Subject: - **Cyber Security Advisory – Prevention against Typosquatting Attacks (Advisory No. 33)**

Context. It has been observed that cyber actors are using malicious websites with names similar to the names of legitimate government websites. The fake websites' names comprises of common misspellings or short-names of government websites (called typosquatting attack) to deceive users to unwittingly type their passwords and other sensitive information or download malware on their systems/devices.

2. **Common Techniques Used**

a. Attackers use web-based redirections to legitimate websites on their malicious webpages. This technique masquerades malicious websites as legitimate government websites.

b. Above in view, there is a dire need for all government organizations (both civil and military) to take measures to prevent such attacks against their websites. Moreover, rigorous awareness campaign must be carried out by the website owners (CII organizations) to make their users aware of such attacks.

3. **Preventive Measures for Typosquatting Attacks**. Few preventive techniques (but not limited to) against Typosquatting attacks are as under:-

a. Web servers to be configured to restrict cross-domain redirections from unknown websites to legitimate domains.

b. Open Source tools and scripts such as dnstwist (https://github.com/elceef/dnstwist) must be regularly used to enumerate possible malicious domains aiming at a typosquatting attack. Such domains (once found) will be blocked through PTA.

c. Awareness campaigns must be carried out by all the organizations/ departments to educate their users about such attacks.