Mobile Phone Apps and Privacy Protection

Target Group
University Students

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

Mobile Phone Apps and Privacy Protection

Target Group: University Students

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Intellectual Property Rights

January 2025
Doha, Qatar

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

To contact the National Cyber Security Academy

📱 00974 404 663 79
☎ 00974 404 663 62
🌐 www.ncsa.gov.qa/
✉ academy@ncsa.gov.qa

Dear Participant

Considering the rapid technological advancements and the pervasive presence of the internet in various aspects of life, cyber threats have become a challenge all segments of society encounter. This necessitates efforts to raise awareness about digital safety concepts, which serve as the shield protecting society from these threats.

As part of the «National Initiative for Digital Safety» efforts to enhance digital safety standards within the community, the National Cyber Security Agency presents this booklet with a collection of general tips and guidelines related to digital safety.

Introduction

Mobile phone applications have become an integral part of our daily lives, providing ready access to a diverse array of services and information - from online shopping to banking services, health management, and beyond.

These applications rely on collecting user data to personalise services and enhance user experience. However, with this increasing dependence on applications comes growing concerns about data privacy and protection. Many applications collect sensitive information, including geographical location, personal data, health records, and financial transactions, making them potential targets for cyber attacks and misuse.

To address these challenges, privacy protection has become paramount in application development. Developers employ advanced techniques such as encryption to ensure data security during transmission and storage, and multi-factor authentication to enhance security and prevent unauthorised access. Furthermore, data protection laws worldwide have been strengthened, such as the General Data Protection Regulation (GDPR), requiring companies to adhere to stringent practices for protecting user privacy.

Users themselves bear responsibility through understanding the permissions granted to applications and managing privacy settings meticulously. Digital marketplaces such as Google Play and the Apple App Store maintain policies requiring developers to clearly disclose how data is collected and processed, thereby increasing transparency and fostering trust between users and service providers.

CYBER SECURITY

01

Chapter One

Understanding Mobile Phone Applications

- First: **Mechanisms and Reasons for Mobile Applications Collection of User Data**
- Second: **Types of Data Collected in Mobile Applications**
- Third: **Risks Associated with Mobile Applications**

Understanding Mobile Phone Applications

Mobile phone applications are software designed to operate on smartphones and tablets, aimed at delivering a diverse range of services and functions to users.

These applications serve numerous domains, including social communication, business, education, health, entertainment, and beyond.

Such applications facilitate daily life by providing swift and direct access to information and tools, thereby enhancing efficiency and productivity. Thanks to rapid technological advancement, mobile applications have become fundamental to both individual and corporate life, offering an interactive and seamless experience that rely on advanced mobile technology.

First: Mechanisms and Reasons for Mobile Phone Applications Collection of User Data

Researchers at Oxford University conducted a study on mobile application privacy, discovering that these applications typically transmit data to a small number of major corporations, such as Alphabet (Google's parent company), Facebook, Twitter (now X), Microsoft, and Amazon. It's noted that these companies rely on a network of subsidiaries to collect data from applications, helping to obscure the concentration of data in the hands of the world's largest technology companies.

Based on your usage behaviors like average usage time, pages you follow, the place where you logged in to the app, etc., they know enough to know your location, your current interest, behavior, plans, and financial status as well.

The data collected by third parties through mobile applications may encompass anything from profile information such as age and gender to location details, including Wi-Fi router data, and information about every application installed on the phone[1].

This raises considerable concerns about personal data privacy when using various applications. However, it's worth noting that users can verify what data an application collects and revoke permissions if necessary, as most application providers comply with such requests. Nevertheless, feeling uncomfortable and threatened is natural when being tracked by an unknown entity without one's awareness.

Did you know?

A study of almost 1m Android apps has revealed how data from smartphones are harvested and shared, with nearly 90 per cent of apps set up to transfer information back to third parties, aiming to enhance customer experience, assess product quality, and evaluate consumer-brand relationships[2].

1. How Mobile Apps Collect Your Data And What You Should Do, December 2022. follow link: https://ready.io/blog/how-mobile-apps-collect-your-data
2. Aliya Ram, et al, How smartphone apps track users and share data, October 2018. follow link: https://ig.ft.com/mobile-app-data-trackers/

Caution!

Data collection aids in identifying user behaviors and preferred patterns to display content matching their interests, as demonstrated by social media platforms where algorithms play a vital role in enhancing user browsing quality and displaying compatible content to extend platform engagement time.

Did you know?

In April 2022, Google mandated all developers publishing applications on Google Play Store to declare how they collect and handle user data for the apps they publish on Google Play, and provide details about how they protect this data through security practices like encryption. This includes data collected and handled through any third-party libraries or SDKs used in their apps. This policy aims to increase application transparency and enhance user data protection[1].

[1] https://support.google.com/googleplay/android-developer/answer/10787469?hl=en

Second: Types of Data Collected in Mobile Applications

Mobile phone applications can collect a wide range of data, depending on their functions, features, and permissions granted by users. Here are the types of data collected:

Personal Information

This includes names, email addresses, telephone numbers, social security numbers, and other information that identifies the user.

Location Data

Many applications collect user location information through Global Positioning System (GPS) data, Wi-Fi networks, or mobile networks. This is used for various purposes such as providing location-based services, targeted advertising, or analysing user behaviour[1].

[1] Mahesh Atapattu, Mobile Application Data Collection and Data Sharing: What You Need to Know, July 2023. follow link: https://www.linkedin.com/pulse/mobile-application-data-collection-sharing-what-you-need-atapattu/

Device Information

Some applications collect data about the user's device, including device model, operating system version, browser type, Unique Device Identifiers (UDID), IP address, network connections, and hardware specifications. This information helps developers improve application performance.

Usage Data

Some applications collect users' behavioural data, including which features they use, time spent using the application, and their navigation patterns. This helps developers understand user behaviour and improve application features and mechanisms accordingly.

Authentication Data (or Login Data)

Many applications collect usernames, passwords, or other authentication tokens to allow users to securely log in and access content or services.

Social Media Data

Applications typically request access to users' social media profiles, friend lists, and other information that can be used for targeted advertising.

Payment Information

E-commerce applications collect payment information such as credit card numbers, billing addresses, and transaction history for processing purchases and managing accounts.

Health and Fitness Data

Health and fitness applications collect personal data such as exercise patterns, dietary habits, sleep patterns, and biometric measurements to track and analyse users' health-related metrics.

Did you know?

According to a study by the Pew Research Center, 72% of smartphone users expressed concern about their data being collected by mobile applications. Meanwhile, 68% of users are unaware that their data is being sold by the applications they use[1].

[1] McClain, Colleen,et al, How Americans View Data Privacy, PEW, October 2023, follow link: https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

Third: Risks Associated with Mobile Phone Applications

Mobile phone security risks differ from those of personal and desktop computers. Protecting mobile applications is crucial, particularly as they are available to nearly 80% of the world's population, with annual application downloads increasing - **2021 alone recorded approximately 230 billion downloads.** Securing a mobile phone application differs entirely from securing a website, web application, or even software application for portable or desktop computers. Therefore, developers must work within the constraints of both the phone's operating system (iOS or Android) and the respective application store where they wish to publish their application.

It's worth noting that most mobile application security problems begin during the development process and extend to code negligence, which allows cybercriminals to infiltrate the application and initiate data theft or account takeover.

Security Risks of Mobile Phone Applications:

1. Insecure Communications

In common mobile applications, data exchange occurs through the application transmitting data via the Internet and mobile carrier network. Attackers may exploit security vulnerabilities in devices to intercept sensitive information or user data during transmission over the network[1].

Main threats in insecure communications include:

- ✓ **Malicious software on the mobile device**
- ✓ **Unsecured or compromised Wi-Fi network**

  Mobile developers typically use SSL/TLS protection protocol only during authentication, but not elsewhere, resulting in insufficient security layers. This increases the risk of sensitive data exposure - such as login credentials, personal information, session identifiers, and other crucial data - to interception by criminals. The mere presence of SSL/TLS protocol doesn't guarantee complete mobile application security.

Caution!

In common mobile applications, data exchange occurs through the application transmitting data via the Internet and mobile carrier network. Attackers may exploit security vulnerabilities in devices to intercept sensitive information or user data during transmission over the network.

[1] M3: Insecure Communicatio, Clouddefense, follow link: https://www.clouddefense.ai/owasp/2016/3

2. Insecure Personal Data Storage

Mobile applications, including banking applications, often store sensitive data locally. This means that PIN numbers, credit card numbers, passwords, login details, and other data are simply stored somewhere on the smartphone. Worse still, this data is often stored insecurely, meaning a cybercriminal could remotely access the device, locate this data, and steal it[1].

Sensitive data is stored insecurely due to improper encryption. Some mobile applications don’t either encrypt local data at all; perform encryption but store encryption keys incorrectly; or use unsafe custom encryption protocols.

⚠ **Caution!**

Mobile applications, including banking services, frequently store sensitive data locally, meaning that PIN numbers, credit card numbers, passwords, login details, and other data are simply stored somewhere on the smartphone.

[1] mobile app security risks and how to mitigate them, Cypress Data Defense, July 2020. follow link: https://2u.pw/PKH0B660

◆ 3. Sensitive Data Leakage

Sensitive data may be exposed to leakage and breaches, either accidentally or deliberately. A notable example of this occurred with the popular parking and mobility application ParkMobile, when a security vulnerability in third-party software led to a data breach in 2021. This resulted in the exposure of email messages, birth dates, licence plate numbers, phone numbers, and other personal data of approximately 21 million users[1].

Sometimes, these leaks occur unintentionally. For instance, Firebase is one of the most common data storage solutions for Android applications. However, it is often misconfigured, meaning anyone who knows the correct URL for an application built using Firebase can easily access that application's databases, potentially leading to user data leakage.

To prevent sensitive data leakage, data storage in cache memory can be prohibited, as criminals may use this data to attempt account breaches. Users should also manually clear their cache memory, as this makes the application more secure.

[1] Twingate Team, what happened in the park mobile data breach?. Twingate, may 2024, follow link: https://www.twingate.com/blog/tips/park-mobile-data-breach

4. Malicious Software

Mobile malware consists of harmful software specifically designed to target smartphones and tablets, with the aim of accessing users' private data. It poses an increasing threat because many companies now allow employees to access corporate networks using their personal devices, which may lead to increased opportunities for compromising the work environment.

Recent years have witnessed numerous security issues with Android mobile devices. However, Apple is not entirely immune to malicious software either.

02

Chapter Two

Protection of Application Data

- First: **Application Breach Methods**
- Second: **Risks of Using Free Applications**
- Third: **Risks of Mobile Phone Data Misuse**
- Fourth: **Signs of Malicious Software on Mobile Devices**
- Fifth: **Methods of Mitigating Privacy Breach Risks When Using Mobile Applications**

Protection of Application Data

In today's technological world, protecting user data in applications is among the top priorities, particularly as security threats and cyber attacks continue to increase.

Data protection strategies encompass various practices and techniques aimed at securing personal and sensitive information collected from users by applications.

These strategies include:

- ✓ Implementing encryption techniques to ensure data protection during transfer and storage
- ✓ Configuring access management to control data accessibility
- ✓ Enabling multi-factor authentication to enhance security
- ✓ Providing guarantees of application compliance with applicable laws and regulations

First: Application Breach Methods

Cybercriminals employ various tactics to compromise mobile devices. The most common types include:

Remote Access Tools

These tools provide extensive access to data on infected devices, commonly used for gathering information for intelligence purposes. They can typically access information such as installed applications, call logs, address books, web browsing history, and SMS data. These tools may also be used to send SMS messages, enable device cameras, and record GPS data[1].

Ransomware

This is a type of malicious software used to prevent users from accessing their device data and demanding ransom payment, typically requested in Bitcoin cryptocurrency due to its difficult traceability. Once the victim pays the ransom, access codes may be provided to allow device unlocking.

[1] Ben Forster, why hackers like your remote access and what you can do about it, Paloalto Networks, Jun 2021. follow link: https://www.paloaltonetworks.com/blog/2021/06/why-hackers-like-your-remote-access/

Bank Trojans

These appear as legitimate applications and target users who conduct financial transactions, including money transfers and bill payments through their mobile devices. This type of malware steals login details and passwords[1].

Did you know?

The concept of the Trojan horse dates back to the Trojan War (1260-1180 BC), when Greeks used a wooden horse filled with warriors to enter the Turkish city of Troy. Today, the same term is metaphorically used to describe various malicious tactics for gaining access to secure user data.

[1] Adam Hayes, Banker Trojan: What it Means, How it Works, July 2022. follow link: https://2u.pw/Ys1Bc3lq

Cryptomining Malware

This malicious tool allows cybercriminals to execute hidden computational operations on the victim's device, enabling them to generate cryptocurrency through Trojan codes hidden in seemingly legitimate applications[1].

Advertising Click Fraud

This type of malware allows cybercriminals to generate financial income through fake advertisement clicks[2].

Did you know?

A click fraud state report for 2023 AD revealed that click fraud cost advertisers approximately 35.7 billion dollars in 2022 AD[3].

[1] Kurt Baker, What is Mobile Malware?, CROWDSTRIKE, November 2023. Follow link: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/mobile-malware/

[2] Sanja Trajcheva, et al, What is Click Fraud? how it works, examples, and red flags, Cheq, January 2024. follow link: https://cheq.ai/blog/what-is-click-fraud/

[3] The State of Fake Traffic 2023. Cheq, follow link: https://cheq.ai/blog/what-is-click-fraud/

Second: Risks of Using Free Applications

Free mobile app users pay a high price for using these seemingly free applications. Researchers have discovered various health and psychological symptoms resulting from using free apps, including: task procrastination; sleep deprivation; and lack of concentration. Major technology companies analyze users' digital behavior patterns to deliver targeted advertisements directly to them. This means users' attention is the commodity these companies exploit. For example, YouTube's three billion users generate estimated monthly revenues of 30 billion euros from services perceived as free.

⚠ **Caution!**

Free app users pay a physical and psychological price when they use these seemingly free Apps including: task procrastination, sleep deprivation, and reduced concentration.

Personal data is often collected through free mobile apps that don't cost money to download and install. Researchers have confirmed that there are costs associated with free apps, dubbing this phenomenon the "zero-price economy" - where service providers (or free app providers) offer their services in exchange for user data and interests without monetary exchange, as those applications take up user time[1].

This raises key question: Where does user personal data go and who can access it?

The world of data privacy has changed significantly, with growing concerns about app privacy and many phone owners' inability to identify real threats. In mobile apps, advertisements typically follow a specific mechanism where developers embed code from specialized software development groups that can collect all types of information, including user location and app usage data.

[1] Linköping University, The hidden costs of free apps – more than personal data, Alpha Galileo, October 2024. follow link: https://2cm.es/OeMk

As long as the users don't read the privacy policy details or terms of service statement, they won't be aware whether data collection and transmission to third parties is occurring or not.

App developers seeking to monetize their applications implement various advertising software development kits (SDKs) to benefit from the largest possible number of networks, without verifying the privacy practices of these advertising networks. This results in the SDKs capturing all data passing through them during app usage, collecting this passing data, and then selling it. Through these entities' continuous transmission of user data and merging it with data from other companies, a clear picture of user behavior is formed.

Among the grave potential risks in data transfer is who can see that data, and unfortunately, identifying these parties is not easy. Anyone working at the company that makes an application, any of the third parties to whom the application sends data, or even employees at the company hosting the server that stores the data can access some or all of the data[1].

The only situation where access by these external parties to the data becomes impossible is when the application properly implements end-to-end encryption.

Caution!

Misuse of mobile phone data feeds targeted advertising through collection and analysis of user behavior, preferences, and engagements.

[1] Thorin Klosowski, how mobile phones became a privacy battleground, September 2022. follow link: https://www.nytimes.com/wirecutter/blog/protect-your-privacy-in-mobile-phones/

Third: Risks of Mobile Phone Data Misuse

Among the most prominent common risks that users may face when mobile phone data is misused:

Identity Theft

Mobile phone data misuse leads to identity theft, where criminals use stolen personal information such as names and addresses to impersonate individuals, open fraudulent accounts, or conduct unauthorized transactions.

Financial Fraud

Risks from mobile phone data leaks include financial fraud operations including unauthorized access to bank accounts and credit card fraud and loans; criminals can exploit stolen financial information to make unauthorized purchases or drain bank accounts.

Caution!

Mobile phone data leaks have grave consequences including: financial fraud, unauthorized access to bank accounts, and exploiting stolen financial information to make unauthorized purchases or drain bank accounts.

Privacy Violations

One of the most prominent risks resulting from phone data misuse by criminals is represented in collecting sensitive information without user consent, tracking locations, monitoring online activities, and accessing communications; meaning the user is under constant surveillance.

Reputational Damage

The risks can go beyond disclosing unauthorized sensitive data, causing damage to individuals' reputations, such as: disclosing private message content, personal photos, or videos, exposing users to abuse and cyber extortion.

Caution!

The risks sometimes extend to disclosing unauthorized sensitive data, causing damage to individuals' reputations, such as: publishing private message content, personal photos, or videos.

Targeted Advertising and User Manipulation

Mobile phone data misuse can feed targeted advertising and user manipulation tactics through collecting and analyzing their behavior, preferences, and interactions, enabling criminals or unethical advertisers to create customized advertisements targeted at specific user groups, meaning manipulation of users' choices and decisions.

Social Engineering Attacks

Known as "phishing" or "social engineering," internet criminals craft and send deceptive messages to their victims, pushing them to reveal sensitive data like usernames, passwords, and credit card details. When there's a profile of the user, internet criminals can customize phishing messages to attract more attention or deceptively gain users' trust, thus increasing attack effectiveness. Phishing attacks don't just affect individuals but can affect large companies through their employees, as well as government institutions. Interpol has classified social engineering as one of the world's emerging fraud trends[1].

Caution!

Internet criminals craft and send deceptive messages to their victims, pushing them to reveal sensitive data such as: usernames, passwords, and credit card details.

[1] Jacob Leon Kröger, how data can beused against people:a classification of personal data misuses, December 2021. follow link: https://linksshortcut.com/KGJvq

Fourth: Signs of Malicious Software on Mobile Devices

- An unusual frequency of pop-up advertisements or unexpected new applications. Whilst most pop-up ads are merely marketing tools rather than malware, if you find yourself closing pop-ups more frequently than usual, this may indicate malicious software on your device[1].
- You have unfamiliar applications on your phone that you haven't downloaded or installed. These should be removed immediately, followed by a thorough antivirus scan of your device.
- Phone overheating. Mobile devices aren't designed to support malware, and when an infected application is inadvertently downloaded, your device works harder than usual, causing increased heat generation.
- Your device sending spam emails or social media messages containing suspicious links or unknown files to your contacts. It's advisable to alert all recipients that your phone has been compromised to prevent them from downloading malware or forwarding these links.

[1] 7 Signs Your Phone Has a Virus and What You Can Do, Mcafee, August 2022. follow link: https: //www.mcafee.com/blogs/mobile-security/7-signs-your-phone-has-a-virus-and-what-you-can-do/

- ✓ Unusually slow phone response times. This occurs because your device is expending extra effort to support the downloaded virus, while unfamiliar applications consume storage space and run background tasks, leading to slower performance.
- ✓ Fraudulent charges appearing on your accounts, necessitating regular monitoring of your bank statements to detect any unauthorised purchases.
- ✓ Conspicuous data usage; sudden spikes in data consumption or phone bills may indicate malware running background operations or using your internet connection to transfer data off your device for malicious purposes.
- ✓ Abnormally rapid battery drain.

Caution!

Quick battery drain, phone overheating, and fraudulent account charges are all indicators of malware infection on mobile devices.

Fifth: Methods of Mitigating Privacy Risks When Using Mobile Applications

Whilst it's impossible to completely prevent applications from collecting user data once installed, you can reduce associated risks by:

- ✓ Only downloading applications from trusted sources like the Apple App Store and Google Play Store.
- ✓ Reviewing user feedback before downloading apps; reconsider if there are negative reviews about permissions.
- ✓ Reviewing user feedback before downloading apps; reconsider if there are negative reviews about permissions.
- ✓ Carefully considering any permission requests when using applications.
- ✓ Avoiding linking apps to personal accounts (email, phone number, social media) to prevent cross-platform data sharing.
- ✓ Using a VPN to protect data through encrypted internet connections and IP address masking.

- ✓ Avoiding public Wi-Fi networks for accessing sensitive information.
- ✓ Using a secure browser that blocks tracking tools and advertisements to help in data protection.
- ✓ A simple digital safety precaution is the screen lock. A 2017 Pew Research Center report revealed that nearly 30% of smartphone owners don’t use screen locks or other security features, making them vulnerable to cybersecurity breaches including personal data and password theft[1].

Did you know?

The Financial Times revealed that Apple’s App Tracking Transparency privacy policy, which ensures transparency in how apps track user data, costs social media platforms approximately $10 billion annually[2].

Caution!

Closing pop-up windows more frequently than usual indicates the presence of malware on your phone.

[1] Stephanie Taylor, 10 ways to make your phone safer, September 2011. follow link: https://linksshortcut.com/fUmGE

[2] Anna Yaskiv, App Tracking Transparency: what Data do Apps Collect and why?, January 2022. follow link: https://linksshortcut.com/xXsmi

Exercises

Exercises in this part are based on the presented material. An answer key is provided at the end of the booklet.

First Exercise

What is it?

1. A type of malware used to prevent users from accessing their device in exchange for payment, typically made in Bitcoin cryptocurrency.

2. Software that allows cybercriminals to perform hidden computational operations on the victim's device using Trojan horse codes hidden in seemingly legitimate applications.

3. A type of malware that allows cybercriminals to generate financial income through user clicks.

4. Attacks that rely on mobile phone data leaks to gain unauthorized access to bank accounts and make unauthorized purchases.

5. Through fraudulent techniques, cybercriminals create and send deceptive messages to their victims, compelling them to reveal sensitive data. Note that these attacks affect not only individuals but can also target large companies through their employees.

Second Exercise

Mark the following statements as (True) or (False) and correct the mistake, if any:

1. Based on app user behaviors, data carriers can determine user location and interests. (..........)

   ....

2. Some phone applications collect user data to display advertisements for companies wanting to advertise their products or services. (..........)

   ....

3. Device model data, operating system version, and browser type are not among the data collected by phone applications. (..........)

   ....

4. E-commerce applications prohibit collecting information such as credit card numbers and billing addresses. (..........)

   ....

5 Third-party data collection through mobile applications includes any profile information such as age and location details. (..........)

....

6 Some app developers may sell users' data to market research companies. (..........)

....

7 User browsing data helps institutions better determine and communicate with targeted customers and understand and solve their demands. (..........)

....

8 Applications avoid accessing user profiles on social media, including friends' lists. (..........)

....

Third Exercise

Complete the following statements

1. .... refers to companies that buy and sell personal data, who in turn sell it to other companies.

2. .... functions include utilizing app user data to understand behavior and improve app features and efficiency.

3. Threat factors in unsecured communications include ...., ..., ...

4. .... are intrusive programs specifically designed to target smartphones and tablets, aiming to access private data.

5. .... are tools used to send SMS messages, enable device cameras, and record GPS data.

Answer Key

Question

First Exercise: What is it?

Answer

1. Ransomware
2. Cryptomining software
3. Click fraud advertising
4. Financial fraud
5. Social engineering attacks

Question

Second Exercise: Mark the following statements as (True) or (False) and correct the mistake, if any:

Answer

- 1. True
- 2. True
- 3. False; this is actually one of the types of data collected
- 4. False; e-commerce applications do collect payment information, such as credit card numbers, billing addresses, and transaction history for processing purchases and account management
- 5. True
- 6. True
- 7. True
- 8. False; applications typically request access to user profiles on social media, including friends lists and other information that can be used in targeted advertising

Question

Third Exercise: Complete the following statements

Answer

1 Data Brokers

2 Market research companies

3
- Mobile device malware
- Unsecured or hacked Wi-Fi networks
- Telecommunications company or network devices

4 Mobile malware

5 Remote access tools

References

1. How Mobile Apps Collect Your Data And What You Should Do, December 2022. follow link: https://ready.io/blog/how-mobile-apps-collect-your-data

2. Aliya Ram, et al, How smartphone apps track users and share data, October 2018. follow link: https://ig.ft.com/mobile-app-data-trackers/

3. https://support.google.com/googleplay/android-developer/answer/10787469?hl=en

4. Mahesh Atapattu, Mobile Application Data Collection and Data Sharing: What You Need to Know, July 2023. follow link: https://www.linkedin.com/pulse/mobile-application-data-collection-sharing-what-you-need-atapattu/

5. McClain, Colleen,et al, How Americans View Data Privacy, PEW, October 2023, follow link: https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

6. M3: Insecure Communicatio, Clouddefense, follow link: https://www.clouddefense.ai/owasp/2016/3

7. mobile app security risks and how to mitigate them, Cypress Data Defense, July 2020. follow link: https://2u.pw/PKH0B660

8. Twingate Team, what happened in the park mobile data breach?. Twingate, may 2024, follow link: https://www.twingate.com/blog/tips/park-mobile-data-breach

9. Ben Forster, why hackers like your remote access and what you can do about it, Paloalto Networks, Jun 2021. follow link: https://www.paloaltonetworks.com/blog/2021/06/why-hackers-like-your-remote-access/

10. Adam Hayes, Banker Trojan: What it Means, How it Works, July 2022. follow link: https://2u.pw/Ys1Bc3lq

11. Kurt Baker, What is Mobile Malware?, CROWDSTRIKE, November 2023. Follow link: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/mobile-malware/

12. Sanja Trajcheva, et al, What is Click Fraud? how it works, examples, and red flags, Cheq, January 2024. follow link: https://cheq.ai/blog/what-is-click-fraud/

13. The State of Fake Traffic 2023. Cheq, follow link: https://cheq.ai/blog/what-is-click-fraud/

14. Linköping University, The hidden costs of free apps – more than personal data, Alpha Galileo, October 2024. follow link: https://2cm.es/OeMk

15. Jacob Leon Kröger, how data can beused against people:a classification of personal data misuses, December 2021. follow link: https://linksshortcut.com/KGJvq

16. 7 Signs Your Phone Has a Virus and What You Can Do, Mcafee, August 2022. follow link: https://www.mcafee.com/blogs/mobile-security/7-signs-your-phone-has-a-virus-and-what-you-can-do/

17. Stephanie Taylor, 10 ways to make your phone safer, September 2011. follow link: https://linksshortcut.com/fUmGE

18. Anna Yaskiv, App Tracking Transparency: what Data do Apps Collect and why?, January 2022. follow link: https://linksshortcut.com/xXsmi

الوكالة الوطنية للامن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنية للسلامة الرقمية
Digital Safety National Initiative