इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY

सत्यमेव जयते

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

Digital India
Power To Empower

एन आई सी
National
Informatics
Centre

सी-डैक
CDAC

www.isea.gov.in

Information Security Education and Awareness (ISEA) Project

staysafeonline.in

Celebrating “ Safer Internet Day”

Together for a Better Internet

- Safer Internet Day is observed worldwide on the second Tuesday of every February to
  - Raise awareness
  - Promote the safe and responsible use of the internet
  - Particularly among children, women, and young people

- Ministry of Electronics and Information Technology (MeitY) is celebrating a nationwide awareness campaign on 11th February, 2025 under the aegis ISEA Project in collaboration with NIC.

- Conduct Awareness Workshops at the district / block / gram panchayat levels in districts with support from DIOs/ ADIOs
- Educate local citizens and officials on safe internet practices
- The workshops will focus on
  - Promoting cyber hygiene,
  - Raising awareness about key cyber threats,
  - Equipping participants with effective mitigation techniques.

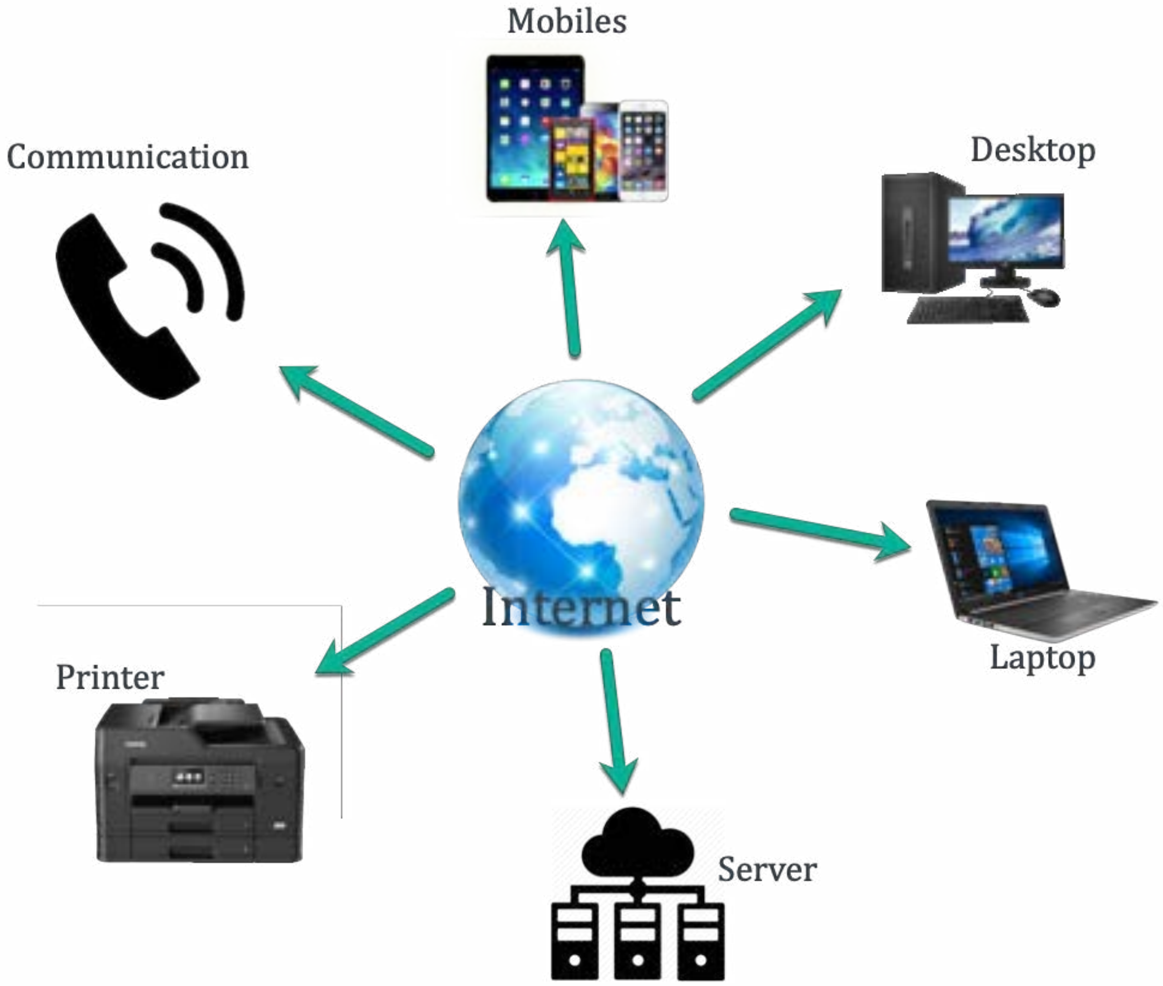
Date & Time: 11th February, 2025 (10.30 AM – 12:00 PM)

Outline of the presentation:

- Brief Introduction
- About the Internet
- Use of Internet in our Day-to-Day life
- Safe Use of Internet (Internet Safety)
- Common Cyber Threats
- Cyber Hygiene Practices
- Mechanism to report cyber-crimes (1930)
- Awareness Resources for Staying Safe Online (www.staysafeonline.in)

What is Internet

- Internet is basically network of networks that connects billions of devices worldwide
- It's kind of library, where you can find almost anything you're looking for



Places where Internet is used

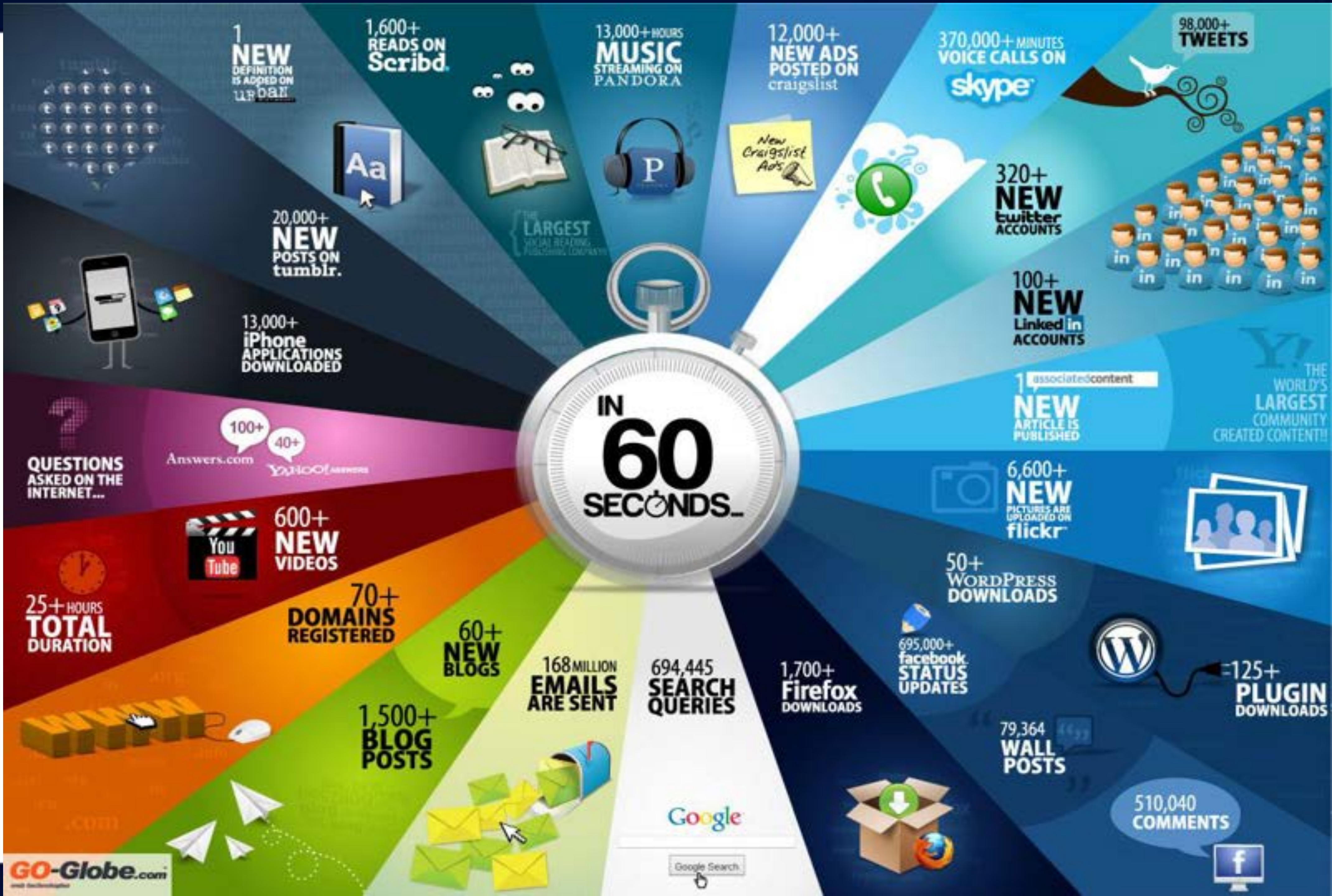
- Home
- School
- Office
- Malls
- Driving
- Banks

In today's world, we depend on Internet at home, in officers for doing several activities

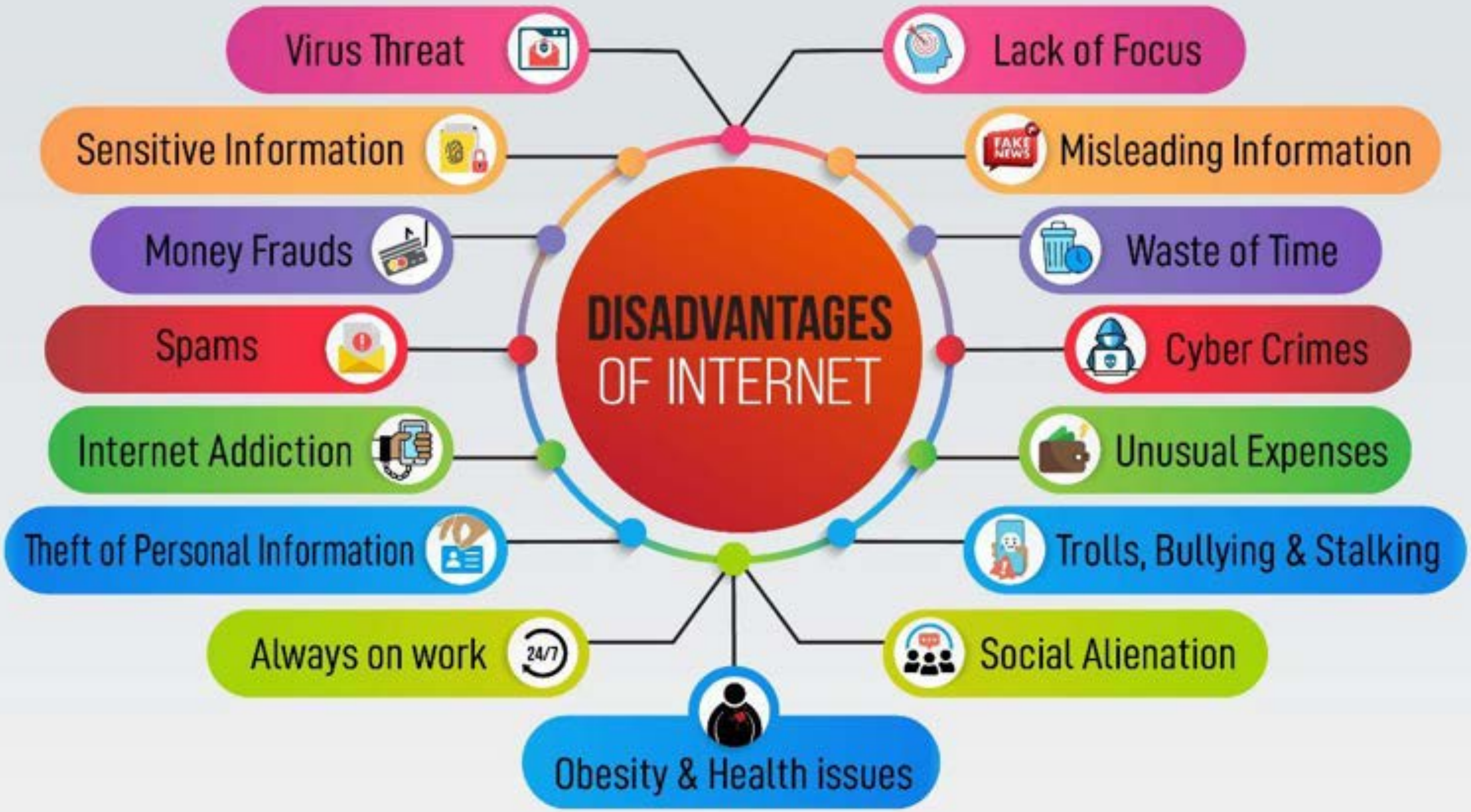
Use of Internet in our Day-to-Day life

Social Networking
Job Search
E-Commerce
Shopping
Payments
Browsing
Communication
Travel

Data Never Sleep



DISADVANTAGES OF INTERNET



DISADVANTAGES OF INTERNET

- Virus Threat
- Sensitive Information
- Money Frauds
- Spams
- Internet Addiction
- Theft of Personal Information
- Always on work
- Lack of Focus
- Misleading Information
- Waste of Time
- Cyber Crimes
- Unusual Expenses
- Trolls, Bullying & Stalking
- Social Alienation
- Obesity & Health issues

feonline.in

Common Cyber Threats

Phishing

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Common Phishing keywords:

- A “required action” as a part of a system or quota upgrade
- A “required action” to prevent email account closure
- A “trusted” vendor, such as a fake Dropbox or Google alert
- A “legitimate” banking alert

staysafeonline.in

Examples of Phishing Websites

- www.gmai1.com
- www.icici6ank.com
- www.bank0findia.com
- www.yah00.com

Phishing Videos

www.youtube.com/embed/IwzUsN9u8xk?si=YBUUXtHov2WxEl3t

www.youtube.com/embed/j_J4AL8_hHk?si=ERjVtgiE2o_XLy2i

www.youtube.com/embed/8c7XlqHj3-o?si=-ceuQ0bNQvhepa4L

Security tips

Beware of emails/links providing special offers like rewards, winning prize, cashback offers etc.,

Do not click on unknown/direct links, that requests for critical personal data

Always install antivirus software on devices for protection

Never share personal details or financial information like login credentials/ passwords/credit or debit card details/ CVV/OTP

Only visit authorized/ legitimate company/organization website for valid information

Never download unauthorized apps or software as they can infect devices

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

Vishing

Vishing - Phone calls made by fraudsters to steal your personal information and sensitive information

- they communicate

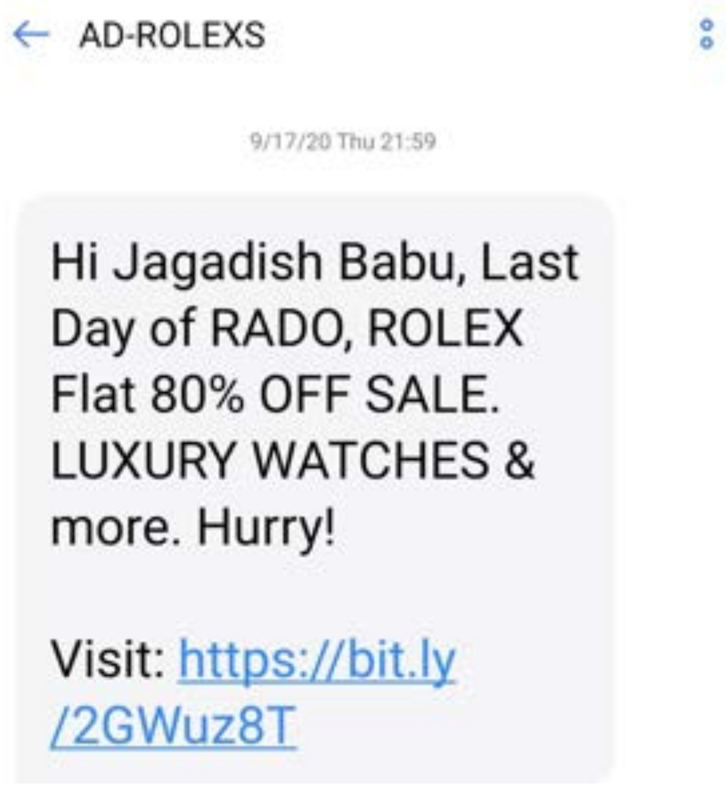
- as bank officer
- referring your shopping

OR

you may land up callin phishing number

through search engines

Smishing

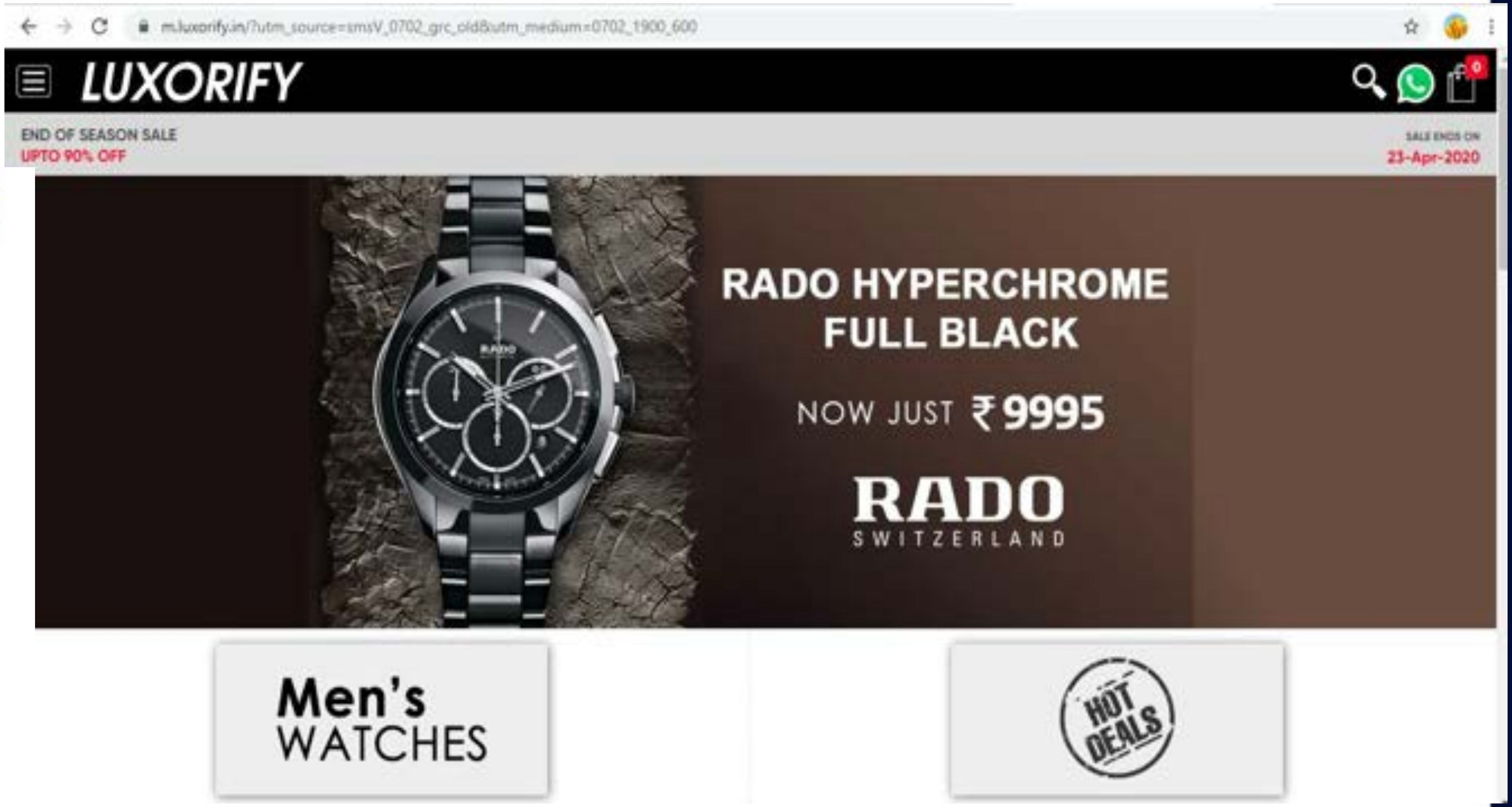


AD-ROLEXS

9/17/20 Thu 21:59

Hi Jagadish Babu, Last Day of RADO, ROLEX Flat 80% OFF SALE. LUXURY WATCHES & more. Hurry!

Visit: https://bit.ly/2GWuz8T



m.luxorify.in/?utm_source=smsV_0702_grc_old&utm_medium=0702_1900_600

Phishing, Vishing and Smishing Video

www.youtube.com/embed/r2srMQYMPrU?si=1LHJwCrh5WZuM-nu

Identity Theft

- Identity theft involves a range of tactics used by cybercriminals to illicitly obtain personal information for fraudulent purposes.
  - Financial fraud
  - Opening unauthorized accounts
  - Making purchases
  - Committing other crimes
  - Emotional distress for victims

Identity Theft Video

www.youtube.com/embed/w2XHNtr55M8?si=UvAx4PVdaZi3VAaL

Financial Fraud

- Financial fraud refers to the act of committing fraudulent activities or deception to obtain money, assets, or other property owned or held by a bank, financial institution, or its customers.

- It can involve a wide range of illegal and dishonest schemes and activities intended to defraud a bank or manipulate its systems for financial gain.

Financial Fraud

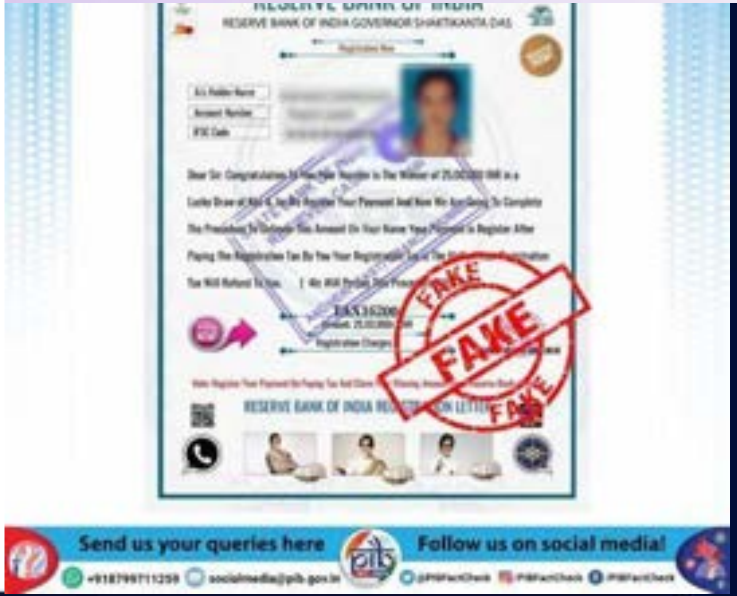
INDICATORS

- Unauthorized transactions or charges
- Notifications of changes to account information you didn’t make
- Sudden changes in credit scores
- Phishing attempts linked to financial institutions

Lottery Scams

Lottery scams prey on excitement, tricking victims into believing they've won a huge prize—without ever entering.

- Fraudsters send fake emails, messages
- Calls claiming you must pay taxes or fees to claim your winnings
- They pressure you to act fast, demanding personal and financial details
- The truth? Real lotteries never ask for upfront payments
- Ignore unsolicited lottery notifications, verify with official sources, and never share sensitive information.


RESERVE BANK OF INDIA GOVERNOR SHAKTIKANTA DAS
FAKE
FAKE
FAKE
RESERVE BANK OF INDIA REGISTRATION LETTER
Send us your queries here
Follow us on social media!
+918799711259
socialmedia@pib.gov.in

Lottery Scam Videos

www.youtube.com/embed/5bXr5KawZDU?si=pYIoFfnqZodzFu7U

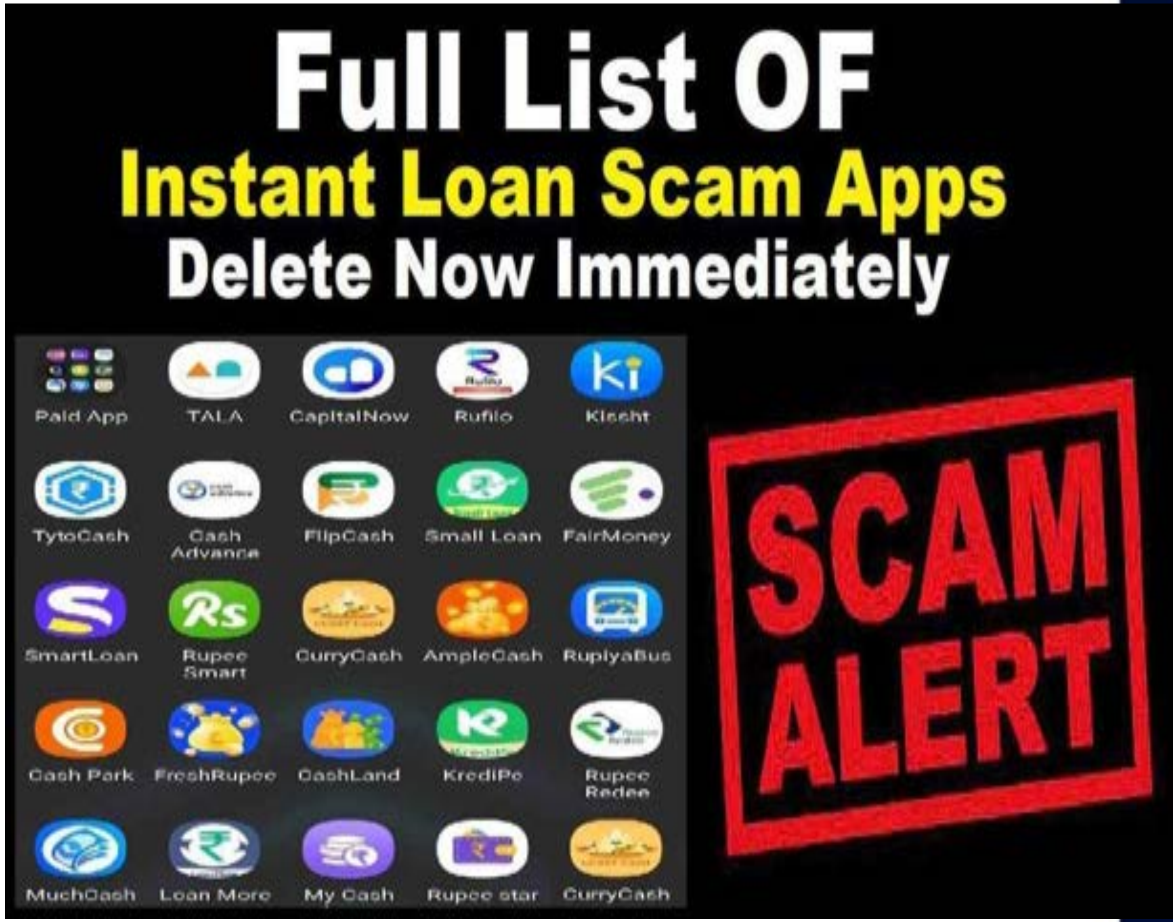
www.youtube.com/embed/5-_ojBsxsJo?si=gW15QgqP5DbGzorB

Fake Apps

A fake loan application is a type of financial scam where fraudsters impersonate legitimate financial institutions or lenders and trick individuals into applying for loans under false deceptions.

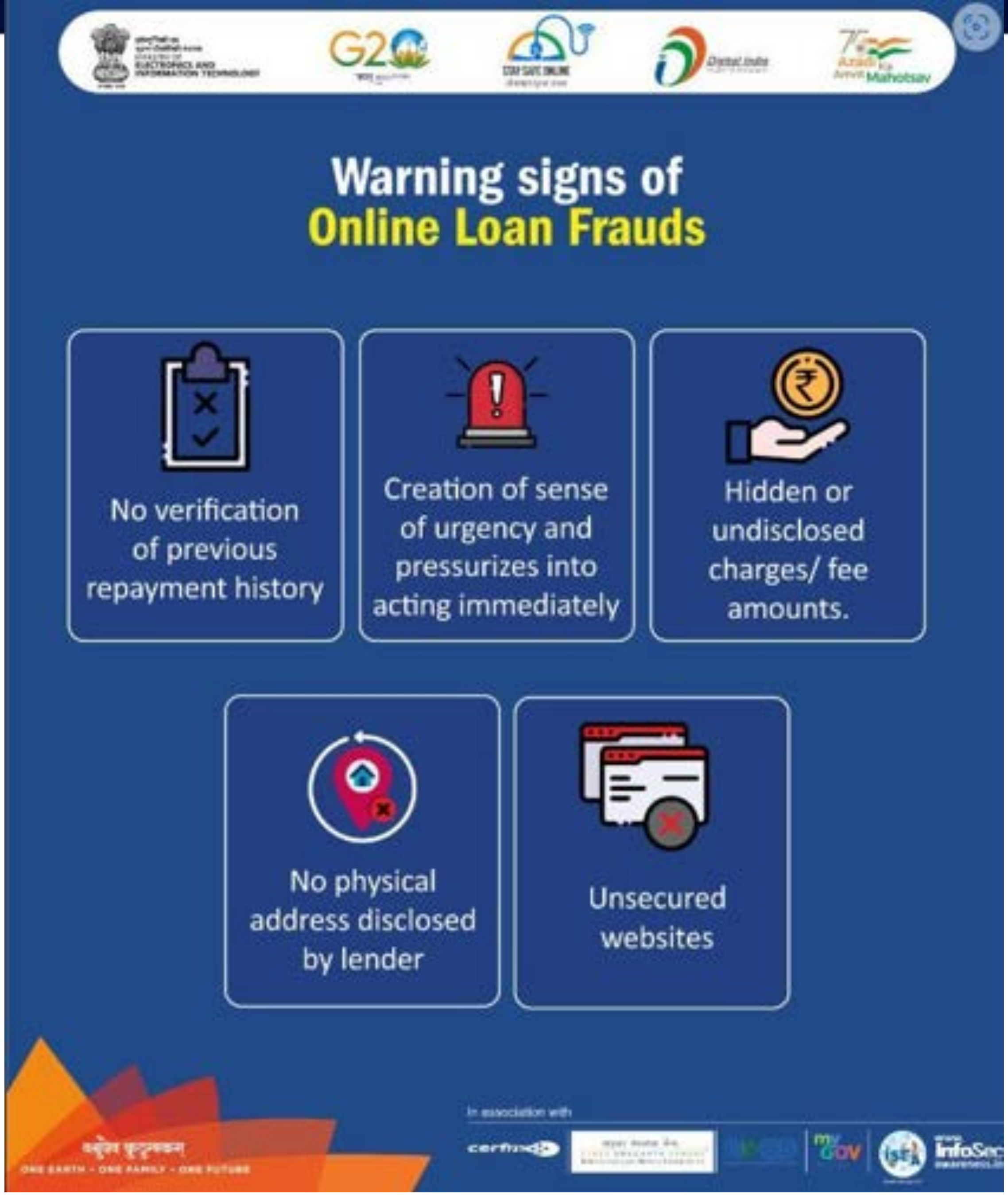
- Malware Installation – Once installed, fake apps may collect personal data, track keystrokes, or install additional malicious software.

- Phishing & Scams – Some fake apps prompt users to enter login credentials or payment details, which hackers then steal.



Fake App Video

Fake App: https://youtube.com/shorts/tAdI6gteHYI?si=8Rh1n8_UXY3_71XK



Warning signs of Online Loan Frauds

- No verification of previous repayment history
- Creation of sense of urgency and pressurizes into acting immediately
- Hidden or undisclosed charges/ fee amounts.
- No physical address disclosed by lender
- Unsecured websites

वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE

In association with

www.isea.gov.in

staysafeonline.in

Investment Frauds

Investment frauds deceive individuals into investing in fake or misleading opportunities, promising high returns with little to no risk.

- Scammers use money from new investors to pay earlier investors, creating an illusion of profits. Eventually, the scheme collapses.
- Fake crypto projects promise huge returns but disappear with investors’ money.
- Fake Real Estate Investments – Fraudsters sell non-existent properties or promise unrealistic rental income.

staysafeonline.in

Investment Fraud Video

www.youtube.com/embed/0hzFS3OA23U?si=kE9GAGw4ujXpiLGd

Cyber Hygiene Practices

Cyber Hygiene

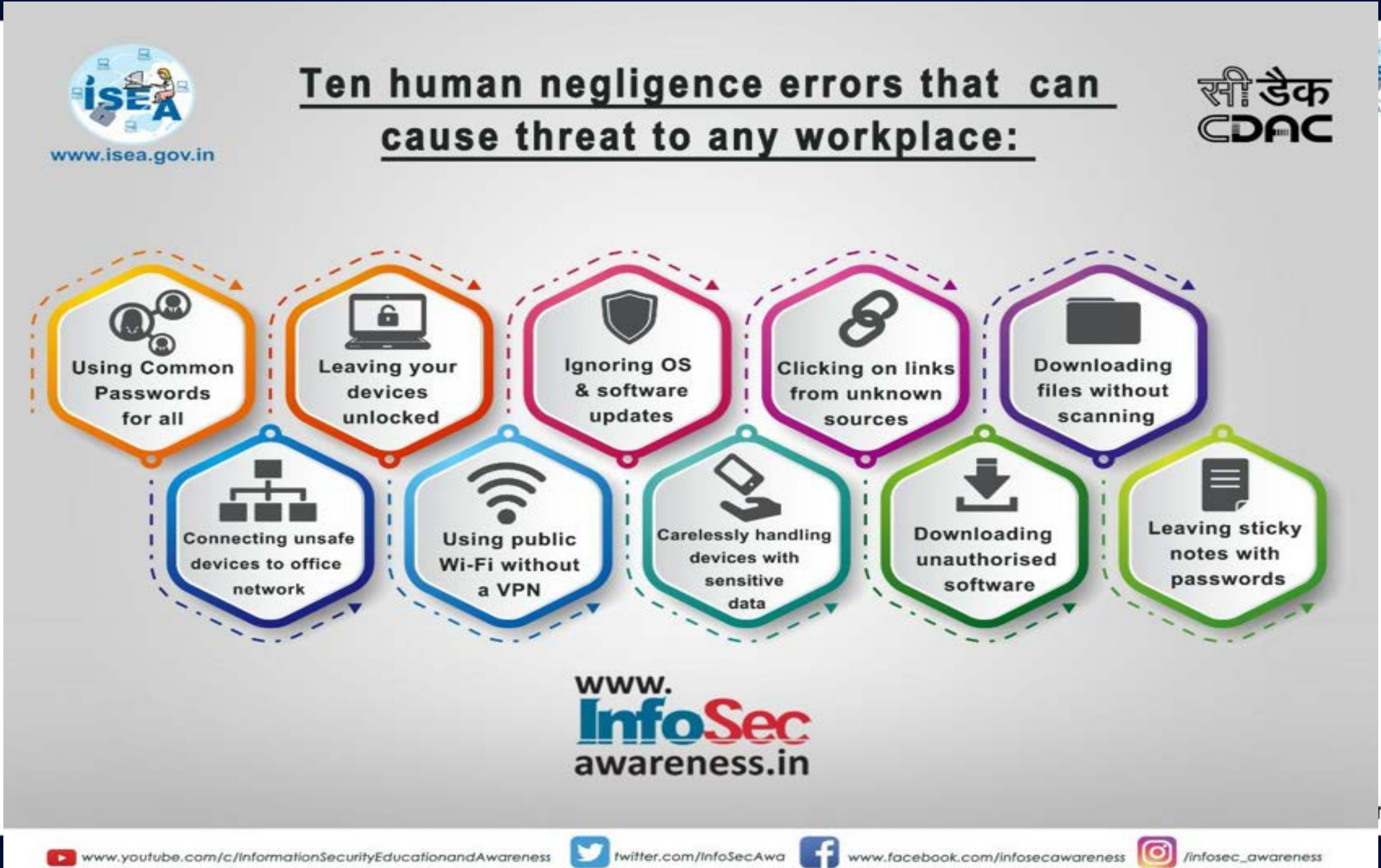
- Training yourself to form good habits around cybersecurity and stay ahead of cyber threats and online security issues.
- Cyber hygiene aims to maintain
  - Hardware and
  - Software's basic health and security,
- Cyber hygiene helps to keep data safe and secure.
- Help prevent cybercriminals from causing security breaches or stealing personal information.

awareness.isea.app

Benefits of cyber hygiene practices

- **Individual / organization minimizes the risk of**
  - Financial loss,
  - Damage to the organization's reputation
  - Protect user data
  - Identify software problems
- **Handle existing and emerging threats**
- **Predicting threats can be challenging, preparing and preventing**

staysafeonline.in



www.isea.gov.in

Ten human negligence errors that can cause threat to any workplace:

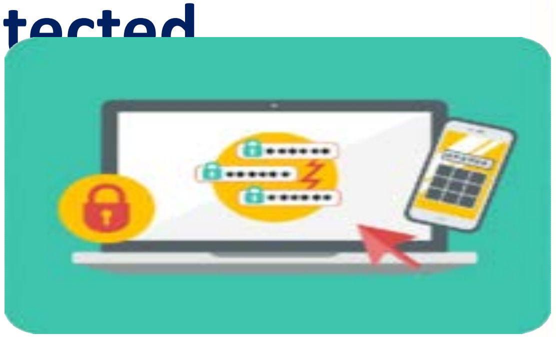
सी डैक
CDAC

- Using Common Passwords for all
- Leaving your devices unlocked
- Ignoring OS & software updates
- Clicking on links from unknown sources
- Downloading files without scanning
- Connecting unsafe devices to office network
- Using public Wi-Fi without a VPN
- Carelessly handling devices with sensitive data
- Downloading unauthorised software
- Leaving sticky notes with passwords

www.InfoSecawareness.in

www.youtube.com/c/InformationSecurityEducationandAwareness twitter.com/InfoSecAwa www.facebook.com/infosecawareness /infosec_awareness

Cyber hygiene checklist to ensure you’re keeping yourself protected



Keeping passwords safe and secure

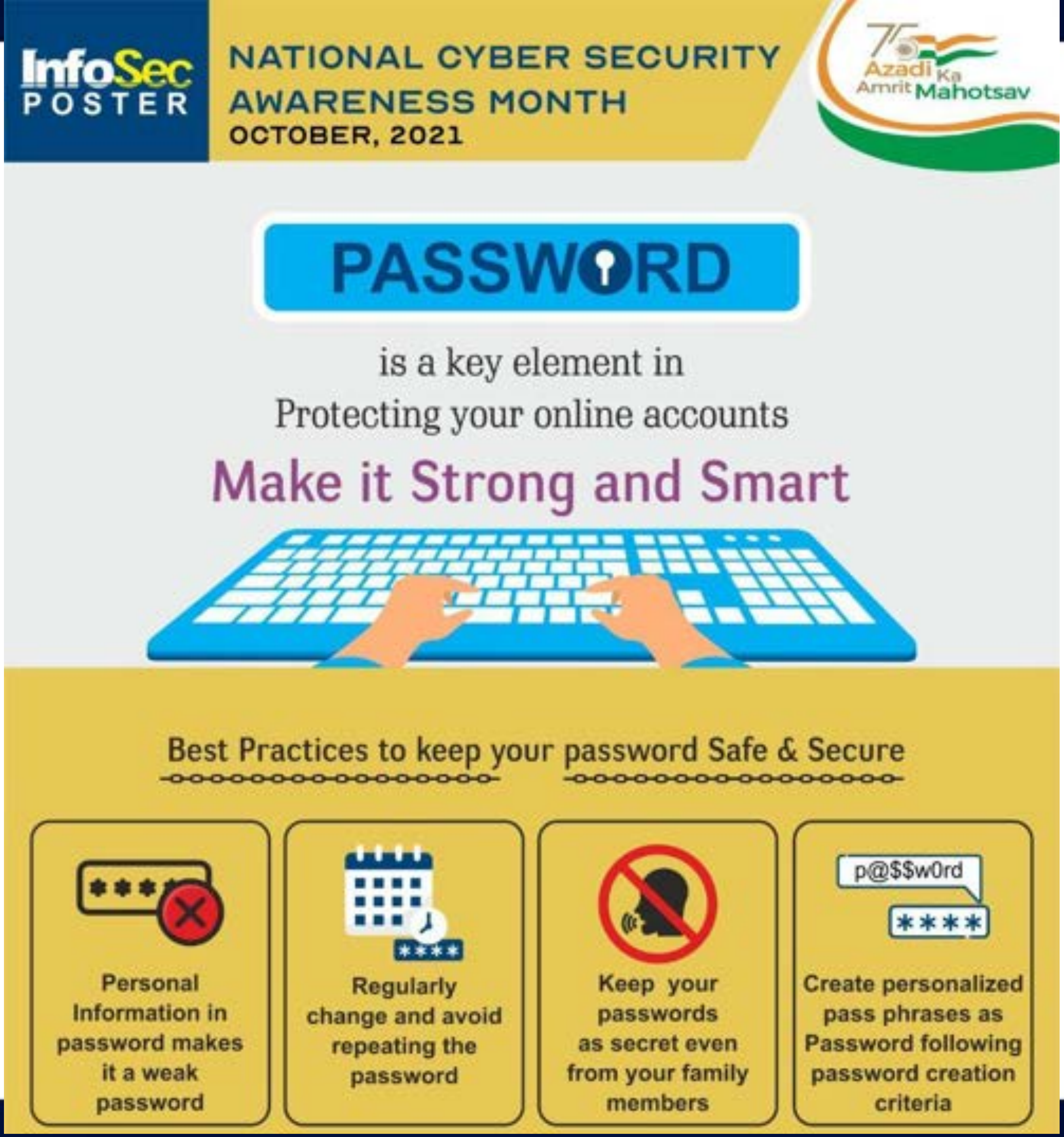
- I avoid using the same password for different accounts
- I change my passwords on a regular basis
- My passwords are at least 12 characters long (and ideally longer)
- My passwords involve a mix of upper- and lower-case letters plus symbols and numbers
- My passwords avoid the obvious - such as using sequential numbers (“1234”) or personal information that someone who knows me might guess, such as my date of birth or a pet’s name
- I change the default passwords on my Internet of Things (IoT) devices
- I avoid writing my passwords down or sharing them with others

Using multi-factor authentication

- All my essential accounts – such as email, social media, or banking apps – are protected with multi-factor authentication (MFA)

Login
Logged In

more than one form of identity to authenticate a user and approve access



InfoSec POSTER

NATIONAL CYBER SECURITY AWARENESS MONTH
OCTOBER, 2021

75 Azadi Ka Amrit Mahotsav

PASSWORD

is a key element in
Protecting your online accounts

Make it Strong and Smart

Best Practices to keep your password Safe & Secure

- Personal Information in password makes it a weak password
- Regularly change and avoid repeating the password
- Keep your passwords as secret even from your family members
- Create personalized pass phrases as Password following password creation criteria

ISEA
www.isea.gov.in

staysafeonline.in

National Cyber Security Awareness Month

October, 2022

SEE YOURSELF IN CYBER

Update your software

Five reasons to update software

1. Patch security flaws
2. Get new features
3. Protect data
4. Improve performance
5. Ensure compatibility

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Ensuring privacy

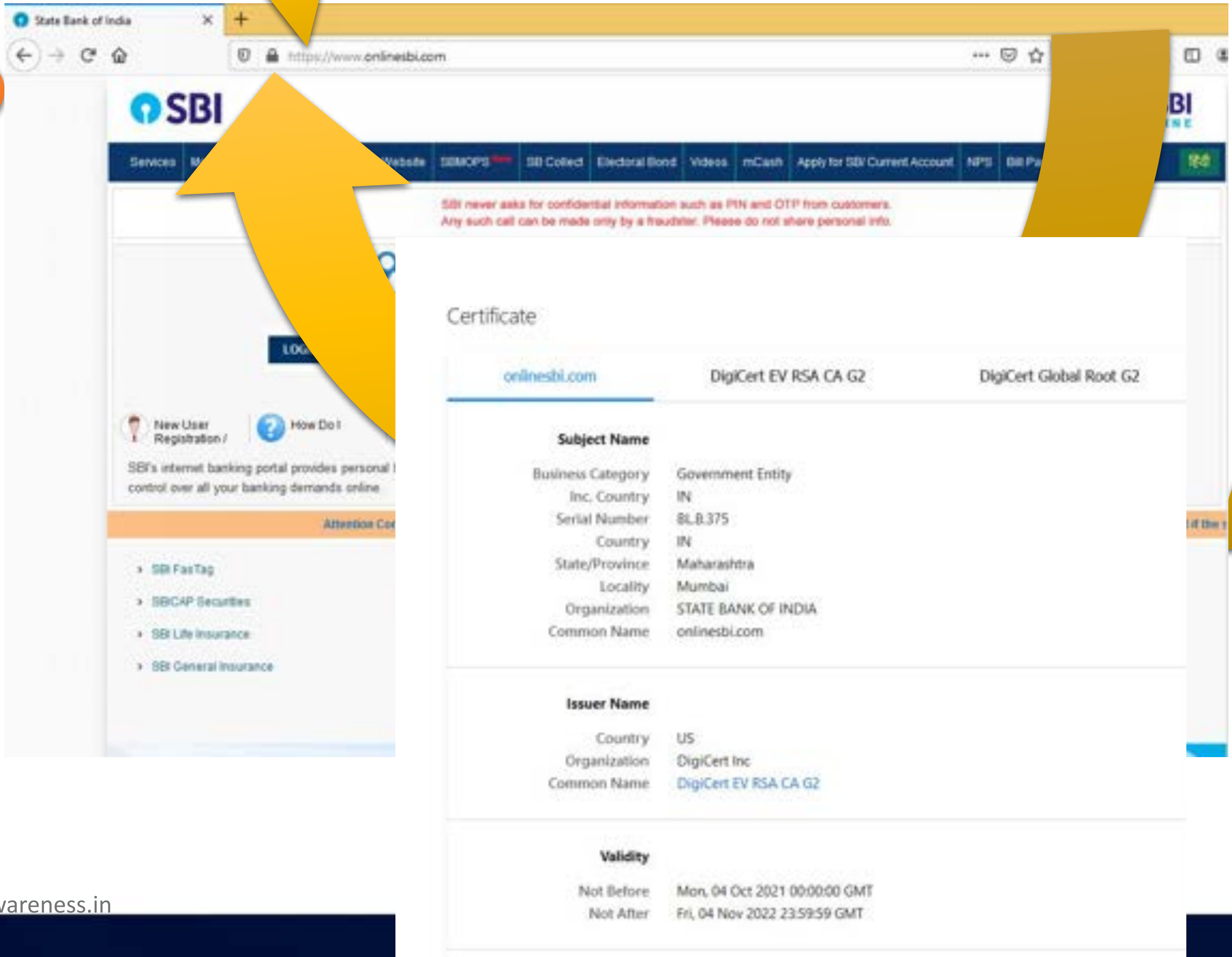
- Don't post private information such as my home address, private pictures, phone number, or credit card numbers publicly on social media
- Avoid quizzes, games, or surveys on social media that ask for sensitive personal information
- Phone locked with a password or PIN
- Take care not to disclose private information when using public Wi-Fi
- Make sure any online transactions I make are via a secure website – where the URL starts with https:// rather than http:// and there is a padlock icon to the left of the address bar
- Share information about online privacy with family and friends to help keep them safe

How to be Safe – Always look for

HTTPS

Padlock Symbol

Digital Certificate



SBI never asks for confidential information such as PIN and OTP from customers.
Any such call can be made only by a fraudster. Please do not share personal info.

SBI's internet banking portal provides personal
control over all your banking demands online

Certificate

onlinesbi.com | DigiCert EV RSA CA G2 | DigiCert Global Root G2

Subject Name

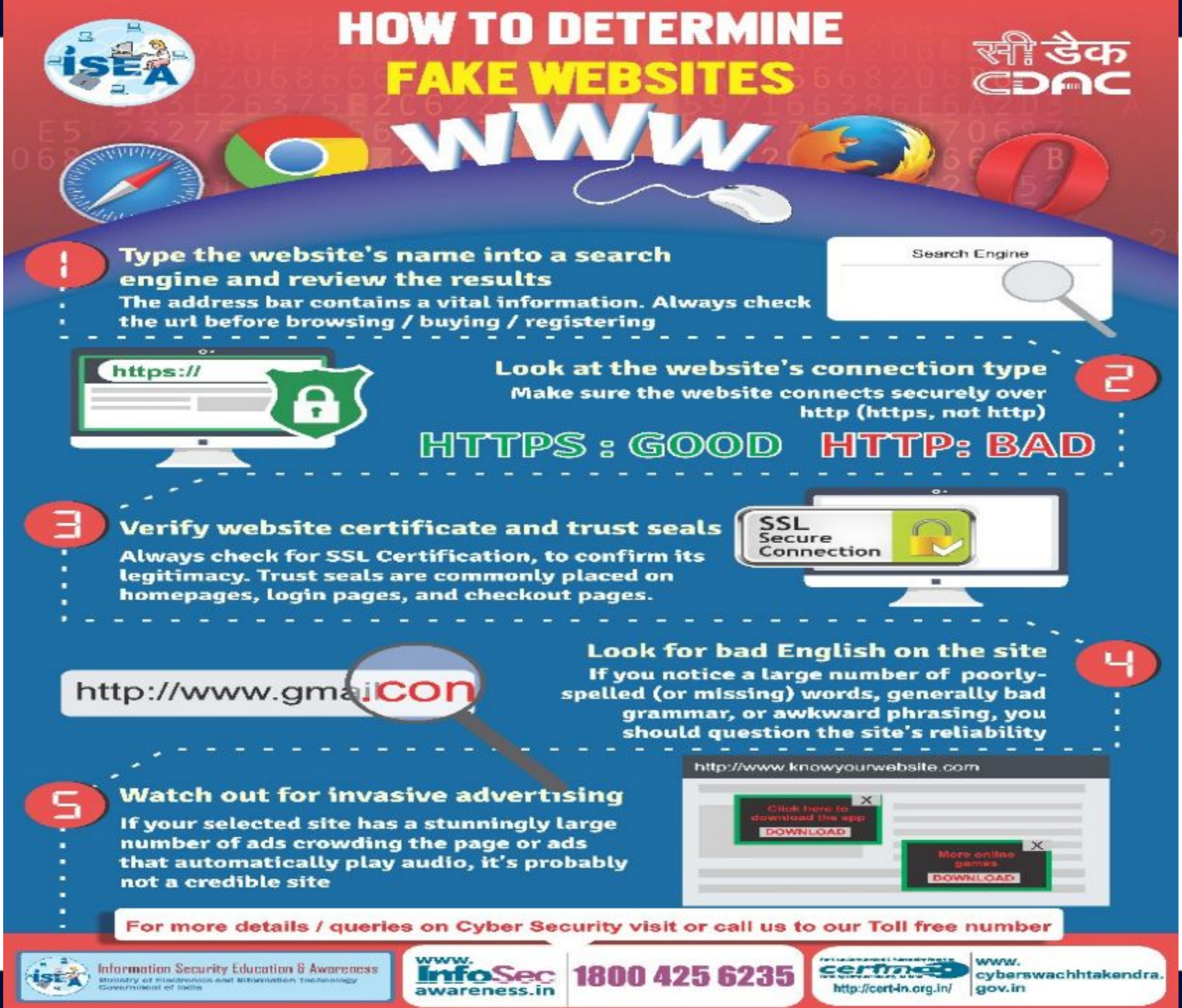
Business Category	Government Entity
Inc. Country	IN
Serial Number	BLB375
Country	IN
State/Province	Maharashtra
Locality	Mumbai
Organization	STATE BANK OF INDIA
Common Name	onlinesbi.com

Issuer Name

Country	US
Organization	DigiCert Inc
Common Name	DigiCert EV RSA CA G2

Validity

Not Before	Mon, 04 Oct 2021 00:00:00 GMT
Not After	Fri, 04 Nov 2022 23:59:59 GMT



HOW TO DETERMINE FAKE WEBSITES

1 **Type the website's name into a search engine and review the results**

The address bar contains a vital information. Always check the url before browsing / buying / registering

2 **Look at the website's connection type**

Make sure the website connects securely over http (https, not http)

HTTPS : GOOD HTTP: BAD

3 **Verify website certificate and trust seals**

Always check for SSL Certification, to confirm its legitimacy. Trust seals are commonly placed on homepages, login pages, and checkout pages.

4 **Look for bad English on the site**

If you notice a large number of poorly-spelled (or missing) words, generally bad grammar, or awkward phrasing, you should question the site's reliability

5 **Watch out for invasive advertising**

If your selected site has a stunningly large number of ads crowding the page or ads that automatically play audio, it's probably not a credible site

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

Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

www.InfoSecawareness.in

1800 425 6235

cert-in
http://cert-in.org.in/

www.cyberswachhtakendra.gov.in

ISEA
www.isea.gov.in

staysafeonline.in

Fraudulent calls

If you share you may loose your money

No bank will ask for bank account, debit / credit card details, CVV number etc.,

staysafeonline.in

UPI – Best Practices

Use a PIN or Biometric lock
keep your e- wallet safe from any shock
#Be Safe Stay Safe
www.staysafeonline.in
G20

UPI – Best Practices

- UPI PIN is most important
- Never share your UPI PIN
- Do not use easy to guess UPI PIN
- Beware of cameras while entering UPI PIN
- Use trusted app from trusted source
- Ensure using updated app
- Avoid using Public Wifi
- Remember that QR codes are only a means to MAKE payments and NOT RECEIVE them

How to secure - Credit card and Debit card

- Use Strong Passwords
- Sign the back of your Card
- Monitor your Account
- Be Careful with your Card
- Use Two-Factor Authentication
- Use Secure Websites
- Check your Credit Report
- Report Lost or Stolen Cards Immediately
- Set Limits

Online banking services

Best Security Practices for Digital users

Security practices to protect Personal Identifiable Information (PII)

Create hard-to-guess security access codes / passwords for Online Banking and make them unique

Use a personalized passphrase while creating a password, it will ensure that you can remember it even though it is long. Example - iL0v3Bl@Ckc0L0r

Avoid writing down passwords, memorize them and keep it strictly personal and confidential

User should not disclose to ANYONE security access codes – like passwords, PIN, OTP, account no. etc.,

User should never leave PC unattended when logged into Online Banking

After accessing online banking services, always remember to “log off ” from online session and not close the browser directly.

Keeping apps, software, and firmware up to date

- I update apps, web browsers, operating systems, and firmware regularly to make I'm using the latest versions, which have eliminated or patched possible security glitches

- Where possible, I have set up features to ensure automatic software updates
- I delete apps I no longer use

- I only download apps from reputable or official sources

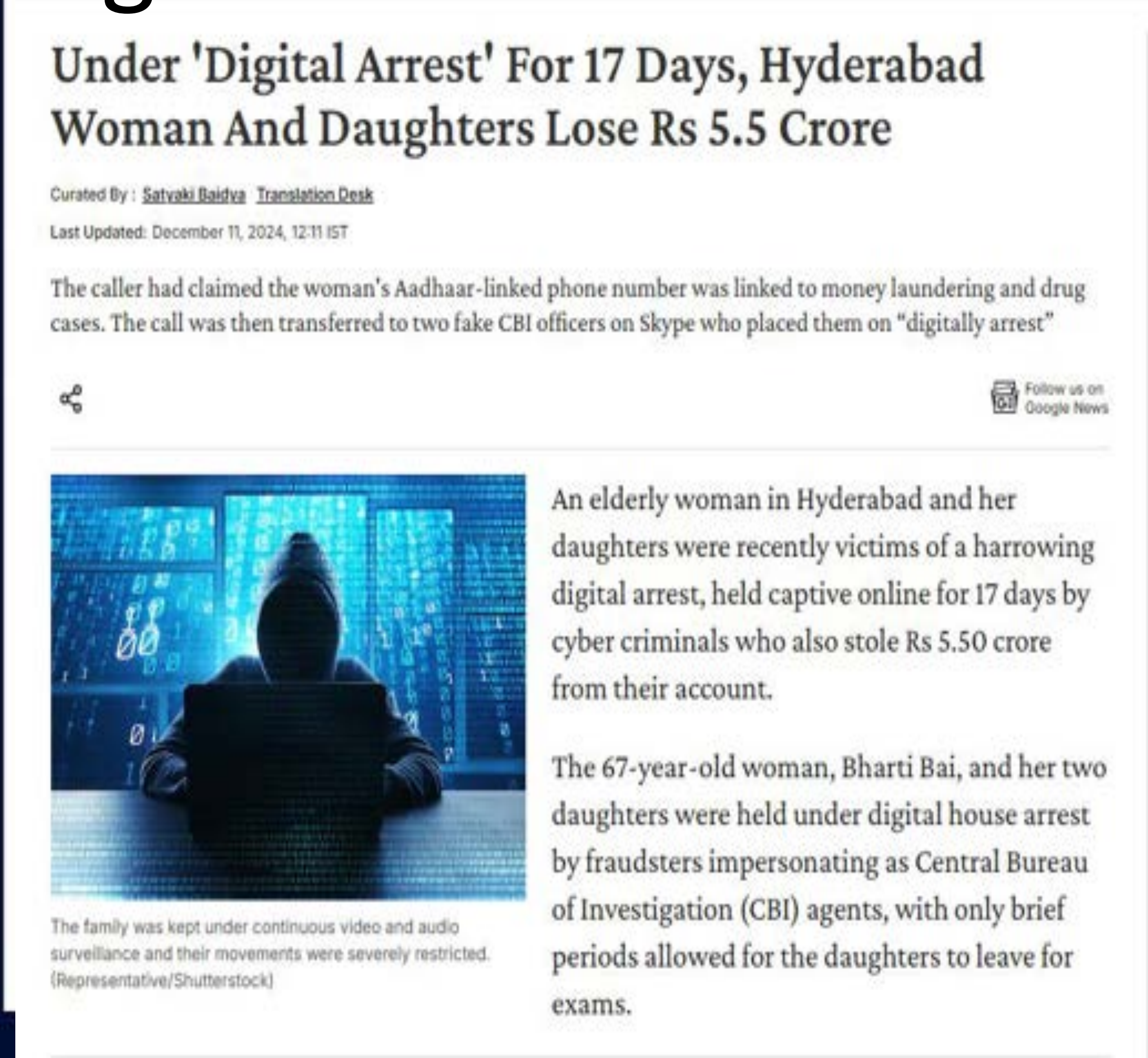
Public Wi-Fi: Avoid making financial transactions over public Wi-Fi networks.

Personal Info: Be careful about sharing your full name, address, phone number, or financial details online.

TOP SECRET
NEVER GIVE AWAY TO SOMEONE YOU ONLY KNOWLEDGE
⊘ Your Full Name
⊘ Your Photos
⊘ Your Phone Number
⊘ Your Address
⊘ Your School Name
⊘ Your Passwords
WHY ?
Because cyber - creeps can use this info to find you.

Recent Cyber Incidents

Digital Arrest is Fraud



Under 'Digital Arrest' For 17 Days, Hyderabad Woman And Daughters Lose Rs 5.5 Crore

Curated By : Satyaki Baidya Translation Desk

Last Updated: December 11, 2024, 12:11 IST

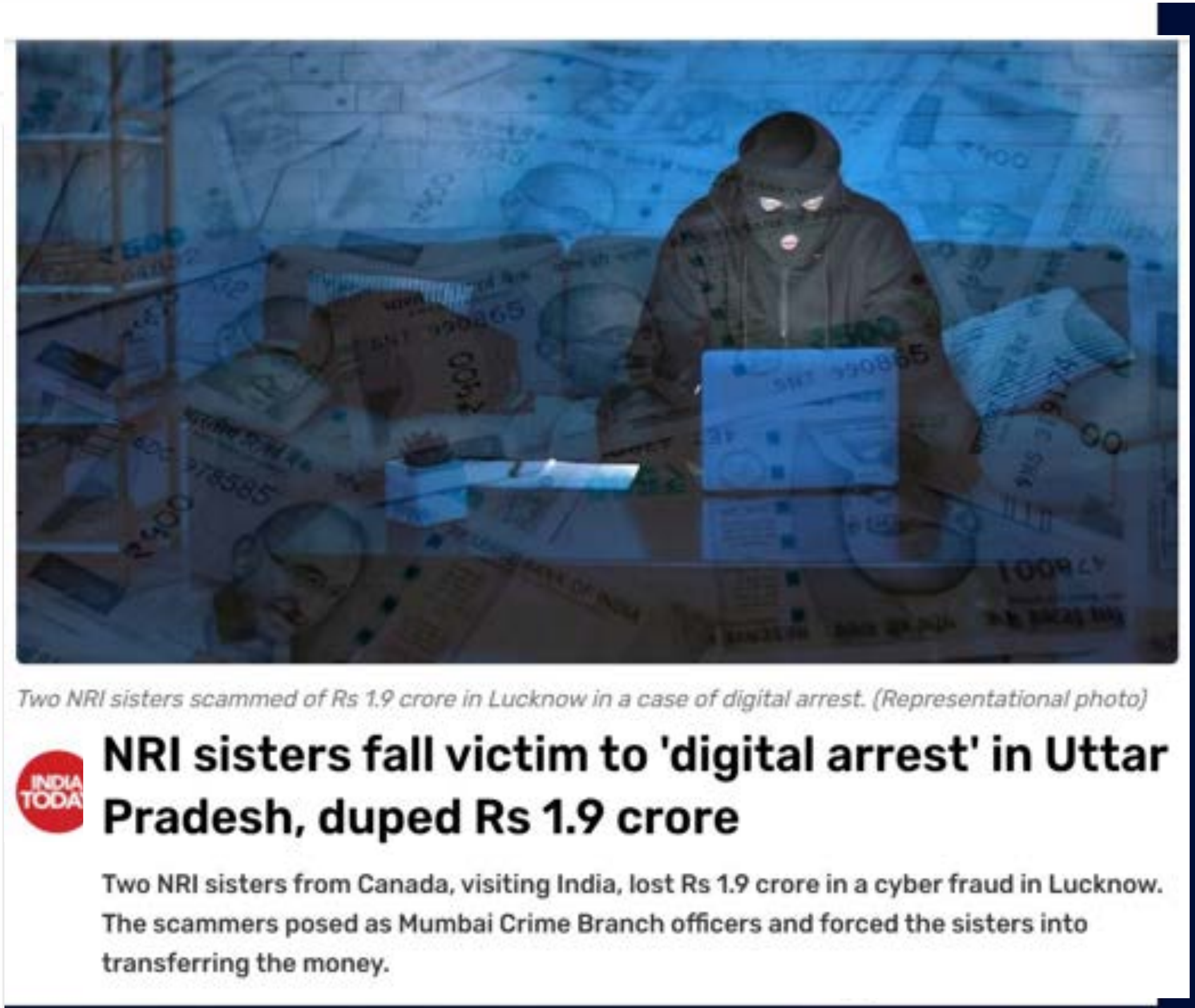
The caller had claimed the woman's Aadhaar-linked phone number was linked to money laundering and drug cases. The call was then transferred to two fake CBI officers on Skype who placed them on "digitally arrest"

Follow us on Google News

The family was kept under continuous video and audio surveillance and their movements were severely restricted. (Representative/Shutterstock)

An elderly woman in Hyderabad and her daughters were recently victims of a harrowing digital arrest, held captive online for 17 days by cyber criminals who also stole Rs 5.50 crore from their account.

The 67-year-old woman, Bharti Bai, and her two daughters were held under digital house arrest by fraudsters impersonating as Central Bureau of Investigation (CBI) agents, with only brief periods allowed for the daughters to leave for exams.



Two NRI sisters scammed of Rs 1.9 crore in Lucknow in a case of digital arrest. (Representational photo)

NRI sisters fall victim to 'digital arrest' in Uttar Pradesh, duped Rs 1.9 crore

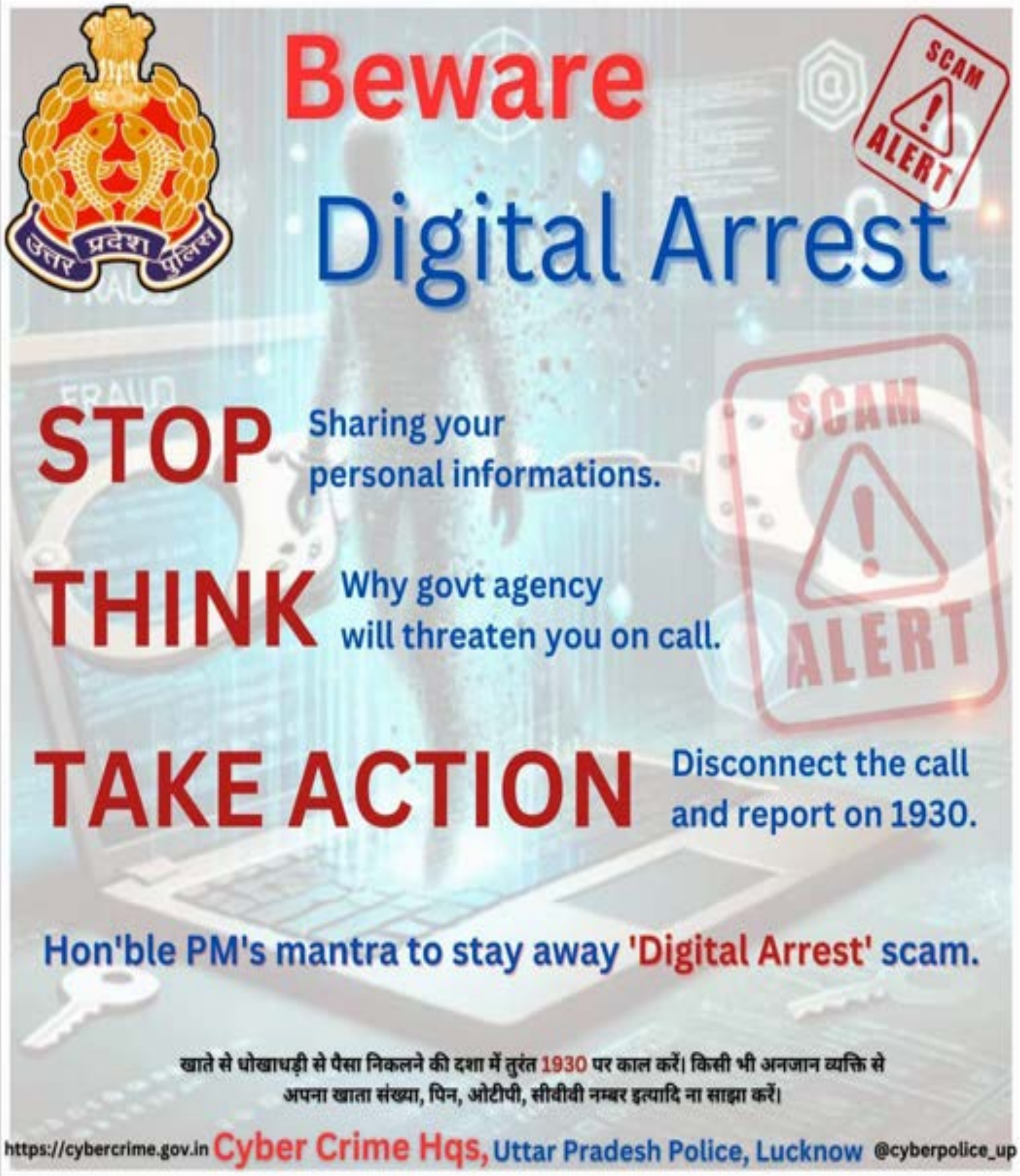
Two NRI sisters from Canada, visiting India, lost Rs 1.9 crore in a cyber fraud in Lucknow. The scammers posed as Mumbai Crime Branch officers and forced the sisters into transferring the money.

<< Scan to know mre about Digital Arrest

DIGITAL ARREST IS A FRAUD

- **No Government agency (Police, CBI, ED) can investigate or arrest you over video or voice calls.**
- **Don't Panic! Do not share any personal information over calls**
- **Before acting, check and confirm with concerned authority.**
- **Preserve evidence.**

- कोई भी सरकारी एजेंसी (पुलिस, सीबीआई, ईडी) वीडियो या वॉयस कॉल पर आपकी जांच या गिरफ्तारी नहीं कर सकती।
- घबराये नहीं! कोई भी निजी जानकारी कॉल पर साझा न करें।
- कुछ भी करने से पहले, परिवार या संबंधित अधिकारी से पुष्टि करें।
- सबूत सुरक्षित रखें



Beware

Digital Arrest

STOP Sharing your personal informations.

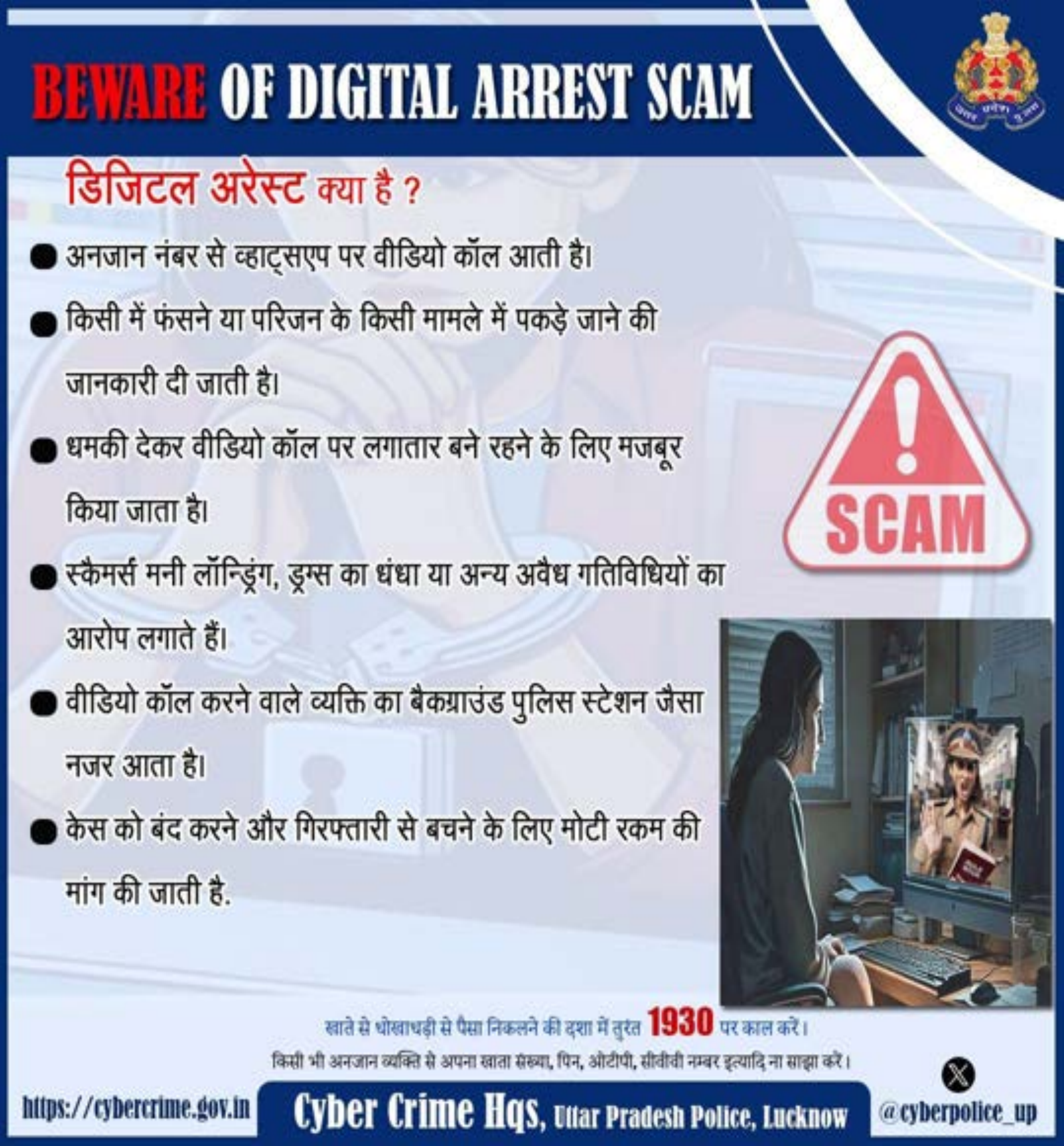
THINK Why govt agency will threaten you on call.

TAKE ACTION Disconnect the call and report on 1930.

Hon'ble PM's mantra to stay away 'Digital Arrest' scam.

खाते से धोखाधड़ी से पैसा निकलने की दशा में तुरंत 1930 पर काल करें। किसी भी अनजान व्यक्ति से अपना खाता संख्या, पिन, ओटीपी, सीवीवी नम्बर इत्यादि ना साझा करें।

https://cybercrime.gov.in **Cyber Crime Hqs,** Uttar Pradesh Police, Lucknow @cyberpolice_up



BEWARE OF DIGITAL ARREST SCAM

डिजिटल अरेस्ट क्या है ?

- अनजान नंबर से व्हाट्सएप पर वीडियो कॉल आती है।
- किसी में फंसने या परिजन के किसी मामले में पकड़े जाने की जानकारी दी जाती है।
- धमकी देकर वीडियो कॉल पर लगातार बने रहने के लिए मजबूर किया जाता है।
- स्कैमर्स मनी लॉन्ड्रिंग, ड्रग्स का धंधा या अन्य अवैध गतिविधियों का आरोप लगाते हैं।
- वीडियो कॉल करने वाले व्यक्ति का बैकग्राउंड पुलिस स्टेशन जैसा नजर आता है।
- केस को बंद करने और गिरफ्तारी से बचने के लिए मोटी रकम की मांग की जाती है.

खाते से धोखाधड़ी से पैसा निकलने की दशा में तुरंत **1930** पर काल करें।

किसी भी अनजान व्यक्ति से अपना खाता संख्या, पिन, ओटीपी, सीवीवी नम्बर इत्यादि ना साझा करें।

https://cybercrime.gov.in **Cyber Crime Hqs,** Uttar Pradesh Police, Lucknow @cyberpolice_up

Advantages and Disadvantages of Social Networking

staysafeonline.in

Advantages:

- Connects people globally.
- Facilitates professional networking.
- Enables real-time information sharing.
- Supports learning and information exchange
- Raises Awareness

Disadvantages:

- Privacy concerns.
- Risk of cyberbullying.
- Can promote misinformation.
- Potential for addiction and reduced face-to-face interactions.
- Losing Focus

WhatsApp Security

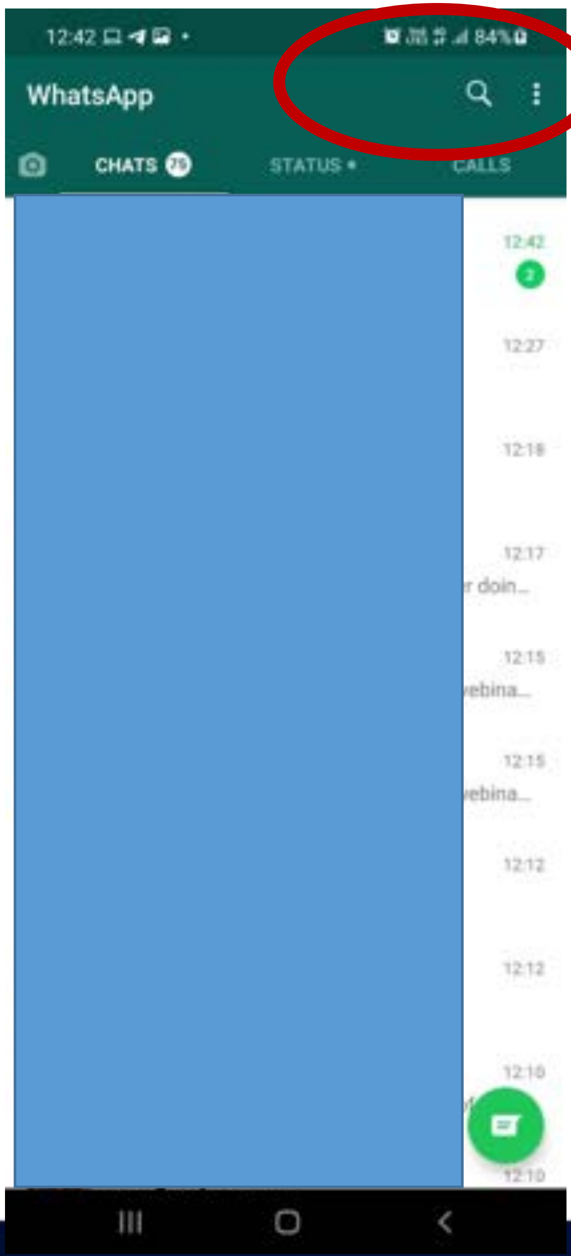
- WhatsApp is the favorite medium for hackers.

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

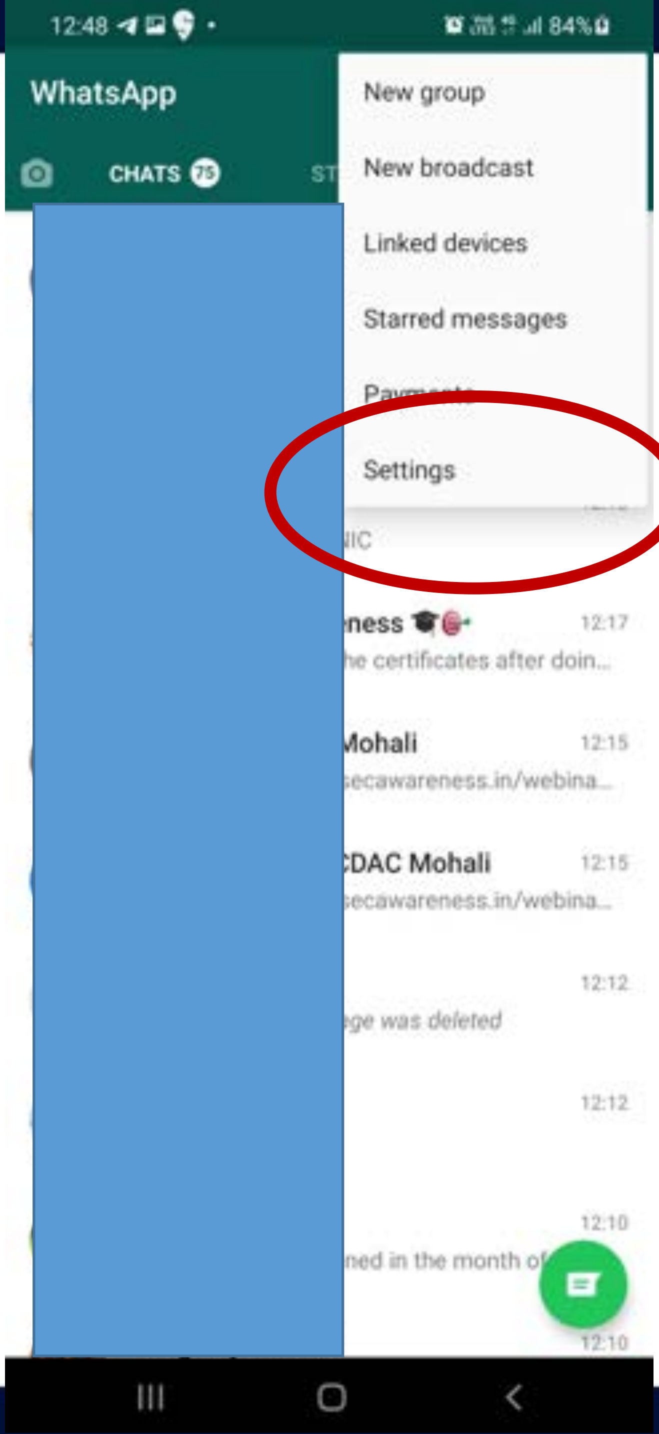
- There is a simple way to protect oneself from such an attack.

staysafeonline.in

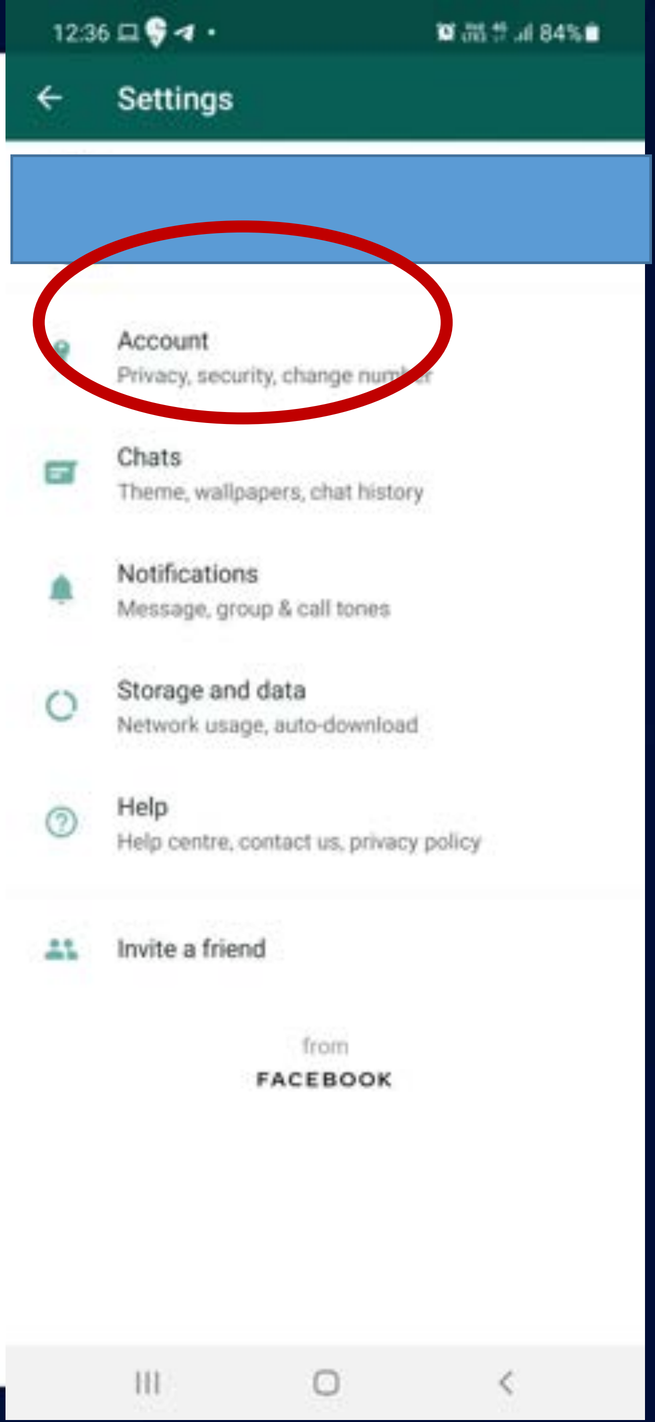
WhatsApp Security



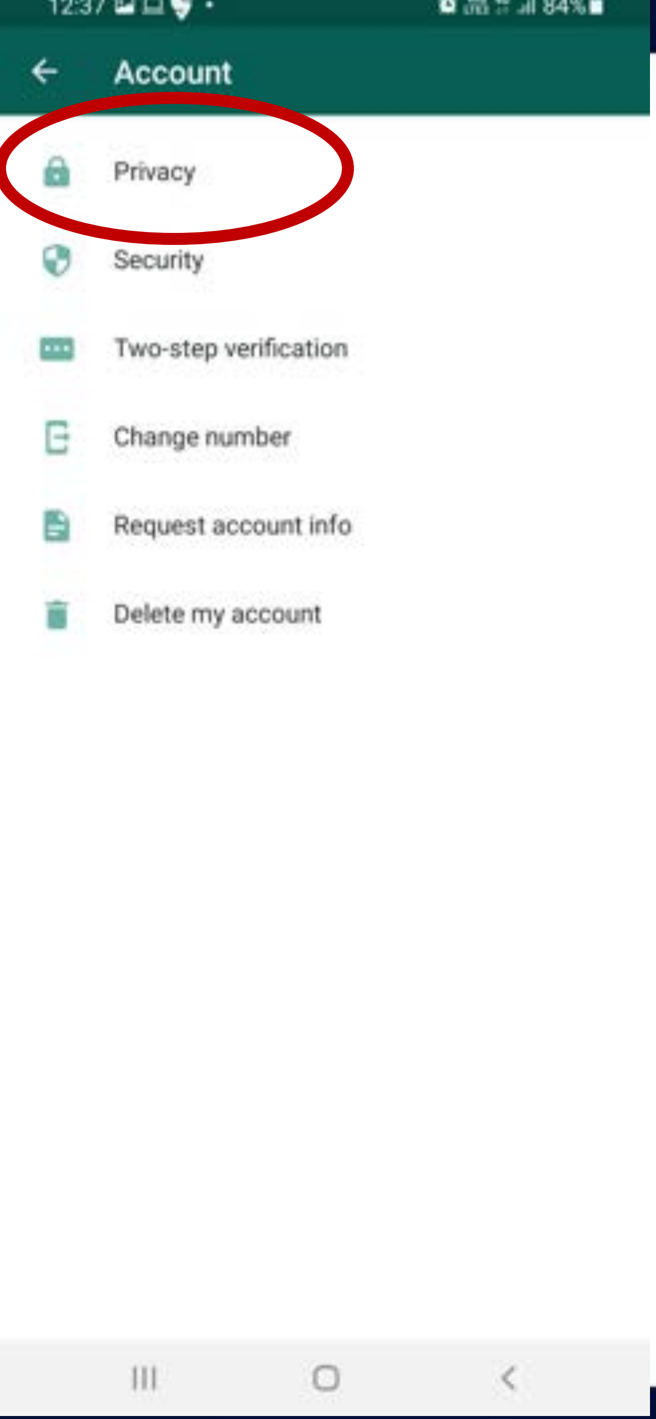
[redacted]



[redacted]


12:36
84%
Settings
Account
Privacy, security, change number
Chats
Theme, wallpapers, chat history
Notifications
Message, group & call tones
Storage and data
Network usage, auto-download
Help
Help centre, contact us, privacy policy
Invite a friend
from
FACEBOOK

[redacted]



12:37 84%

← Account

Privacy

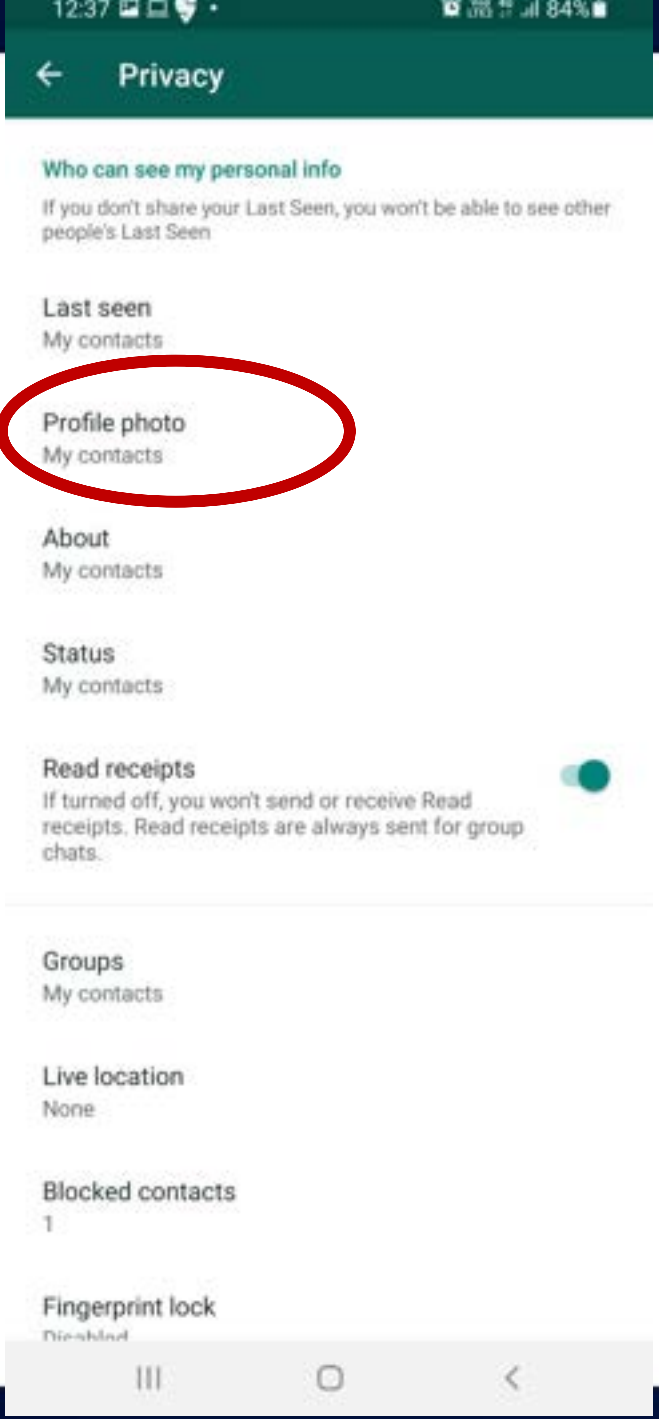
Security

Two-step verification

Change number

Request account info

Delete my account



12:37 84%

← Privacy

Who can see my personal info

If you don't share your Last Seen, you won't be able to see other people's Last Seen

Last seen
My contacts

Profile photo
My contacts

About
My contacts

Status
My contacts

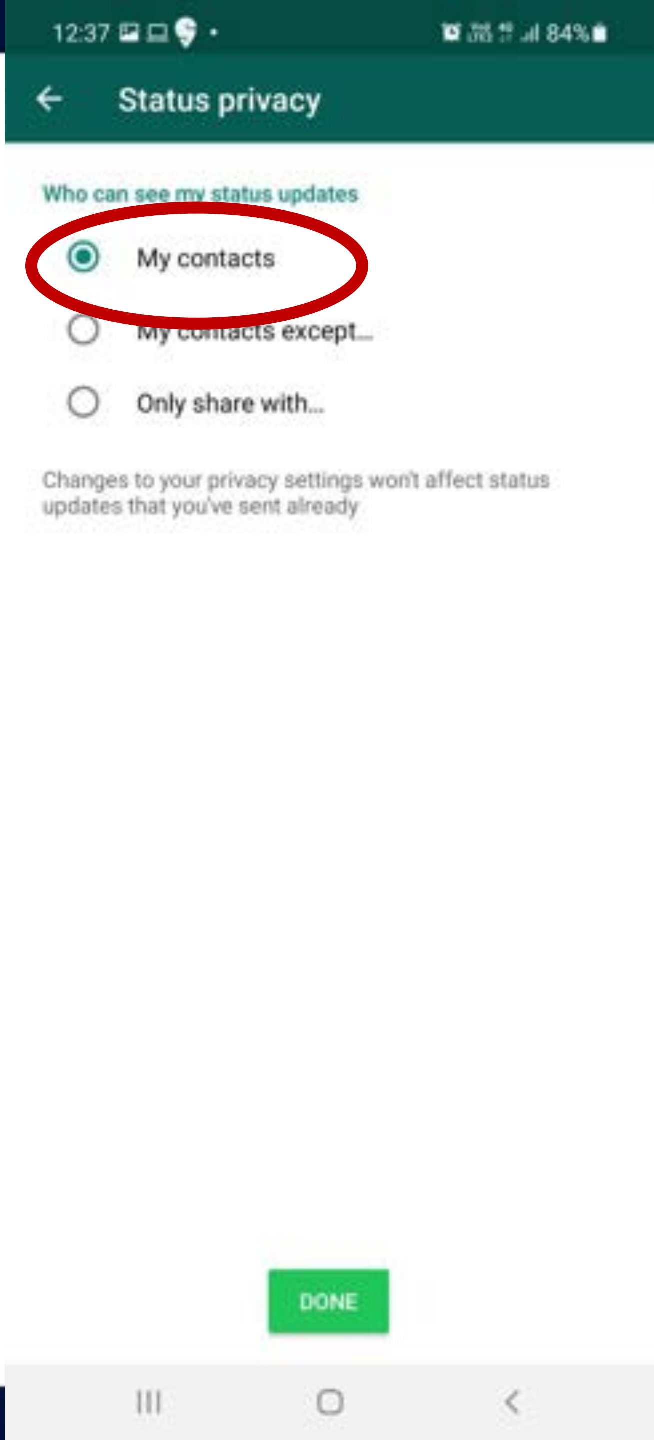
Read receipts
If turned off, you won't send or receive Read receipts. Read receipts are always sent for group chats.

Groups
My contacts

Live location
None

Blocked contacts
1

Fingerprint lock
Disabled



12:37 84%

← Status privacy

Who can see my status updates

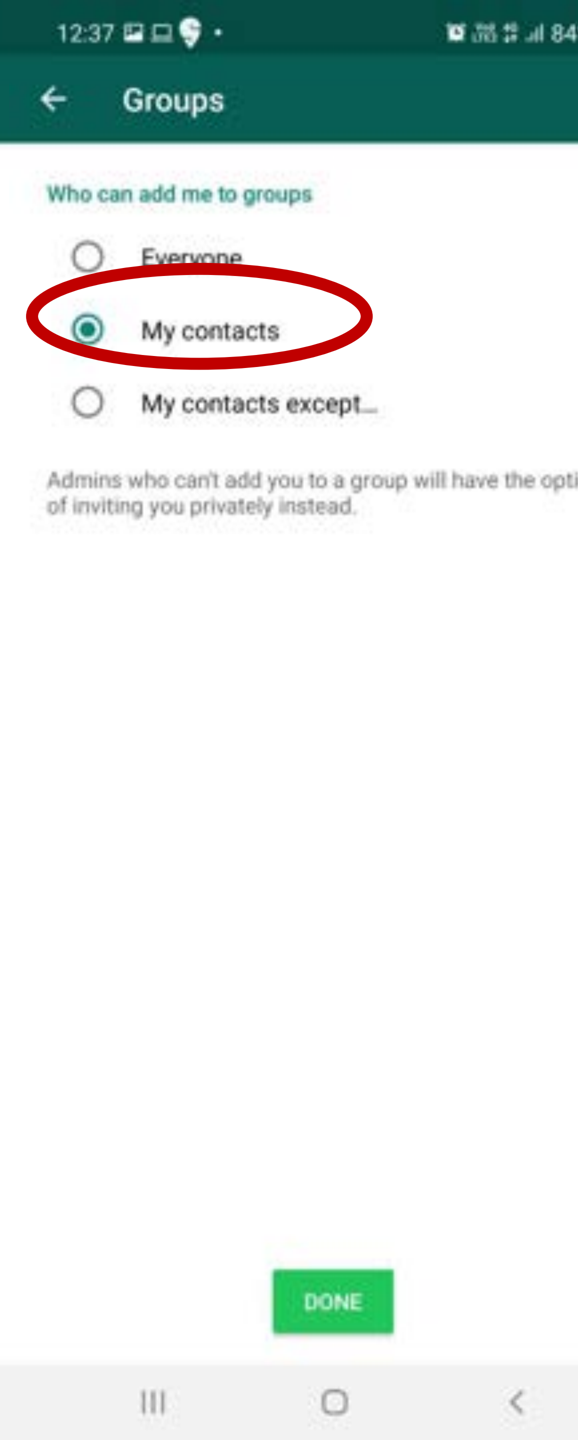
● My contacts

○ My contacts except...

○ Only share with...

Changes to your privacy settings won't affect status updates that you've sent already

DONE



12:37 84

← Groups

Who can add me to groups

○ Everyone

● My contacts

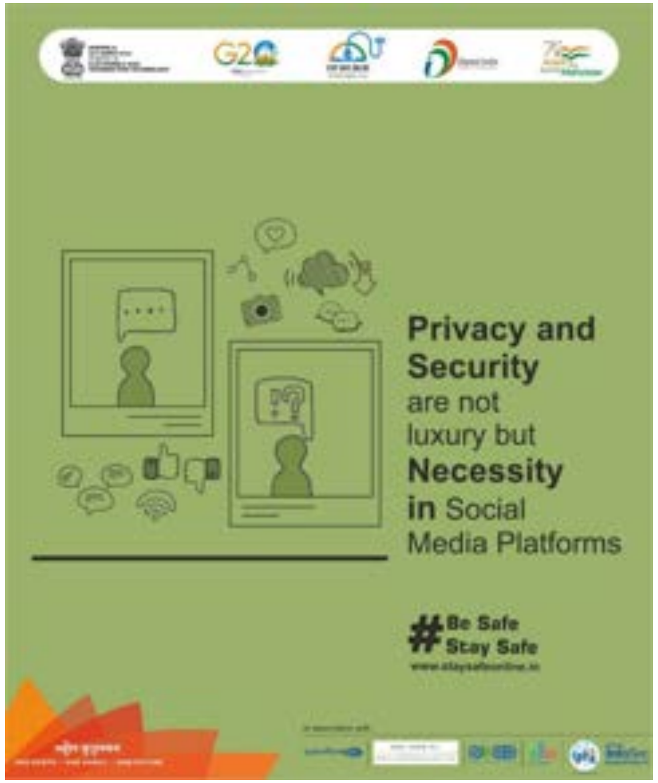
○ My contacts except...

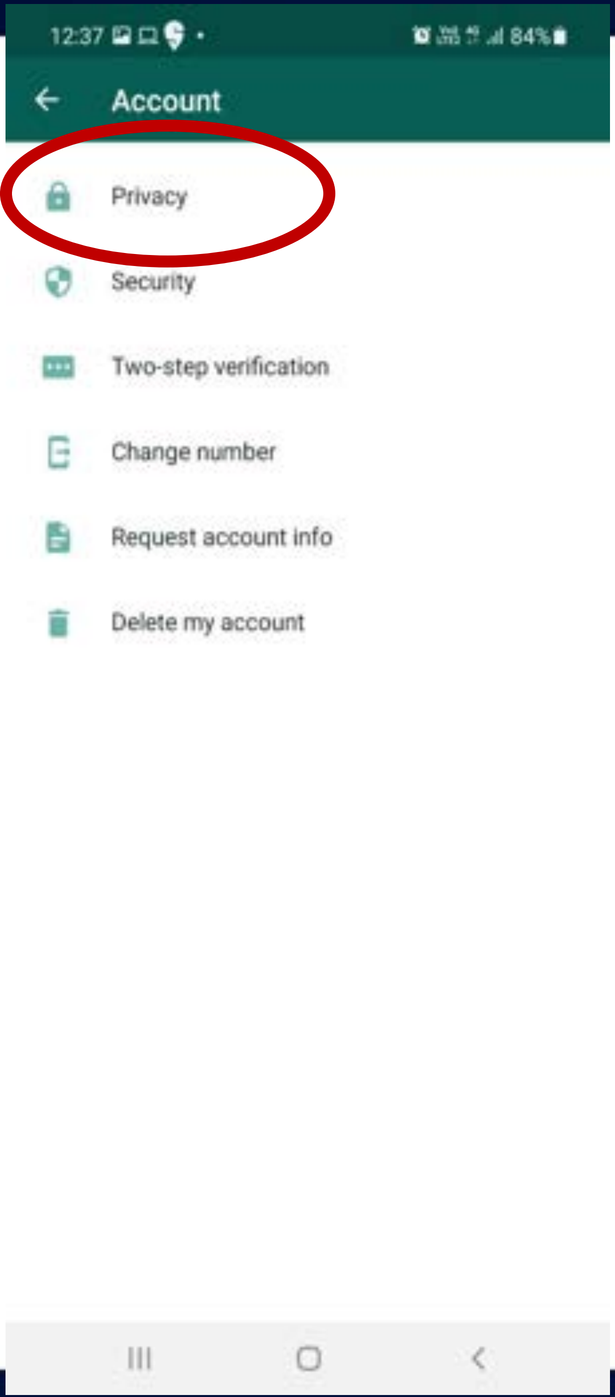
Admins who can't add you to a group will have the opti
of inviting you privately instead.

DONE

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

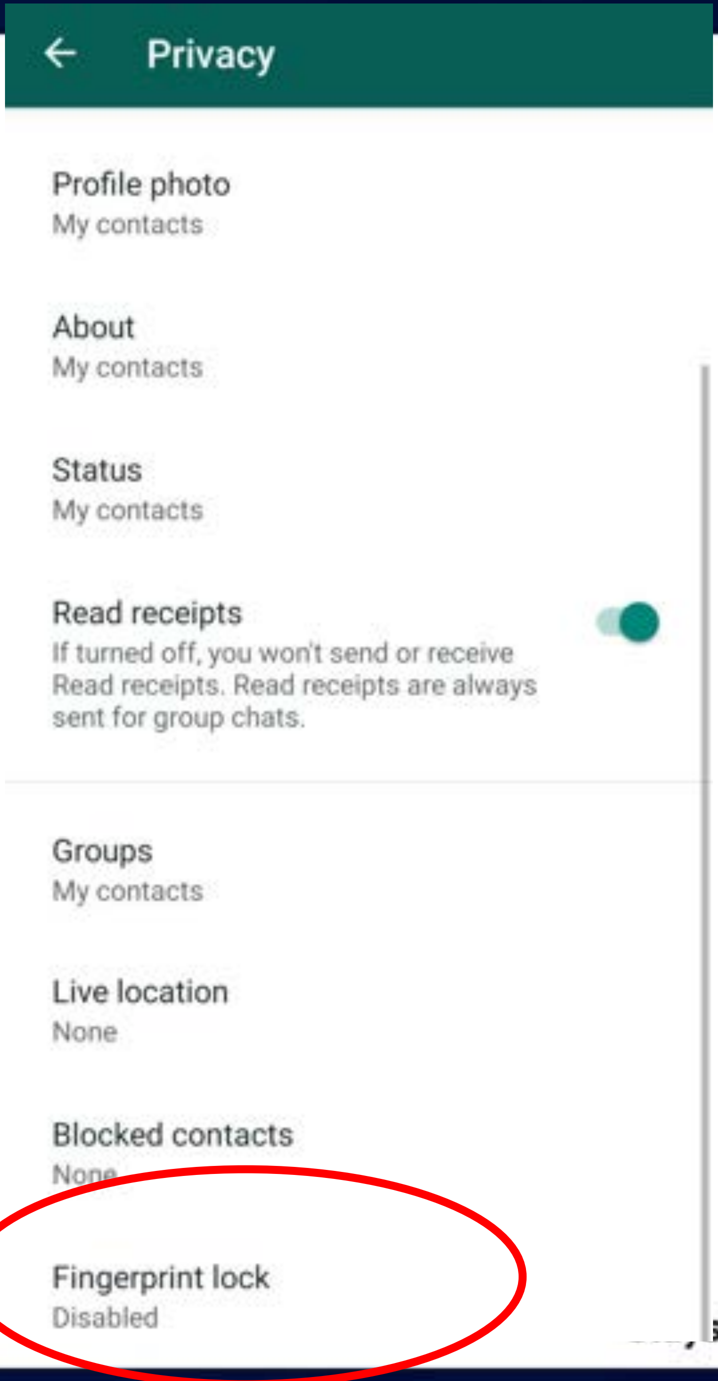
Setting password


G2C
Privacy and Security are not luxury but Necessity in Social Media Platforms
#Be Safe Stay Safe
www.staysafeonline.in


12:37 84%

Account

- Privacy
- Security
- Two-step verification
- Change number
- Request account info
- Delete my account


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

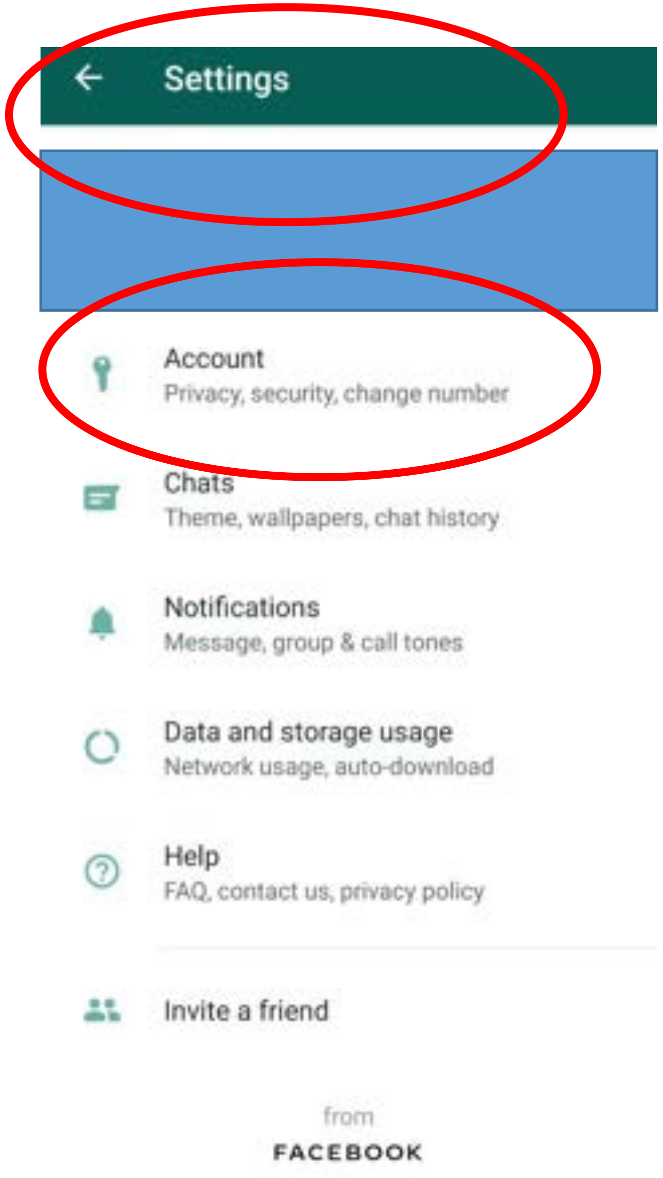
Live location
None

Blocked contacts
None

Fingerprint lock
Disabled

safeonline.in

Two Step Verification on WhatsApp should also be enabled



← Settings

Account
Privacy, security, change number

Chats
Theme, wallpapers, chat history

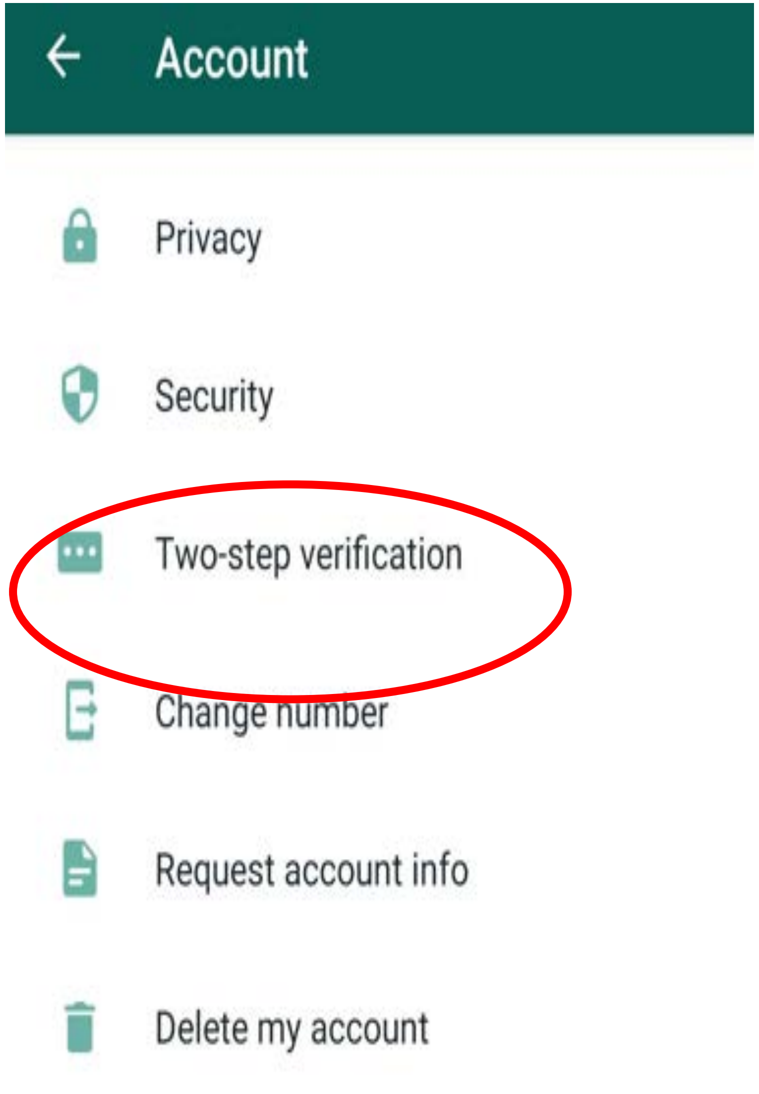
Notifications
Message, group & call tones

Data and storage usage
Network usage, auto-download

Help
FAQ, contact us, privacy policy

Invite a friend

from
FACEBOOK



← Account

Privacy

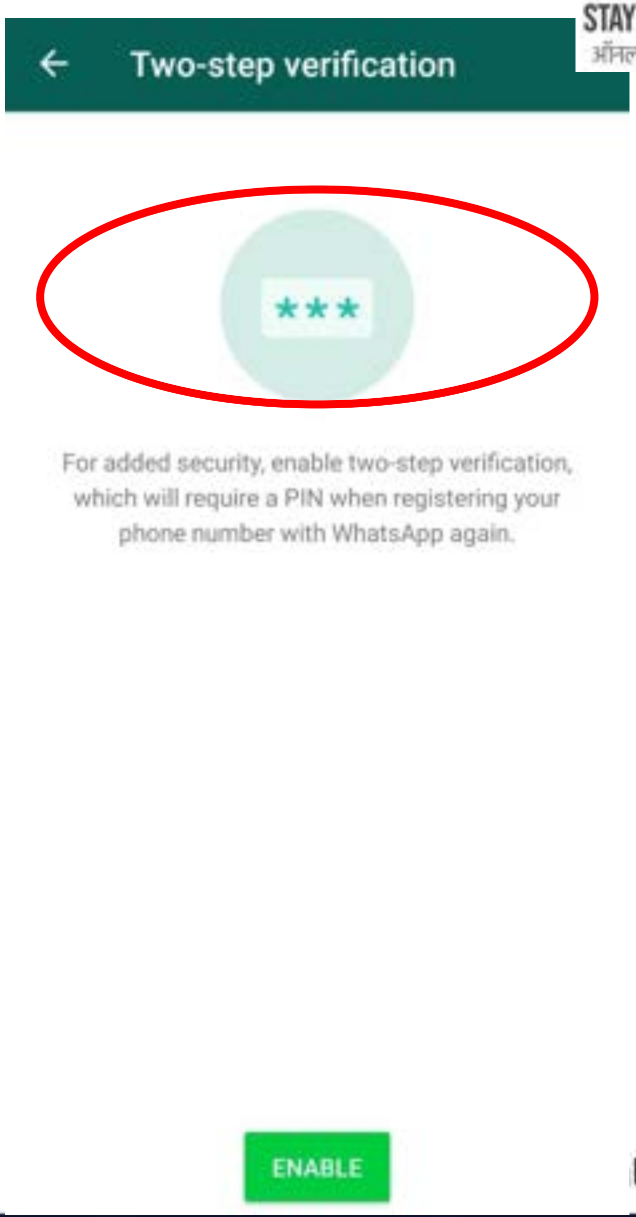
Security

Two-step verification

Change number

Request account info

Delete my account



← Two-step verification

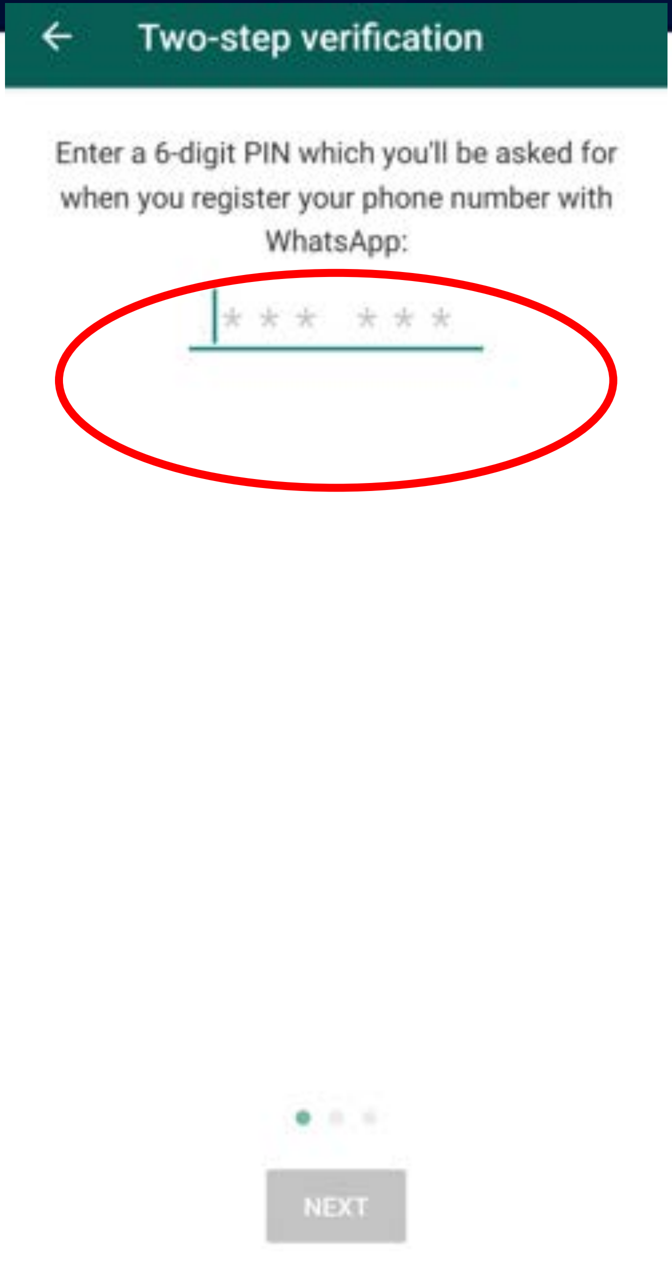
***

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

ENABLE

line.in

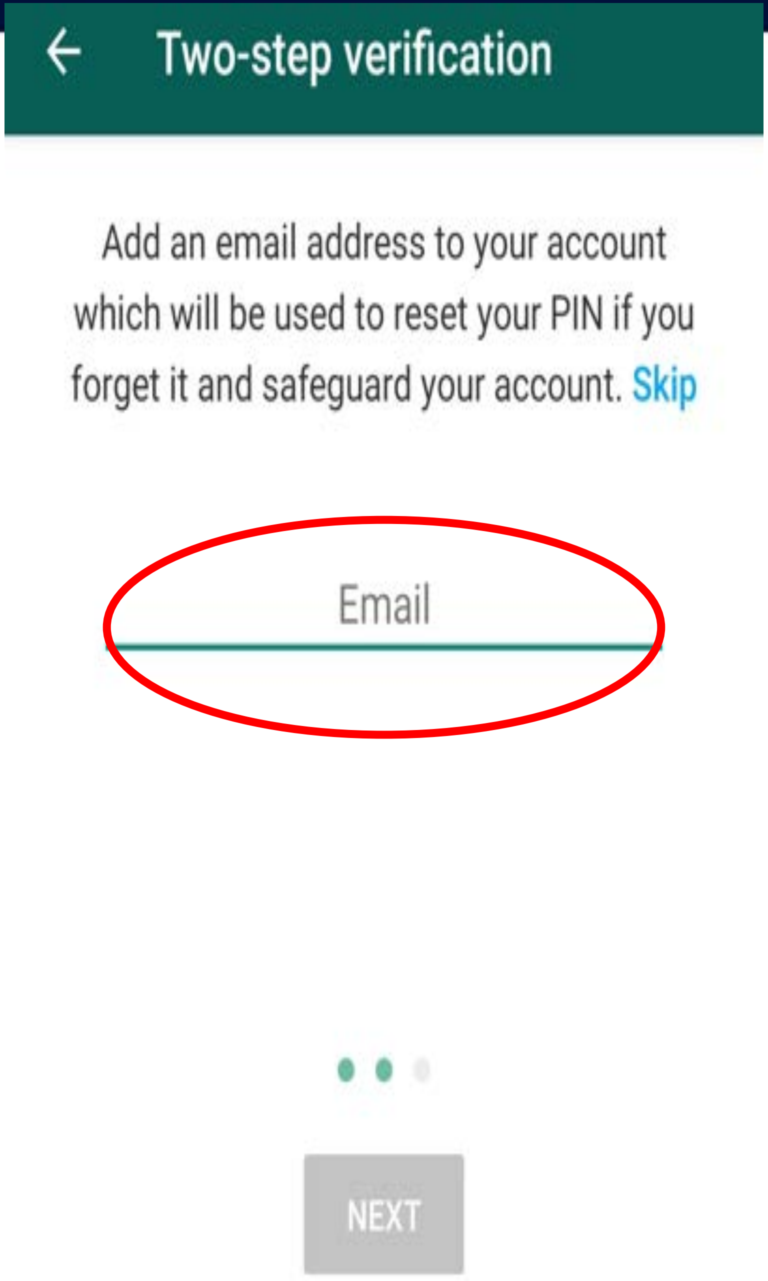
STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच



Two-step verification

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

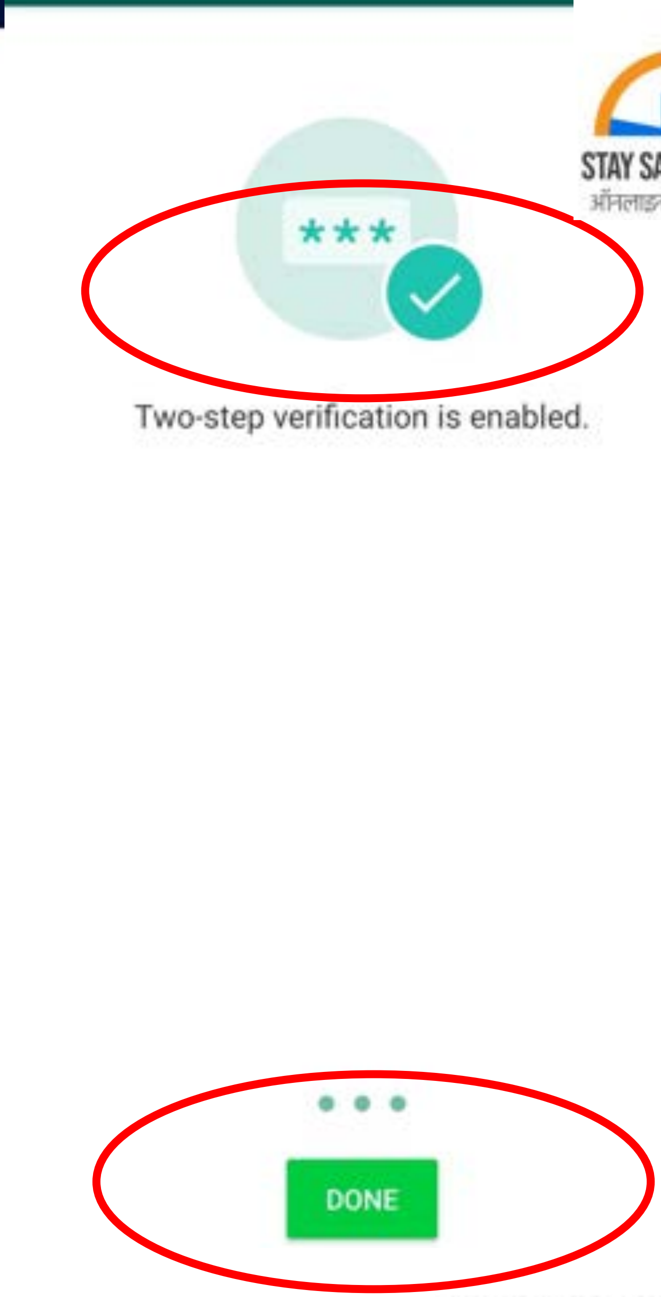
*** ***



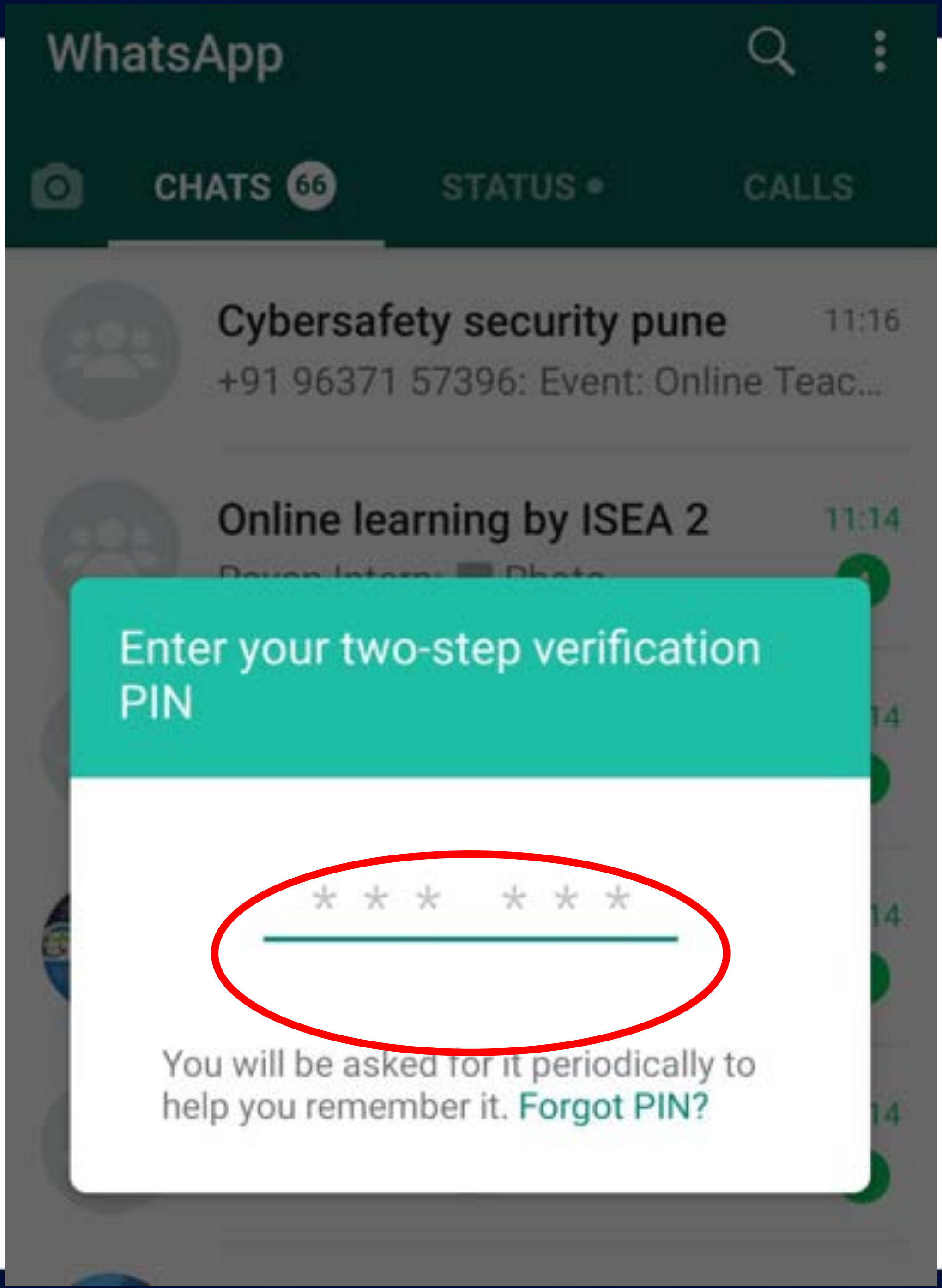
Two-step verification

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

Email



Two-step verification is enabled.



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

Online learning by ISEA 2 11:14

Enter your two-step verification PIN

* * * * * *

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

Tips to ensure a safer online social experience

Two-Factor Authentication (2FA): Enable 2FA whenever possible to add an extra layer of security to your accounts.

Be Skeptical of Strangers: Exercise caution when interacting with strangers online.

- Not everyone may have good intentions,
- Avoid sharing personal information with people you don't know well.

Think Before You Click: Be cautious about clicking on links or downloading attachments, especially from unknown sources.

- Phishing attempts or contain malware.

Regularly Update Software: Keep your computer, smartphone, and apps up to date with the latest security patches. Regular updates help protect against potential vulnerabilities.

Monitor Your Online Presence: Periodically review your online presence. Conduct a search on yourself to see what information is publicly available and make adjustments as needed.

Report and Block: If you encounter suspicious or harmful behavior online, report it to the platform administrators.

Educate Yourself: Stay informed about online safety practices and evolving threats.

Learning through Game

Learning through Game

Who is Secure??

Payal set her password as:
Daz^2l!n9Dan@p^R

Mihir set his password as:
Cdacpatna@2023

Learning through Game

Who is Smart..?

Babar Azam and Virat faces Financial Fraud

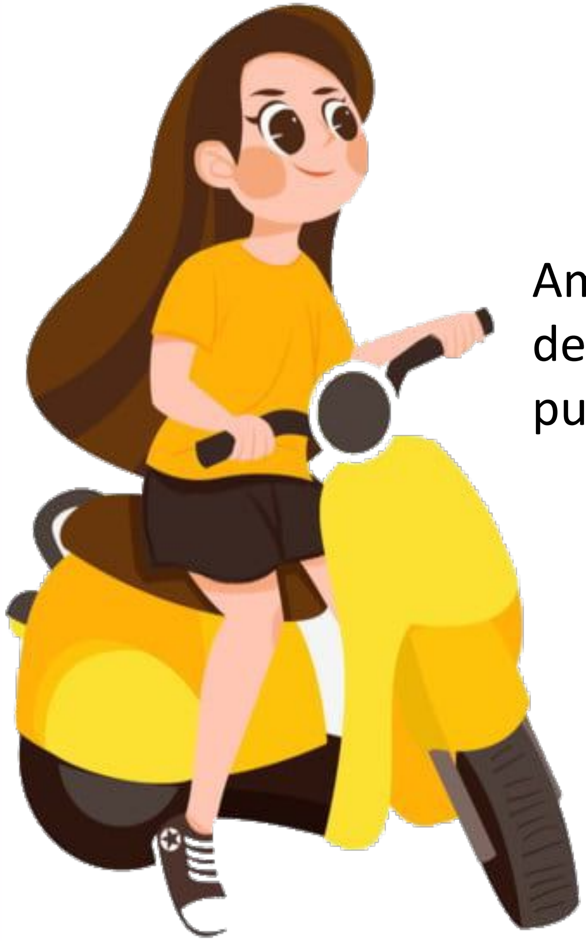
Babar Azam: Leave it yaar….report kiya to to media majak bana degi..log kya kahenge!!

Virat: Let’s immediately block the account and call 1930 in golden time

Learning through Game

Who is Smart..?

Social Media Photos Sharing



Ameesha: Post every photos with all details and keeps the account and album public

Sunny: Keeps and account private and post album with access rights

Who is Smart..?

Nidhi and Ajeet are reporters who received a email from Harvard University with an offer to deliver a lecture on reporting and ethics

Nidhi: click on the registration link and share all the details..She is excited to go and post it on social media

Ajeet: Verifies it by calling from official website and confirms before taking any action

STAY SAFE ONLINE

ऑनलाइन सुरक्षा कवच

Anti Virus

Don't share your mobile and confidential data

Strong Password and Pin

Don't Click on Unknown Links

Two-factor Authentication

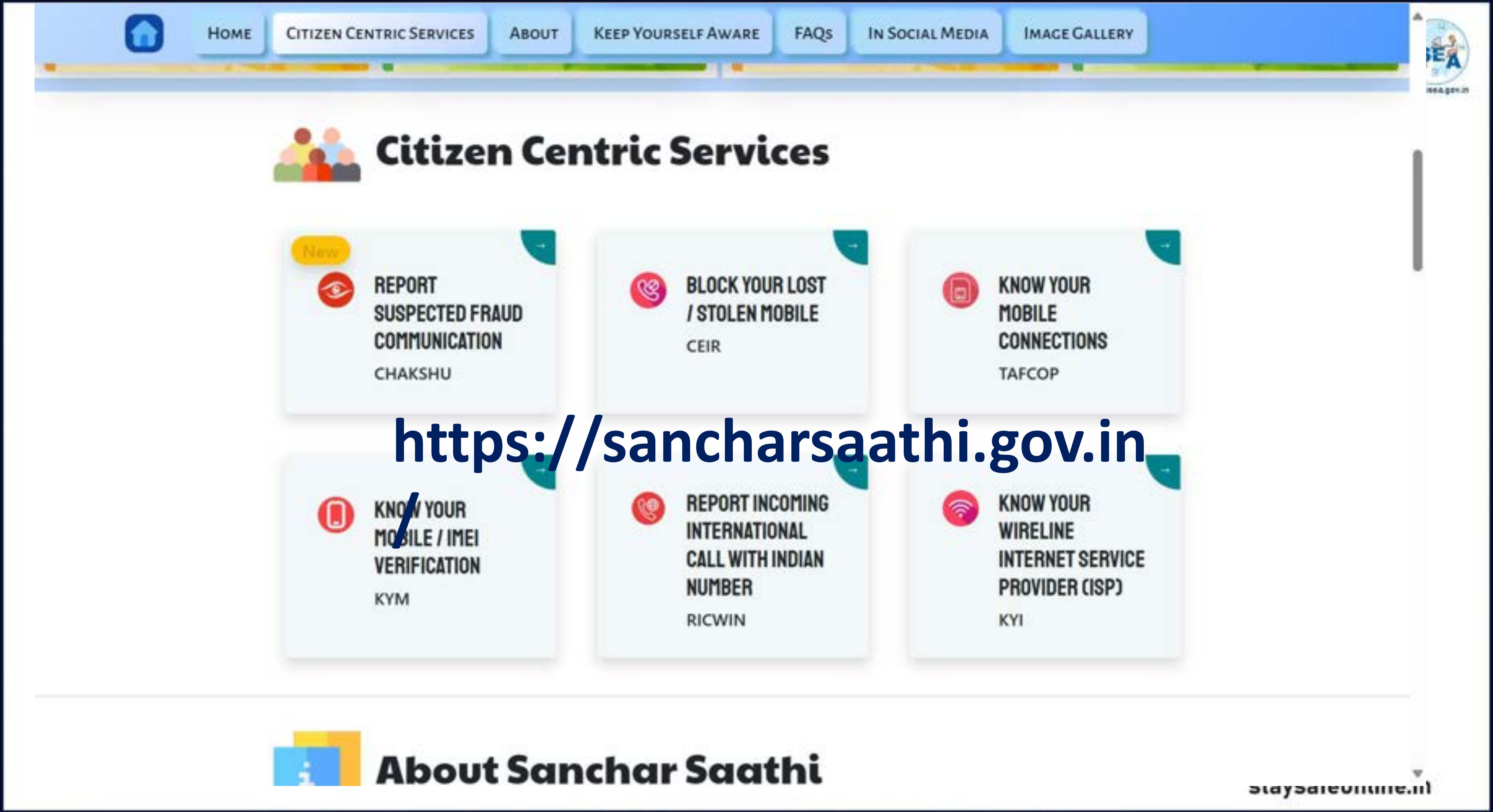
Don't install malicious apps

Stay Safe Online

Tool Kit

staysafeonline.in

Incident Reporting



Citizen Centric Services

REPORT SUSPECTED FRAUD COMMUNICATION
CHAKSHU

BLOCK YOUR LOST / STOLEN MOBILE
CEIR

KNOW YOUR MOBILE CONNECTIONS
TAFCOP

KNOW YOUR MOBILE / IMEI VERIFICATION
KYM

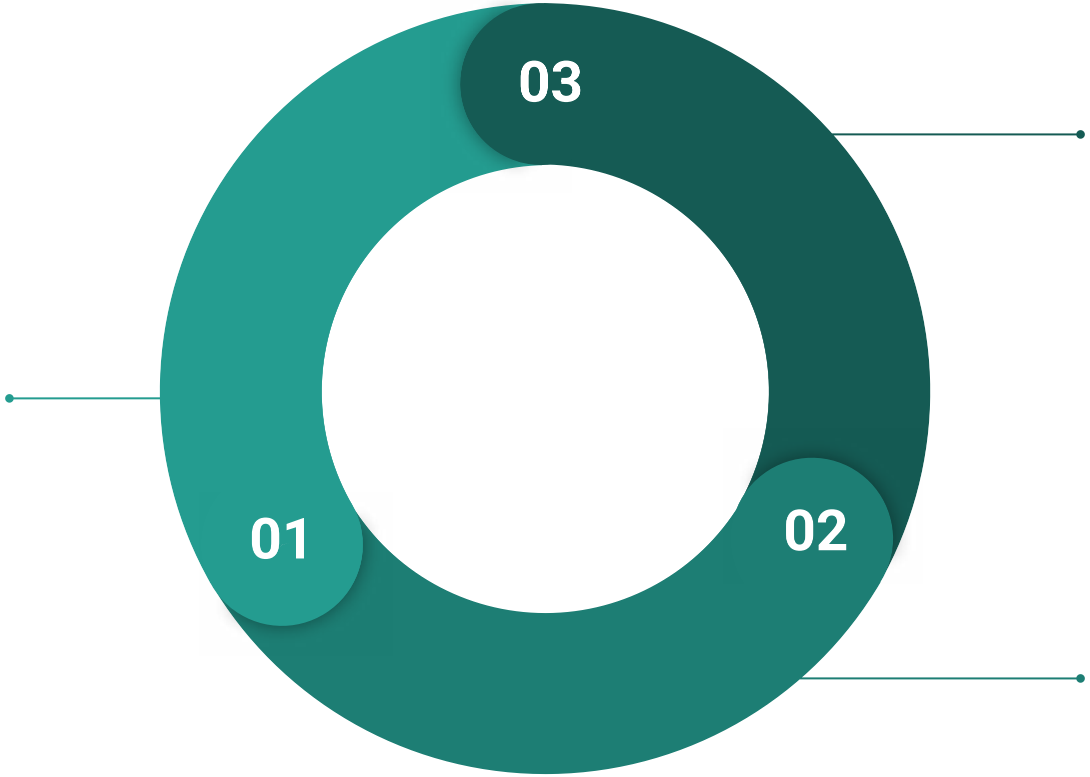
REPORT INCOMING INTERNATIONAL CALL WITH INDIAN NUMBER
RICWIN

KNOW YOUR WIRELINE INTERNET SERVICE PROVIDER (ISP)
KYI

About Sanchar Saathi

https://sancharsaathi.gov.in/

staysafeonline.in



Call ☎ **1930** (Helpline number)

to register any complaint about cybercrime.

You can also file your complaint 📝 online through **www.cybercrime.gov.in**

You can also file your complaint at the **nearest police station**

👮

www.isea.gov.in

staysafeonline.in

ISEA Whatsapp Number for Incident Reporting

+91 9490771800

Join our WhatsApp and Telegram Channel at

ISEA - Digital Naagrik

To Share Tips / Latest News, mail us to

isea@cdac.in

c/InformationSecurityAwareness

/company/information-security-awareness/

/infosecawarenesss/

/InfoSecAwa

/infosec_awareness/

/Informationsecuritytips/