Subject: **Cyber Security Advisory – Threat Actors Targeting Government Offices/Officials Through Impersonation (Advisory No. 50)**

Context. It has been reported that hackers have accelerated their activities against Government offices/officials by exploiting the human curiosity to open malicious links being sent through social media platforms and emails etc. These threat actors are impersonating high level officials, and if the malicious links are clicked, the targeted mobiles and computer systems are infected. The infected systems then can lead to launch of sophisticated attacks including extraction of sensitive information and gaining unauthorized access to the target device to become transmitters of information and even voice.

2. **Modus Operandi**. Target may receive an email link on social media platforms/emails from a familiar originator to deceive people into opening of the malicious link, which is exploited by threat actors in following ways:

a. Impersonation of high-level government officers or trusted contacts of reputable organizations/ individuals for further luring in the victims to exploit their mobile phones.

b. Mobile numbers of high-level officials (since most of the contact lists had been leaked/hacked over a period of time from mobile phones of officials) are being used by threat actors to send phishing emails/spoofed SMS/WhatsApp messages to selected targets.

c. Well-crafted message to trick the victims to disclose their sensitive information or click on suspicious links/ attachments.

3. **Guidelines/Preventive Measure against Phishing Emails**

a. If a link is received in email/message from a known/unknown user, always confirm it from sender before opening.

b. Before downloading any attachments, including trusted attachments, scan them with the antivirus provided by the email-service provider. If email service does not provide virus scanning services, all downloaded files may be scanned with local antivirus before opening.

c. Apply updates to Operating System and Software Applications on all computing devices such as PCs, laptops, mobiles, wearables etc.

d. Use well-reputed and trusted antivirus/antimalware in all computing devices.

e. Never use personal accounts on official devices.

f. Use Multi Factor Authentication (MFA) wherever possible.

g. Never share personal details and credentials with unauthorized/ suspicious users, websites, applications etc.

h. Always type URLs in the browser rather than clicking on links.

i. Always open websites with HTTPS and avoid visiting HTTP websites.