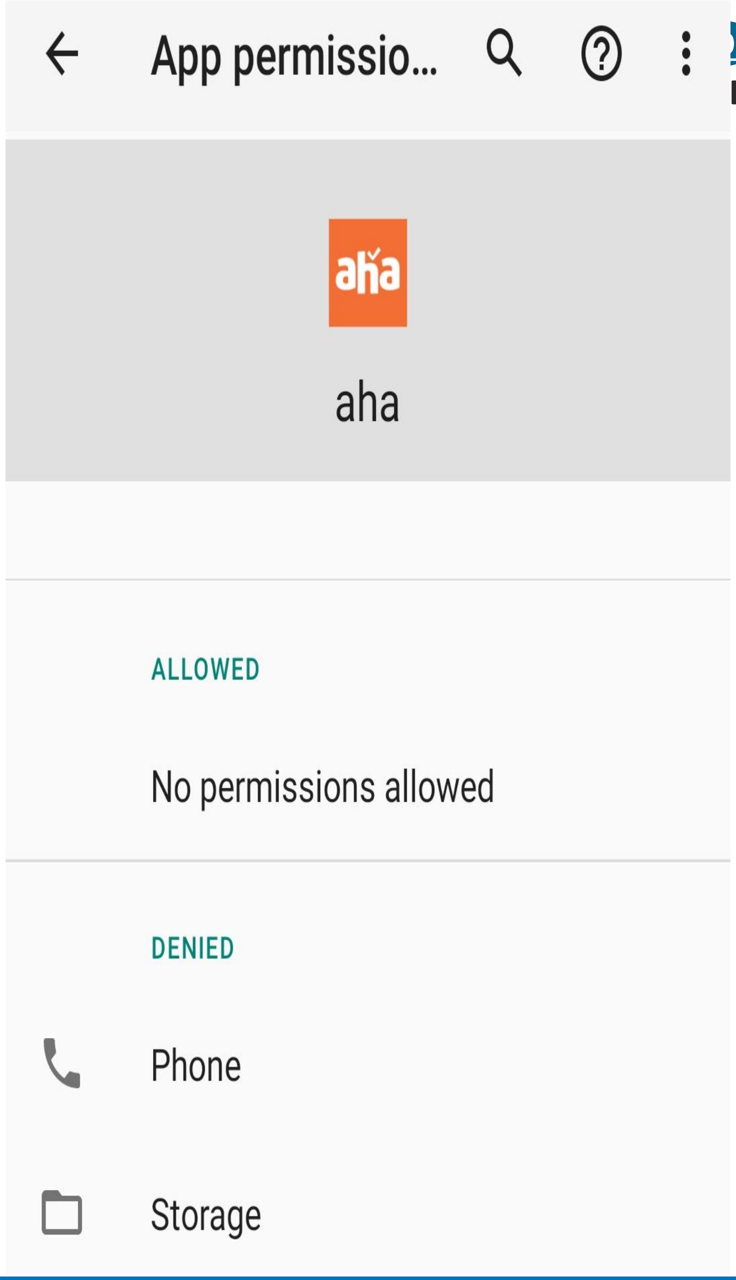
Amazon

CAMERA ACCESS FOR THIS APP

○ Allow

● Deny

See all apps with this permission



App permissio…

aha

ALLOWED

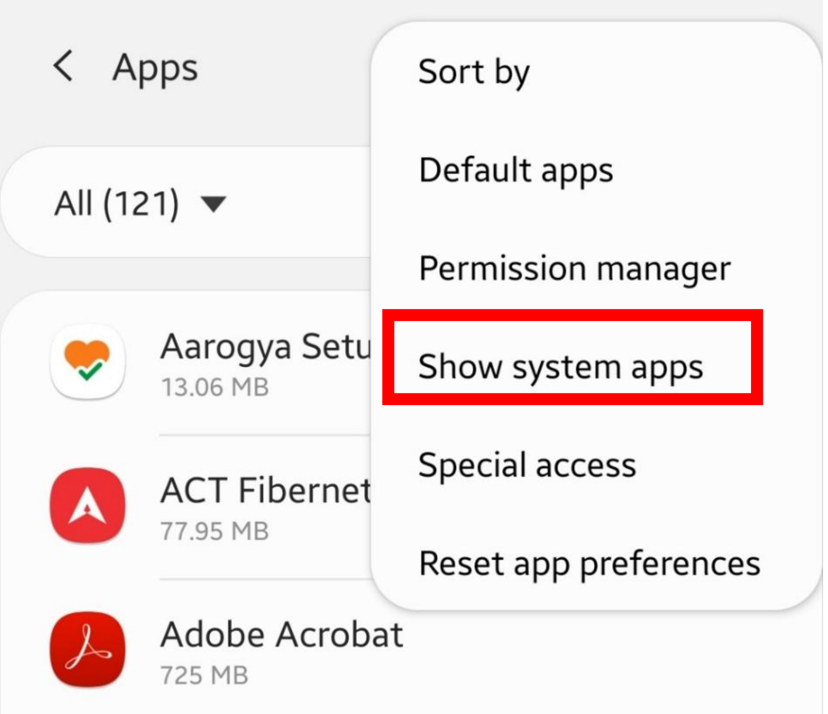
No permissions allowed

DENIED

- Phone
- Storage

Monitor all critical permissions at one place

- Access Permission Manager in your Mobile
- Settings – Apps – Permission Manager (OR)
- Settin



< Apps

All (121) ▼

Aarogya Setu
13.06 MB

ACT Fibernet
77.95 MB

Adobe Acrobat
725 MB

Sort by

Default apps

Permission manager

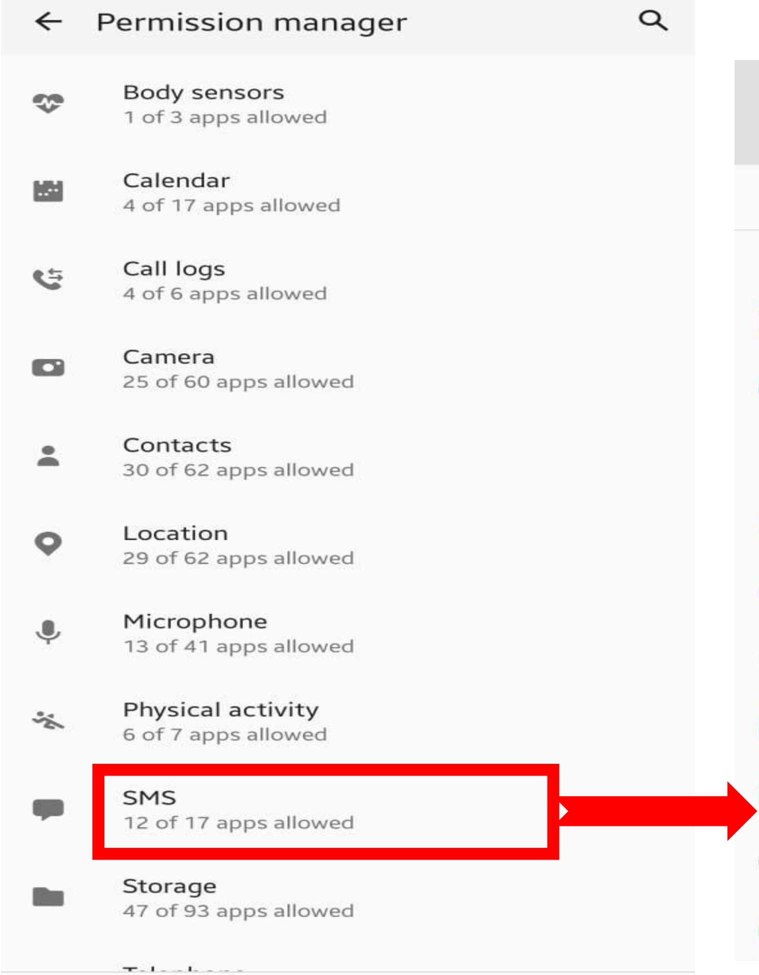
Show system apps

Special access

Reset app preferences

Monitor all critical permissions at one place

- Permission Manager



Permission manager

Body sensors
1 of 3 apps allowed

Calendar
4 of 17 apps allowed

Call logs
4 of 6 apps allowed

Camera
25 of 60 apps allowed

Contacts
30 of 62 apps allowed

Location
29 of 62 apps allowed

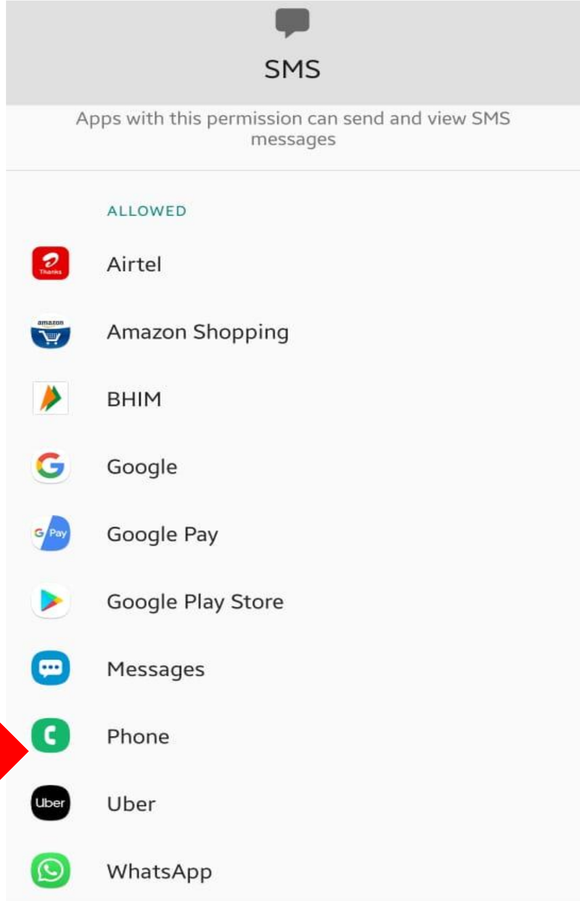
Microphone
13 of 41 apps allowed

Physical activity
6 of 7 apps allowed

SMS
12 of 17 apps allowed

Storage
47 of 93 apps allowed

Telephone



SMS

Apps with this permission can send and view SMS messages

ALLOWED

Airtel

Amazon Shopping

BHIM

Google

Google Pay

Google Play Store

Messages

Phone

Uber

WhatsApp

Installing Apps

- Search in stores can lead to malicious/phishing apps.
- For apps related to payment, banking , social networking etc., prefer to download app from company’s owned website rather than searching in the stores.

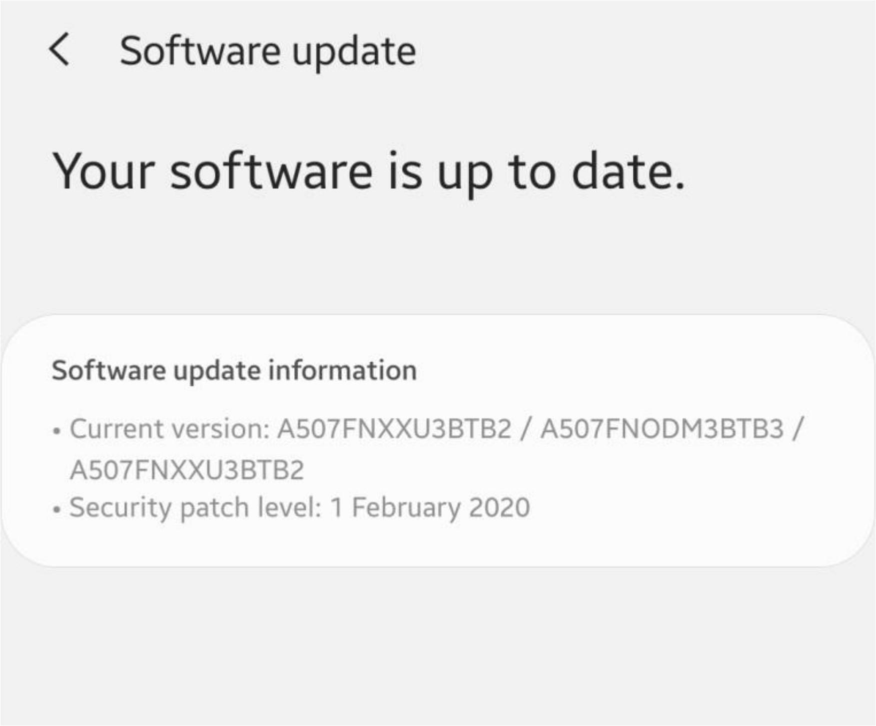
QUICK TIP

Download apps from genuine link & avoid all in one apps for any requirement

Updated Operating System and Apps

- Ensure your anti-virus and operating system are always updated

- Settings -> Software Update



Software update

Your software is up to date.

Software update information

- Current version: A507FNXXU3BTB2 / A507FNODM3BTB3 / A507FNXXU3BTB2
- Security patch level: 1 February 2020

Ensure Auto Updates are enabled for OS, Apps and Anti-Virus

Tips for your daily practice

- Turn OFF Bluetooth and WiFi when not in use
- Set time limit and Lock mobile automatically when not in use
- Prefer PIN/ finger print / face recognition locks as supported by your mobile.
  - Pattern lock are to be avoided - beware of shoulder surfing , screen reading by placing mobile in different positions.
- Track your mobile for unnecessary and unused apps

How to protect your Smart Phones

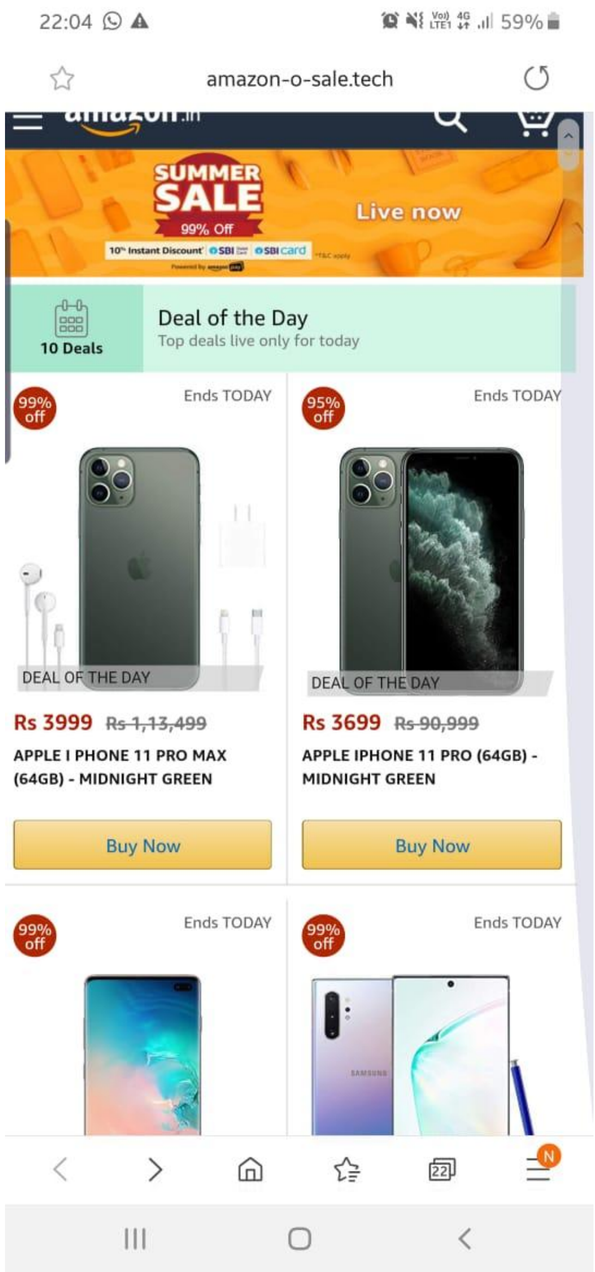
- Always update your devices with the latest software
- Especially, install all security patches provided by the OEMs to patch various security threats
- Never visit any shady websites by clicking on the links you have received over SMS, Whatsapp or by any other means
- Never install apps or software from unfamiliar publishers or from third-party app-stores
- Never use public WiFi hotspots for performing critical transactions

Some Recent Attacks

- Phishing attacks remain an effective method of stealing credentials and identities, distributing malware, eliciting fraudulent payments etc.
- Research shows that a new phishing site is launched every 20 seconds
- 87% of successful mobile phishing attacks take place outside of e-Mail
- •60% of mobile phishing attacks occur over HTTPS

www.isea.gov.in

www.InfoSec awareness.in



22:04 59%

amazon-o-sale.tech

amazon.in

SUMMER SALE 99% Off Live now

10% Instant Discount SBI SBI card *T&C apply

10 Deals

Deal of the Day

Top deals live only for today

99% off Ends TODAY

DEAL OF THE DAY

Rs 3999 ~~Rs 1,13,499~~

APPLE I PHONE 11 PRO MAX (64GB) - MIDNIGHT GREEN

Buy Now

95% off Ends TODAY

DEAL OF THE DAY

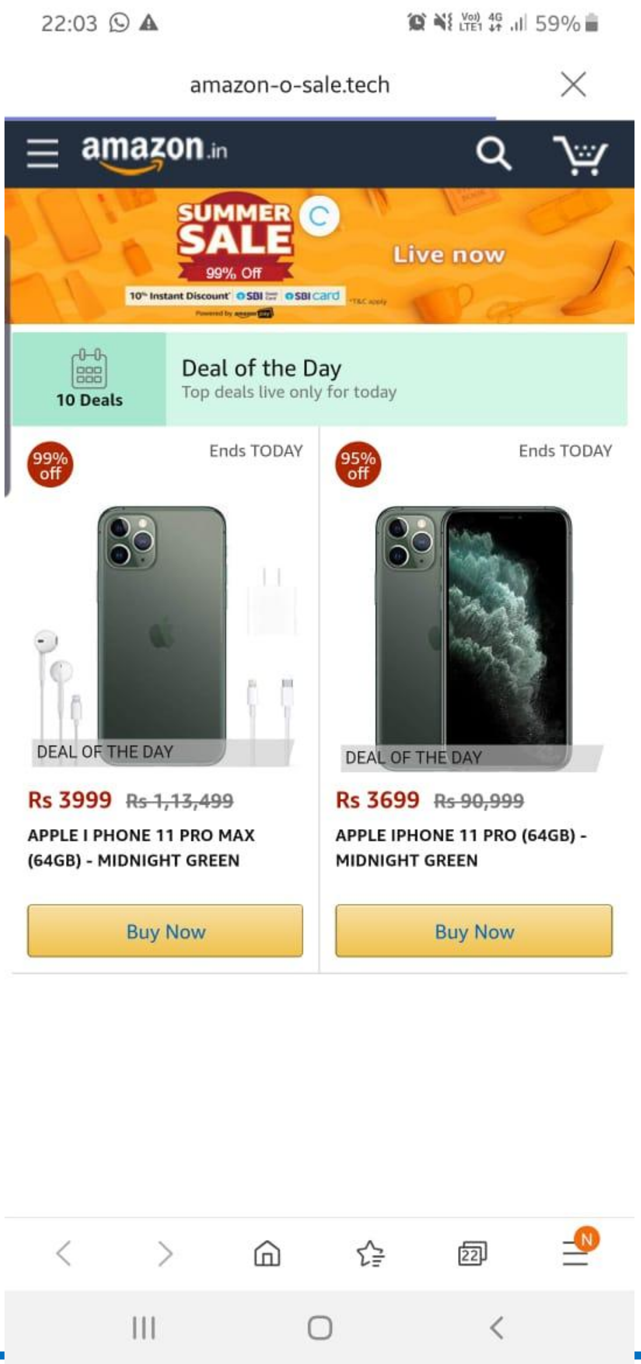
Rs 3699 ~~Rs 90,999~~

APPLE IPHONE 11 PRO (64GB) - MIDNIGHT GREEN

Buy Now

99% off Ends TODAY

99% off Ends TODAY



22:03 59%

amazon-o-sale.tech

amazon.in

SUMMER SALE 99% Off Live now

10% Instant Discount SBI SBI card *T&C apply

10 Deals

Deal of the Day

Top deals live only for today

99% off Ends TODAY

DEAL OF THE DAY

Rs 3999 ~~Rs 1,13,499~~

APPLE I PHONE 11 PRO MAX (64GB) - MIDNIGHT GREEN

Buy Now

95% off Ends TODAY

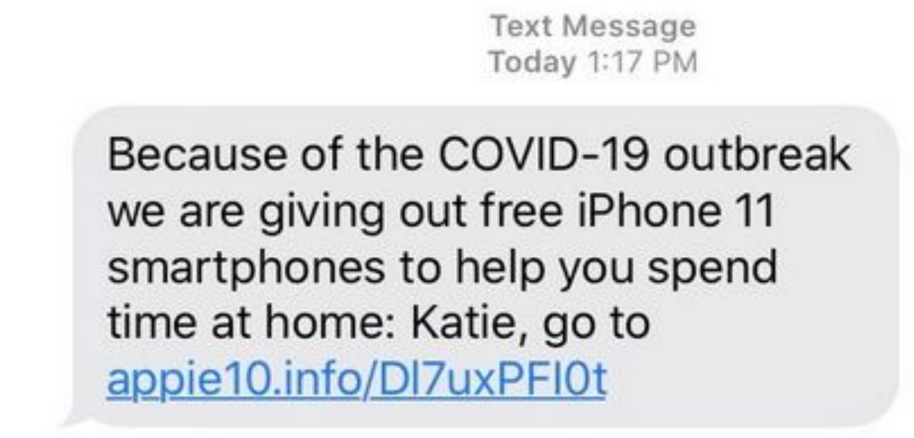
DEAL OF THE DAY

Rs 3699 ~~Rs 90,999~~

APPLE IPHONE 11 PRO (64GB) - MIDNIGHT GREEN

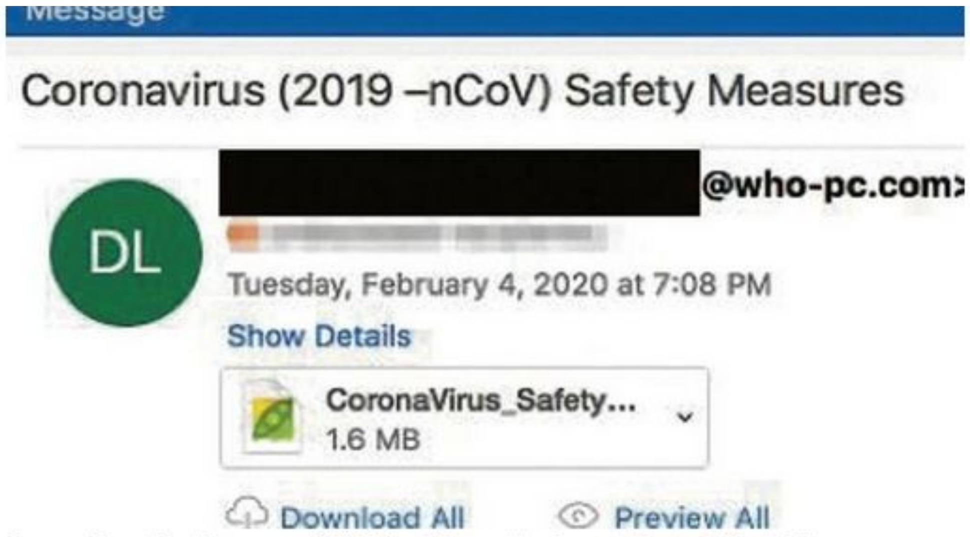
Buy Now

SMS phishing & Vishing



Text Message
Today 1:17 PM

Because of the COVID-19 outbreak we are giving out free iPhone 11 smartphones to help you spend time at home: Katie, go to appie10.info/Dl7uxPFI0t



Coronavirus (2019 –nCoV) Safety Measures

[redacted]@who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

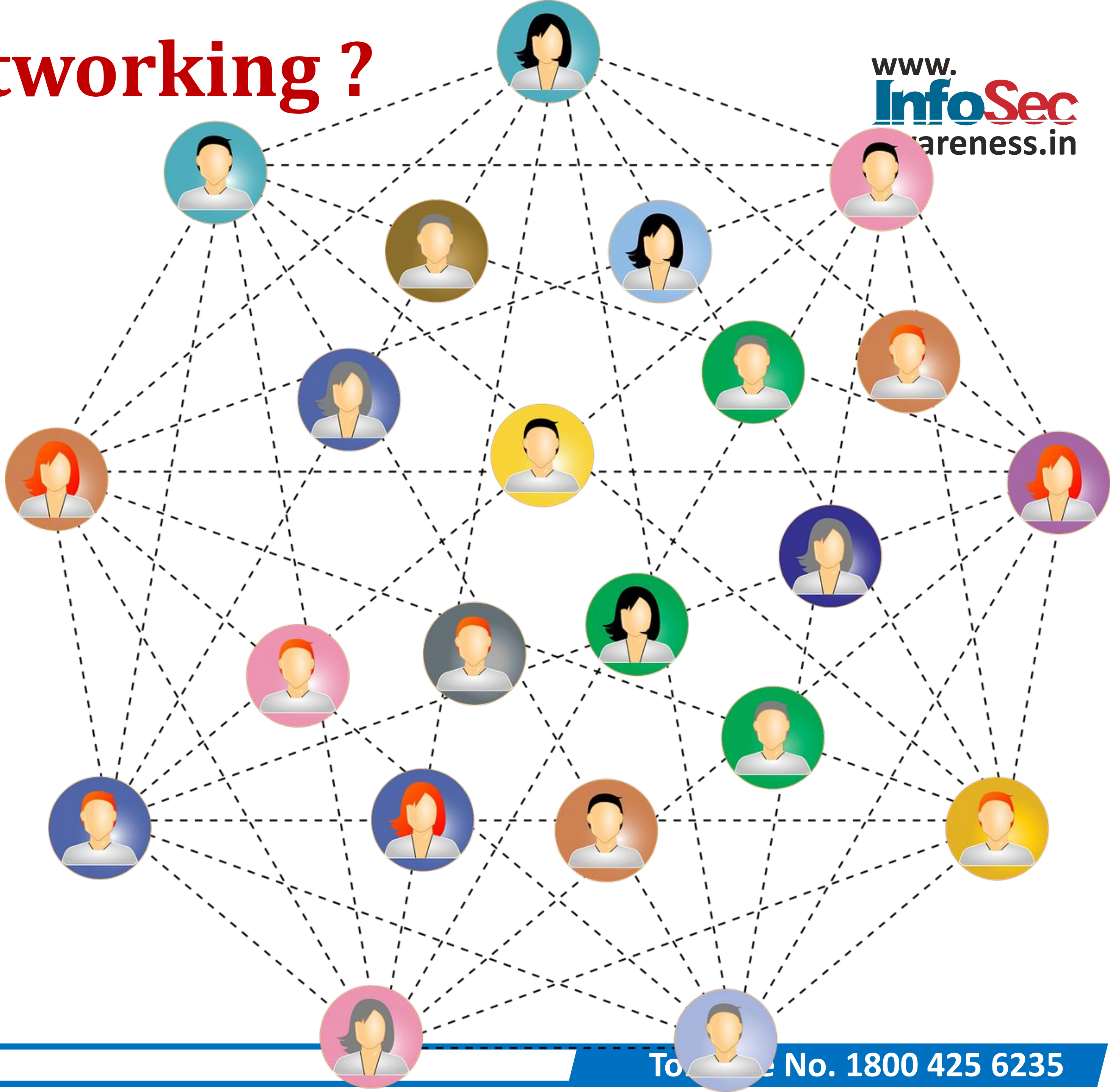
An email sent in the name of WHO with an attachment that will install the AgentTesla Keylogger to record all keystrokes and send them to attackers.
(Proofpoint)

Precautions

- Always check the link before clicking. Hover over it to preview the URL, and look carefully for misspelling or other irregularities.
- Enter your username and password only over a secure connection. Look for the “https” prefix before the site URL, indicating the connection to the site is secure.
- Be cautious about opening any attachments or downloading files you receive regardless of who sent them.
- Look for the sender email ID before you enter/give away any personal information.
- Use antivirus, antispyware and firewall software (update them regularly too).
- Always update your web browser and enable phishing filter.
- If you receive any suspicious e-mail do call a company to confirm if it is legitimate or not.
- Do use a separate email accounts for things like shopping online, personal etc.

What is Social Networking ?

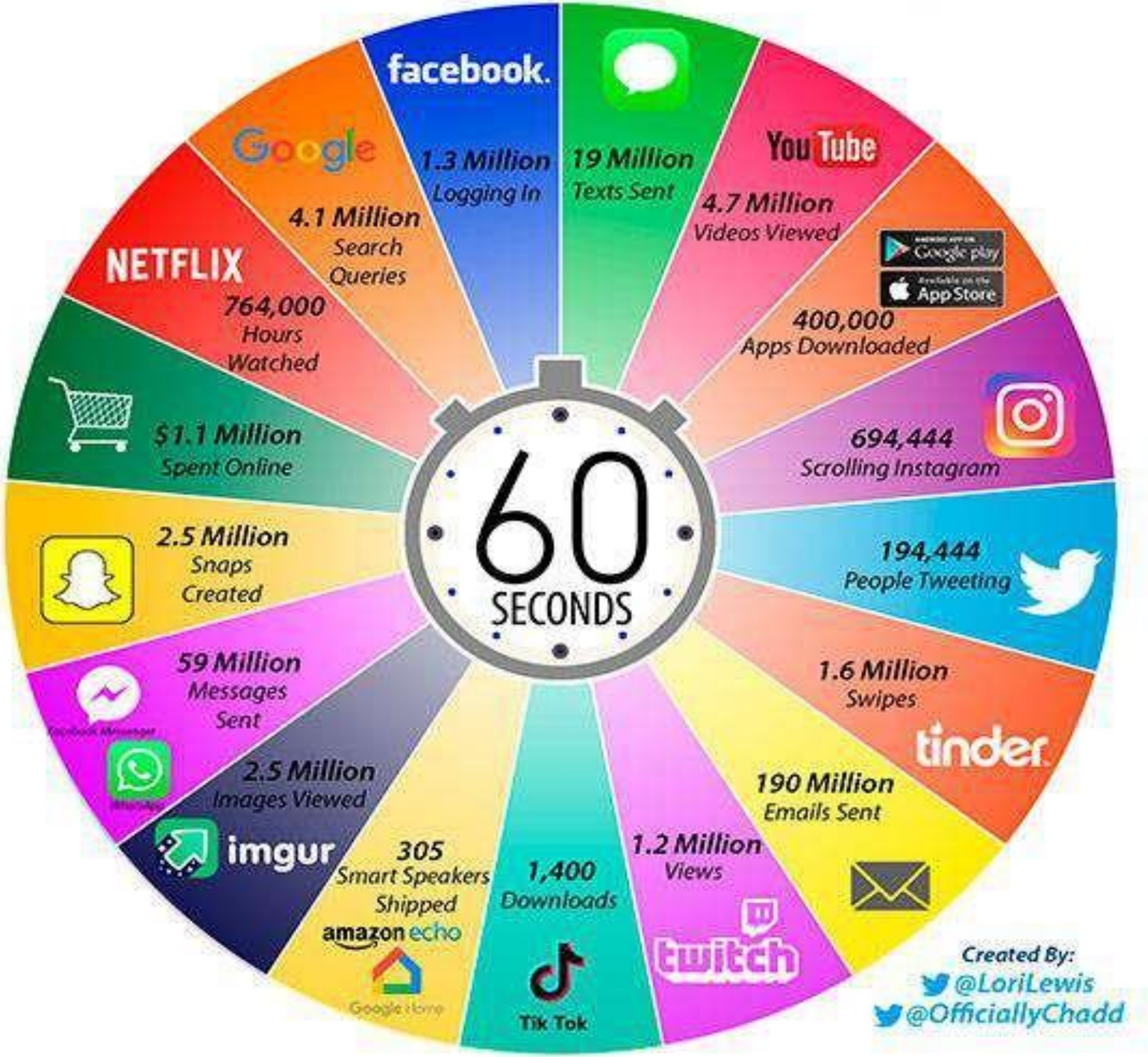
A social networking service is an online platform used to build social networks or social relations with other people who share similar personal or career interests, activities, backgrounds or real-life connections.



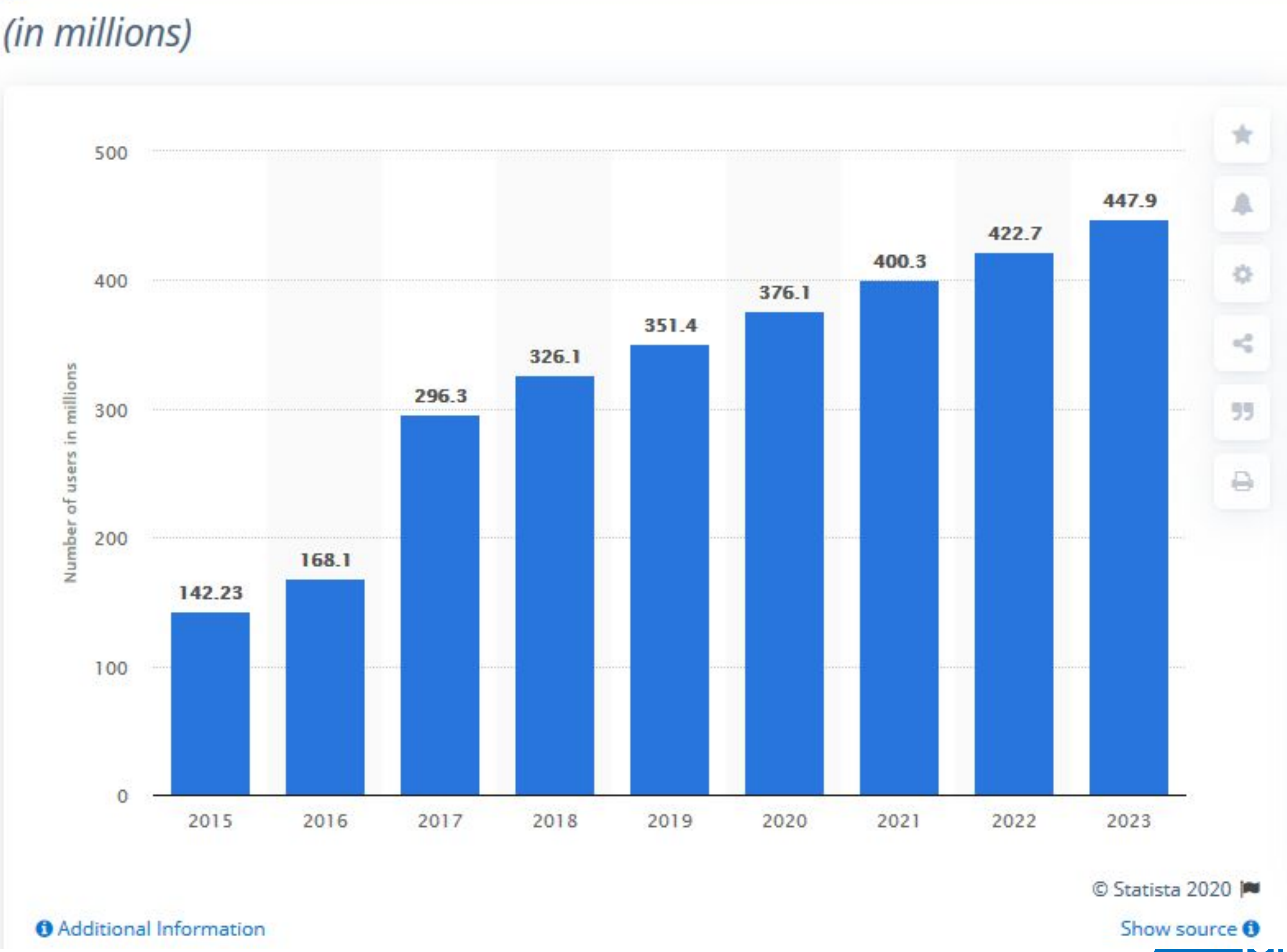
Types of Social Networks

SOCIALIZING	CAREER & BUSINESS OPPORTUNITIES	ONLINE MATCH MAKING	ONLINE SHOPPING SITES
FACEBOOK	LINKEDIN	SHAADI.COM	AMAZON
INSTAGRAM	NAUKRI.COM	BHARATMATRIMONY.COM	FLIPKART
WHATSAPP	MEETUP	MATCH.COM	MYNTRA
SNAPCHAT	XING		
TWITTER			

2020 This Is What Happens In An Internet Minute



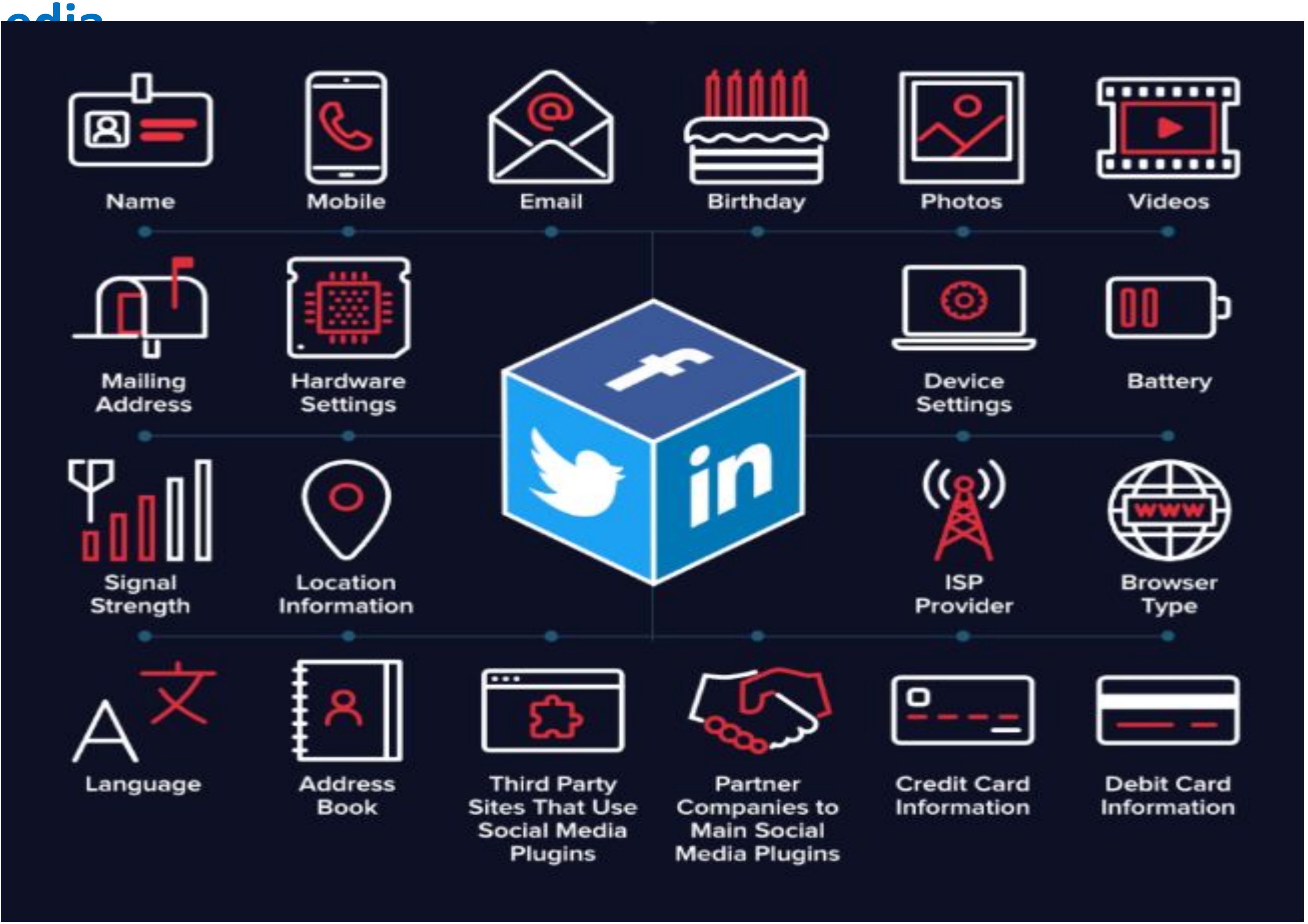
Number of social network users in India from 2015 to 2018 with a forecast until 2023



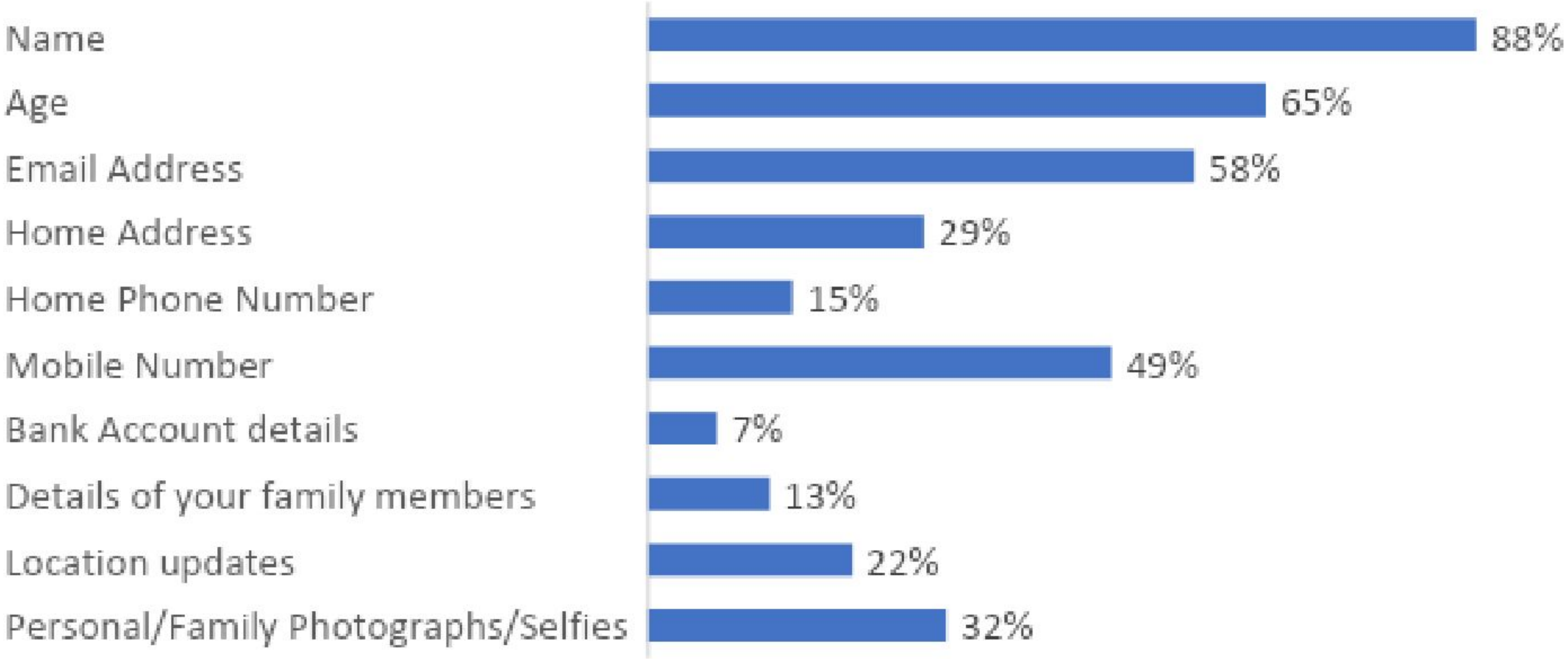
Social Networking

- Social Networking sites may be used for
- Meeting the people online across the world
- Making friendship with the people who are far away
- Profile building
- Self representation
- Exchanging / Sharing the information related to studies or education, current affairs, sports, business, transport, movies, latest news updates, event announcements, exchanging the thoughts etc
- Share the data files, videos, music, photos

What Personal Information You Share on Social Media



Personal Information available publicly on internet



www.isea.gov.in

www.InfoSecawareness.in

Social Networking Risks and Challenges

Social Networking Risks and Challenges

Social networking has become most popular activity in today's Internet world and epically growing kinds

Disadvantage : Trapped by scammers or hackers leading to loss of confidentiality and identity theft,

- expose the kids to various risks like
  - online bullying,
  - disclosure of personal information,
  - cyber-stalking,
  - access to inappropriate content,
  - online grooming,
  - child abuse,
  - fake profiles with false information,
  - malicious application,
  - Spam, and fake links which leads to phishing attacks etc.,

Some more Risks

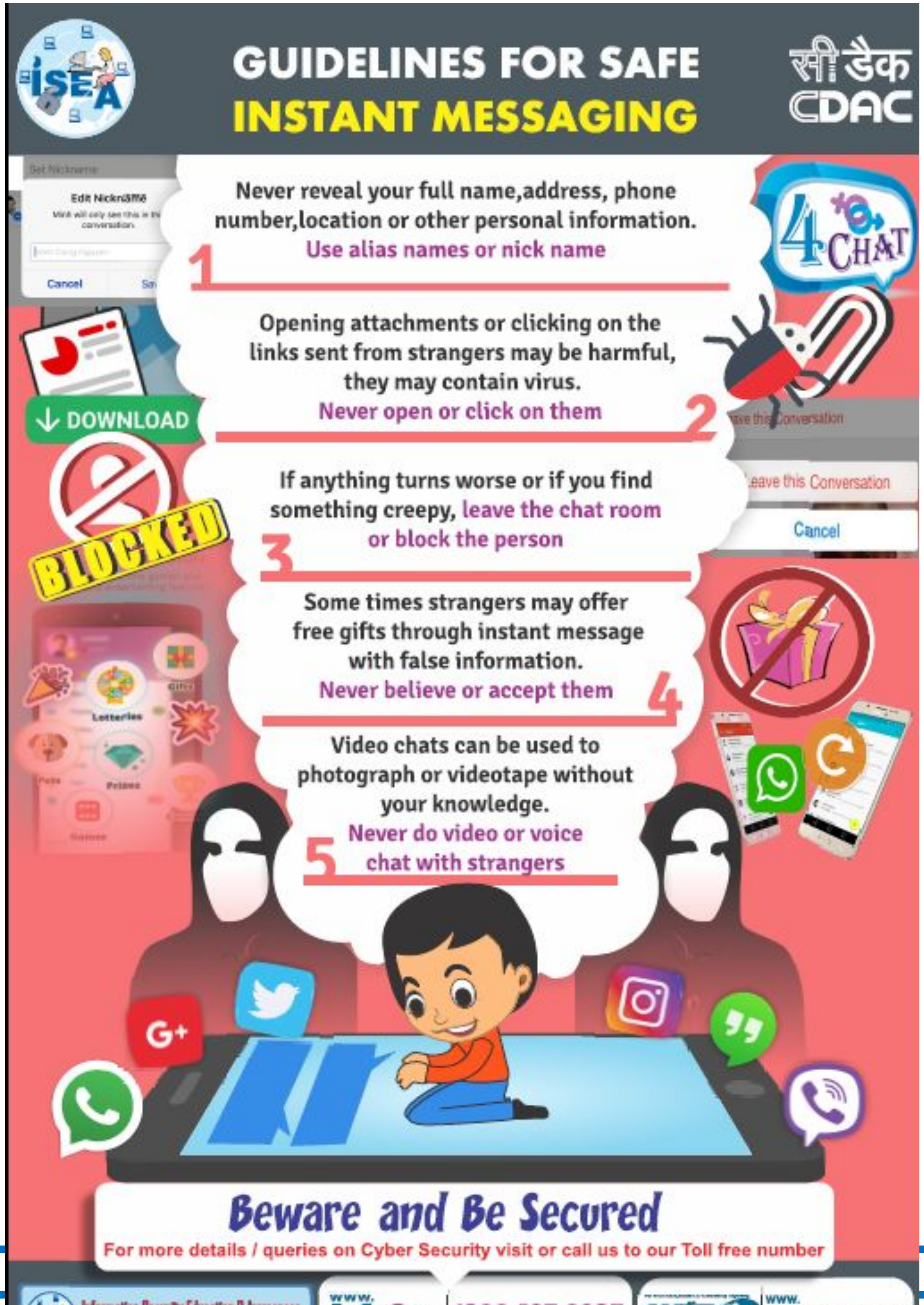
- Spam
- Scams
- Phishing
- Clickjacking
- Malicious applications and
- Many more

Reasons for SNS Risks

- Younger generations tend to be more trusting
- Adding people they don‟t know
- Talking to those people
- Arranging meetings with online social contacts
- Believing people are who they say they are on their SNS
- Revealing private information
- Believe there are little to no risks
- More trusting when someone is a "friend", even if they‟ve never met in person or have a very brief meeting

Tips to avoid risks by social networking

- Limit the information you put in the social networking sites.
- Don’t put personal information
- Most of the sites and services provide options for privacy settings
- Be careful if you want to meet social networking friends in person,
- Don’t ever click suspicious link while logged into social networking accounts.
- Always clean browser’s cookies and cache.
- Install a good and latest version of Anti-virus to keep your system free from malicious applications
- Don’t ever share your password and keep changing your password regularly.
- Don’t ever login to any site other than the legitimate sites
- Use Virtual Keyboard, wherever possible to enter your password for better security as these cannot be captured b key-loggers.



GUIDELINES FOR SAFE INSTANT MESSAGING

1 Never reveal your full name,address, phone number,location or other personal information. Use alias names or nick name

2 Opening attachments or clicking on the links sent from strangers may be harmful, they may contain virus. Never open or click on them

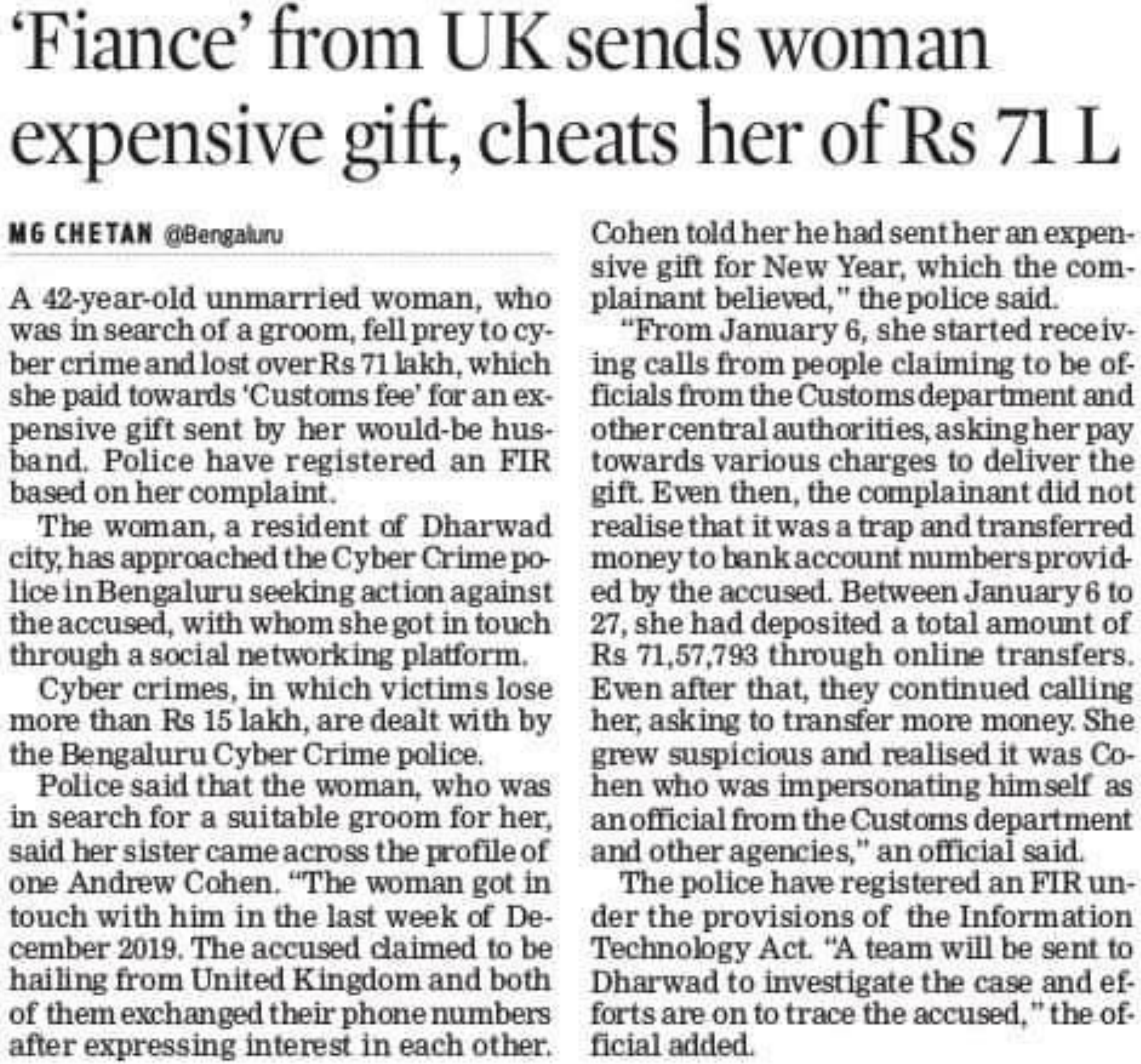
3 If anything turns worse or if you find something creepy, leave the chat room or block the person

4 Some times strangers may offer free gifts through instant message with false information. Never believe or accept them

5 Video chats can be used to photograph or videotape without your knowledge. Never do video or voice chat with strangers

Beware and Be Secured

For more details / queries on Cyber Security visit or call us to our Toll free number



‘Fiance’ from UK sends woman expensive gift, cheats her of Rs 71 L

MG CHETAN @Bengaluru

A 42-year-old unmarried woman, who was in search of a groom, fell prey to cyber crime and lost over Rs 71 lakh, which she paid towards ‘Customs fee’ for an expensive gift sent by her would-be husband. Police have registered an FIR based on her complaint.

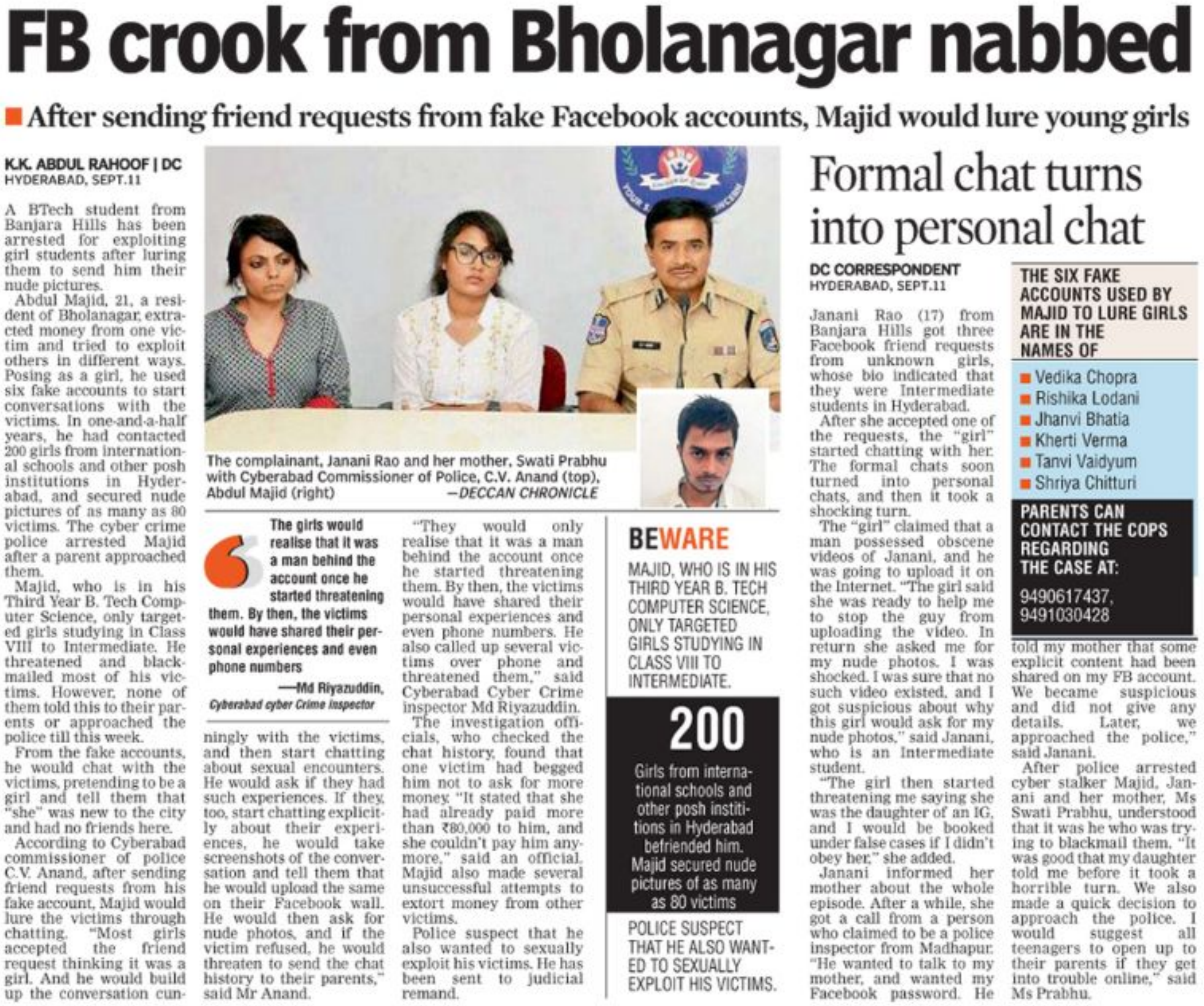
The woman, a resident of Dharwad city, has approached the Cyber Crime police in Bengaluru seeking action against the accused, with whom she got in touch through a social networking platform.

Cyber crimes, in which victims lose more than Rs 15 lakh, are dealt with by the Bengaluru Cyber Crime police.

Police said that the woman, who was in search for a suitable groom for her, said her sister came across the profile of one Andrew Cohen. “The woman got in touch with him in the last week of December 2019. The accused claimed to be hailing from United Kingdom and both of them exchanged their phone numbers after expressing interest in each other. Cohen told her he had sent her an expensive gift for New Year, which the complainant believed,” the police said.

“From January 6, she started receiving calls from people claiming to be officials from the Customs department and other central authorities, asking her pay towards various charges to deliver the gift. Even then, the complainant did not realise that it was a trap and transferred money to bank account numbers provided by the accused. Between January 6 to 27, she had deposited a total amount of Rs 71,57,793 through online transfers. Even after that, they continued calling her, asking to transfer more money. She grew suspicious and realised it was Cohen who was impersonating himself as an official from the Customs department and other agencies,” an official said.

The police have registered an FIR under the provisions of the Information Technology Act. “A team will be sent to Dharwad to investigate the case and efforts are on to trace the accused,” the official added.



FB crook from Bholanagar nabbed

After sending friend requests from fake Facebook accounts, Majid would lure young girls

K.K. ABDUL RAHOOF | DC
HYDERABAD, SEPT.11

A BTech student from Banjara Hills has been arrested for exploiting girl students after luring them to send him their nude pictures.

Abdul Majid, 21, a resident of Bholanagar, extracted money from one victim and tried to exploit others in different ways. Posing as a girl, he used six fake accounts to start conversations with the victims. In one-and-a-half years, he had contacted 200 girls from international schools and other posh institutions in Hyderabad, and secured nude pictures of as many as 80 victims. The cyber crime police arrested Majid after a parent approached them.

Majid, who is in his Third Year B. Tech Computer Science, only targeted girls studying in Class VIII to Intermediate. He threatened and blackmailed most of his victims. However, none of them told this to their parents or approached the police till this week.

From the fake accounts, he would chat with the victims, pretending to be a girl and tell them that "she" was new to the city and had no friends here.

According to Cyberabad commissioner of police C.V. Anand, after sending friend requests from his fake account, Majid would lure the victims through chatting. "Most girls accepted the friend request thinking it was a girl. And he would build up the conversation cunningly with the victims, and then start chatting about sexual encounters. He would ask if they had such experiences. If they, too, start chatting explicitly about their experiences, he would take screenshots of the conversation and tell them that he would upload the same on their Facebook wall. He would then ask for nude photos, and if the victim refused, he would threaten to send the chat history to their parents," said Mr Anand.

"They would only realise that it was a man behind the account once he started threatening them. By then, the victims would have shared their personal experiences and even phone numbers. He also called up several victims over phone and threatened them," said Cyberabad Cyber Crime inspector Md Riyazuddin.

The investigation officials, who checked the chat history, found that one victim had begged him not to ask for more money. "It stated that she had already paid more than ₹80,000 to him, and she couldn't pay him anymore," said an official. Majid also made several unsuccessful attempts to extort money from other victims.

Police suspect that he also wanted to sexually exploit his victims. He has been sent to judicial remand.

The complainant, Janani Rao and her mother, Swati Prabhu with Cyberabad Commissioner of Police, C.V. Anand (top), Abdul Majid (right) —DECCAN CHRONICLE

> The girls would realise that it was a man behind the account once he started threatening them. By then, the victims would have shared their personal experiences and even phone numbers
>
> —Md Riyazuddin, *Cyberabad cyber Crime inspector*

BEWARE

MAJID, WHO IS IN HIS THIRD YEAR B. TECH COMPUTER SCIENCE, ONLY TARGETED GIRLS STUDYING IN CLASS VIII TO INTERMEDIATE.

200

Girls from international schools and other posh institi-tions in Hyderabad befriended him. Majid secured nude pictures of as many as 80 victims

POLICE SUSPECT THAT HE ALSO WANTED TO SEXUALLY EXPLOIT HIS VICTIMS.

Formal chat turns into personal chat

DC CORRESPONDENT
HYDERABAD, SEPT.11

Janani Rao (17) from Banjara Hills got three Facebook friend requests from unknown girls, whose bio indicated that they were Intermediate students in Hyderabad.

After she accepted one of the requests, the "girl" started chatting with her. The formal chats soon turned into personal chats, and then it took a shocking turn.

The "girl" claimed that a man possessed obscene videos of Janani, and he was going to upload it on the Internet. "The girl said she was ready to help me to stop the guy from uploading the video. In return she asked me for my nude photos. I was shocked. I was sure that no such video existed, and I got suspicious about why this girl would ask for my nude photos," said Janani, who is an Intermediate student.

"The girl then started threatening me saying she was the daughter of an IG, and I would be booked under false cases if I didn't obey her," she added.

Janani informed her mother about the whole episode. After a while, she got a call from a person who claimed to be a police inspector from Madhapur. "He wanted to talk to my mother, and wanted my Facebook password. He told my mother that some explicit content had been shared on my FB account. We became suspicious and did not give any details. Later, we approached the police," said Janani.

After police arrested cyber stalker Majid, Janani and her mother, Ms Swati Prabhu, understood that it was he who was trying to blackmail them. "It was good that my daughter told me before it took a horrible turn. We also made a quick decision to approach the police. I would suggest all teenagers to open up to their parents if they get into trouble online," said Ms Prabhu.

THE SIX FAKE ACCOUNTS USED BY MAJID TO LURE GIRLS ARE IN THE NAMES OF

- Vedika Chopra
- Rishika Lodani
- Jhanvi Bhatia
- Kherti Verma
- Tanvi Vaidyum
- Shriya Chitturi

PARENTS CAN CONTACT THE COPS REGARDING THE CASE AT:

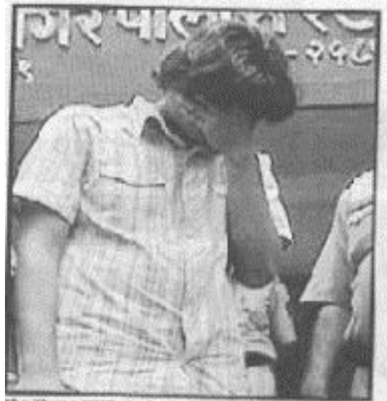
9490617437,
9491030428

Friend created fake profile and posted offensive messages

CITY MUMBAI MIRROR | FRIDAY, SEPTEMBER 29, 2006 4

Youth misuses classmate's profile, posts lewd scraps

He is caught following the girl's complaint



The Thane BMS student was arrested yesterday

NILESH NIKADE

A Bachelor of Management Studies (BMS) student of Thane was arrested on Thursday for creating a classmate's profile and uploading her picture with offensive messages on an online community site without her permission.

The cyber cell of the Thane police got into the act following a complaint by a girl that someone had created her profile on Orkut.com with her picture and posted lewd messages. Within 48 hours the culprit was nabbed.

Orkut.com is an online community that connects people through a network of friends. It is a popular site with collegians who register as members, create their profiles and upload their pictures. But it can be misused, as a Thane student found out to her utter disbelief.

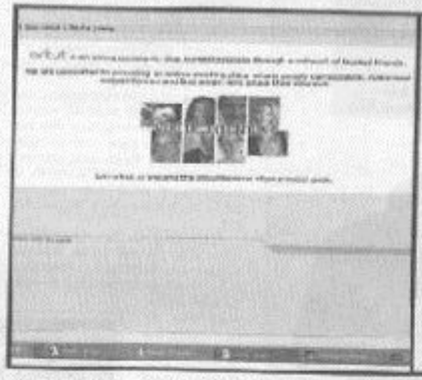
When Sushma Sharma (name changed on request) logged on to Orkut.com, she received a scrap (Orkut comment) saying 'Hi' from a profile that seemed her own. This made her wonder since she never wrote it in her own scrapbook. Out of curiosity she clicked on the profile, and to her utter dismay she was flooded with vulgar comments and cheap descriptions about her. The profile also had her photograph and cellphone number.

After that she started getting vulgar phone calls and her friends also informed her about offensive messages put up on her profile. A harassed Sushma and her parents complained to the Vartak Nagar police station, who forwarded the investigation to the Thane Cyber Cell (TCC)."

Police Inspector Shekhar Tore of TCC who investigated the matter said, "The orkut server is located in Sweden and therefore it was difficult for us to get information about the person who created the profile. We traced the fake yahoo email ID created on Sushma's name and then got information about its log-in details. The IP address details of this yahoo account led to Samer Castle apartment in Thane's Kolbad area and another cyber café nearby.

Abhishek, 19, a BMS student, first denied committing any such crime but soon confessed. "I don't understand what happened to me. I just did it," said Abhishek, who knew Sushama as her classmate in junior college.

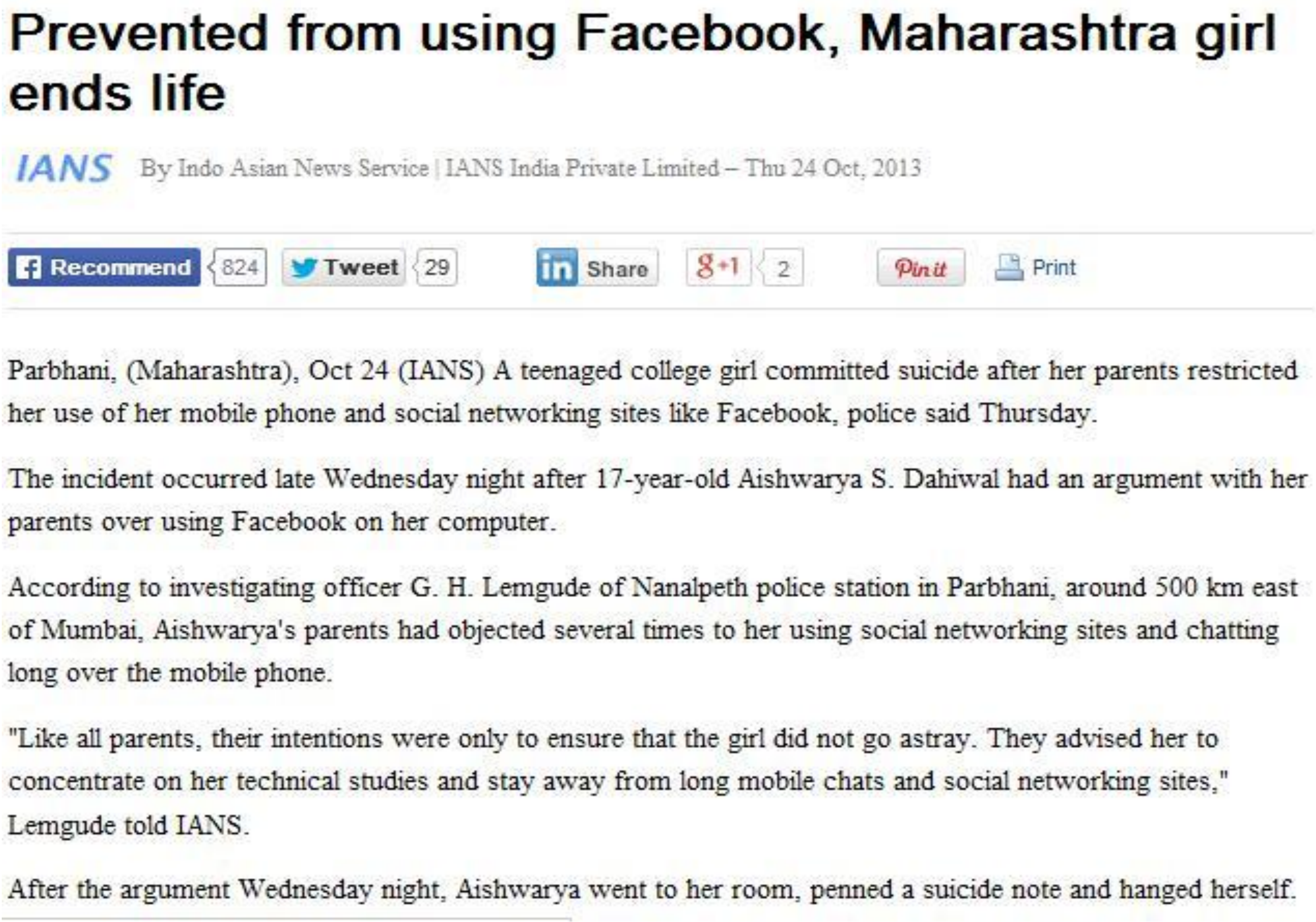
He has been booked under IPC 459 (publicising offensive message) and Section 67 of IT Act, 2000. He can be punished with up to five years in jail.



TIPS FOR ORKUT USERS

According to Police Sub Inspector Ravindra Chavan, "Orkut users should not put up their photographs on the site. They should not reveal personal information in their profile. Also no cellphone numbers or identity should be mentioned in the scrap book, as it is open to all."

Addicted to Facebook and ends her life



Prevented from using Facebook, Maharashtra girl ends life

IANS By Indo Asian News Service | IANS India Private Limited – Thu 24 Oct, 2013

Parbhani, (Maharashtra), Oct 24 (IANS) A teenaged college girl committed suicide after her parents restricted her use of her mobile phone and social networking sites like Facebook, police said Thursday.

The incident occurred late Wednesday night after 17-year-old Aishwarya S. Dahiwal had an argument with her parents over using Facebook on her computer.

According to investigating officer G. H. Lemgude of Nanalpeth police station in Parbhani, around 500 km east of Mumbai, Aishwarya's parents had objected several times to her using social networking sites and chatting long over the mobile phone.

"Like all parents, their intentions were only to ensure that the girl did not go astray. They advised her to concentrate on her technical studies and stay away from long mobile chats and social networking sites," Lemgude told IANS.

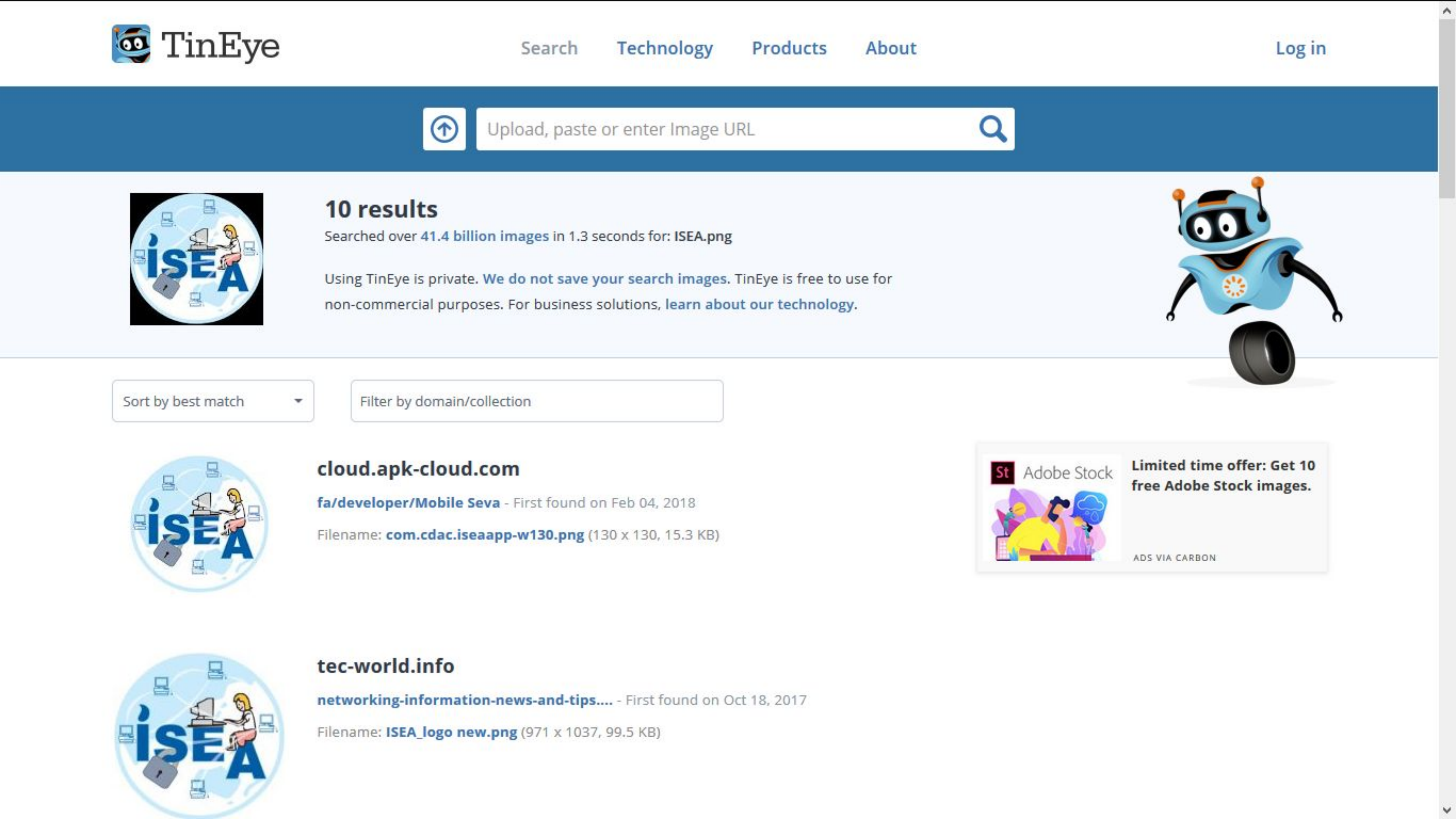
After the argument Wednesday night, Aishwarya went to her room, penned a suicide note and hanged herself.

TinEye

- TinEye is a reverse image search engine.

- Give it an image and it will tell you where the image appears on the web.

LINK: https://tineye.com/



10 results

Searched over 41.4 billion images in 1.3 seconds for: ISEA.png

Using TinEye is private. We do not save your search images. TinEye is free to use for non-commercial purposes. For business solutions, learn about our technology.

cloud.apk-cloud.com

fa/developer/Mobile Seva - First found on Feb 04, 2018

Filename: com.cdac.iseaapp-w130.png (130 x 130, 15.3 KB)

tec-world.info

networking-information-news-and-tips.... - First found on Oct 18, 2017

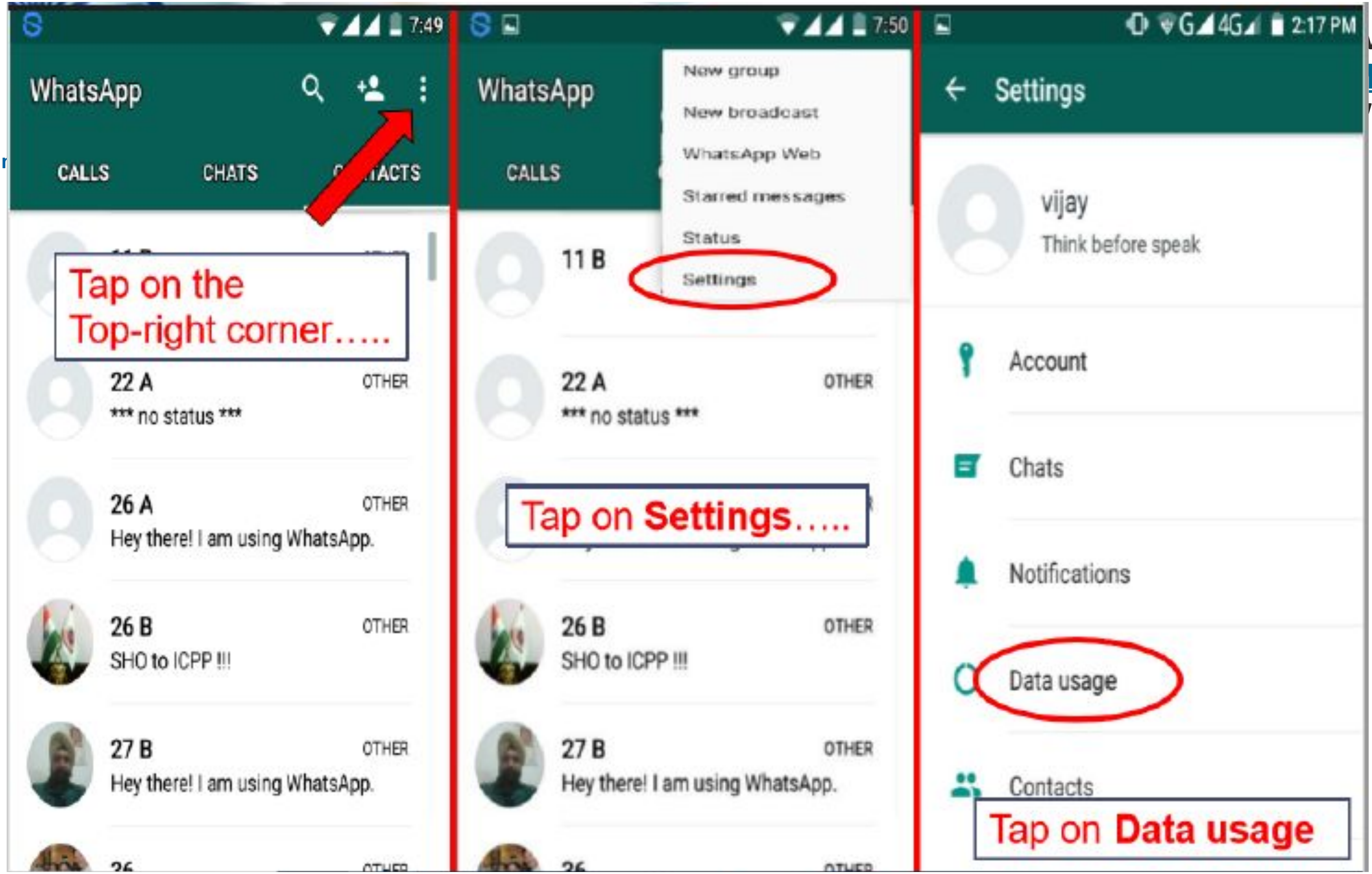
Filename: ISEA_logo new.png (971 x 1037, 99.5 KB)

WhatsApp Security

- WhatsApp is the favorite medium for hackers.

- Malware scripts embedded in photos & videos received on WhatsApp can access your media gallery, contacts, etc. and transmit them to remote servers.

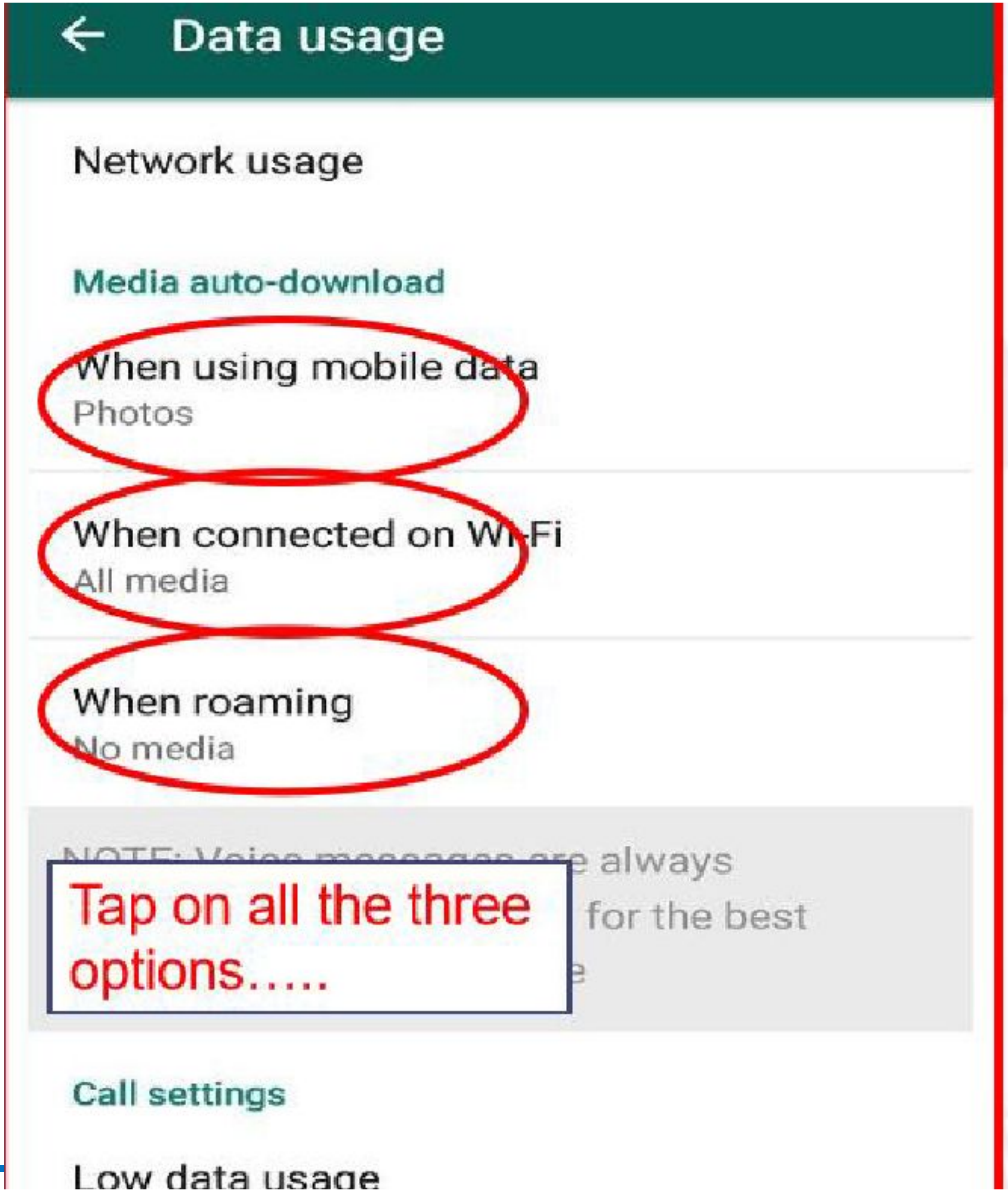
- There is a simple way to protect oneself from such an attack.



Tap on the Top-right corner.....

Tap on **Settings**.....

Tap on **Data usage**



Data usage

Network usage

Media auto-download

When using mobile data
Photos

When connected on Wi-Fi
All media

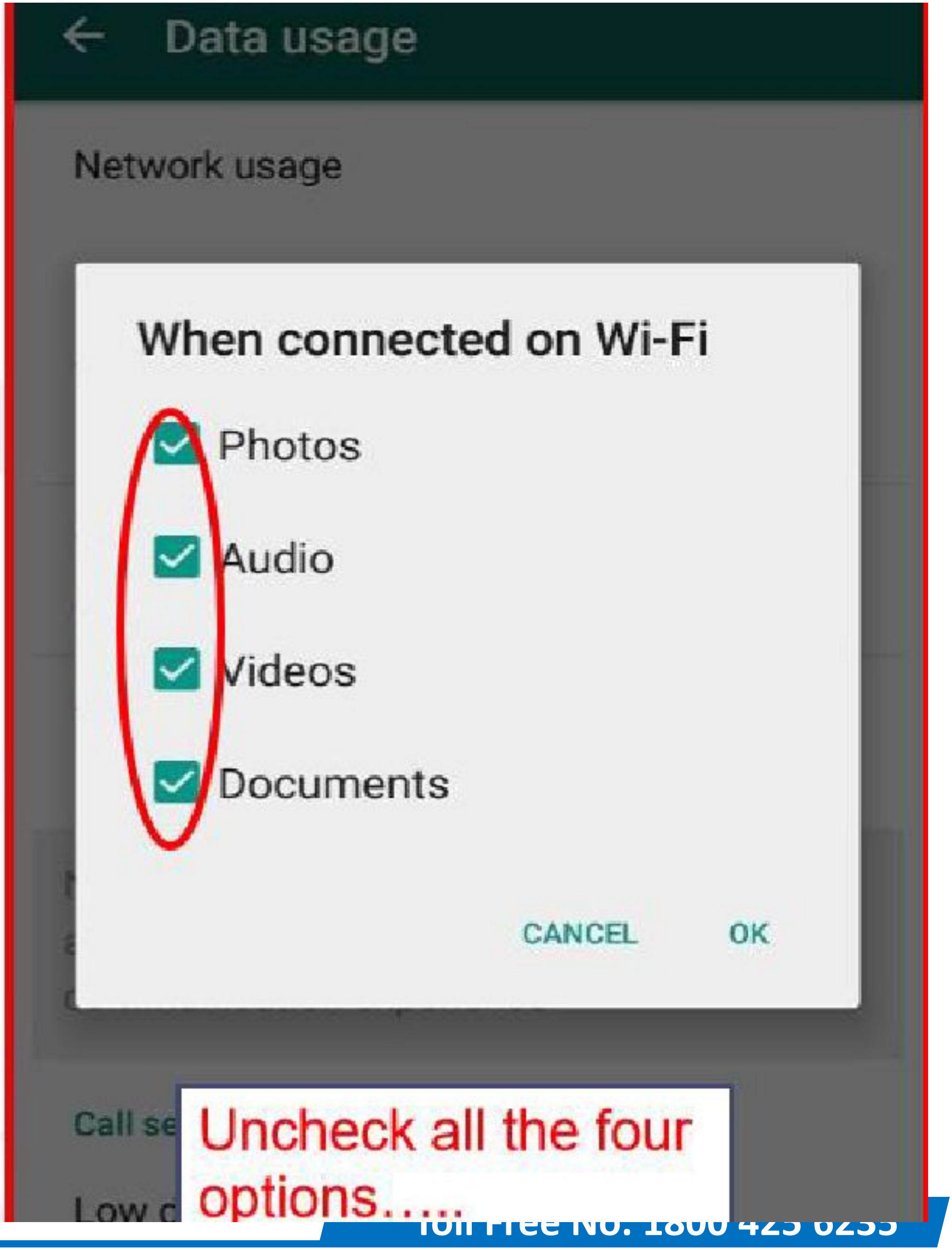
When roaming
No media

NOTE: Voice messages are always ... for the best ... e

Call settings

Low data usage

Tap on all the three options.....



Data usage

Network usage

When connected on Wi-Fi

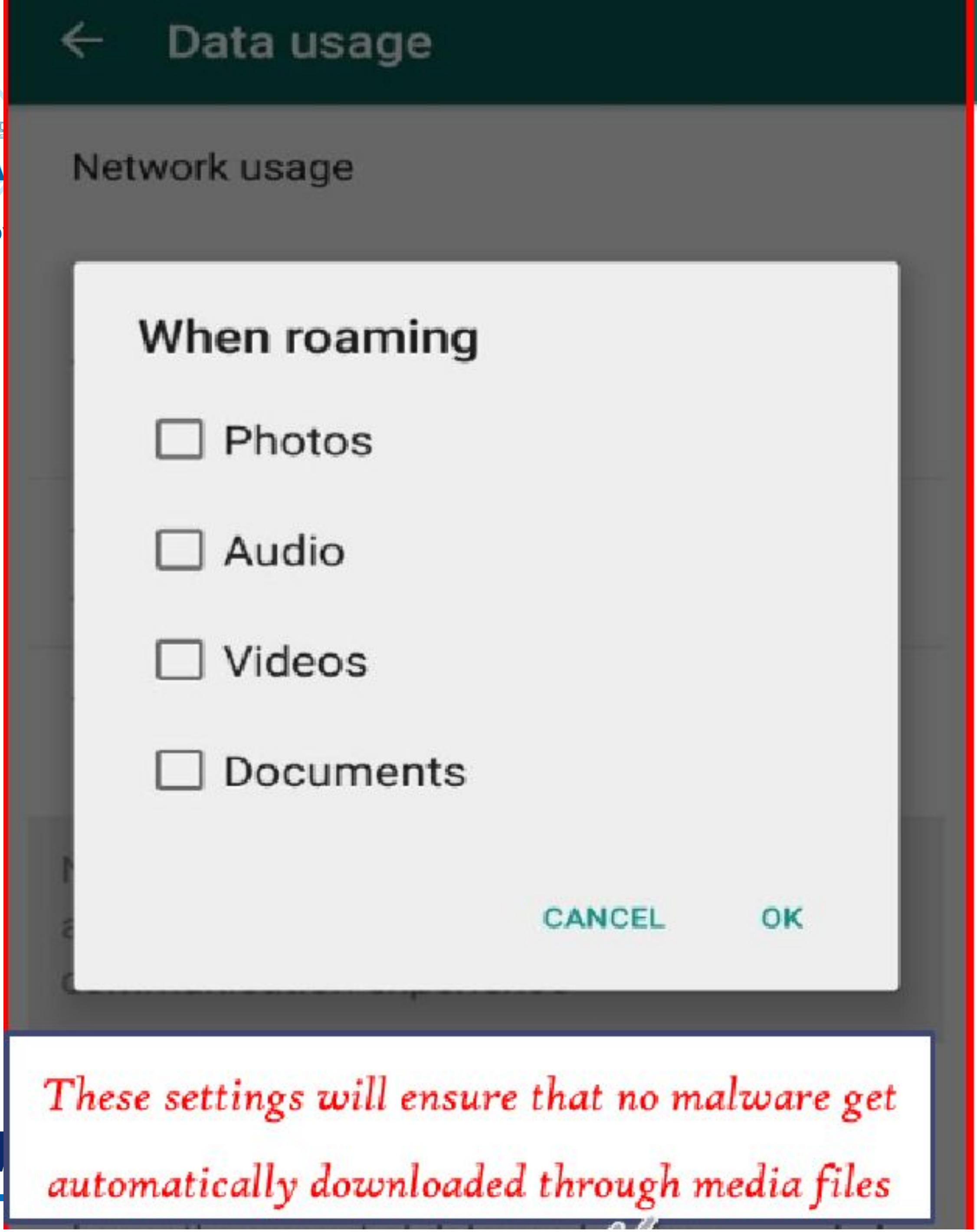
☑ Photos

☑ Audio

☑ Videos

☑ Documents

Uncheck all the four options.....



← Data usage

Network usage

When roaming

□ Photos

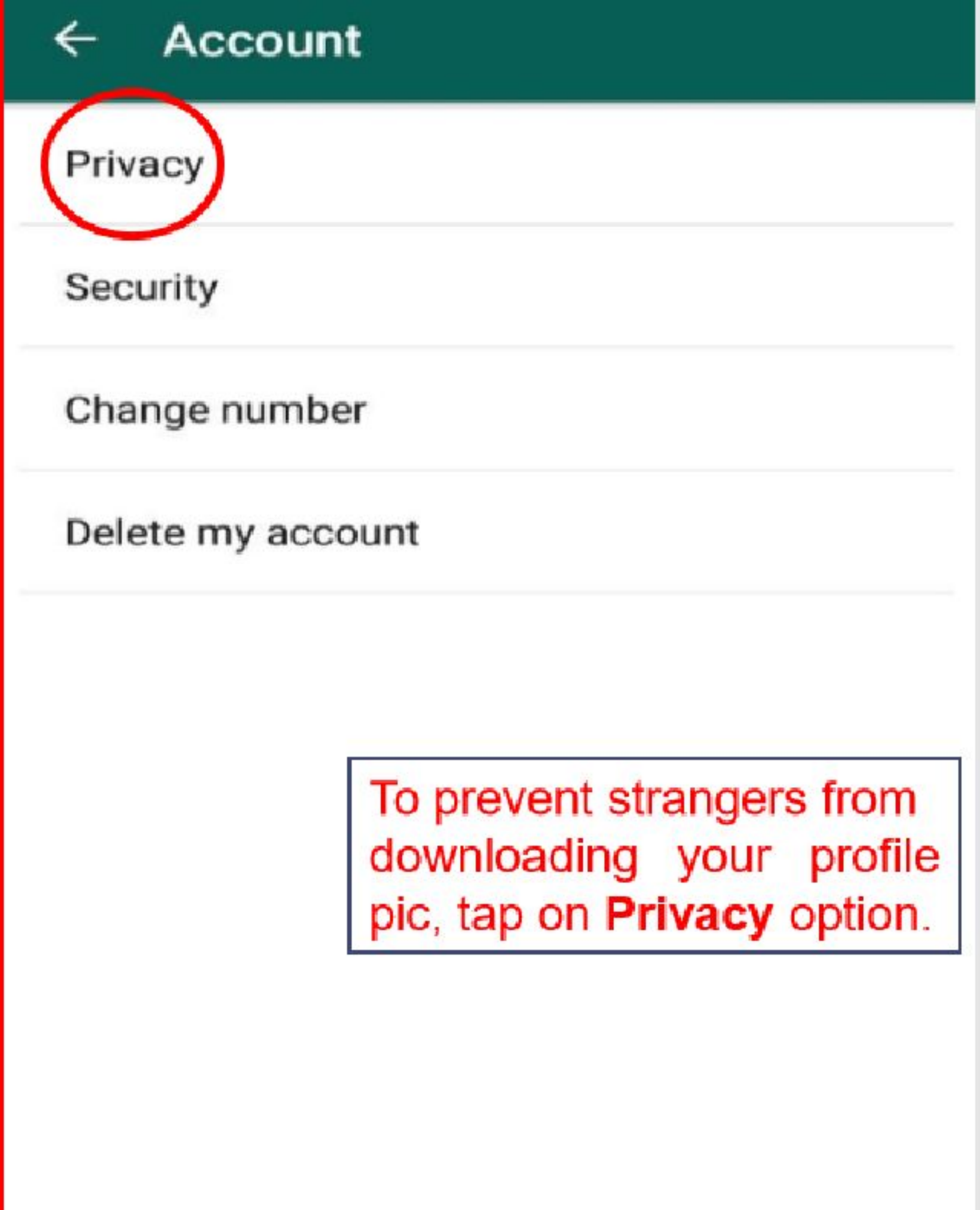
□ Audio

□ Videos

□ Documents

CANCEL OK

These settings will ensure that no malware get automatically downloaded through media files



← Account

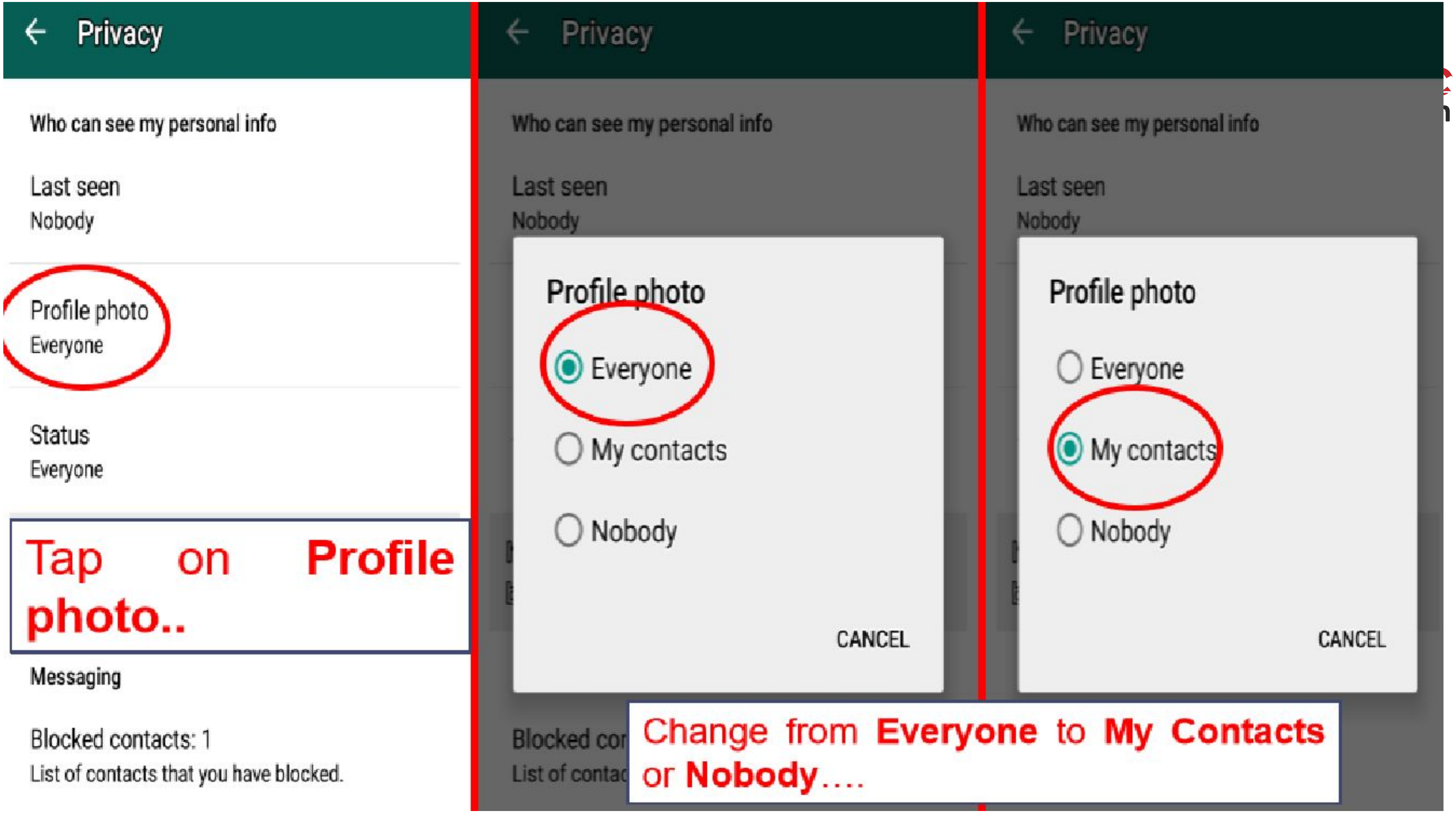
Privacy

Security

Change number

Delete my account

To prevent strangers from downloading your profile pic, tap on **Privacy** option.



Privacy

Who can see my personal info

Last seen
Nobody

Profile photo
Everyone

Status
Everyone

Messaging

Blocked contacts: 1
List of contacts that you have blocked.

Tap on **Profile photo..**

Privacy

Who can see my personal info

Last seen
Nobody

Profile photo

● Everyone
○ My contacts
○ Nobody

CANCEL

Blocked cor
List of contac

Privacy

Who can see my personal info

Last seen
Nobody

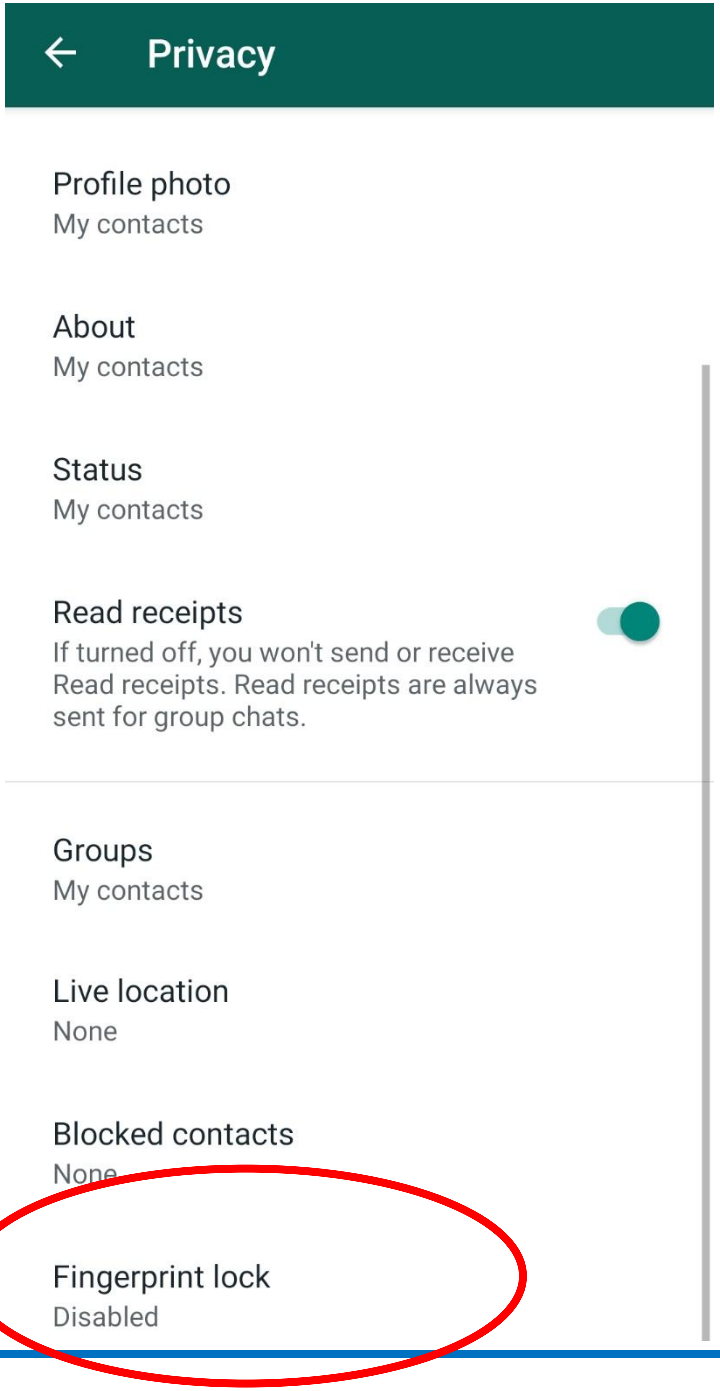
Profile photo

○ Everyone
● My contacts
○ Nobody

CANCEL

Change from **Everyone** to **My Contacts** or **Nobody**....

Setting password



Privacy

Profile photo
My contacts

About
My contacts

Status
My contacts

Read receipts
If turned off, you won't send or receive Read receipts. Read receipts are always sent for group chats.

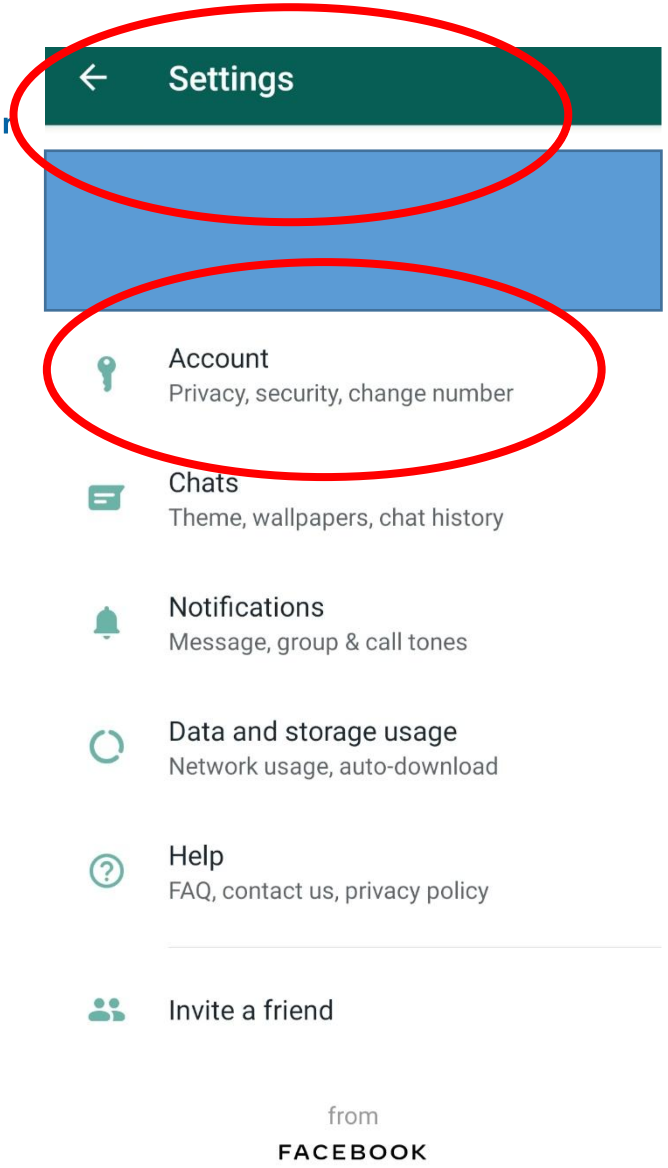
Groups
My contacts

Live location
None

Blocked contacts
None

Fingerprint lock
Disabled

Two Step Verification on WhatsApp should also be enabled



← Settings

Account
Privacy, security, change number

Chats
Theme, wallpapers, chat history

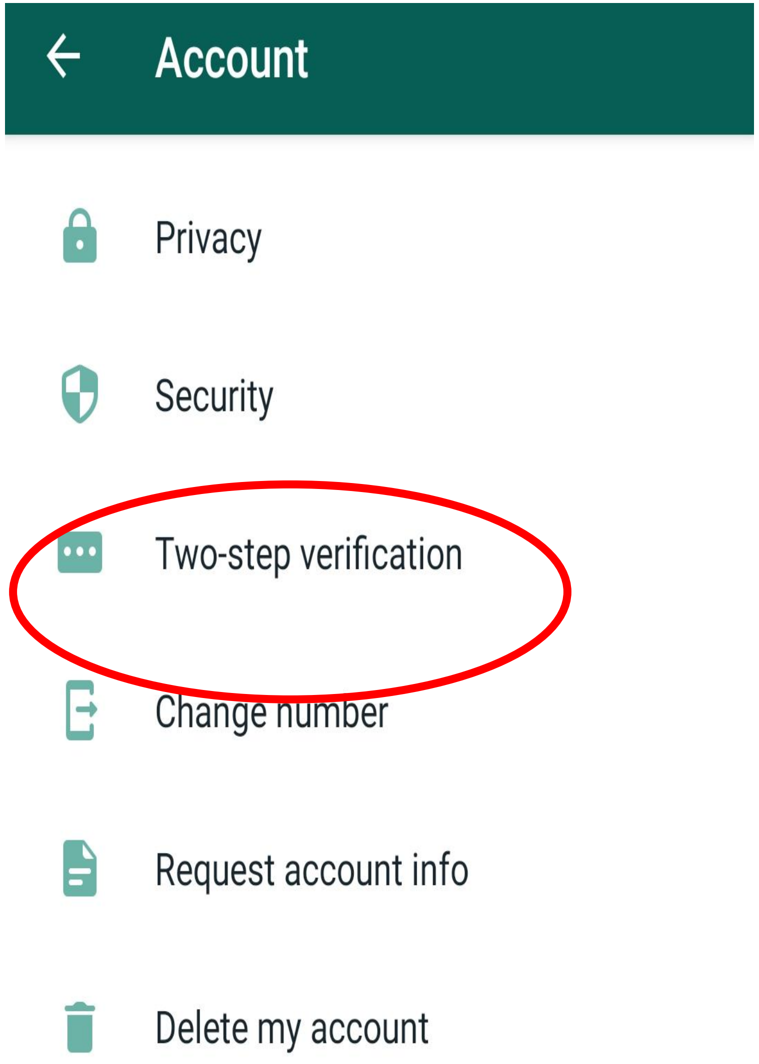
Notifications
Message, group & call tones

Data and storage usage
Network usage, auto-download

Help
FAQ, contact us, privacy policy

Invite a friend

from
FACEBOOK



← Account

Privacy

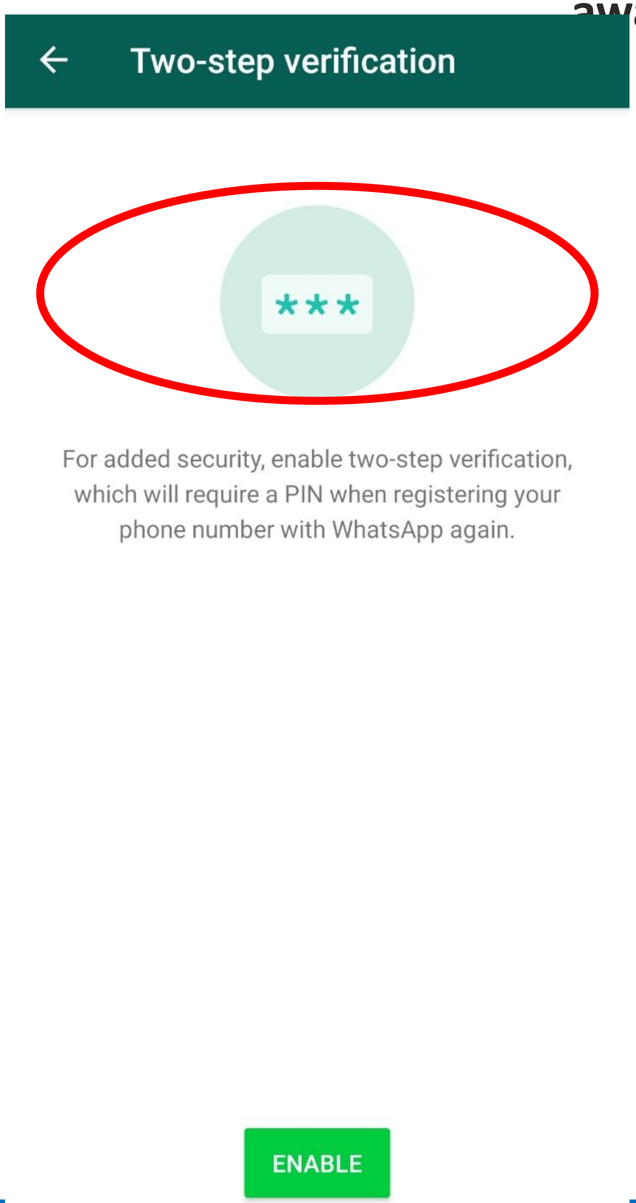
Security

Two-step verification

Change number

Request account info

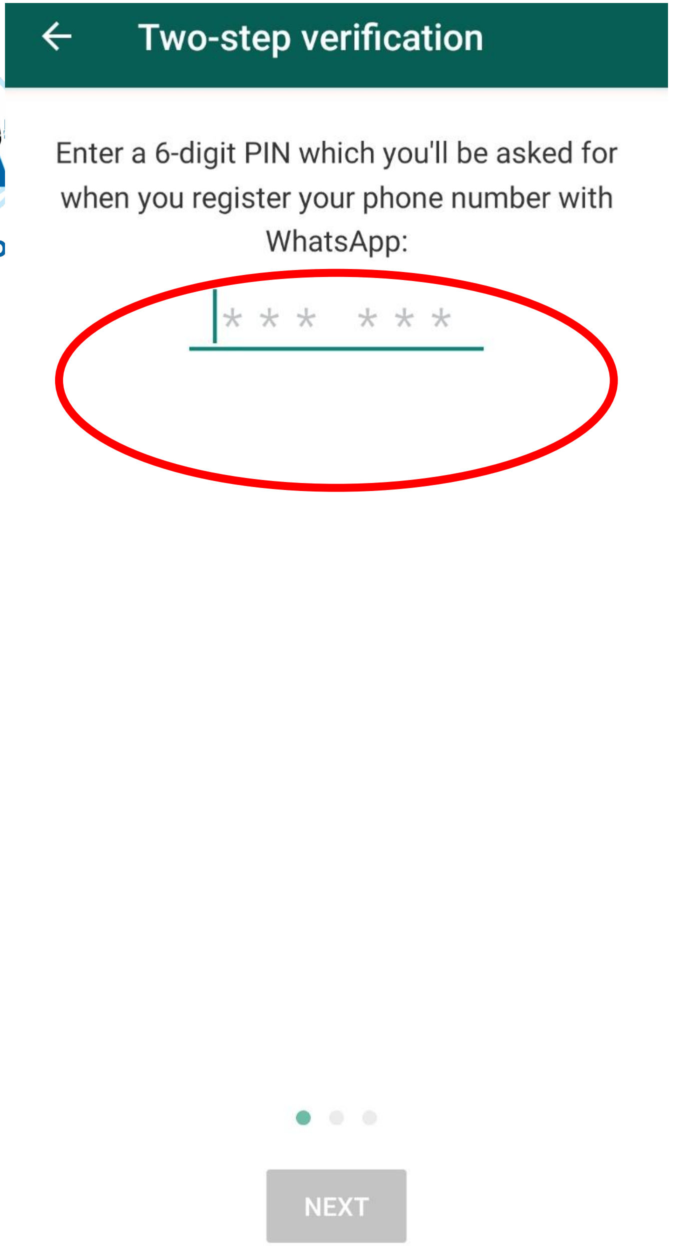
Delete my account



← Two-step verification

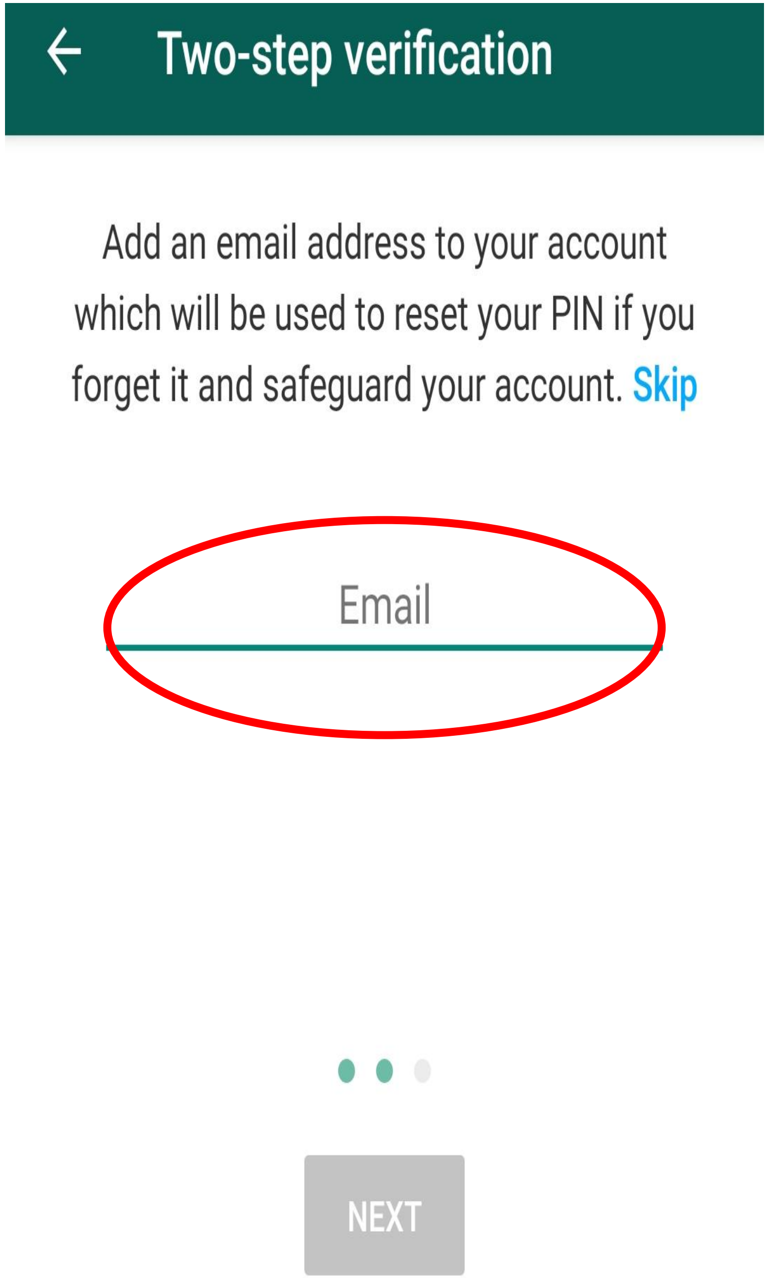
For added security, enable two-step verification, which will require a PIN when registering your phone number with WhatsApp again.

ENABLE



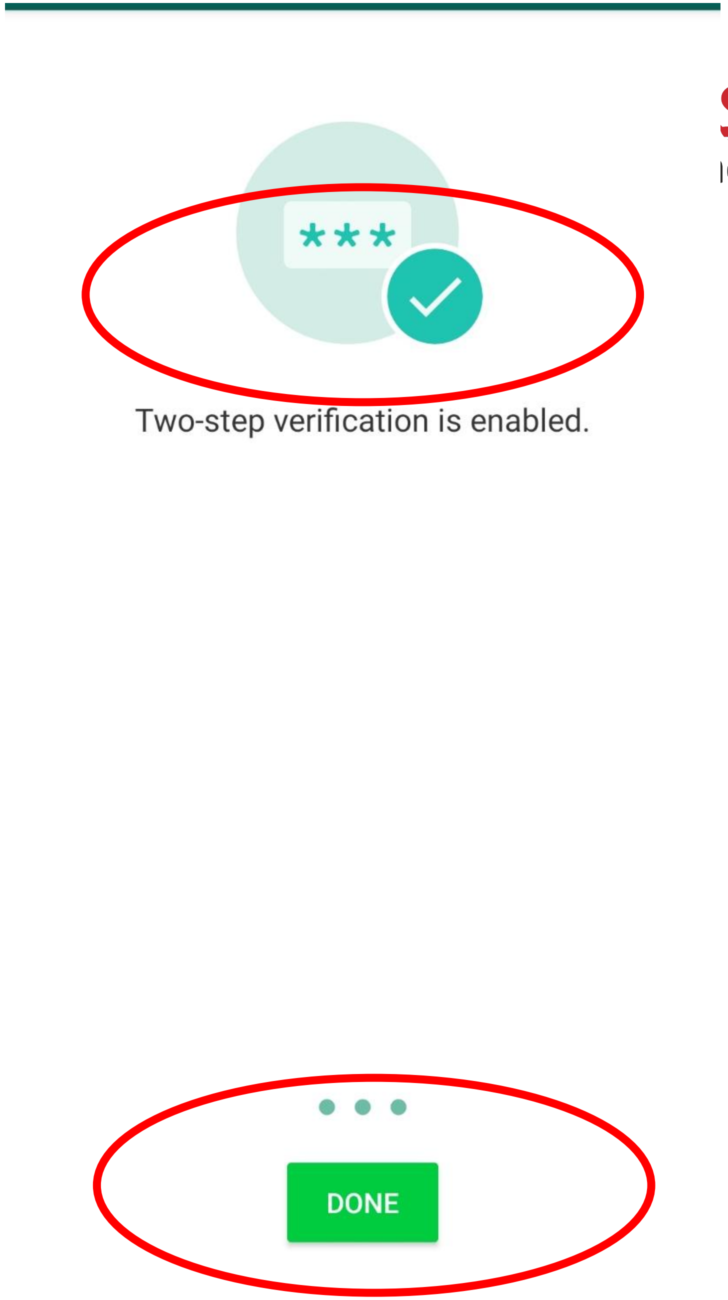
Two-step verification

Enter a 6-digit PIN which you'll be asked for when you register your phone number with WhatsApp:

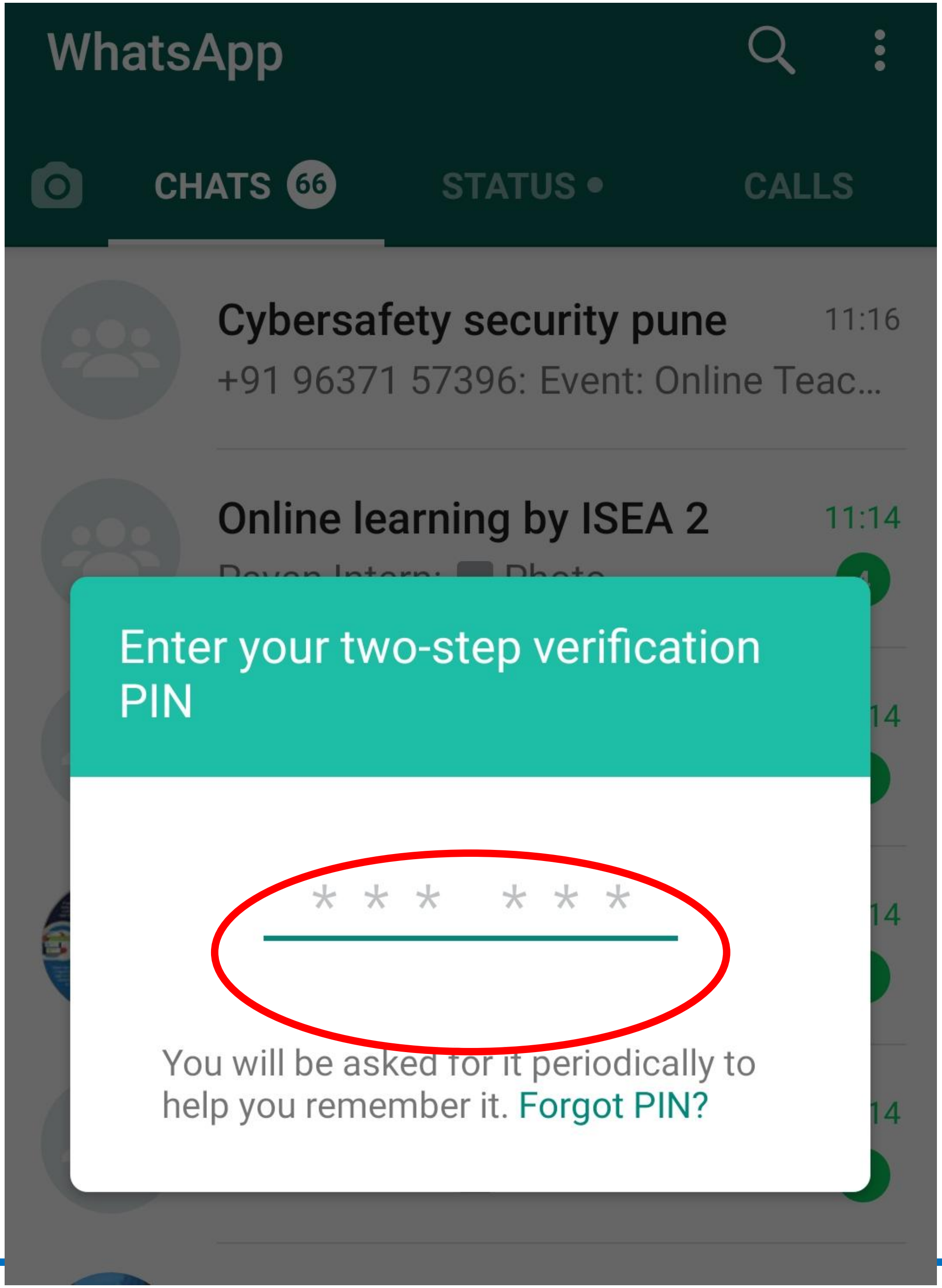


Two-step verification

Add an email address to your account which will be used to reset your PIN if you forget it and safeguard your account. Skip



Two-step verification is enabled.



Cybersafety security pune 11:16
+91 96371 57396: Event: Online Teac...

Online learning by ISEA 2 11:14
Pavan Intern: Photo

Enter your two-step verification PIN

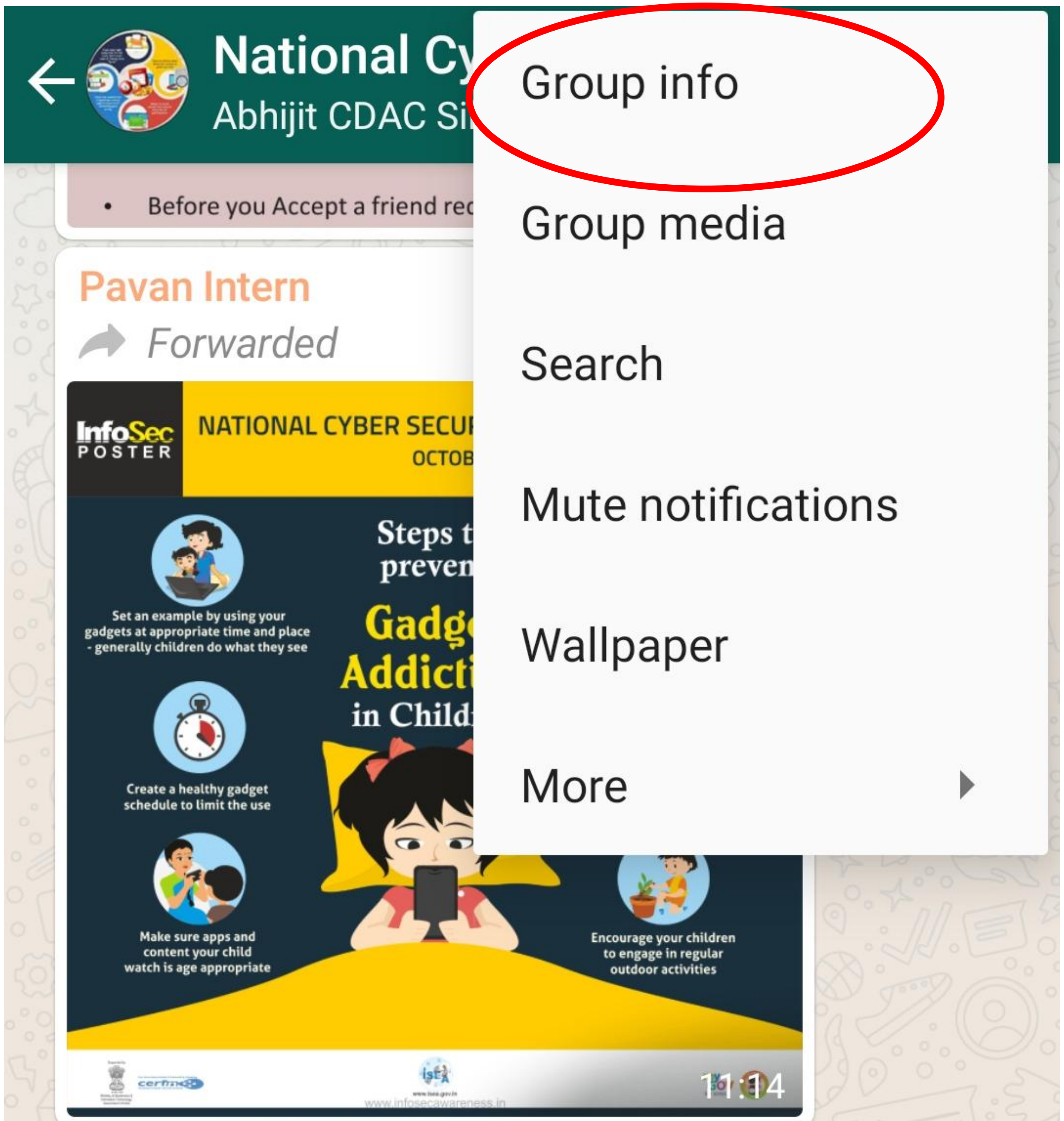
* * *   * * *

You will be asked for it periodically to help you remember it. Forgot PIN?

www.isea.gov.in

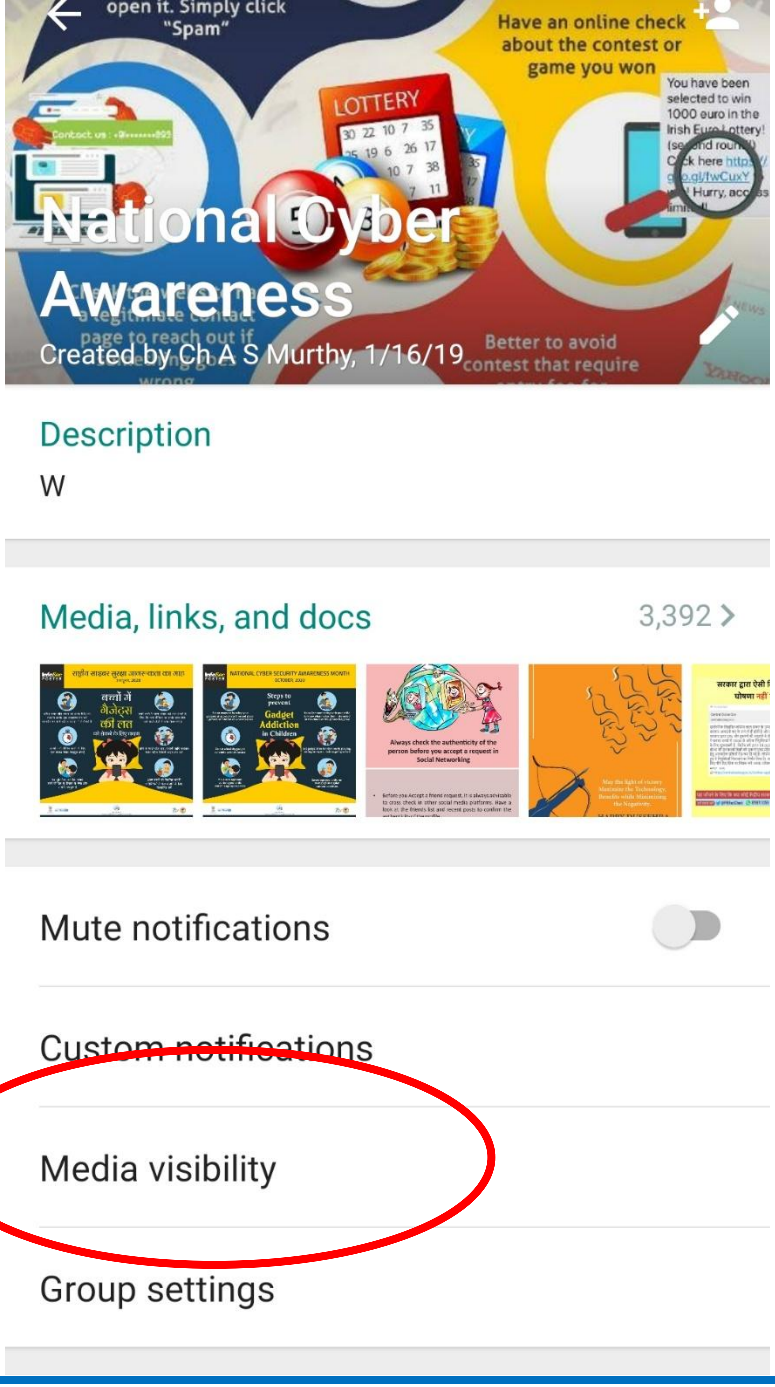
Media Download

- Click on 3 dots shown on the right top corner in the group.
- Click on the first option i.e. GROUP INFO


National Cy
Abhijit CDAC Si
Before you Accept a friend rec
Pavan Intern
Forwarded
InfoSec POSTER
NATIONAL CYBER SECUR
OCTOB
Steps t
preven
Gadg
Addicti
in Child
Set an example by using your gadgets at appropriate time and place - generally children do what they see
Create a healthy gadget schedule to limit the use
Make sure apps and content your child watch is age appropriate
Encourage your children to engage in regular outdoor activities
11:14
Group info
Group media
Search
Mute notifications
Wallpaper
More

www.isea.gov.in

- Three options shown below the group name i.e. mute notifications, custom notification, Media visiblity
- Click on the third option MEDIA VISIBILITY
- Click on "No" option. Now the media will not be saved in your phone. but it will display only in your group chats..
- Now that you know....act and inform your other group members in other groups.
- This feature is only available in Group, not in individuals..



National Cyber Awareness

Created by Ch A S Murthy, 1/16/19

Description

W

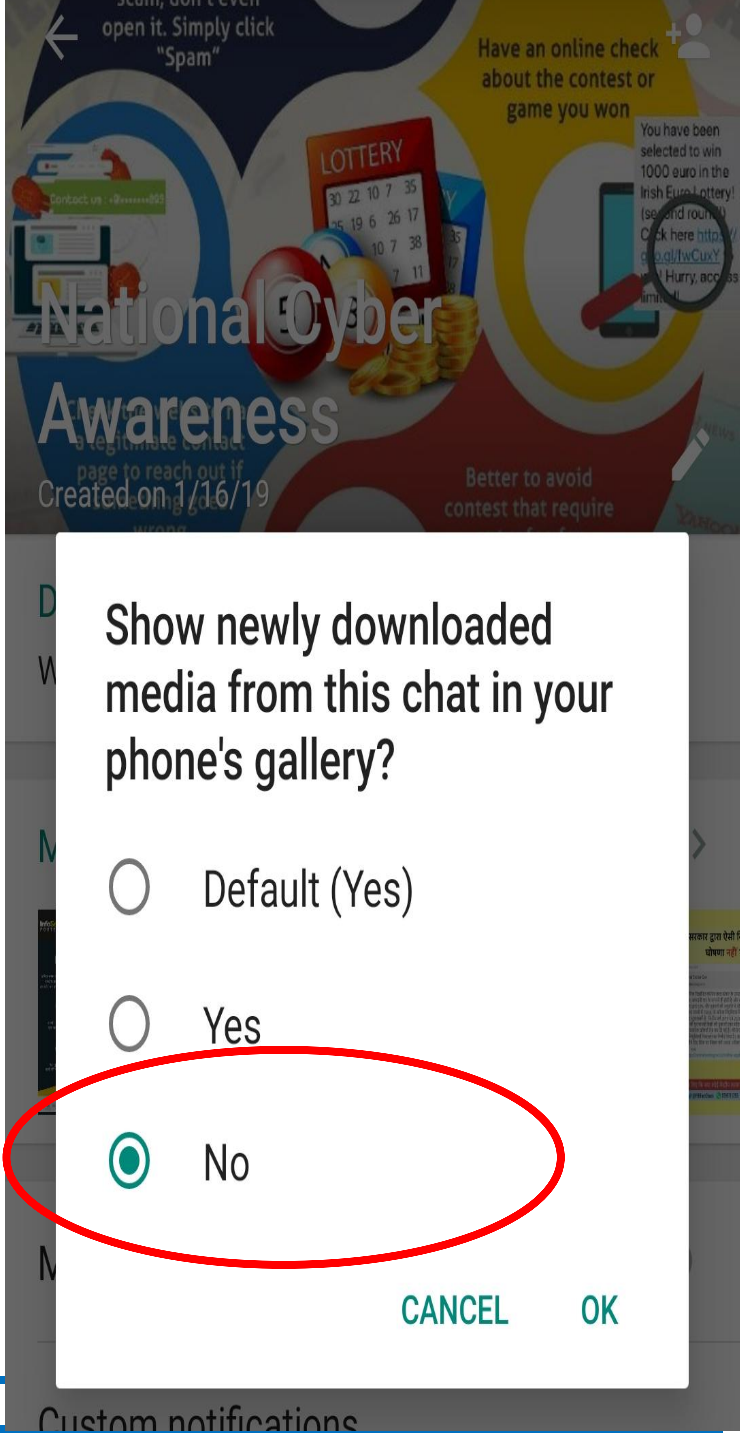
Media, links, and docs 3,392 >

Mute notifications

Custom notifications

Media visibility

Group settings



National Cyber Awareness

Created on 1/16/19

Show newly downloaded media from this chat in your phone's gallery?

○ Default (Yes)

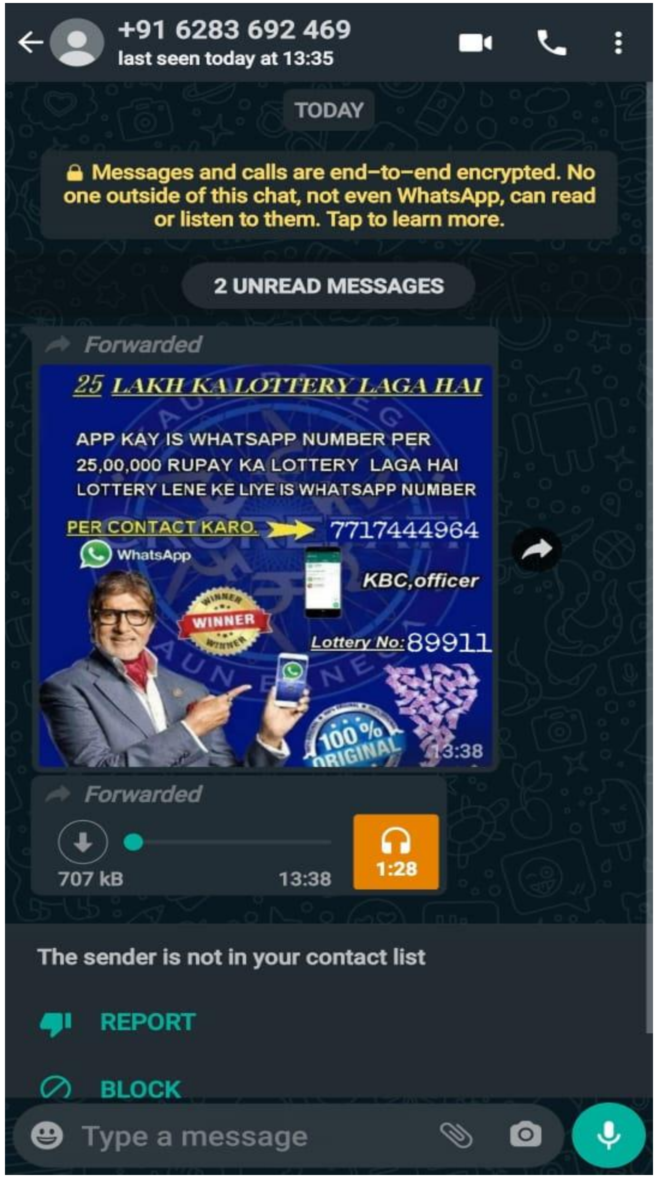
○ Yes

● No

CANCEL OK

Custom notifications

WhatsApp Fraud



+91 6283 692 469
last seen today at 13:35

TODAY

🔒 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

2 UNREAD MESSAGES

Forwarded

25 LAKH KA LOTTERY LAGA HAI

APP KAY IS WHATSAPP NUMBER PER
25,00,000 RUPAY KA LOTTERY LAGA HAI
LOTTERY LENE KE LIYE IS WHATSAPP NUMBER
PER CONTACT KARO. → 7717444964

WhatsApp

KBC,officer

WINNER

Lottery No: 89911

100 % ORIGINAL

13:38

Forwarded

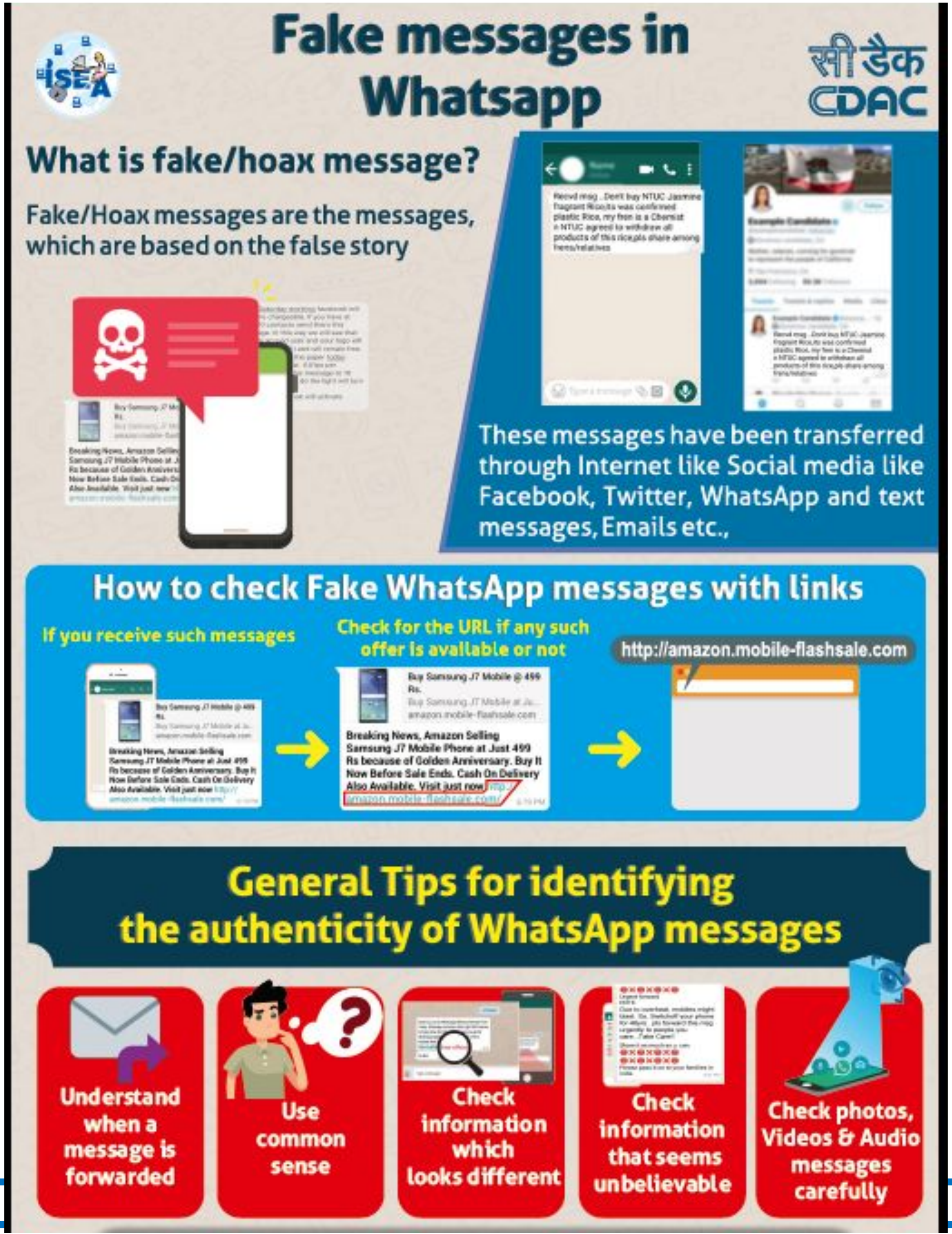
707 kB 13:38 1:28

The sender is not in your contact list

REPORT

BLOCK

Type a message



Fake messages in Whatsapp

सी डैक CDAC

What is fake/hoax message?

Fake/Hoax messages are the messages, which are based on the false story

Recvd msg ..Don't buy NTUC Jasmine fragrant Rice,its was confirmed plastic Rice, my fren is a Chemist n NTUC agreed to withdraw all products of this rice,pls share among frens/relatives

These messages have been transferred through Internet like Social media like Facebook, Twitter, WhatsApp and text messages, Emails etc.,

How to check Fake WhatsApp messages with links

If you receive such messages

Check for the URL if any such offer is available or not

Buy Samsung J7 Mobile @ 499 Rs.

amazon.mobile-flashsale.com

Breaking News, Amazon Selling Samsung J7 Mobile Phone at Just 499 Rs because of Golden Anniversary. Buy It Now Before Sale Ends. Cash On Delivery Also Available. Visit just now http://amazon.mobile-flashsale.com/

http://amazon.mobile-flashsale.com

General Tips for identifying the authenticity of WhatsApp messages

- Understand when a message is forwarded
- Use common sense
- Check information which looks different
- Check information that seems unbelievable
- Check photos, Videos & Audio messages carefully

www.isea.gov.in

www.InfoSecawareness.in

ISEA
सी डैक
CDAC
hi
will talk once I get free
FAKE
Listen to me...!!!!
No.. you... Listen to me...!!!!
Document
Payment
Gallery
Audio
Location
Contact
Report spam and block
Not Spam. Add to contacts

WHATSAPP

BEHAVIORAL TIPS FOR ALL

1 Always be courteous in replying after reading messages

2 Show patience for receiving photos after the party/vacation

3 Avoid making fuss over others online behaviour

4 Make appropriate use of emojis

5 Be clear in both words and approach

6 Avoid spreading fake news

7 Avoid getting into multiple topics at one go

8 Do not argue over silly matters

9 Never begin a topic that would hurt religious or cultural sentiments

10 Don't spam with unnecessary chains and forward messages

11 Control what you see and with whom you interact

12 Control what you share

For more details / queries on Cyber Security visit or call us to our Toll free number

Toll Free No. 1800 425 6235

www.isea.gov.in

www.
InfoSec
awareness.in

Follow us
www.infosecawareness.in

https://www.facebook.com/infosecawareness

https://www.youtube.com/channel/UCWPBKQryyVvydUy4rYsbBfA

https://plus.google.com/u/0/106937869860139709031/posts

Email id: isea@cdac.in

TOLL FREE No. 1800 425 6235