O/o Deputy Director, Department of School Education Bilaspur (H.P.)
Office address: O/o Dy. Director School Education, Bilaspur, Changer Sector Near D.C office, Bilaspur-174001.

Ref.EDN-DDHE(blp)- IT- Misc. 4817 Date: 15/9/2025

To

The Principals & Headmasters
GSSSs/ GHSs/Private Schools
Distt. Bilaspur, Himachal Pradesh.

Subject: Request for Awareness and Precautionary Measures regarding fake APK files circulated on Whatsapp Groups.

Memo,

This is in reference with letter No. CR/Mandi/25-4525/5A dated 11-9-2025, received from Additional Superintendent of Police, Cyber Crime, Police Station Central Range, Distt. Mandi, regarding the subject cited above.

In this context, some urgent preventive actions have been suggested and all the Heads of schools are directed to go through the contents (attached) and aware/ circulate the attached advisory among the staff and aware the students too in this regard.

Encls: Letter and Advisory.

15/09/2025

Dy. Director Secondary Education
Bilaspur, District Bilaspur
Himachal Pradesh-174001.

OFFICE OF THE

ADDITIONAL SUPERINTENDENT OF POLICE

CYBER CRIME POLICE STATION CENTRAL RANGE MANDI (H.P)

E-mail Id- [illegible] Contact No.01905-226900

No: CR/Mandi/ 25- 4525/SA Date: 11-9-2025

G-III

To

The Deputy Director Higher Education,
District Mandi, Bilaspur, Kullu, Hamirpur and L&S, H.P.

Subject: Request for Awareness and Precautionary Measures Regarding Fake APK Files Circulated on WhatsApp Groups.

Respected Sir/Madam,

As you are aware, incidents of cybercrime are increasing rapidly in Himachal Pradesh. Recently, the Cyber Crime Police Station, Central Range Mandi, has received multiple complaints regarding WhatsApp account hacking, financial fraud, and mobile phone compromise. During inquiry, it was found that several individuals had unknowingly downloaded and installed fake/malicious APK files circulated through WhatsApp groups. Though shared as legitimate applications, these files were in fact malicious programs designed to steal personal information and compromise WhatsApp accounts. Some reported examples include:

- **customercare.apk**
- **RTOchalan.apk**
- **Vahan chalan.apk**
- **Invitationcard.apk**
- **SBIcard.apk**

O/o of Deputy Director Higher Edu. Diary No. 3800 Date 11/09/25 Bilaspur Himachal Pradesh

In light of these incidents, you are **requested to take the following urgent preventive actions in your school/institution:**

1. **Awareness among Staff and Students:** Disseminate this advisory immediately among all Principals, Headmasters, teachers, and staff under your jurisdiction.
2. **Circulation of Attached Advisory:**
   - Share the attached Cyber Advisory with staff, students, and parents.
   - Encourage parent-teacher associations to further spread awareness.
   - Display advisory posters/notices at prominent places such as school notice boards, libraries, and community centers.
3. **Direct Immediate Action:** Instruct individuals who may have already downloaded such APK files and are experiencing suspicious activity on their devices to immediately contact the Cyber Helpline **1930**, the nearest Police Station, or the Cyber Crime Police Station, Mandi, HP.

These measures will play a vital role in safeguarding students, staff, and the general public from **cyber frauds and financial losses.**

Encls: Advisory

Your sincerely,

Additional Superintendent of Police
Cyber Crime Police Station
Central Range, District Mandi, H.P.

Endst. No...../ Dated...../

1. The DIG, Cyber Crime, State CID Shimla (HP) – for information please.
2. The SP, Cyber Crime, State CID Shimla (HP) – for information please.

Additional Superintendent of Police
Cyber Crime Police Station
Central Range, District Mandi, H.P.

Malicious APK से बचाव - Step by Step Emergency Checklist

Step 1: तुरंत रुक जाएं

- मोबाइल का Wi-Fi, Mobile Data और Bluetooth बंद करें / Aeroplane Mode ON करें और SIM को तुरंत मोबाईल फोन से remove करें।
- बैंकिंग, ईमेल या सोशल मीडिया में लॉगिन न करें।

Step 2: ऐप हटाएँ

- Settings → Apps → [शक वाला ऐप] → Uninstall करें।
- अगर Uninstall न हो → Safe Mode में जाकर हटाएँ।
- Settings → Apps → Permissions → सभी Permission बंद करें।
- Settings → Security → Device Admin Apps → अनजान ऐप हटाएँ।

Step 3: बैंक और अकाउंट सुरक्षित करें

- किसी दूसरे सुरक्षित मोबाइल/कंप्यूटर से:
  - Banking Password, UPI PIN, Debit/Credit Card PIN बदलें।
  - Two-Factor Authentication (2FA) ON करें।
- बैंक की Fraud Helpline पर कॉल करके जानकारी दें।
- SMS/Email पर आने वाले बैंक अलर्ट चेक करते रहें।

Step 4: मोबाइल को साफ करें

- M-Kavach App (सरकारी सुरक्षा ऐप) इंस्टॉल करें।
- अपने फोन को Scan करें।
- जो भी Risky/Unknown Apps हों उन्हें तुरंत Delete करें।

Step 5: भविष्य के लिए सुरक्षा

- Settings → "Install unknown apps" OFF रखें।
- Google Play Protect ON रखें।
- SMS/WhatsApp/Telegram/Email से आए APK लिंक पर कभी क्लिक न करें।
- बैंक अकाउंट की Activity Regularly चेक करें।

Step 6: हमेशा याद रखें

- कभी भी Social Media Platforms (WhatsApp, Telegram, SMS, Email, Websites) से आए ऐप इंस्टॉल न करें।
- सिर्फ Google Play Store (Android) और App Store (iOS) से ही ऐप डाउनलोड करें।
- किसी भी तरह के Remote Access Apps (AnyDesk, TeamViewer आदि) बिना बहुत ज़रूरी कारण के कभी इंस्टॉल न करें।

Step 7: SMS और Call Forwarding चेक करें

- Settings → Call/SMS → Forwarding Options में जाएं।
- देखें कि Message Forwarding ON तो नहीं है।
- देखें कि Call Forwarding ON तो नहीं है।
- अगर ON हो तो तुरंत Cancel/Disable करें।