**Subject:-** **Hacking Attempts of Hostile Intelligence Agencies (HIAs) Using Spoofed Messages (Advisory No. 46)**

**Context**. Of late, HIAs have accelerated their hacking attempts against officers especially senior officers by exploiting the human psychology/allure of curiosity to call back an unfamiliar number, which if successful, can lead to launch of sophisticated attacks including extraction of sensitive information and gaining unauthorized access to targets' device.

2. **Modus Operandi**. Target may receive a one ring/missed call from a familiar number to trick people into returning missed call or SMS, which is exploited by HIAs in following ways:

a. Impersonation of trusted contacts of reputable organizations/ individuals for further luring in the victims to exploit their mobile phones.

b. Mobile numbers of military/defense forces personnel (since most of the contact lists had been leaked/hacked over a period of time from mobile phones of military/defense personals) are being used by HIAs to send spoofed SMS/WhatsApp messages to selected targets.

c. Missed Call or sharing of a well-crafted message to trick the victims to disclose their sensitive information or click on suspicious links/ attachments.

d. Spoofed numbers can be generated from various websites/ applications. Most spoofing services append originator's country code for international callings, therefore, in some sloppy hacking attempts those numbers are appended with Indian country code (+91) as well.

3. **Remedial Measures**. A few best practices are being enumerated as a basic remedy to avoid any undesirable episode:

a. **Do Not Respond to Unknown Calls/Messages**. Do not pick up/call back to calls from unknown numbers/source and do not respond to unknown messages. Also, carefully examine the number of caller/message sender for spoofing. Treat missed calls and SMS from unfamiliar numbers with suspicion, especially if they are from international numbers.

b. **Enable Two-Factor Authentication (2FA)**. Utilize/enable 2FA for WhatsApp and other relevant platforms to add an extra layer of security to your accounts/applications.

c. **Avoid Clicking Suspicious Links**. Refrain from clicking on links received via SMS or WhatsApp unless confident about their authenticity.

d. **Update and Secure Devices**. Keep mobile devices and applications up to date with the latest security patches/updates to mitigate vulnerabilities.