Subject: - **Cyber Security Advisory - Fake Emails to Ministries/Divisions (Advisory No. 04)**

It has come to our notice that fraudulent emails purportedly originating from "JS (Coord)" are currently in circulation. These emails may contain malicious attachments or payloads aimed at compromising the security of our networks and systems.

2. All Ministries/Divisions and Government departments are urged to exercise caution and adhere to the following:

a. **Remain Vigilant**. Be cautious when receiving emails from both known/familiar sources such as "JS (Coord)" and unknown or suspicious sources. Scrutinize those requesting sensitive information or containing unexpected attachments.

b. **Verify Sender Information**. Verify the authenticity of the sender's emails address and domain. Pay close attention to any discrepancies or irregularities that may indicate fraudulent activity.

c. **Avoid Clicking Links or Opening Attachments**. Refrain from clicking on links or opening attachments from unfamiliar or untrusted sources. Malicious links or attachments may contain malware or phishing material designed to exploit vulnerabilities.

3. Please be advised that legitimate communications from "JS (Coord)" will originate from official government email addresses with appropriate domain extensions. Any deviation from these established channels should be treated with skepticism and reported immediately.