ISSUE 03

Cyber Guardian

Publication for your online safety

2024

Sri Lanka CERT|CC
Sri Lanka Computer Emergency Rediness Team
Coordination Centre

How Untrusted Mobile Apps Threaten Your Security and Privacy

Untrusted mobile apps are applications that pose potential security risks due to their origin, behavior, or lack of verification. These apps may be designed to harm users, steal personal data, or compromise the device's security. Here's a detailed look at what untrusted mobile apps are and the risks they pose:

Characteristics of Untrusted Mobile Apps

1. Unknown or Unverified Sources:

Apps not available on official app stores (Google Play Store, Apple App Store) and instead found on third-party websites or alternative app stores.

2. Excessive Permissions:

Apps requesting more permissions than necessary for their functionality, such as access to contacts, messages, location, camera, and microphone.

3. Malicious Intent:

Apps designed to install malware, spyware, adware, or ransomware on the user's device.

4. Impersonation or Cloning:

Fake apps that mimic legitimate applications to deceive users and steal information.

5. Insecure Coding:

Poorly coded apps that may unintentionally expose user data or device vulnerabilities

Using untrusted mobile apps can pose significant security risks. Here are the primary security concerns associated with using such apps.

Data Theft and Privacy Invasion

· **Access to Personal Information:** Untrusted apps may request permissions to access personal data, such as contacts, messages, photos, and location. This data can be harvested and misused.

· **Unauthorized Data Collection:** These apps might collect sensitive information without user consent and share it with third parties, leading to privacy breaches. Malware and Spyware

Malware and Spyware

· **Malicious Software:** Untrusted apps can contain malware, including viruses, trojans, and spyware, which can infect your device and steal data or cause damage.

· **Keyloggers:** Some malicious apps may install keyloggers that capture everything you type, including passwords and other sensitive information.

Financial Risks

· **Phishing Attacks:** Untrusted apps may facilitate phishing attacks, tricking users into providing financial information, such as credit card details and banking credentials.

· **Unapproved Transactions:** These apps can initiate unauthorized transactions, leading to financial loss.

Device and Network Compromise

· **Root Access Exploits:** Some apps may exploit vulnerabilities to gain root access to your device, giving attackers full control over your device.

· **Network Attacks:** Malicious apps can manipulate network settings or conduct attacks on your network, compromising other connected devices.

Ransomware

· **Data Encryption:** Ransomware apps can encrypt your data and demand a ransom for its release, potentially leading to data loss if the ransom is not paid.

Identity Theft

· **Credential Harvesting:** Untrusted apps may steal login credentials for various services, leading to identity theft and unauthorized access to your accounts.

Adware and Unwanted Ads

· **Intrusive Ads:** Some apps may display intrusive ads or install adware, which can be annoying and potentially harmful by redirecting to malicious websites.

→ Page 02

Reduced Device Performance

· **Resource Drain:** Malicious apps can consume significant system resources, slowing down your device and draining the battery quickly.

How to Protect Yourself

1. Download from Official App Stores: Only download apps from trusted sources like Google Play Store and Apple App Store.

2. Check App Permissions: Review the permissions an app requests and ensure they are necessary for its functionality.

3. Read Reviews and Ratings: Check user reviews and ratings to gauge the app's trustworthiness.

4. Install Security Software: Use reputable antivirus and anti-malware apps to scan and protect your device.

5. Keep Your Device Updated: Regularly update your operating system and apps to patch known vulnerabilities.

6. Avoid Jailbreaking or Rooting: This can expose your device to additional security risks.

7. Be Wary of Links and Downloads: Avoid clicking on suspicious links or downloading apps from unverified sources.

8 By being cautious and taking preventive measures, you can significantly reduce the risk of security breaches associated with untrusted mobile apps.

CERT Conducts Cyber Security Awareness Program for ETF Officials

CERT recently led a cyber security awareness program tailored for selected government officials of the Employees' Trust Fund Board (ETF). This initiative, conducted in collaboration with the NextGenGov Foundation Capacity Building Program under the Integrated Capacity Building Program (ICBA), was organized by the Sri Lanka Information and Communication Technology Agency (ICTA).

Our Services

Comprehensive Software Security Services

We specialize in protecting software applications from cyber threats through comprehensive security measures and cutting-edge technologies. Our services include:

· **Vulnerability Assessments**: For mobile applications (Android, iOS, Harmony), software applications, web applications, and payment gateways.

· **Code Reviews and Penetration Testing**: Identifying potential weaknesses in your applications.

· **Proactive Defense Implementation**: Robust firewalls, intrusion detection systems, and encryption protocols.

· **Compliance**: VAPT for payment-related mobile applications under CBSL guidelines.

· **Security Training and Awareness**: Educating and equipping your team to handle security threats.

· **Security Incident Response**: Immediate action to mitigate and resolve security incidents.

By partnering with us, we ensure that your software applications are resilient against evolving cyber threats, preserving the integrity and confidentiality of your valuable data

An ISC2 CC Training Program

Sri Lanka CERT recently conducted an ISC2 CC training program on cybersecurity for government officials at the Sri Lanka Development Administration Institute.

This training qualifies participants for the ISC2 CC certification. The aim is to provide the necessary support to maintain cybersecurity in the public sector more vigorously. The program was supported by the ISC2 Colombo Chapter.