Cyber Security and Data Privacy Awareness

What we can do about it

Rajendra Kumar Solanki

Indian Institute of Technology Jammu

Jan 21, 2026

विद्याधनं सर्वधन प्रधानम्

भारतीय प्रौद्योगिकी
संस्थान जम्मू
INDIAN INSTITUTE OF
TECHNOLOGY JAMMU

Table of Contents

Safety — Security — Privacy

- *Cyber* → *Internet*
- Safety —— Security —— Privacy
- What comes to your mind?
- What is at stake?

Security and Privacy

- The term “**security**” describes techniques that control who may use or modify the computer or device or the information contained in it.

Security and Privacy

- The term "**security**" describes techniques that control who may use or modify the computer or device or the information contained in it.
- The term "**privacy**" denotes a socially defined ability of an individual (or organization) to determine whether, when, and to whom personal (or organizational) information is to be released.

CIA Triad

Information Security objectives:

- **Confidentiality**
- **Integrity**
- **Availability**

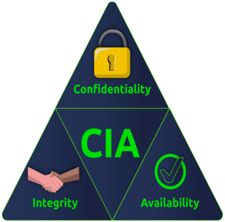


Figure 1: CIA Triad

e.g. Online shopping

*** Authentication, Authorization, Non-Repudiation*

Image Credit: TryHackMe.com

DAD Triad

The Attacker mindset:

- **Disclosure**
- **Alteration**
- **Denial / Destruction**

Disclosure
Alteration
Destruction / Denial

Figure 2: DAD Triad

Image Credit: TryHackMe.com

Security

- Software Security
  - OS Security, Permissions, Access Control
  - Buffer Overflow, Return-to-libc, ROP, Format String, Race Conditions, Memory Writes, Shell Code, Reverse Shell
- Web Security
  - Cookies, Cross-Site Scripting, SQL Injection, CSRF, Clickjacking
- Hardware Security
  - Meltdown, Spector attack, TPM
- Network Security
  - Packet Sniffing, Spoofing, TCP attacks, Firewall, VPN, DNS attacks
- Cryptography
  - Encryption, DES, AES, Hashes, Public Key Cryptography, PKI, Certificates

Passwords

Web browsers and **passwords** remain a weak link in the overall security posture.

Browser permissions to simulate how the browser asks specific permissions: `https://permission.site`

“**Read once**” those pop-ups, messages that appear to make an informed decision!

Browser plug-ins pay attention to what they say and can do.

Default settings move to → Zero-Trust: Never Trust, Always Verify!

Passwords ...

Philosophy of a good and secure password

A secure password is the one:

- you cannot remember
- you can retrieve it - with what you know and what you have
- you never shared over wire/network, and the application never displays you back
- you never shared with anyone
- you never wrote in email drafts/notebook/online accounts
- you never reused it on multiple sites
- you never reused it on other sites with varying one or two digits/characters

Other than passwords

- PIN
- Biometric
  - Iris
  - Face
  - Fingers
- 2FA, MFA
  - OTP
  - Device Prompts

Hacking —— Ethical Hacking —— Learning

- A little long road
- Learn OSINT techniques first
- Some references:
  - `github.com/rks101/eglinux`
  - `github.com/rks101/egnet`
  - `github.com/rks101/isdp` – check Events or Examples
  - `github.com/rks101/webapps`

Malicious and Deceptive Apps

All is not well with apps

Q. Are these apps doing exactly what they say they are doing?

Malicious and Deceptive Apps

All is not well with apps

Q. Are these apps doing exactly what they say they are doing?

- Android's popularity has attracted **malicious** apps
- Growth of potentially unwanted applications (PUA) has brought more data breaches!

Malicious and Deceptive Apps

All is not well with apps

Q. Are these apps doing exactly what they say they are doing?

- Android's popularity has attracted **malicious** apps
- Growth of potentially unwanted applications (PUA) has brought more data breaches!

Malicious and Deceptive apps out in the wild

But, what is the reward for these unwanted apps?

Malicious and Deceptive Apps

All is not well with apps

Q. Are these apps doing exactly what they say they are doing?

- Android's popularity has attracted **malicious** apps
- Growth of potentially unwanted applications (PUA) has brought more data breaches!

Malicious and Deceptive apps out in the wild

But, what is the reward for these unwanted apps?

- **Access to data** - through breach or information leakage
- **Monetary gains** - through card details or ransomware!
- **User Profiling** - track user activities, collect data and sell!

Email

- The primary mode of digital communication for a long time.
- This is going to stay for quite sometime.
- The primary attack vector for Spam and scams.

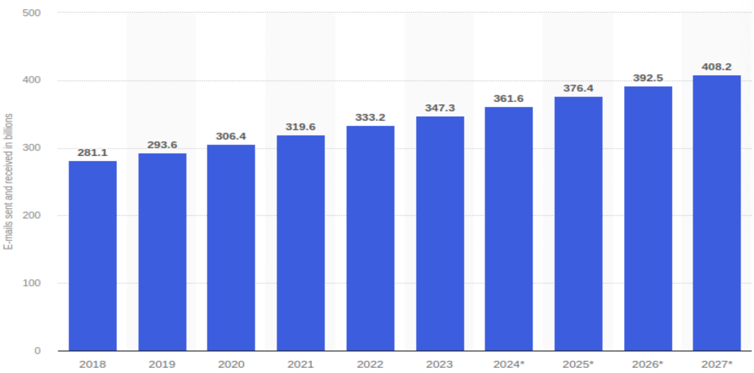


Figure 3: Over 300 billion Emails sent and received per day, Statista2024

Spam

- Look at the email closely.
- Look at the email headers: mailed by, signed by
- Look at "Show Original" information
- SPF, DKIM, DMARC statuses
- Do not click on unknown links and attachments

Q. Before opening, how can I know what is inside it?
A. You need not open. Hover cursor over link in laptop/desktop to see if there is any suspecious text link. On mobile, type the text in the web browser instead of clicking on the unknown links.

Other user messaging apps and challenges

- Chat/messenger apps
- Smishing
- Vishing
- Spear Phishing/Whaling
- Financial loss
- Identity Theft (watch **The Net**)
- Impersonation
- Damage to Reputation
- Misinformation

Cyber Fraud

- Spamming to harvest emails, contacts
- SIM Swap
- SIM Cloning
- Digital Arrest
- Courier fraud to Messaging App takeover

A Handbook on Basics of Cyber Hygiene for Higher Education Institutions by UGC

Education and Awareness is the key to put our best foot forward.

UGC Handbook on Basics of Cyber Hygiene: `https://www.ugc.gov.in/pdfnews/4580600_A_Handbook_on_Basics_of_Cyber_Hygiene.pdf`

Regulations and Reporting

Regulations exist to safeguard us:

- IT Act 2000
- Indian Penal Code (IPC), 1860
- National Cyber Security Policy, 2013

Report in case of Cyber Fraud:

- Cyber Cell `https://cybercrime.gov.in` ←
- State Cyber Nodal Officers
- Banks for financial fraud

Privacy

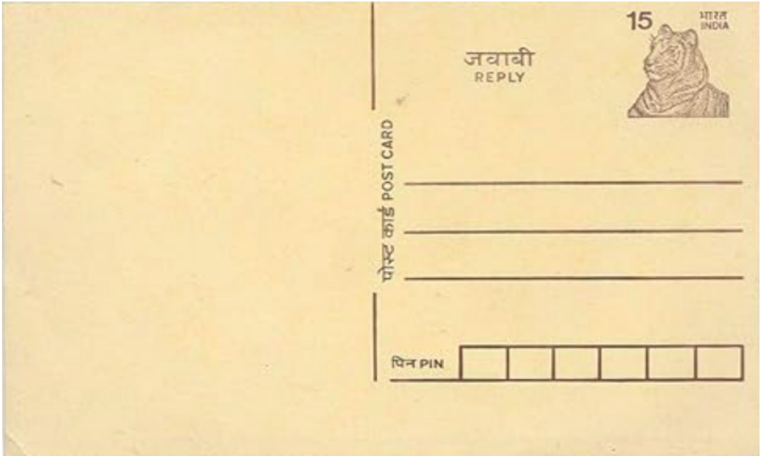


Figure 4: I loved writing postcards, till 2005, was never worried about Privacy

Privacy

1. Privacy - why and what is at stake?
2. Privacy - fundamental principles
   - Notice/Awareness
   - Choice/Consent
   - Access/Participation
   - Integrity/Security
   - Enforcement/Redress
3. Personal Data, Personally Identifiable Information (PII)

Information is Valuable

While we use mobile apps, apps ask Users to share a lot of personal and sensitive data

- phone number, device identifiers
- contacts list, family and friends
- calendar events
- location (latitude and longitude)
- voice
- photos, videos
- sensor and health data
- usage history

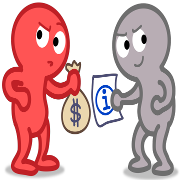


Figure 5: Information is a valuable asset

Information is Valuable

While we use mobile apps, apps ask Users to share a lot of personal and sensitive data

- phone number, device identifiers
- contacts list, family and friends
- calendar events
- location (latitude and longitude)
- voice
- photos, videos
- sensor and health data
- usage history

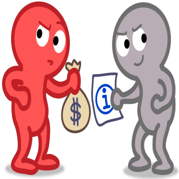


Figure 5: Information is a valuable asset

Challenges of app ecosystem

Potential security and privacy risks associated with using apps on smart devices are reasonably high! It's critical for a **fragmented** ecosystem like Android with multiple OEMs! Are apps vetted for privacy?

We are sharing more information!

- In **2007**: Text
- In **2017**: Contact Details, SMS
- Data shared **today**: Photos, Videos, IDs, Health/Banking/Purchase data, almost everything!
- Reference: The state of mobile app security `https://licelus.com/state-of-mobile-app-security`

Application Description related studies

Apps under-state behaviour

Three of our studies find that **Apps are not transparent about their behaviour** looking at application description, permissions asked and API calls in the app binary. “This increases the attack surface.”

Application Description related studies...

Mapper

Android apps have misconfigured manifest files when it comes to permissions (studied 1192 apps). It could be developer oversight. In reality, apps are over-privileged with 3-7 permissions.

[1] https://github.com/rks101/MapperDroid

[2] https://github.com/rks101/cups

Application Description related studies...

Mapper

Android apps have misconfigured manifest files when it comes to permissions (studied 1192 apps). It could be developer oversight. In reality, apps are over-privileged with 3-7 permissions.

MapperDroid[1]

Android apps under-state behaviour when we compare permissions from descriptions, app manifest and API calls! (25342 apps studied).

[1] https://github.com/rks101/MapperDroid

[2] https://github.com/rks101/cups

Application Description related studies...

Mapper

Android apps have misconfigured manifest files when it comes to permissions (studied 1192 apps). It could be developer oversight. In reality, apps are over-privileged with 3-7 permissions.

MapperDroid[1]

Android apps under-state behaviour when we compare permissions from descriptions, app manifest and API calls! (25342 apps studied).

CUPS[2]

We studied frequently co-occurring and often unused permissions in Android apps. We found, location and device identifier-related permissions were granted and remain unused! (12934 apps studied) 3rd-party libraries can use these permissions! MyProfile++

[1] https://github.com/rks101/MapperDroid

[2] https://github.com/rks101/cups

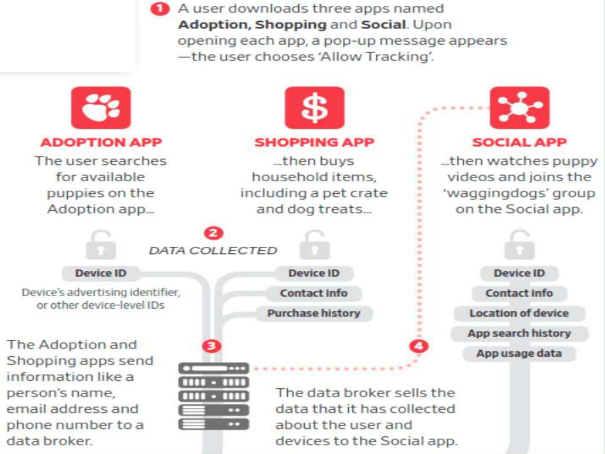
Tracking Users and Profiling: a new economy

- Data is the new oil.
- A new industry is thriving on user data

Tracking Users and Profiling: a new economy

- Data is the new oil.
- A new industry is thriving on user data
- **Personalized advertising** - through tracking user activities
- User activities are tracked through a complex web of websites, apps, tracker sites, data brokers, etc.
- Caution: User profile created for ease of access and personalized experience can be used to modify user's behavior and the choices the user can make.

Scenario



1 A user downloads three apps named **Adoption, Shopping** and **Social**. Upon opening each app, a pop-up message appears —the user chooses 'Allow Tracking'.

ADOPTION APP
The user searches for available puppies on the Adoption app...

SHOPPING APP
...then buys household items, including a pet crate and dog treats...

SOCIAL APP
...then watches puppy videos and joins the 'waggingdogs' group on the Social app.

2 *DATA COLLECTED*

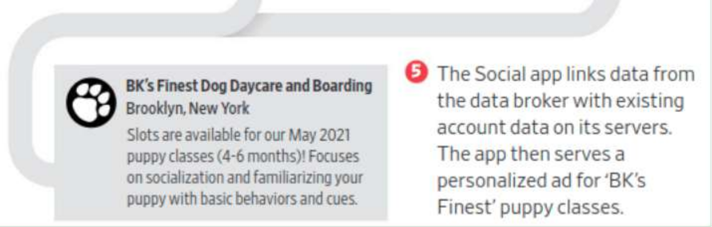
3 The Adoption and Shopping apps send information like a person's name, email address and phone number to a data broker.

4 The data broker sells the data that it has collected about the user and devices to the Social app.

Figure 6: Part 1: Tracking and collecting information[3]

[3] Privacy disclosures of apps on the Apple App Store by Tristan Wyatt, Wall Street Journal

Scenario



BK's Finest Dog Daycare and Boarding
Brooklyn, New York

Slots are available for our May 2021 puppy classes (4-6 months)! Focuses on socialization and familiarizing your puppy with basic behaviors and cues.

5 The Social app links data from the data broker with existing account data on its servers. The app then serves a personalized ad for 'BK's Finest' puppy classes.

Figure 7: Part 2: Serving personalized ads with harvested data

A real **Social Dilemma**!

Scenario

1. User downloads a few apps and grants certain permissions.
2. One or more apps collect some Personally Identifiable Information (PII) - device ID, contact info (email, phone), purchase history, etc. This is actually building a user profile!
3. Data broker (3rd party) companies sell this data to another social app or organization for a fee
4. This organization combines data from the data broker and its profile of the user (location, app usage, search history) to serve personalised ads (best-priced ads in the real-time auction)
5. User sees personalised ads
6. A number of companies update user profiles again in the process.

Advisories and Suggestions

- Pay attention to app permissions, enquire about the app
- Examine why app needs SMS/Phone/Microphone permissions
- If you notice unnecessary permissions, report to developer
- Uninstall / remove apps not getting updated
- Uninstall / remove apps you do not use
- Do not install apps from 3rd party unofficial repositories
- Use PIN / OTP based two factor authentication to protect sensitive data

Advisories and Suggestions continue

- Do not use browsers that take too many permissions and track activities
- Make sure your device receives updates
- Pay attention to backup and sync settings in the cloud
- Watch data you access, store with, and submit to apps
- Review default settings for Privacy and Security
- If you notice activity tracking, opt-out tracking, or uninstall the app

Privacy Policy

What does it contain?

- What data is collected
- How data is collected
- How data can be used
- Redressal mechanism

Regulations

Digital Personal Data Protection (DPDP) Act, 2023, India

- Principle of **consented**, lawful and **transparent** use of personal data
- Principle of **purpose limitation**
- Principle of **data minimization**
- Principle of **data accuracy**
- Principle of **storage limitation**, only till it is needed
- Principle of **reasonable security safeguards**
- Principle of **accountability**, penalty for breaches.

In Europe, GDPR is in force that advocates for purpose specification, consent, data minimization, right to be forgotten.

References

1. Android Permissions: https://github.com/aosp-mirror/platform_frameworks_base/blob/master/core/res/AndroidManifest.xml
2. Best Practices for App Permissions: https://developer.android.com/training/articles/user-data-permissions.html
3. Potentially Harmful Applications https://developers.google.com/android/play-protect/phacategories
4. The state of mobile app security by Licel: https://licelus.com/state-of-mobile-app-security
5. A Day in the Life of Your Data: https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf

Spread this awareness with your students/loved ones.

You are awesome!

Thank You!