Digital Transformation Finance Summit 2025

Use Cases & Studies
Mobile & Social Media Security

Scientist ‘E’
C-DAC Hyderabad

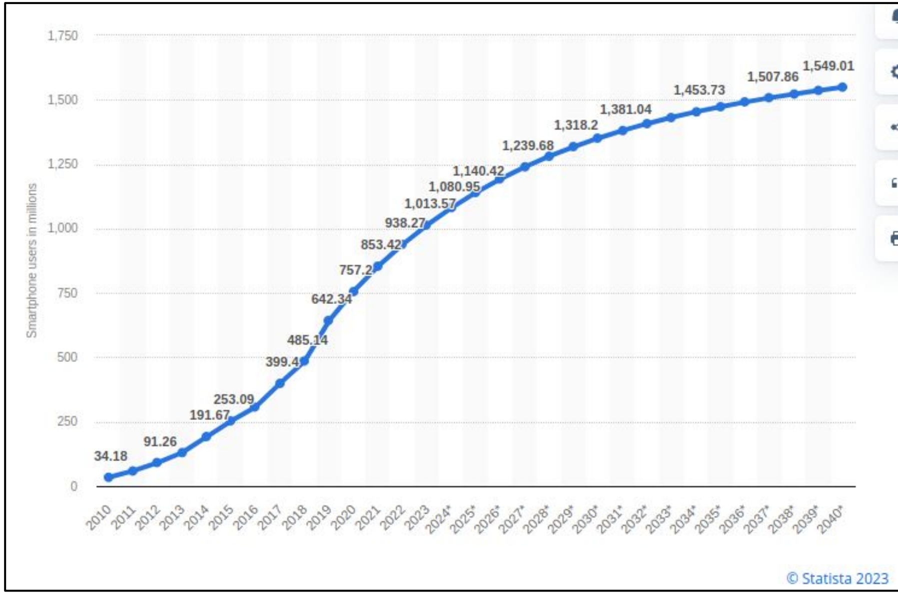
Agenda

- Introduction
- Some Recent Use Cases & Attacks
- Threat Modelling of a Mobile Application
- Secure Way of Using Smartphone
- Social Media Security
- Mobile Security Solutions @ C-DAC Hyderabad

Introduction

India's Smartphone Growth

- The smartphone sector in India is set to surpass one billion users in 2026 and anticipated to surge to 1.55 billion by 2040.
- This expansion highlights the widespread impact of smartphones, particularly in rapidly developing countries like India.
- Endpoints become vulnerable to various threats, including attacks and data breaches, due to exposure to unknown applications and networks



© Statista 2023

INDIA 2ND LARGEST AFTER CHINA

227m Rural India

205m Urban India

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

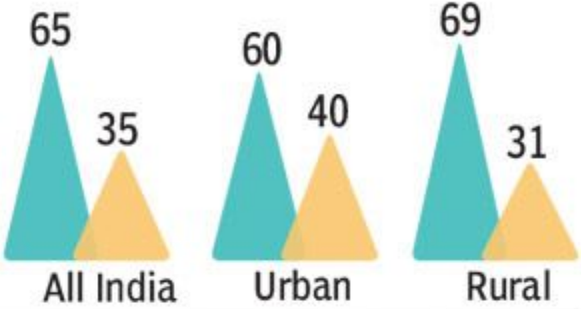
503m India

850m China

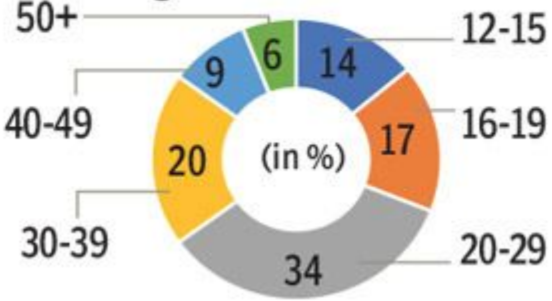
Source: IAMAI/Nielsen

Gender Distribution

(as %)



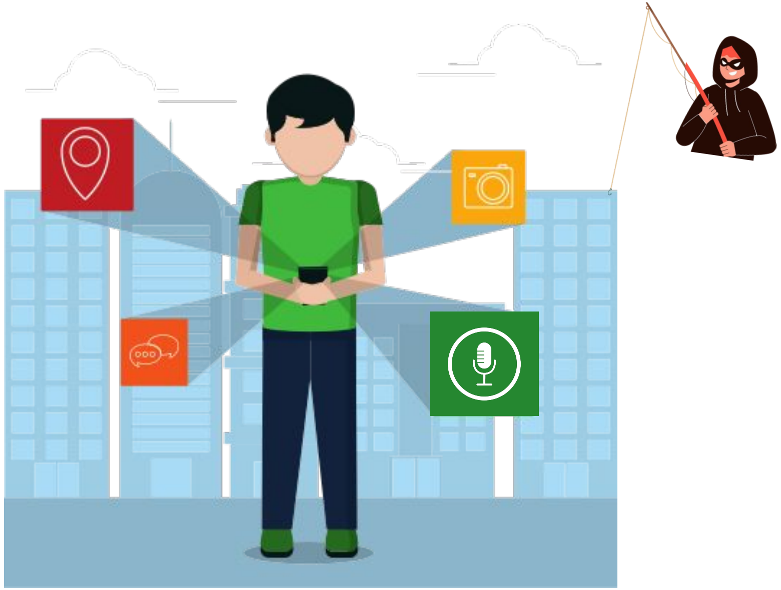
Age Distribution



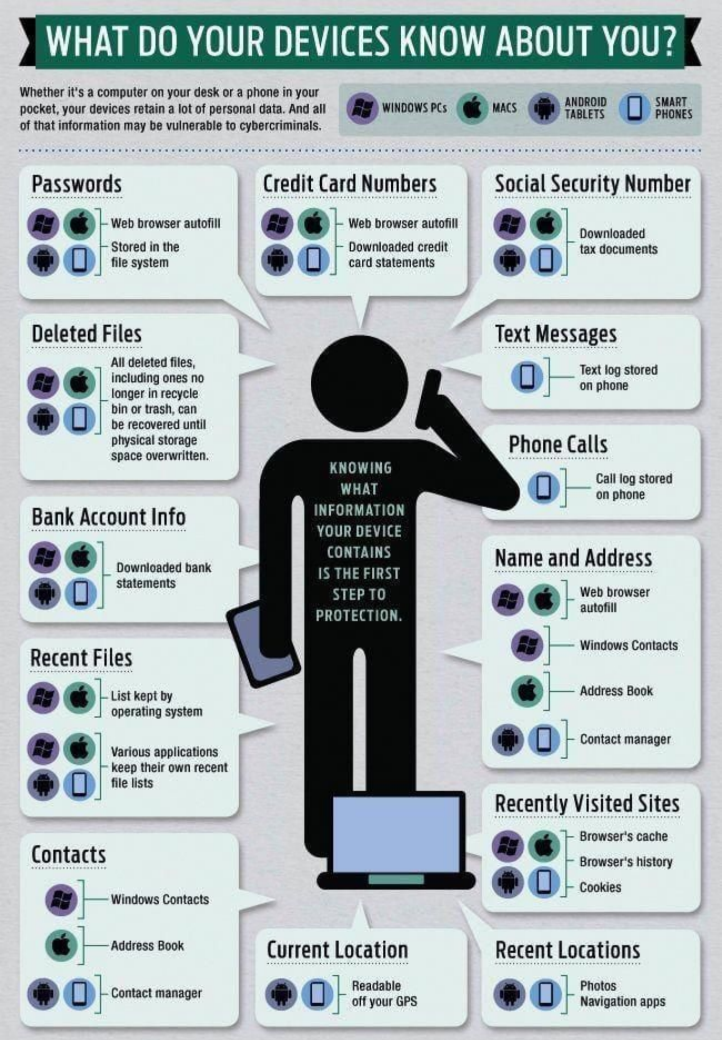
Mobile Applications Dominate the Country's Mobile Space

- 01 Banking and Finance
- 02 Health
- 03 E-commerce
- 04 Social Networks

Rise of Malicious Mobile Apps Amidst Large Scale Evolution



Our complete Personal Sensitive Information is carried by our smartphones



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

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

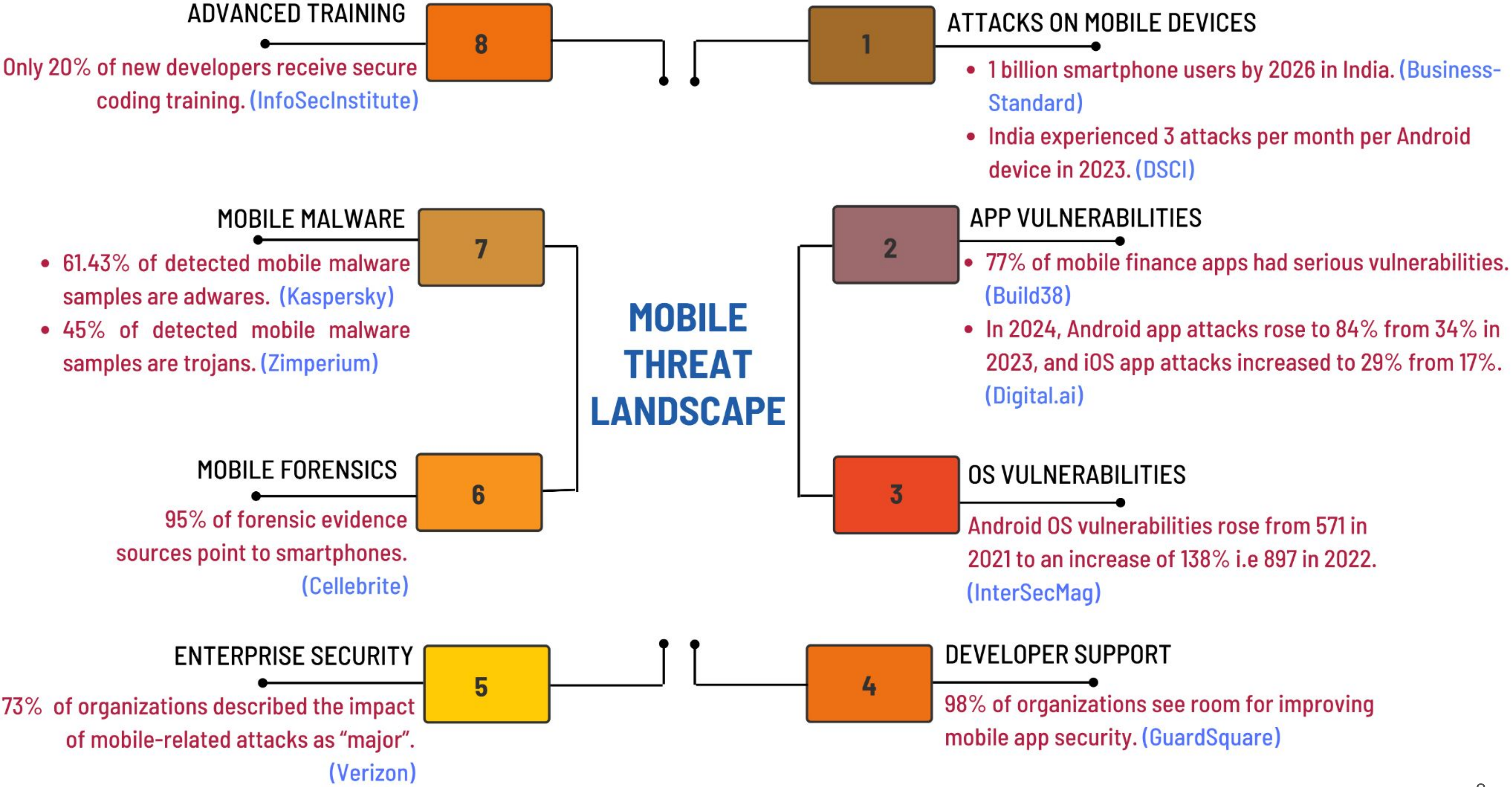
Recently Visited Sites
- Browser's cache
- Browser's history
- Cookies

Contacts
- Windows Contacts
- Address Book
- Contact manager

Current Location
- Readable off your GPS

Recent Locations
- Photos
- Navigation apps

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



MOBILE THREAT LANDSCAPE

1 ATTACKS ON MOBILE DEVICES

- 1 billion smartphone users by 2026 in India. (Business-Standard)
- India experienced 3 attacks per month per Android device in 2023. (DSCI)

2 APP VULNERABILITIES

- 77% of mobile finance apps had serious vulnerabilities. (Build38)
- In 2024, Android app attacks rose to 84% from 34% in 2023, and iOS app attacks increased to 29% from 17%. (Digital.ai)

3 OS VULNERABILITIES

Android OS vulnerabilities rose from 571 in 2021 to an increase of 138% i.e 897 in 2022. (InterSecMag)

4 DEVELOPER SUPPORT

98% of organizations see room for improving mobile app security. (GuardSquare)

5 ENTERPRISE SECURITY

73% of organizations described the impact of mobile-related attacks as “major”. (Verizon)

6 MOBILE FORENSICS

95% of forensic evidence sources point to smartphones. (Cellebrite)

7 MOBILE MALWARE

- 61.43% of detected mobile malware samples are adwares. (Kaspersky)
- 45% of detected mobile malware samples are trojans. (Zimperium)

8 ADVANCED TRAINING

Only 20% of new developers receive secure coding training. (InfoSecInstitute)

Some Use Cases & Recent Attacks

Keshod trader loses 1.8L to cyberfraud via fake app

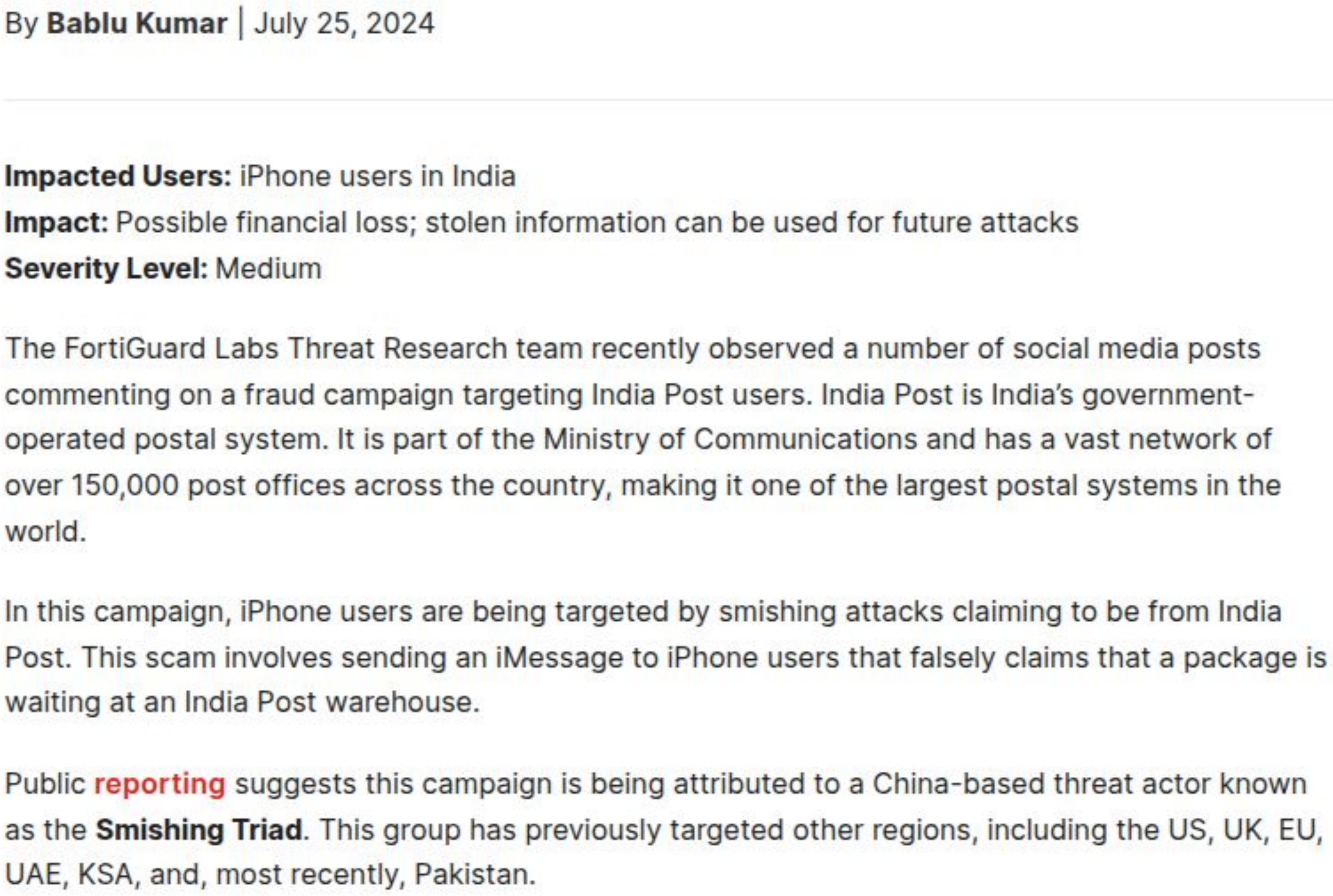
Jul 26, 2025, 00:08 IST

Share AA Follow Us

Rajkot: A trader from Keshod in Junagadh district lost Rs 1.8 lakh after falling victim to a cyber fraud involving a fake mobile application.

According to the FIR registered at the Junagadh Range Cyber police station, Patel received a WhatsApp message on Feb 25, 2025, containing a link to an application falsely claiming to be related to his bank's Aadhaar update process. Believing it to be genuine, Patel downloaded and installed the app on his mobile phone. However, upon suspecting the app to be fraudulent, he quickly uninstalled it.

Soon after, he began receiving SMS alerts from his bank about unauthorised transactions, amounting to Rs 1.8 lakh. Police suspect that the fake app may have granted remote access to Patel's phone or banking credentials, enabling the cybercriminals to carry out the theft.



By **Bablu Kumar** | July 25, 2024

Impacted Users: iPhone users in India
Impact: Possible financial loss; stolen information can be used for future attacks
Severity Level: Medium

The FortiGuard Labs Threat Research team recently observed a number of social media posts commenting on a fraud campaign targeting India Post users. India Post is India's government-operated postal system. It is part of the Ministry of Communications and has a vast network of over 150,000 post offices across the country, making it one of the largest postal systems in the world.

In this campaign, iPhone users are being targeted by smishing attacks claiming to be from India Post. This scam involves sending an iMessage to iPhone users that falsely claims that a package is waiting at an India Post warehouse.

Public reporting suggests this campaign is being attributed to a China-based threat actor known as the **Smishing Triad**. This group has previously targeted other regions, including the US, UK, EU, UAE, KSA, and, most recently, Pakistan.

Mumbai police constable loses money after opening malicious file from WhatsApp group

Jul 29, 2025, 20:43 IST

Share AA Follow Us

Mumbai: A 36-year-old police constable from the Trombay police station lost Rs 7.54 lakh after opening a malicious APK file shared in an official WhatsApp group, Mohalla Committee Trombay. An FIR was registered against unidentified cyber criminals for cheating and data theft.

The victim, Sachin Kashid, serving with the police since 2016, received a file titled ‘RTO Challan.apk' in the group on July 22. The file was shared by a member whose phone was unknowingly compromised.

Kashid clicked on it, after which his mobile phone was hacked. Shortly, fraudulent loan transactions began reflecting in his HDFC Bank salary account. A personal loan of Rs 7.58 lakh was sanctioned in his name without his consent, and within minutes, Rs 4.99 lakh and Rs 2.55 lakh were siphoned off to a payment system labelled ‘CCAHPPAY'.

Former loan recovery agent arrested for extortion, blackmail scam via apps; police say pan-India racket exposed

TNN / Jul 14, 2025, 05:28 IST

Share AA Follow Us

Pune: A 29-year-old resident of Vashi in Navi Mumbai has been arrested by the Pimpri Chinchwad police in connection with cheating and blackmailing people through fake loan apps, which he allegedly executed on the instructions of handlers based in Singapore.

The arrest, said the police, throws open a pan-India loan fraud racket.

Accused Isaki Thevar of Vashi, who worked as a loan recovery agent, has been duping people through at least eight fake loan apps, police officers told TOI, adding that the apps have at least 10,000 complaints registered against them across the country as determined from the national cybercrime portal.

You Can Also Check: Pune AQI | Weather in Pune | Bank Holidays in Pune | Public Holidays in Pune

Investigations further revealed that the suspect and his handlers used Pakistani cellphone numbers to cheat and blackmail several victims.

Goldoson

- Goldoson is an Android adware integrated into a third-party library used unknowingly by legitimate app developers
- It was found in over 60 apps with a cumulative download count exceeding 100 million globally, including well-known apps
- Goldoson collects sensitive information, including:
    - List of installed apps
    - GPS location history
    - Data from WiFi and Bluetooth-connected devices
- Collected data is sent to a remote server every two days for processing

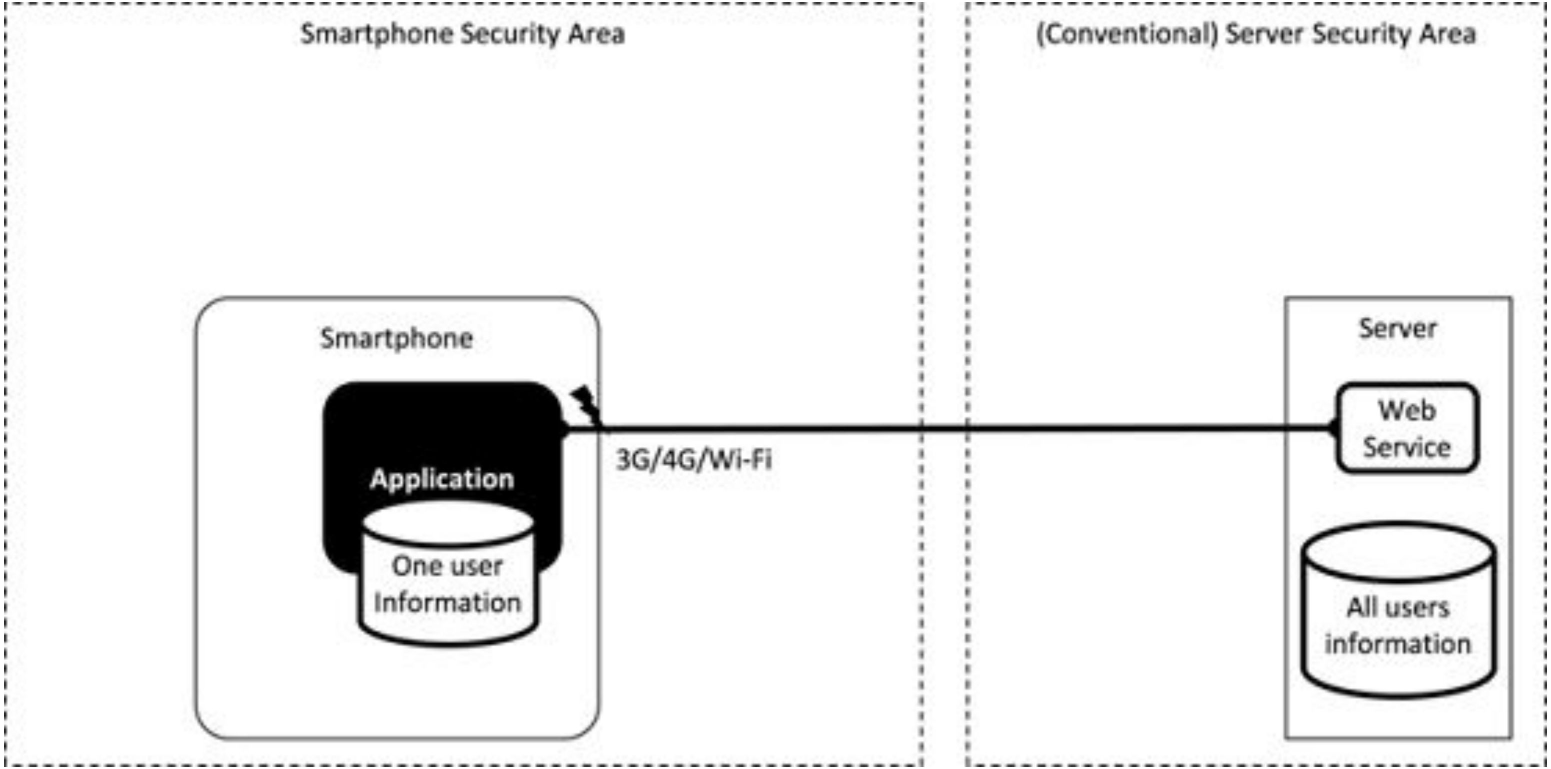
Threat Modelling of Mobile Applications

Threat Modelling of a Mobile Application

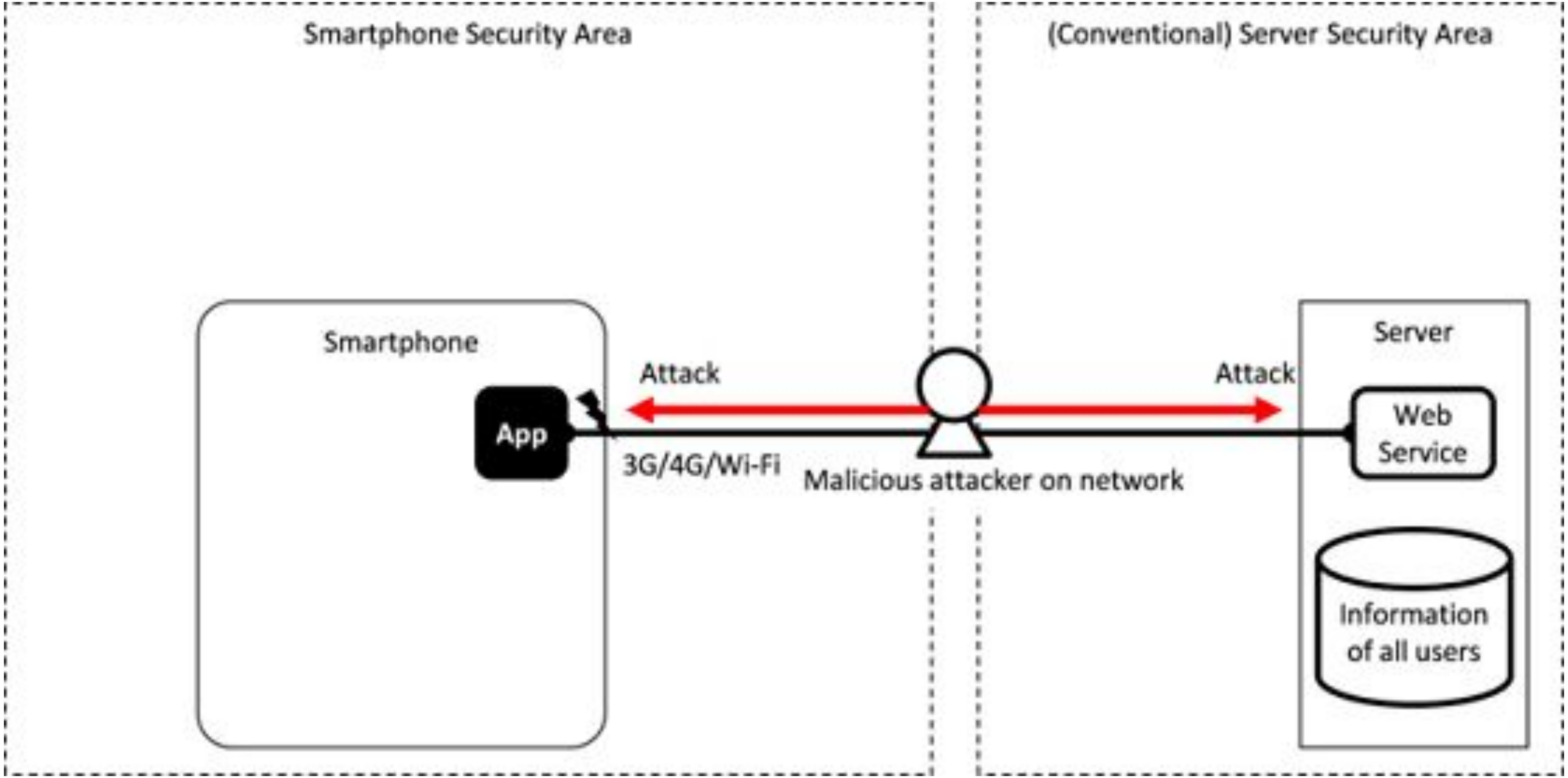
- Threat modeling is a structured approach used in security analysis to identify, evaluate, and address potential threats and vulnerabilities in an application, system, or infrastructure before they can be exploited.

- When it comes to a mobile application, threat modeling can help identify potential vulnerabilities and design flaws, and determine the appropriate security controls to protect against them.

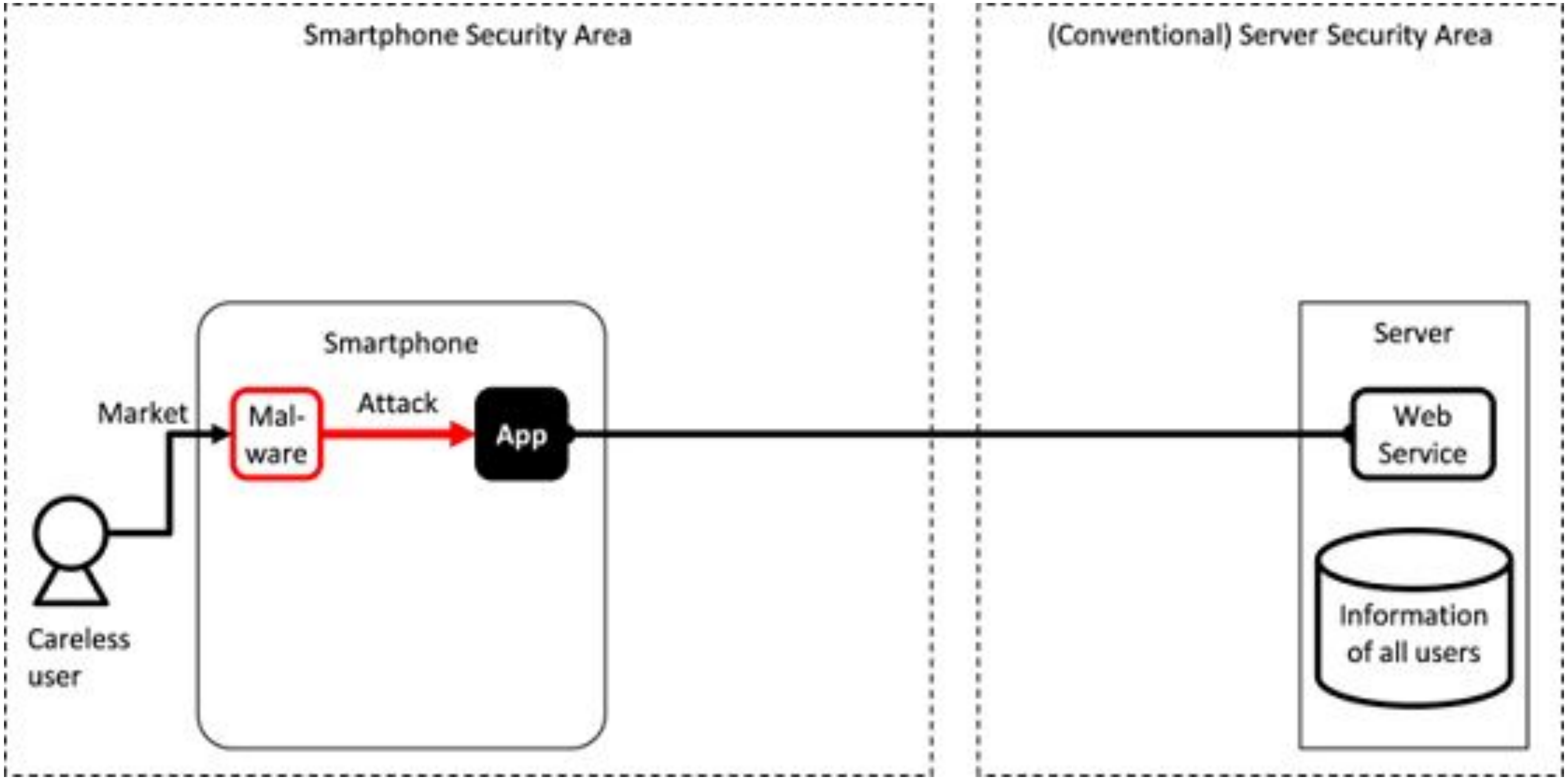
Typical Mobile Application Behaviour



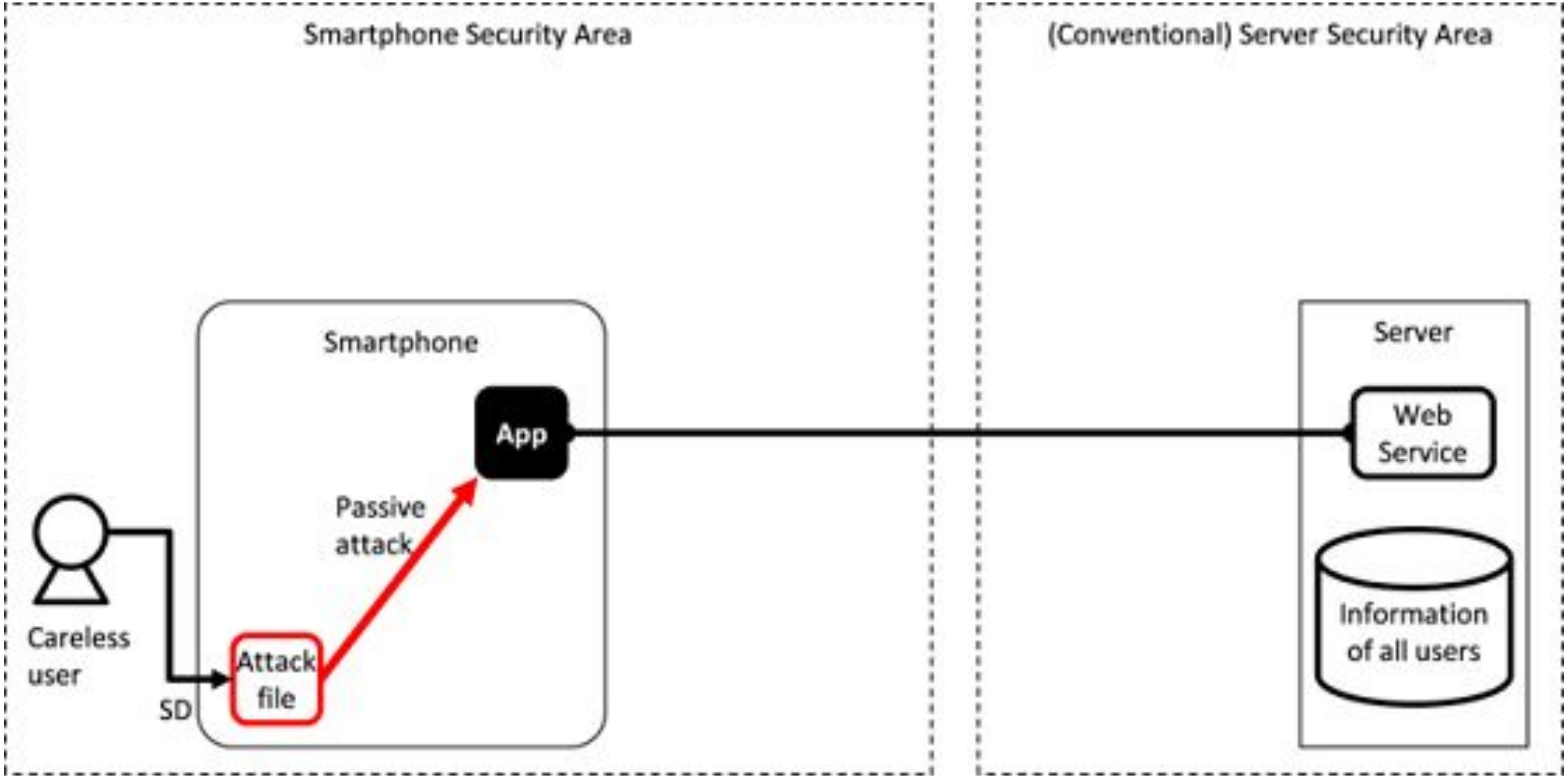
Network Based Third-Party



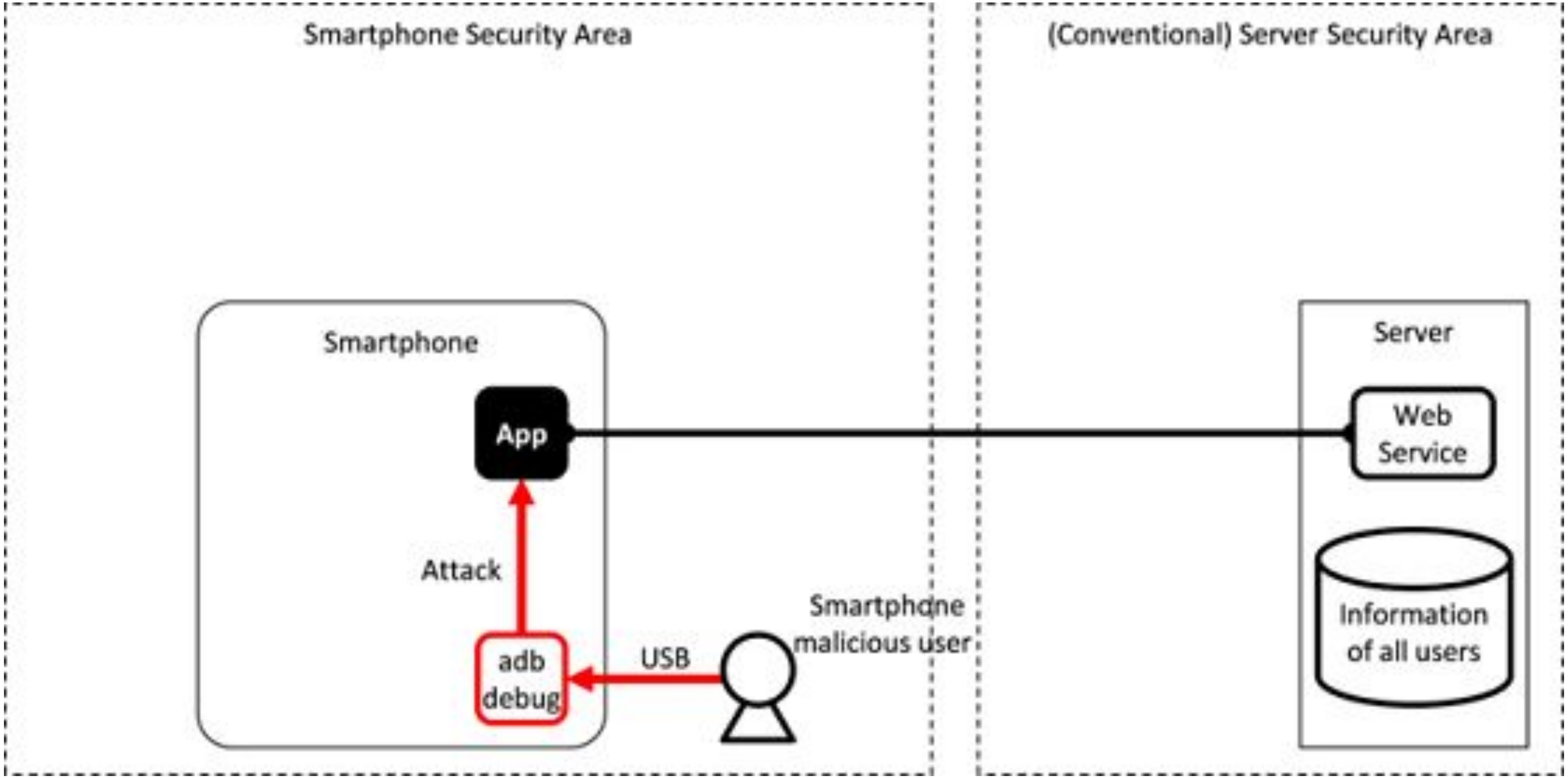
User Installed Malware



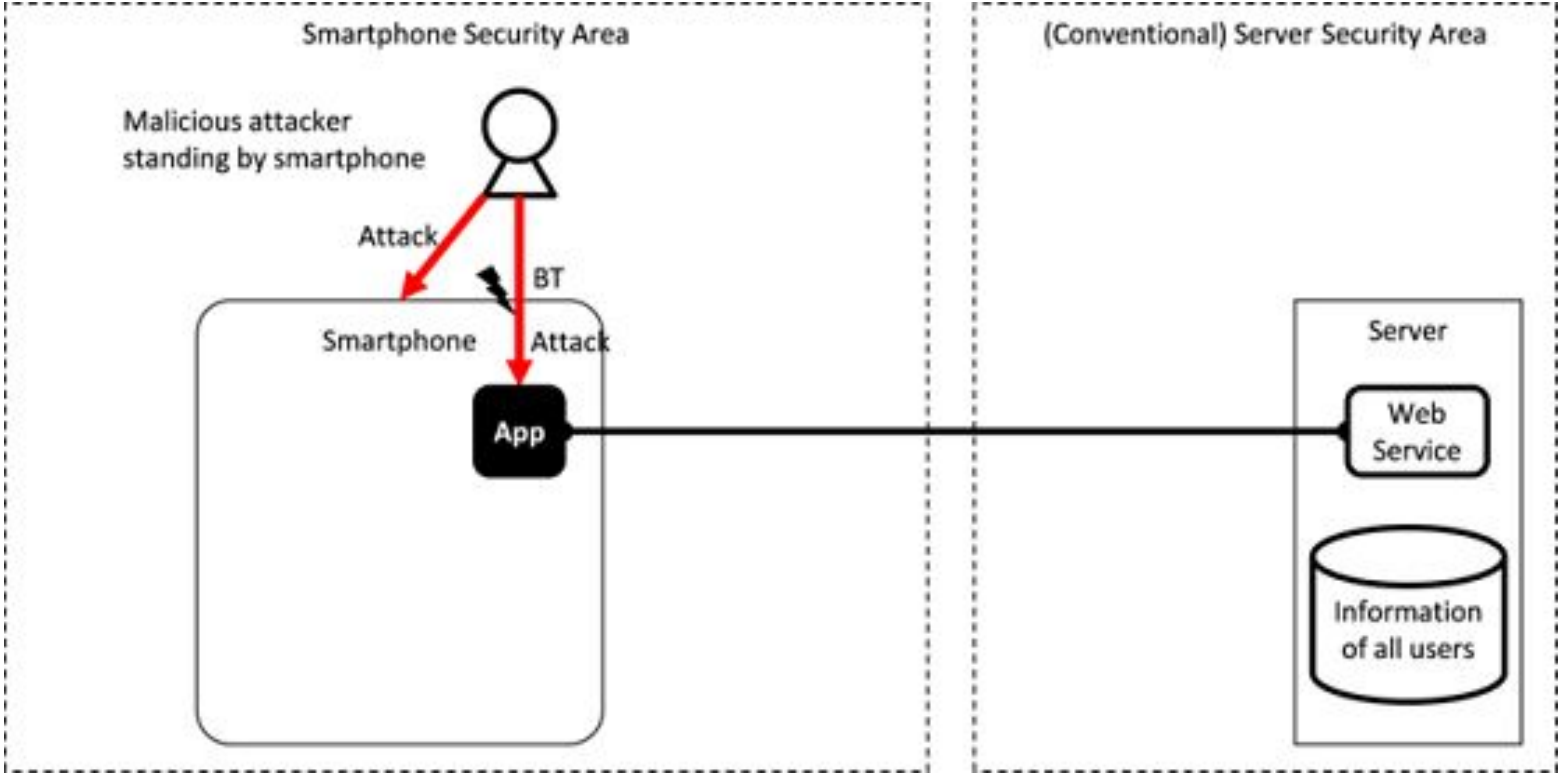
Malicious File Exploiting Vulnerabilities



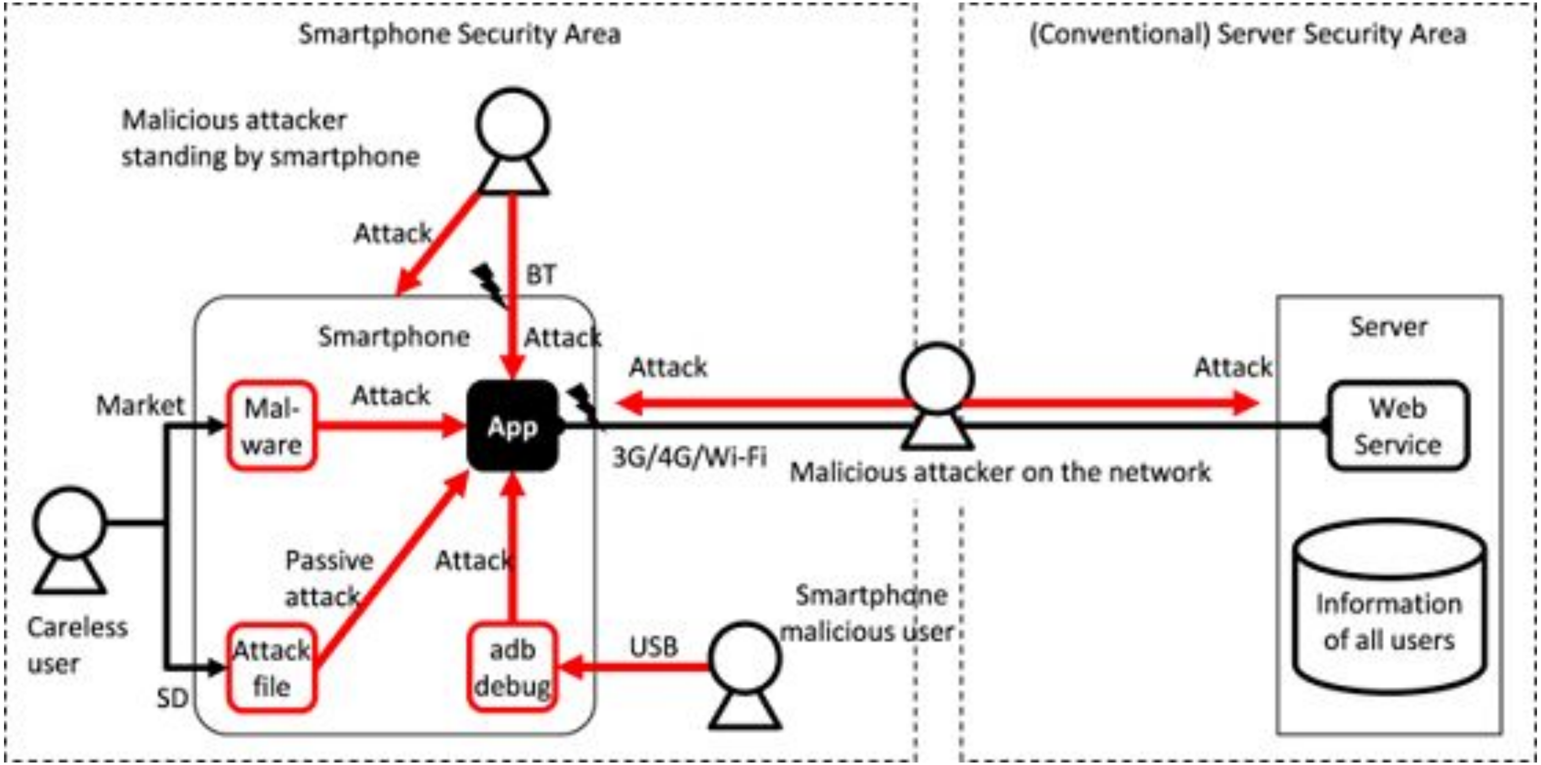
Malicious User



Third parties in the proximity



Summary of Threats



Secure way of using Smart Phone

Critical Features of your mobile

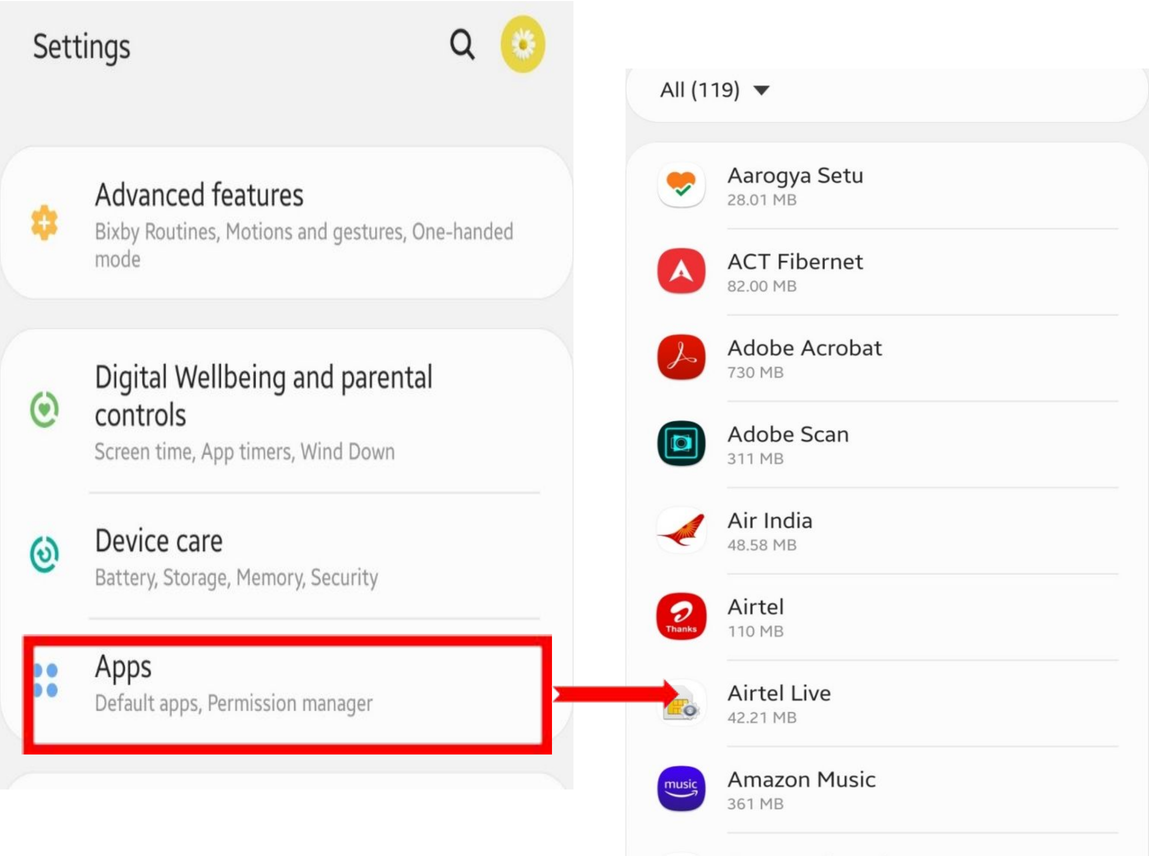
- Messaging – OTP , password reset codes etc.,
- Camera
- Microphone
- Gallery
- Contacts
- Location

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

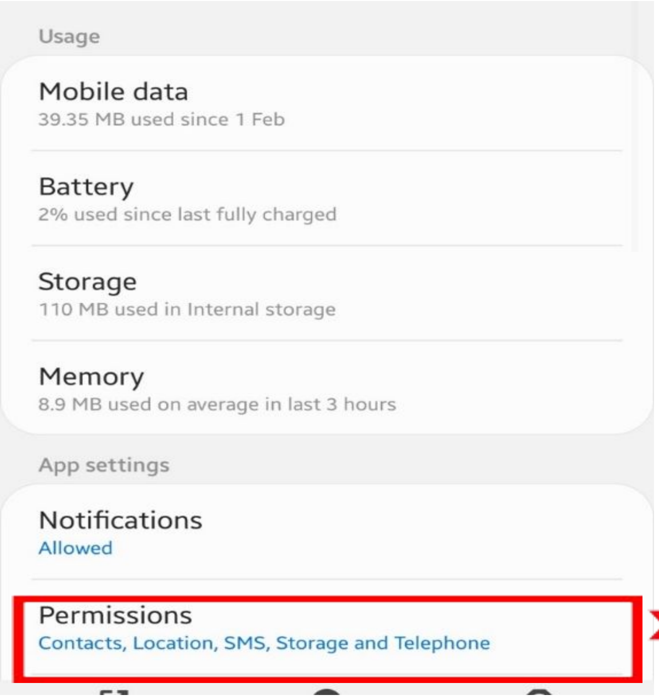
Air India
48.58 MB

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

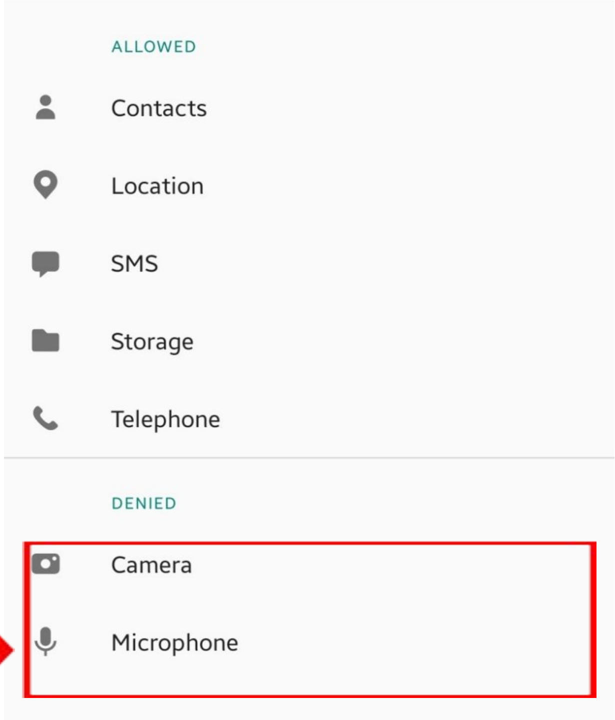
Storage
110 MB used in Internal storage

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

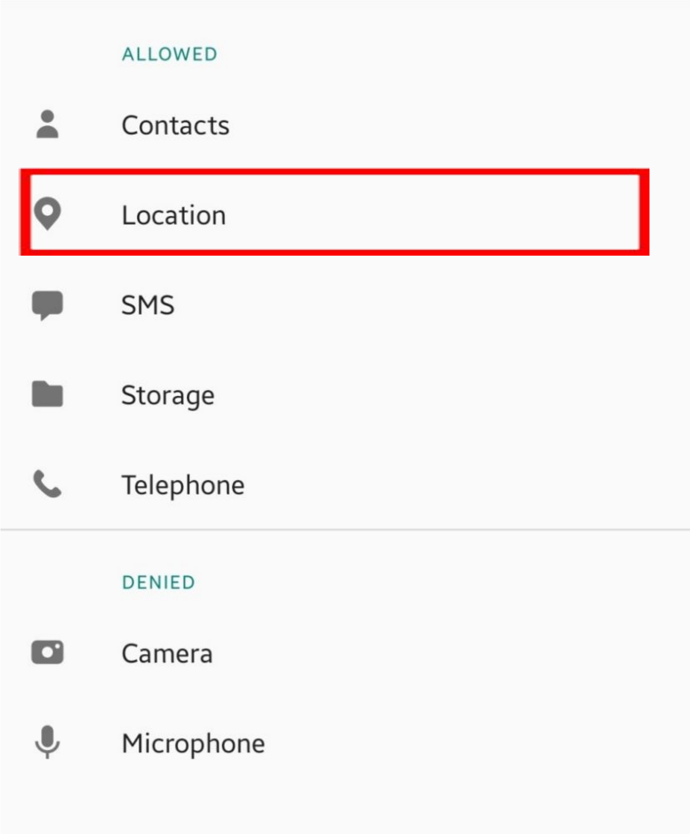
DENIED

Camera

Microphone

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

Monitor Permissions

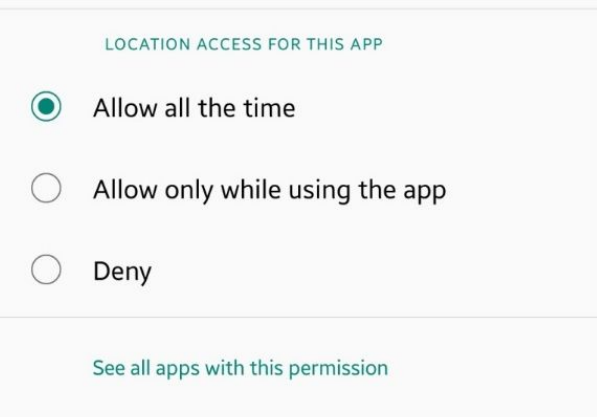


ALLOWED

- Contacts
- Location
- SMS
- Storage
- Telephone

DENIED

- Camera
- Microphone



LOCATION ACCESS FOR THIS APP

● Allow all the time

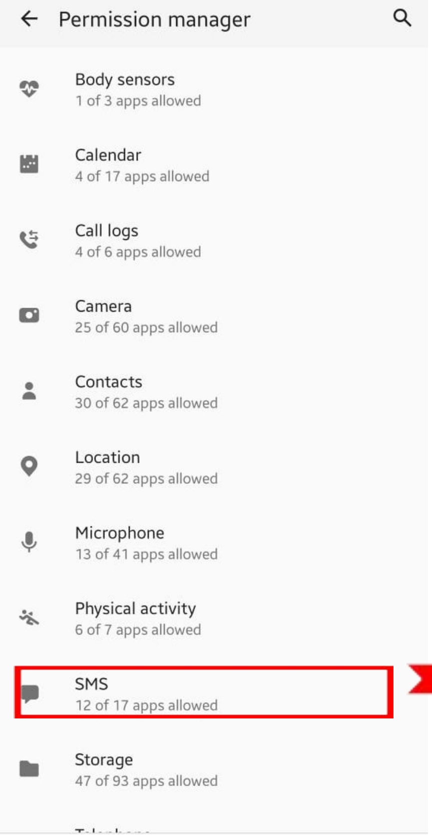
○ Allow only while using the app

○ Deny

See all apps with this permission

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

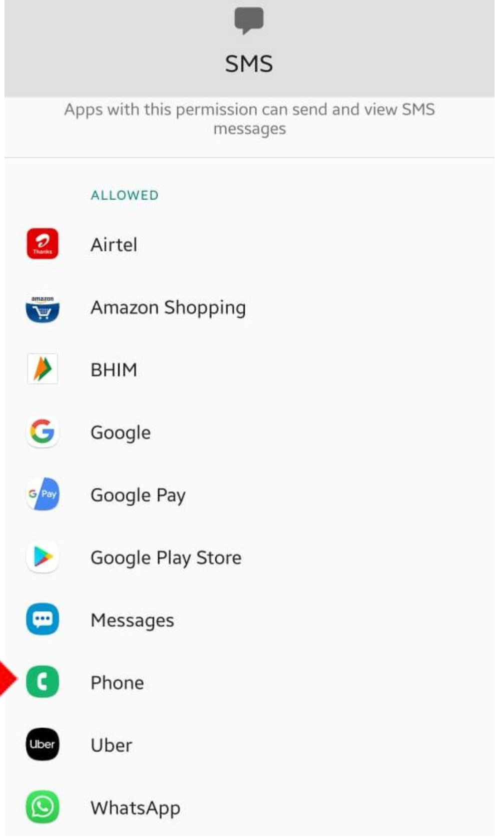
Microphone
13 of 41 apps allowed

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

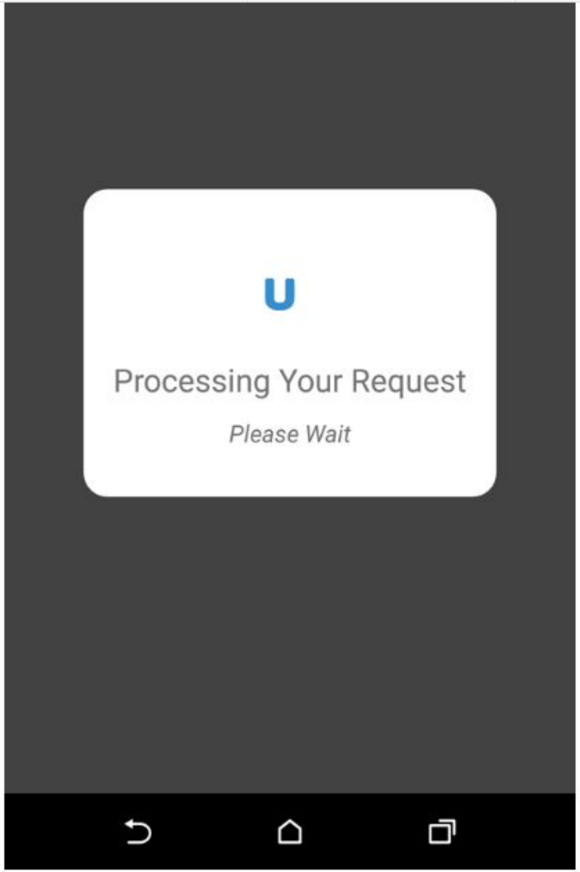
WhatsApp

Warning sign

- If OTP is filled automatically by your application while performing any transaction or filling any page, it means that the app is having permissions to read your SMS automatically.

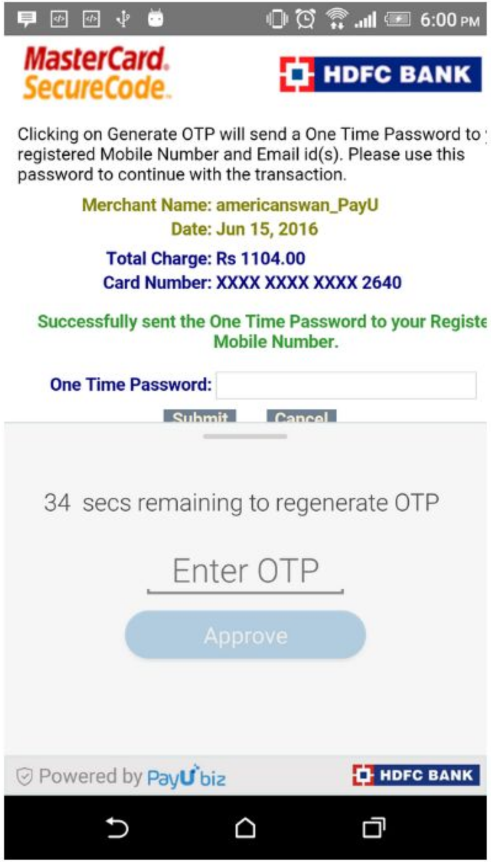
- If in your browser without entering your credentials, you are able to see the logged in state of website, it means you browser saved your credentials

OTP Autofill looks like



Processing Your Request

Please Wait



Clicking on Generate OTP will send a One Time Password to registered Mobile Number and Email id(s). Please use this password to continue with the transaction.

Merchant Name: americanswan_PayU
Date: Jun 15, 2016

Total Charge: Rs 1104.00
Card Number: XXXX XXXX XXXX 2640

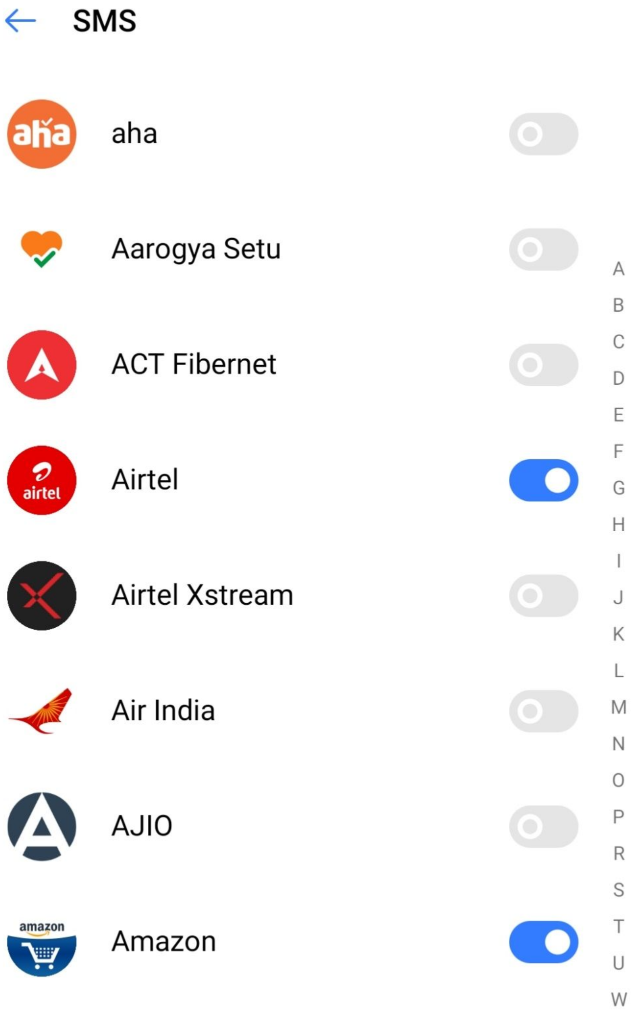
Successfully sent the One Time Password to your Registe
Mobile Number.

One Time Password:

34 secs remaining to regenerate OTP

Enter OTP

Removal of SMS permission



SMS

aha ○

Aarogya Setu ○

ACT Fibernet ○

Airtel ●

Airtel Xstream ○

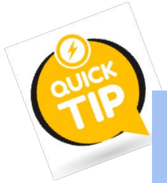
Air India ○

AJIO ○

Amazon ●

Installing Apps

- Advertisements could be one of the medium to bring malware to your mobiles or steal personal information
- Sometimes, App download page itself states that it contains advertisements or you can see the reviews to know if it contains advertisements
- Reviews also can help understand Good and Bad about apps

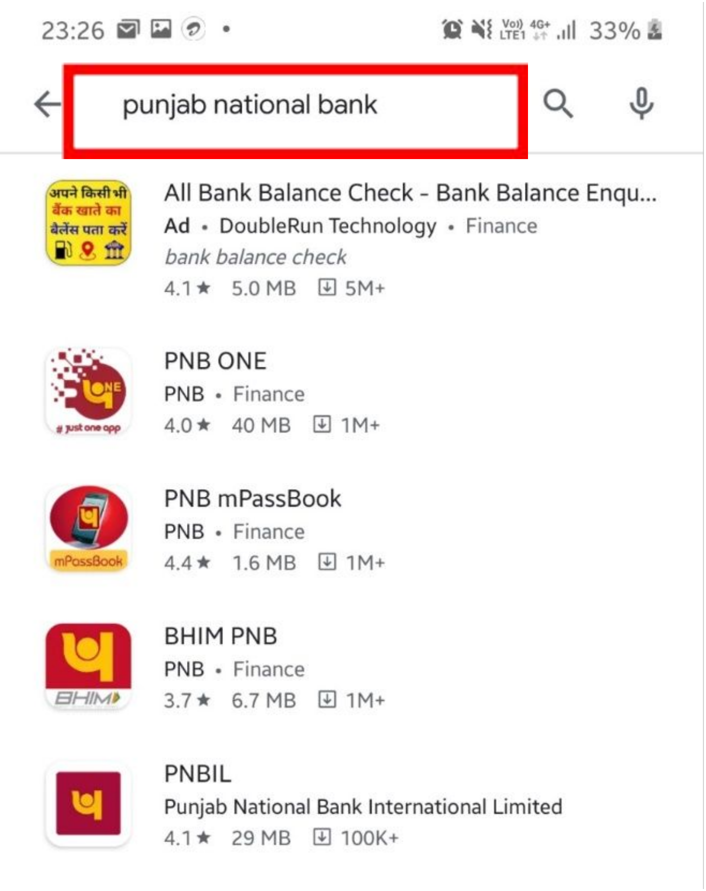


Avoid installing apps which contains advertisements and read reviews before installing

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 owned website rather than searching in the stores.

Example – search for PNB banking app



23:26 33%

punjab national bank

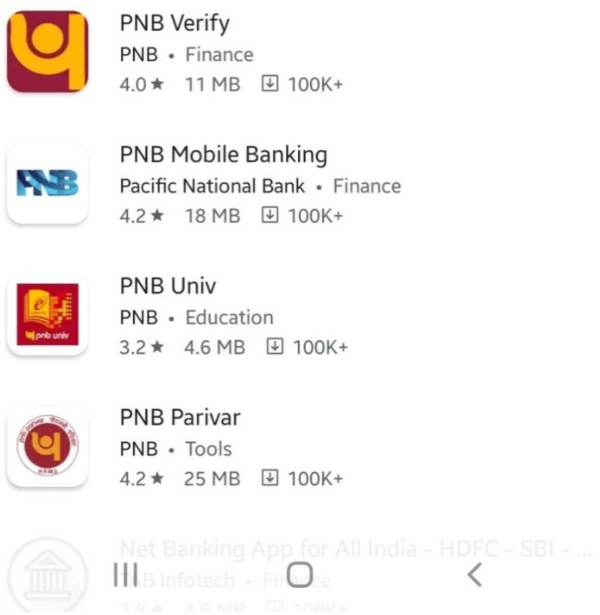
All Bank Balance Check - Bank Balance Enqu...
Ad • DoubleRun Technology • Finance
bank balance check
4.1★ 5.0 MB 5M+

PNB ONE
PNB • Finance
4.0★ 40 MB 1M+

PNB mPassBook
PNB • Finance
4.4★ 1.6 MB 1M+

BHIM PNB
PNB • Finance
3.7★ 6.7 MB 1M+

PNBIL
Punjab National Bank International Limited
4.1★ 29 MB 100K+



PNB Verify
PNB • Finance
4.0★ 11 MB 100K+

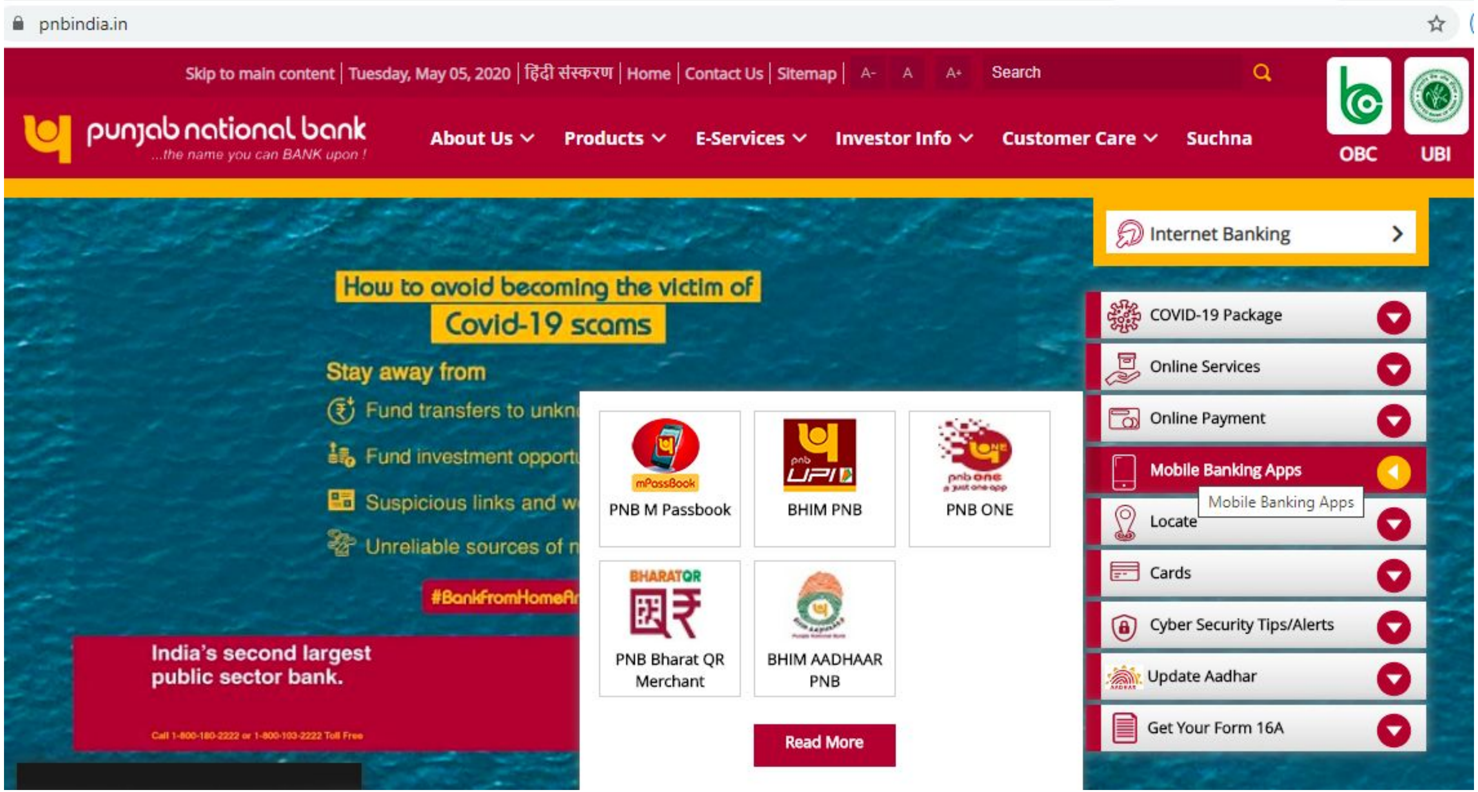
PNB Mobile Banking
Pacific National Bank • Finance
4.2★ 18 MB 100K+

PNB Univ
PNB • Education
3.2★ 4.6 MB 100K+

PNB Parivar
PNB • Tools
4.2★ 25 MB 100K+

Net Banking App for All India - HDFC - SBI - ...
B Infotech • Finance

Example - Link from Original Bank website



pnbindia.in

Skip to main content | Tuesday, May 05, 2020 | हिंदी संस्करण | Home | Contact Us | Sitemap | A- A A+ Search

punjab national bank ...the name you can BANK upon !

About Us | Products | E-Services | Investor Info | Customer Care | Suchna

OBC UBI

Internet Banking

How to avoid becoming the victim of Covid-19 scams

Stay away from

- Fund transfers to unkn
- Fund investment opport
- Suspicious links and w
- Unreliable sources of n

#BankfromHomeA

India's second largest public sector bank.

Call 1-800-180-2222 or 1-800-103-2222 Toll Free

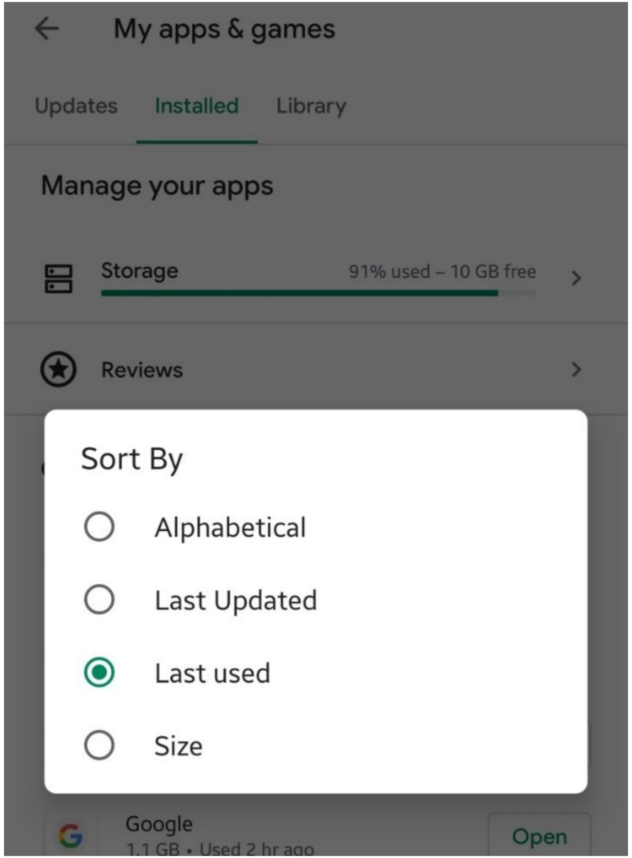
- PNB M Passbook
- BHIM PNB
- PNB ONE
- PNB Bharat QR Merchant
- BHIM AADHAAR PNB

Read More

- COVID-19 Package
- Online Services
- Online Payment
- Mobile Banking Apps
- Locate
- Cards
- Cyber Security Tips/Alerts
- Update Aadhar
- Get Your Form 16A

Unused Apps

- Monitor your mobile for unused apps – Look in play store by sorting with Last used to know which apps were not used by you since long time.



Sort By

○ Alphabetical

○ Last Updated

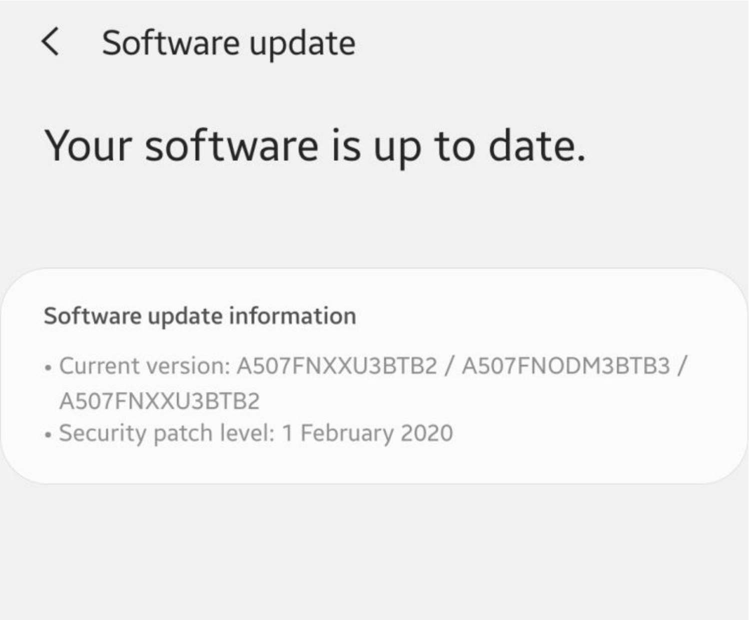
● Last used

○ Size

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

Safe Mobile Usage - Recap

1. Regularly Monitor the permissions of critical features of your mobile

2. Avoid installing apps which contains advertisements and read reviews before installing

3. Download apps from genuine link

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

Tips for your daily practice

1. Turn OFF Bluetooth and WiFi when not in use

2. Set time limit and Lock mobile automatically when not in use

3. Prefer PIN/ finger print / face recognition locks as supported by your mobile.

4. Pattern lock are to be avoided - beware of shoulder surfing , screen reading.

5. 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

Signs of Infected Device

- Device overheating
- Rapid battery drainage
- Excessive internet usage without active apps running

STAY SAFE ONLINE

ऑनलाइन सुरक्षा कवच

Anti Virus

Don't Click on Unknown Links

Don't share your mobile and confidential data

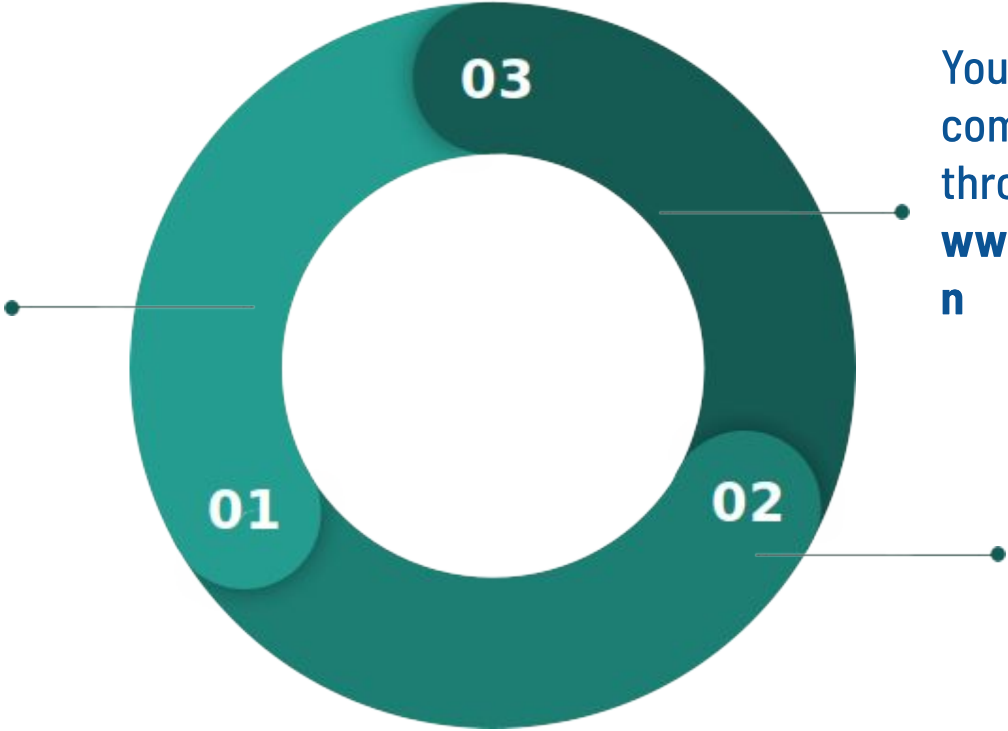
Two-factor Authentication

Strong Password and Pin

Don't install malicious apps

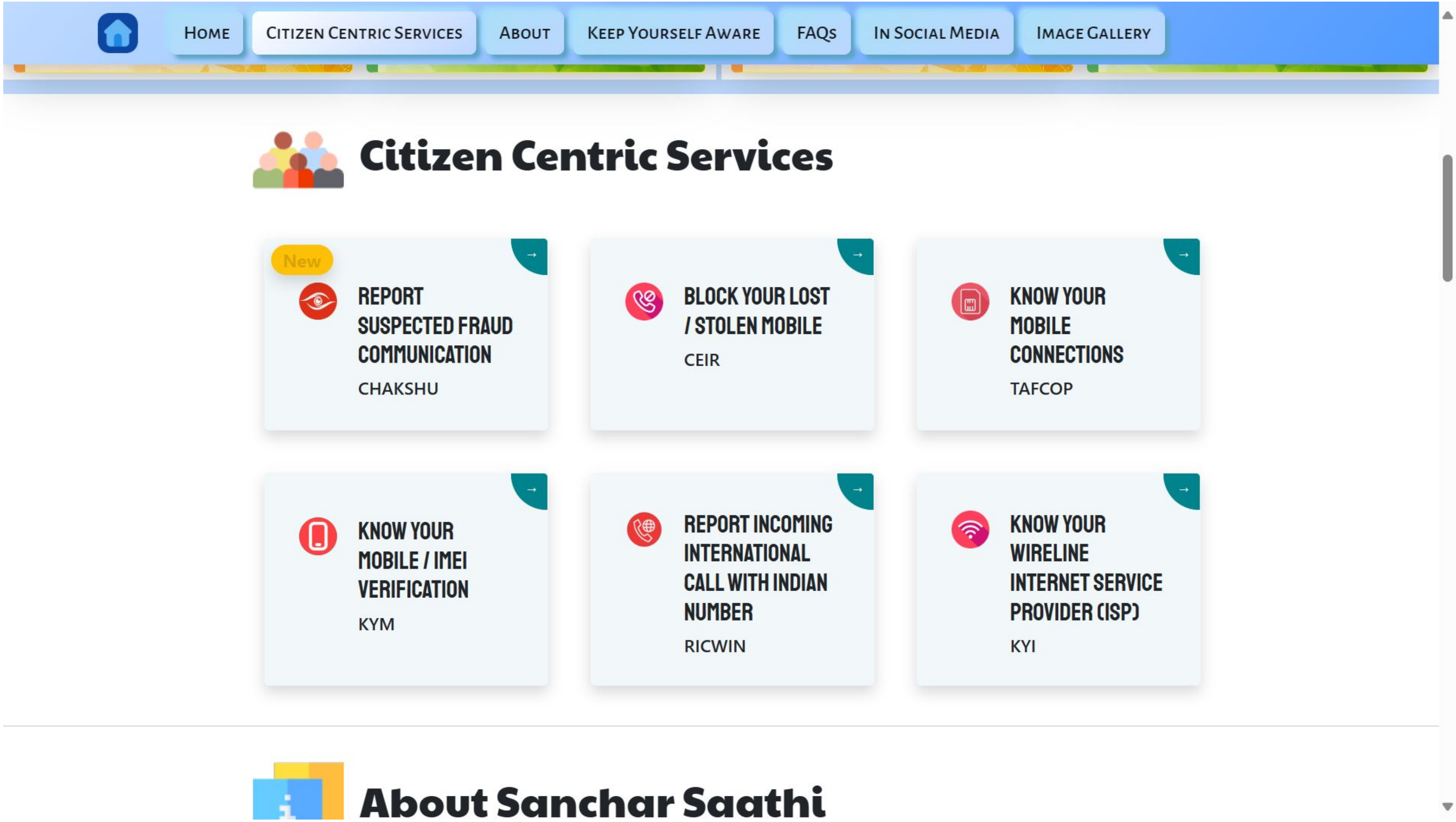
Stay Safe Online

Call ☎ **1930** (Helpline number)
to register any complaint about cybercrime.



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

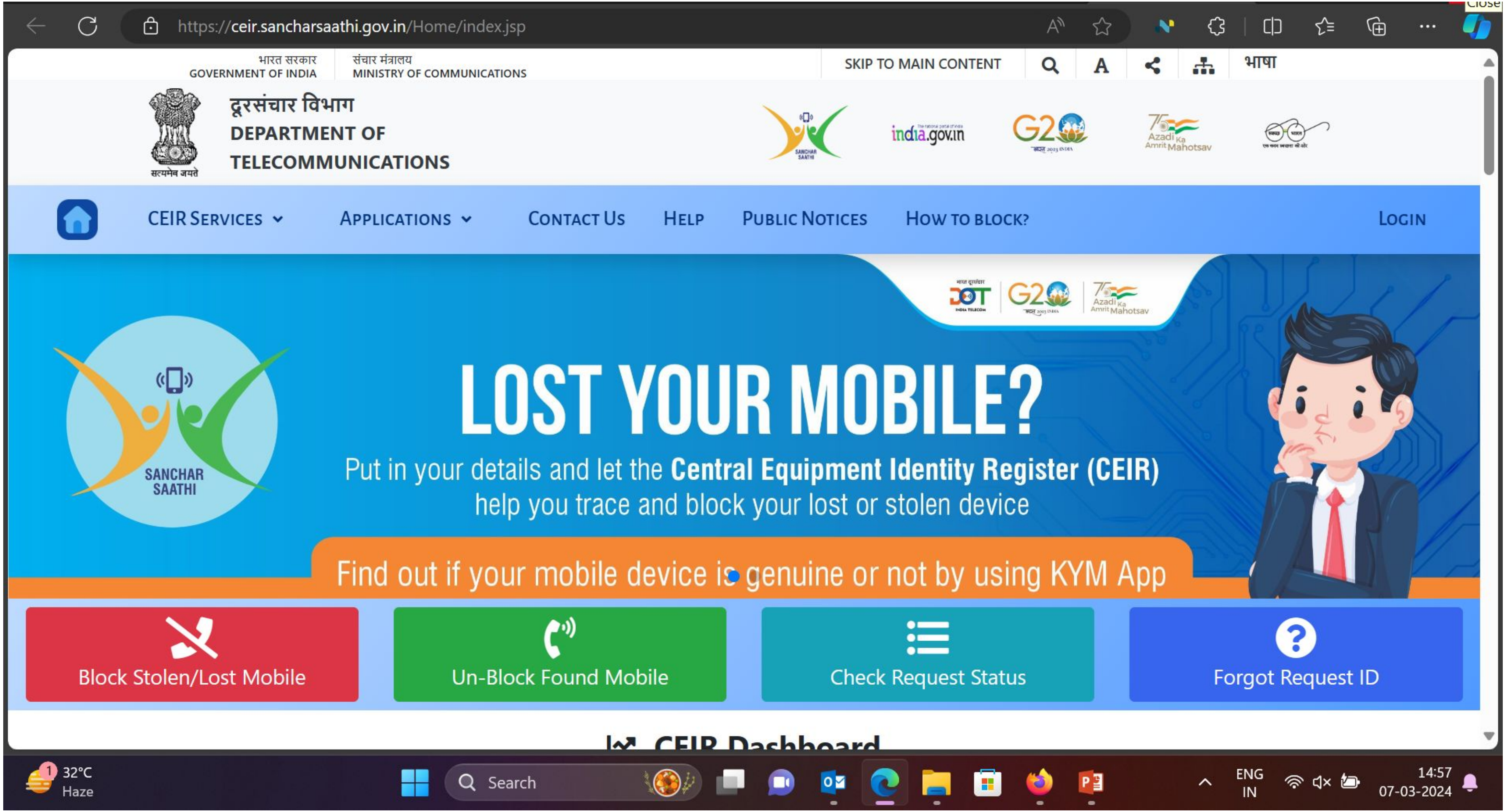
You can also file your complaint at the **nearest police station**
👮



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://ceir.sancharsaathi.gov.in/Home/index.jsp

भारत सरकार
GOVERNMENT OF INDIA

संचार मंत्रालय
MINISTRY OF COMMUNICATIONS

SKIP TO MAIN CONTENT

भाषा

दूरसंचार विभाग
DEPARTMENT OF TELECOMMUNICATIONS

CEIR Services | Applications | Contact Us | Help | Public Notices | How to block? | Login

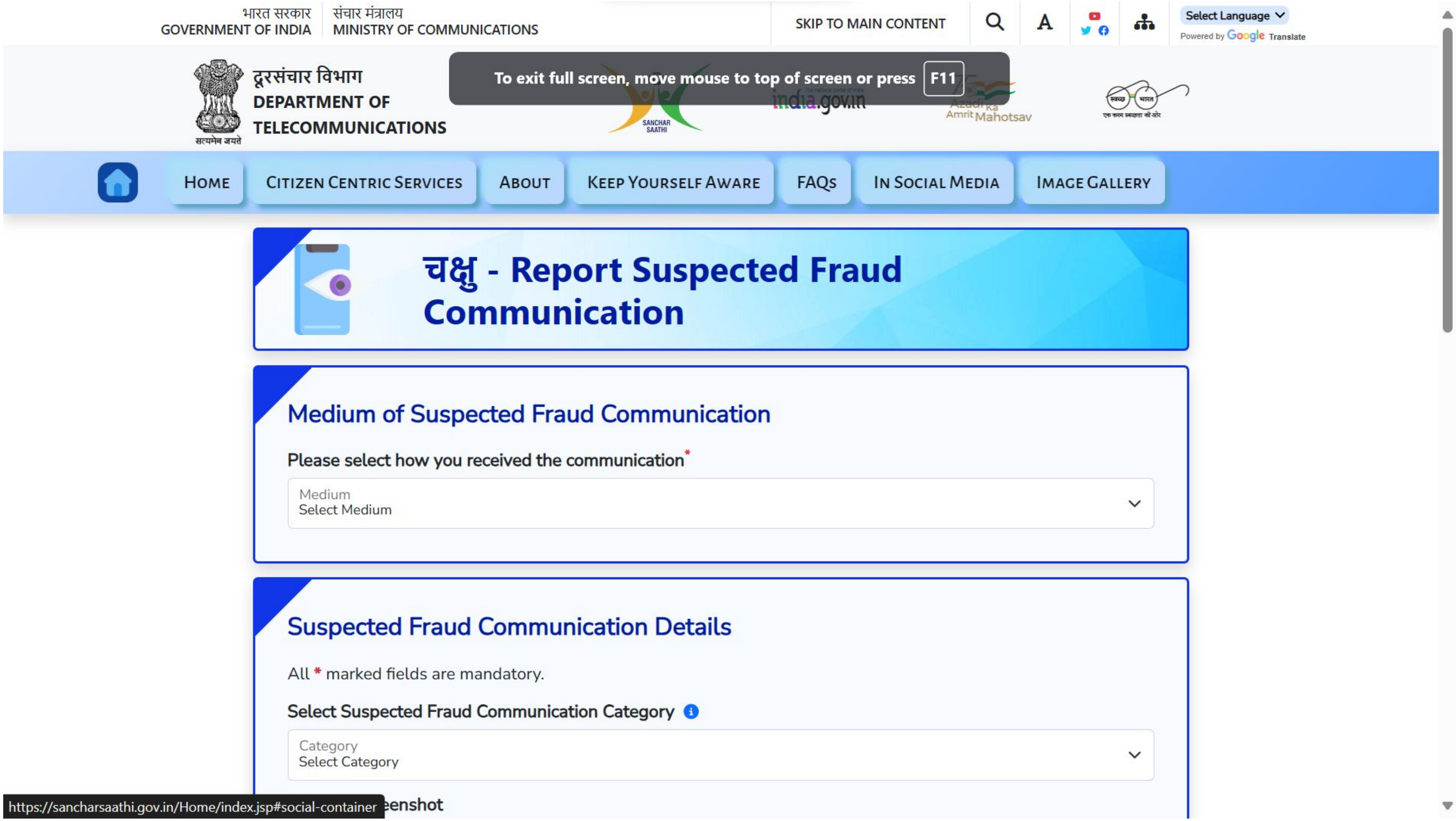
LOST YOUR MOBILE?

Put in your details and let the **Central Equipment Identity Register (CEIR)** help you trace and block your lost or stolen device

Find out if your mobile device is genuine or not by using KYM App

Block Stolen/Lost Mobile | Un-Block Found Mobile | Check Request Status | Forgot Request ID

CEIR Dashboard



चक्षु - Report Suspected Fraud Communication

Medium of Suspected Fraud Communication

Please select how you received the communication*

Medium
Select Medium

Suspected Fraud Communication Details

All * marked fields are mandatory.

Select Suspected Fraud Communication Category

Category
Select Category

eenshot

https://sancharsaathi.gov.in/Home/index.jsp#social-container

Social Media Security

Privacy Setting Weaknesses

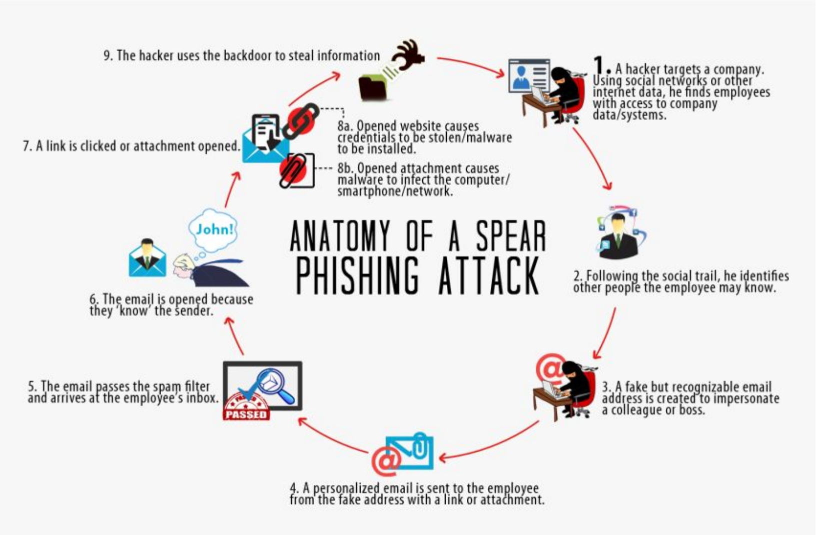
Many users are unaware of the privacy settings on social media platforms, or they may not fully understand how their data is being used.

This can lead to unintentional exposure of personal information and increased vulnerability to threats.

Hacking and Account Takeovers:

Social media accounts are frequently targeted by hackers who aim to steal personal information or spread malware.

Attackers may use stolen credentials or phishing techniques to gain unauthorized access to accounts.



ANATOMY OF A SPEAR PHISHING ATTACK

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

2. Following the social trail, he identifies other people the employee may know.

3. A fake but recognizable email address is created to impersonate a colleague or boss.

4. A personalized email is sent to the employee from the fake address with a link or attachment.

5. The email passes the spam filter and arrives at the employee's inbox.

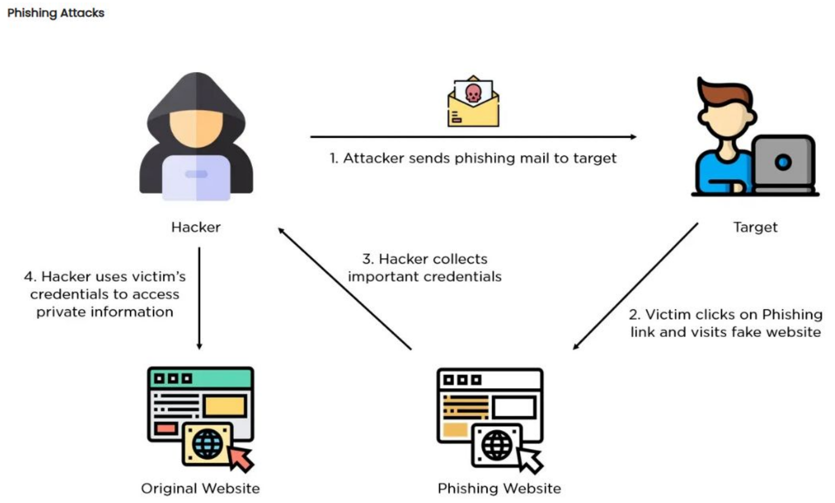
6. The email is opened because they 'know' the sender.

7. A link is clicked or attachment opened.

8a. Opened website causes credentials to be stolen/malware to be installed.

8b. Opened attachment causes malware to infect the computer/smartphone/network.

9. The hacker uses the backdoor to steal information



Phishing Attacks

1. Attacker sends phishing mail to target

2. Victim clicks on Phishing link and visits fake website

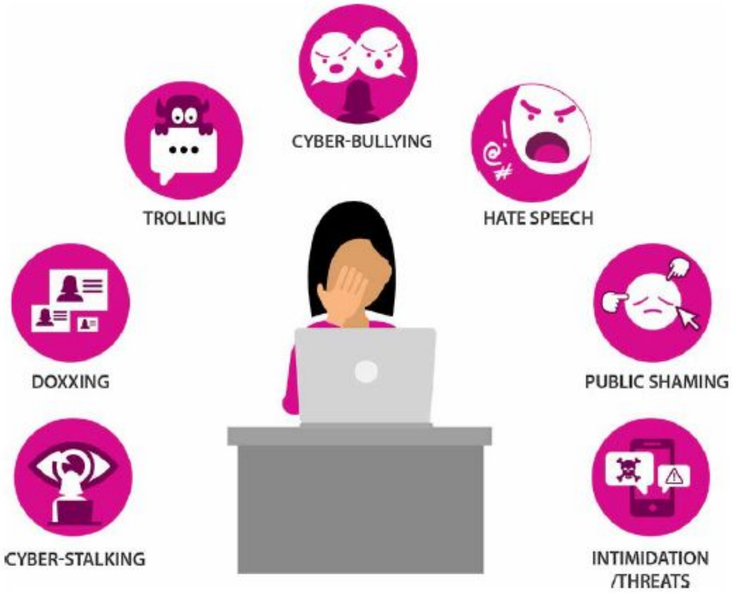
3. Hacker collects important credentials

4. Hacker uses victim's credentials to access private information

Cyberbullying and Harassment:

Social media can be a platform for cyberbullying, harassment, and online stalking.

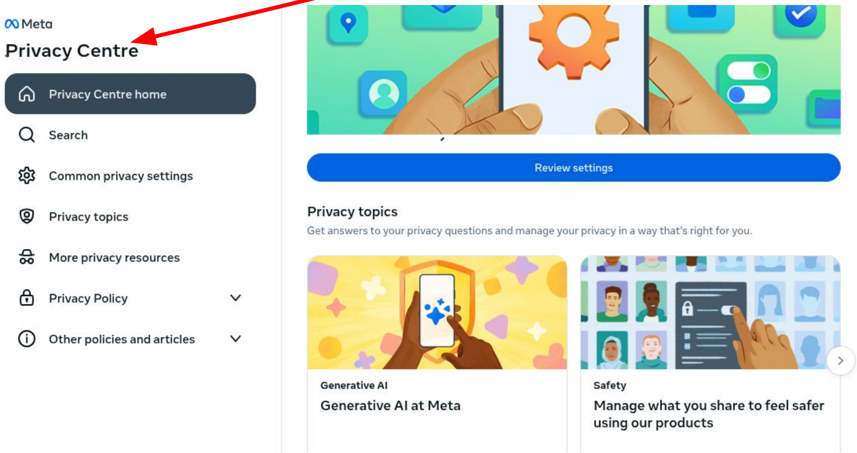
Attackers can use social media to spread rumors, share private information, or send threatening messages.



Facebook

- Set post visibility or “Only Me.”
- Hide your email, phone, from your profile.
- Disable face recognition and limit app access.

To review privacy settings:



Privacy topics

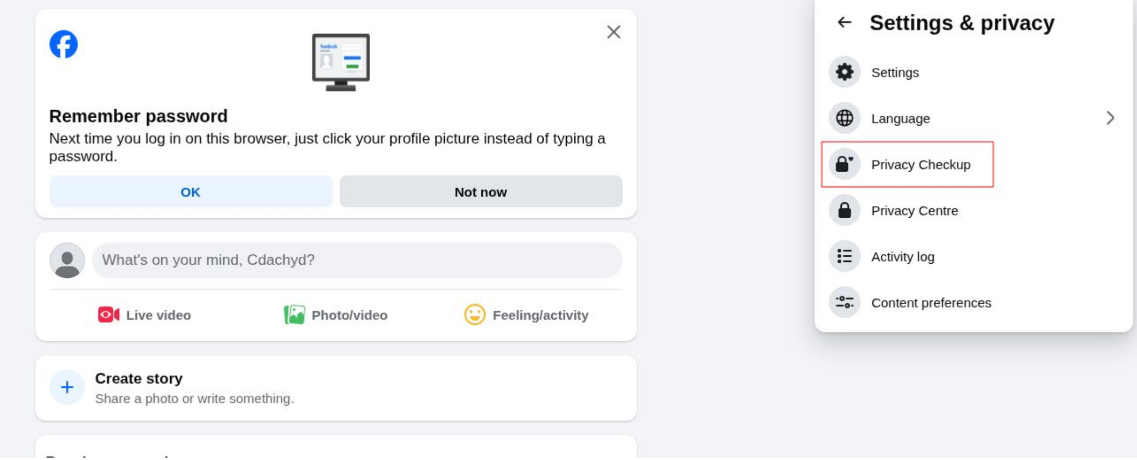
Get answers to your privacy questions and manage your privacy in a way that's right for you.

Generative AI

Generative AI at Meta

Safety

Manage what you share to feel safer using our products



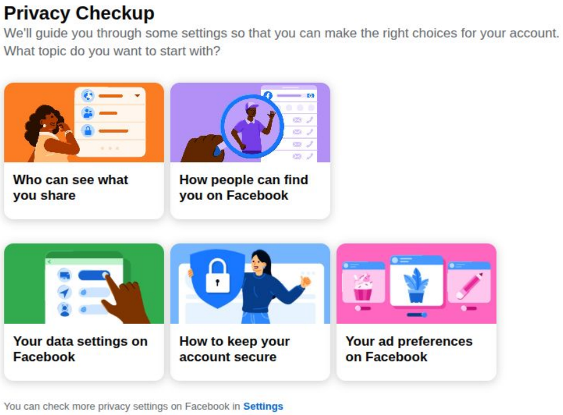
Remember password

Next time you log in on this browser, just click your profile picture instead of typing a password.

Create story

Share a photo or write something.

Settings & privacy

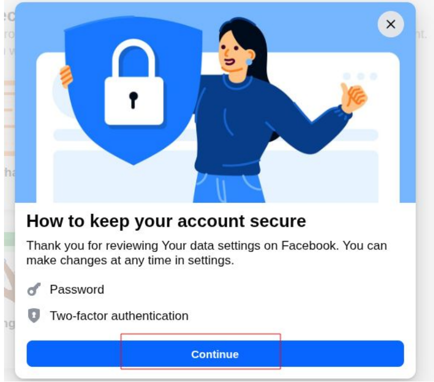


Privacy Checkup

We'll guide you through some settings so that you can make the right choices for your account. What topic do you want to start with?

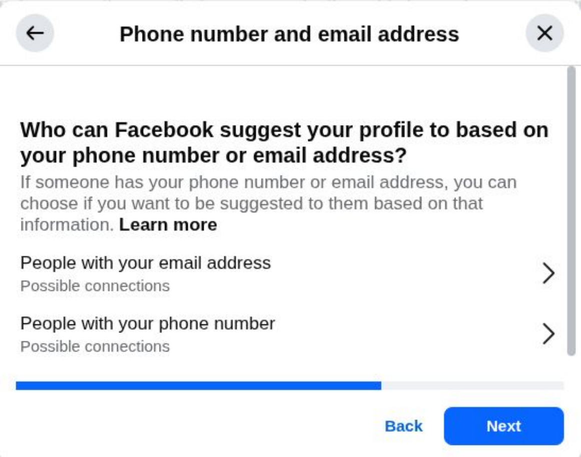
Who can see what you share
How people can find you on Facebook
Your data settings on Facebook
How to keep your account secure
Your ad preferences on Facebook

You can check more privacy settings on Facebook in **Settings**



How to keep your account secure

Thank you for reviewing Your data settings on Facebook. You can make changes at any time in settings.



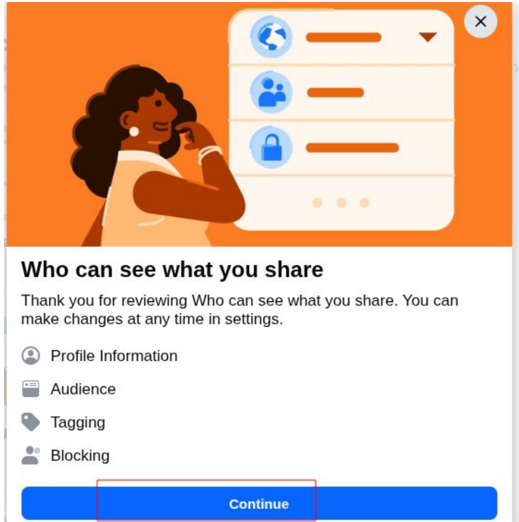
Phone number and email address

Who can Facebook suggest your profile to based on your phone number or email address?

If someone has your phone number or email address, you can choose if you want to be suggested to them based on that information. **Learn more**

People with your email address
Possible connections

People with your phone number
Possible connections

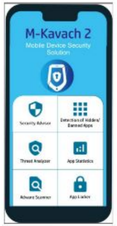


Who can see what you share

Thank you for reviewing Who can see what you share. You can make changes at any time in settings.

Mobile Security Solutions
@
C-DAC Hyderabad

Mobile Security Products Developed @ C-DAC



1. M-Kavach 2

- Mobile Device Security solution for Android devices
- Targeted for the General Public of the country
- 1.8 Million+ downloads
  - Google Playstore & MSeva Appstore
- Other Users
  - Recommended by Headquarters - Integrated Defence Staff - Ministry of Defence for Internal usage
  - Indian Army

2. M-Prabandh

- Mobile Device Management solution for Android devices
  - Centralized Management Dashboard
  - Security Policy Management
  - Role-based Access Control
- Targeted for the Enterprise Users, Strategic Users and SMEs of the country
- Shri. Jayesh Ranjan, IAS, Principal Secretary, Government of Telangana, and Shri. Raja Neravati Chief Product & Technology Officer, Wearables, Titan company, launched M-Prabandh on Feb 14th, 2024 at C-DAC, Hyderabad

3. Vishleshak

- Android based threat analysis platform
  - Evade & bypass strong anti-reversing defenses
  - Insights of Android applications
- Targeted for the Security Analysts, LEAs & Developers
- 1000+ Apps analysed till date
- Deployed at IB, DCyA, CERT-in, MeitY, NCIIPC, Army Intelligence and other User Agency

4. Parikshan

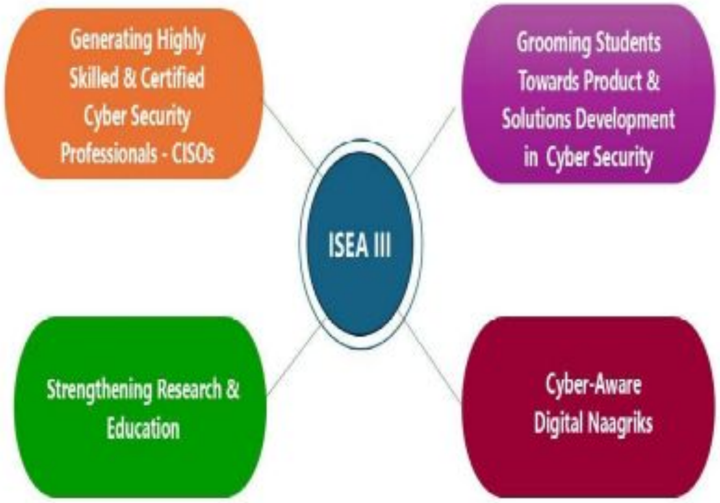
- Mobile App Security Analysis
  - Static & Dynamic Analysis of Mobile (Android) Apps
  - Identify security vulnerabilities and perform exploitation for few of them
  - A detailed Security Audit report as an outcome
- Targeted for the Security Analysts, Developers & Security Audit Labs
- Launched by Shri S Krishnan, Secretary, MeitY on 03rd Febraury, 2024

ISEA Ph-III (at a glance)

Goal : Human Resource Development for Safe, Trusted and Secure Cyber-space

Scope: Capacity / Capability Building in following areas:

- Generating Skilled & Certified Cyber Security Professionals **(Creating Robust Mechanism for Training & Certification of CISOs**,Dy.CISOs etc.)
- Grooming students towards Products/Solutions development in **Cyber Security (Driving Ideation & Innovation activities for students)**
- Strengthening Research & Education in Information Security **(Enhance Capacity/Capabilities in emerging areas; Academic Activities)**
- **Creating Mass Awareness on Cyber Security** (Cyber Aware Digital Naagriks)
- **Establishing Common Infrastructure & Shared** Resources for synergizing ISEA activities at a national level.


Generating Highly Skilled & Certified Cyber Security Professionals - CISOs
Grooming Students Towards Product & Solutions Development in Cyber Security
ISEA III
Strengthening Research & Education
Cyber-Aware Digital Naagriks

Key Verticals

Training & Certification of CISOs: Overview

Goal

- ❑ Generating Highly Skilled and Certified Cyber Security Professionals – CISOs, etc.

Objectives

- ❑ Creating a Robust Mechanism for Training and Certification of Professionals in Cyber Security

Target Audience

- ❑ CISOs, Deputy CISOs, Associate team of CISOs of Government and other sectors (MSMEs)

Deliverables

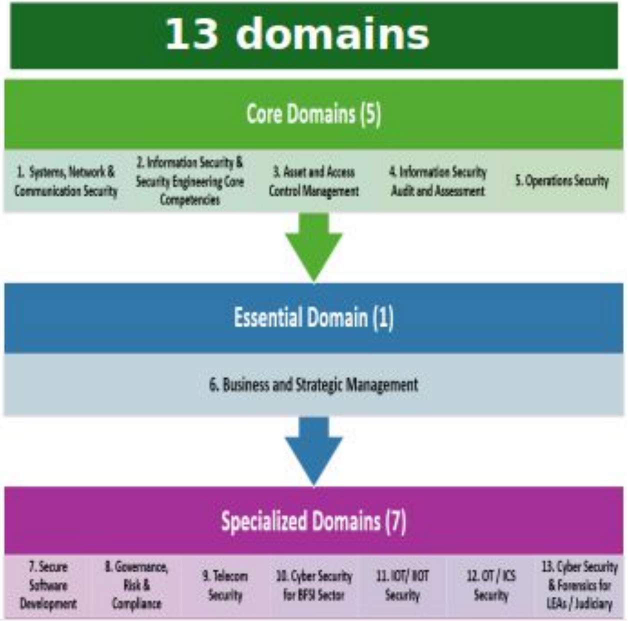
- ❑ 45,000 professionals from Government/other sectors to be trained/certified/re-certified over 5 years

Implementing Agencies

- ❑ C-DAC Hyderabad (nodal agency) jointly with select C-DAC & NIELIT Centers

Certification

- ❑ ISEA (C-DAC, Hyderabad) endorsed by CERT-In/ NIC



13 domains

Core Domains (5)

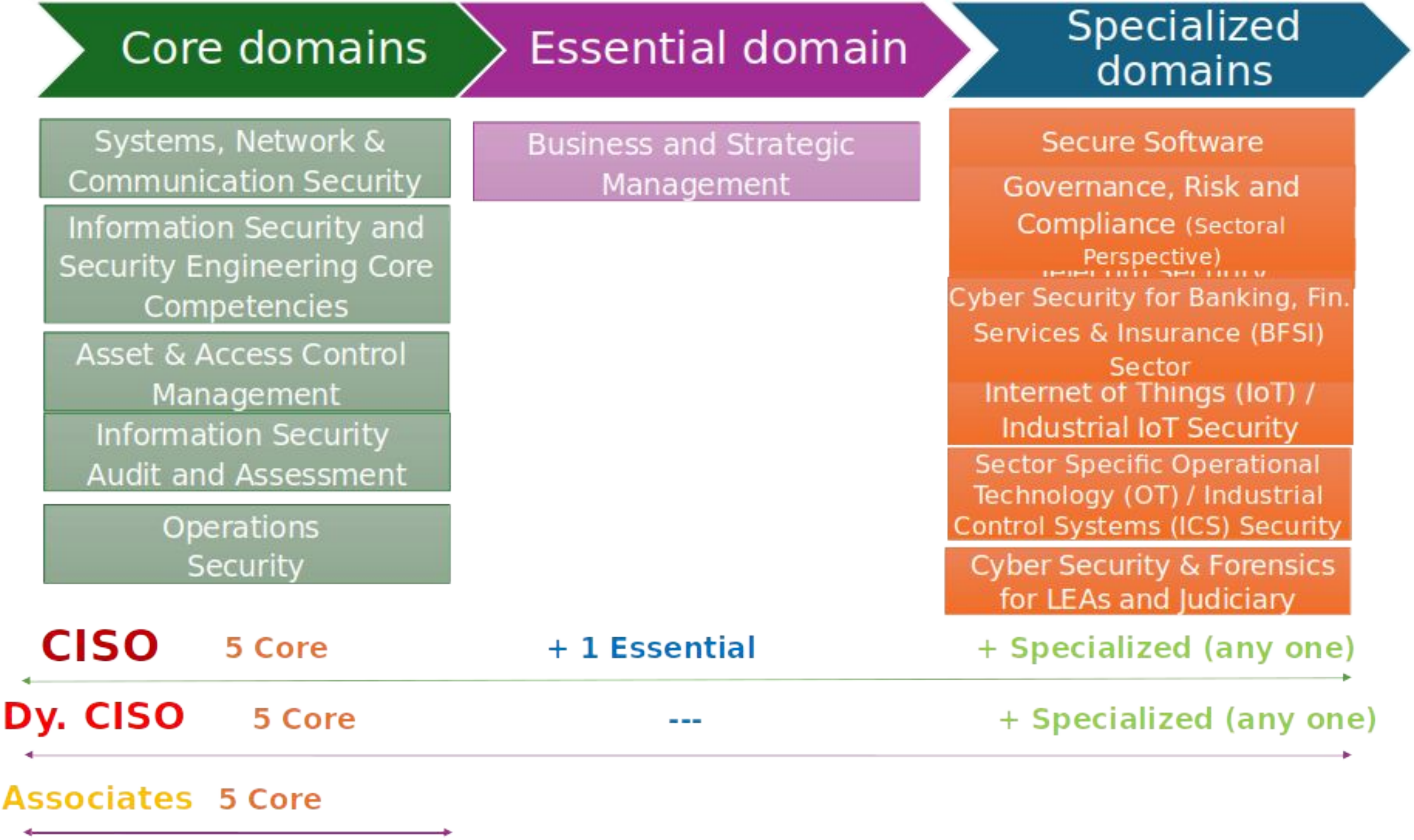
1. Systems, Network & Communication Security
2. Information Security & Security Engineering Core Competencies
3. Asset and Access Control Management
4. Information Security Audit and Assessment
5. Operations Security

Essential Domain (1)

6. Business and Strategic Management

Specialized Domains (7)

7. Secure Software Development
8. Governance, Risk & Compliance
9. Telecom Security
10. Cyber Security for BFSI Sector
11. IOT/ IIOT Security
12. OT / ICS Security
13. Cyber Security & Forensics for LEAs / Judiciary



Core domains

- Systems, Network & Communication Security
- Information Security and Security Engineering Core Competencies
- Asset & Access Control Management
- Information Security Audit and Assessment
- Operations Security

Essential domain

- Business and Strategic Management

Specialized domains

- Secure Software
- Governance, Risk and Compliance (Sectoral Perspective)
- Cyber Security for Banking, Fin. Services & Insurance (BFSI) Sector
- Internet of Things (IoT) / Industrial IoT Security
- Sector Specific Operational Technology (OT) / Industrial Control Systems (ICS) Security
- Cyber Security & Forensics for LEAs and Judiciary

CISO 5 Core + 1 Essential + Specialized (any one)

Dy. CISO 5 Core --- + Specialized (any one)

Associates 5 Core

THANK YOU!