SUBJECT: **CYBER SECURITY ADVISORY - MULTIPLE COMMONLY USED WEB BROWSER EXTENSIONS HACKED (ADVISORY NO. 03/2025)**

Context. Reportedly, a new attack campaign has been unearthed targeting commonly used browser extensions to steal personal information and credentials of applications used via browser e.g. facebook, banking websites etc.

2. **Technical Details**. Malicious code is sent through phishing techniques in order to compromise targeted publishers of legitimate extensions; further stealing user's PII using said extensions. At least 16 common extensions (including VPN and AI ChatBots) are suspected to be compromised:

a. AI Assistant – ChatGPT and Gemini for Chrome

b. Bard AI Chat Extension

c. GPT 4 Summary with OpenAI

d. Search CoPilot AI Assistant for Chrome

e. Wayin AI

f. VPNCity

g. Internxt VPN

h. Vidniz Flex Video Recorder

i. VidHelper Video Downloader

j. Bookmark Favicon Changer

k. UVoice

l. Reader Mode

m. Parrot Talks

n. Primus

o. Trackker – Online Keylogger Tool

p. AI Shop Buddy

q. Rewards Search Automation etc.

3. **Recommendation**. Above in view, following safe usage guidelines are suggested for all browser extension users:

a. Avoid above mentioned extensions for time being and use alternate well reputed options.

b. Only install trusted extensions.

c. Read and review permissions and ratings.

d. Limit permissions where possible.

e. Regularly update extensions.

f. Remove unused extensions.

g. Use well reputed and licensed Antivirus software.

h. Be wary of free extensions.

i. Actively monitor system utilities and data usage for abnormal activity.

4. Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments and ensure necessary protective measures.