

February 14 ,2025  
SBI Holdings, Inc.  
SBI EVERSPIN Co., Ltd.

**Notice of Attention Regarding Malicious Apps Detected by Fake Finder,  
an AI-based App for Detecting Fraudulent Apps for Android OS**

SBI EVERSPIN Co., Ltd. (Head office: Minato-ku, Tokyo; Representative Director: Jamyung Yoon; hereinafter “SBI EVERSPIN”), a consolidated subsidiary of SBI Holdings, Inc. (Head office: Minato-ku, Tokyo; Representative Director, Chairman, President & CEO: Yoshitaka Kitao), which provides the AI-based apps for detecting fraudulent apps series on Android “Fake Finder,” announces that a malicious apps have been detected in the “Fake Finder” app, which is provided free of charge to customers using Wealth Advisor’s “My Investment Trust” and “MY Cryptocurrency” Android app services. This is to notify and alert customers for security awareness.

**1. Type of Malicious Apps**

- 1.1. **Type** : Fraudulent apps that attempt to steal personal information or fake apps that impersonate financial institutions or public agencies
- 1.2. **Description** : Apps created with malicious intent, such as those that steal the names or icons of relevant institutions, or fake apps that impersonate security program updates, user authentication functions, and other additional programs for financial apps.
- 1.3. **Example** : Once the app is installed, it automatically connects to the app developer’s server and downloads and installs other malicious apps onto the smartphone.

**2. Information and Initial Detection Time of Malicious Apps**

Case	PACKAGE_NAME	Initial Detection Time
①	chrome	2024-11-02 5:08
②	JPpost	2025-1-02 13:28
③	Chrome	2025-1-28 08:17
④	Chrome	2025-2-1 12:40

**3. Characteristics of Malicious Apps (Example of Impersonating Chrome)**



**3.1. Basics** : In the case of the fake Chrome app, the characters ‘ r ’ and ‘ *r* ’ look almost identical but use different fonts from the usual ones, utilizing Unicode.

-Request for access permissions to phone, files and media, SMS, and contacts

**3.2. Operation** : Due to an Android version issue, after a forced shutdown,  
an ‘invisible’ malicious app is automatically reinstalled.

**3.3. UI features** : The icon becomes hidden and is no longer visible.



(Please refer to the reproduction screen in 4.2 Case Example②.)

3.1. Reproduction of the 'Fake Finder' Malicious App Detection Screen	3.2. Error Message When the App is Force Closed
	

## 4. Operation of Malicious Apps

### 4.1. Initial Screen After Installation

: Request for access permissions to phone, files and media, SMS, and contacts

事例① JPpost	事例② Chrome
	

### 4.2. Execution Screen of Malicious App

: An 'invisible' malicious app is additionally installed.

目には見えない「オマケアプリ」がインストールされている。該当箇所を押すとアプリ情報が表示される

SMSを読み取る権限許可が自動設定されている

【事例① JPpostの偽アプリ実行画面】





## 5. Other detection results of remote control apps (\*) in “Fake Finder”


Aggregation Period	Number of Remote Control Apps Detected
From October 15, 2024, to February 14, 2025	647 cases

(\*) Remote control app : An app that monitors or controls a smartphone remotely

Malicious apps, such as the ones mentioned above, are often distributed outside official marketplaces. On Android devices, apps can be obtained from sources other than Google Play, which is exploited to distribute fraudulent apps. Recently, a wide variety of apps are offered by numerous developers, and it has become common for users to install apps on their smartphones. Taking advantage of this situation, attackers try to guide users to malicious apps. Therefore, downloading apps carelessly may lead to unexpected harm.

To avoid damage from malicious apps, it is essential to primarily obtain apps from official marketplaces and carefully check the reliability of the developer, app features, terms of use, and other details when choosing an app. We are currently offering the “[Fake Finder for SBI Group](#)” a free Android app for detecting fraudulent apps with 24/7 monitoring and comprehensive notifications. Please feel free to make use of it.

“Fake Finder for SBI Group” (for Android OS users) can be downloaded from the link below

	<a href="#">Fake Finder for SBI Group - Google Play App</a>
---	---

Free coupon code for “Fake Finder for SBI Group” is as below.

(Free coupon code is valid from February 14 to March 31, 2025)



SBI EVERSPIN leverages its extensive expertise gained through continuous research in cutting-edge security technologies and security vulnerability assessments to protect customers’ systems from evolving threats, such as hacking and unauthorized access. Through its collaboration with Wealth Advisor in the field of security, SBI EVERSPIN will support a digital environment in which customers using Wealth Advisor’s services can engage in asset management with peace of mind, and together we will work to create a safe and trustworthy society.

\*\*\*\*\*

For further information, please contact:

SBI EVERSPIN Co., Ltd. [contact@sbieverspin.co.jp](mailto:contact@sbieverspin.co.jp)