bject: **Advisory – Cyber Security Threat of ChatGPT (Advisory No. 31)**

Context. ChatGPT is an Artificial Intelligence (AI) backed chatbot developed by (Microsoft-funded Company) OpenAI, which has gained an explosion of interest and popularity among masses since its prototype launch on 30 November, 2022. Even though such a close-to pinnacle development of AI brings the promise of augmenting work of cyber threat hunters and defenders, it carries critical risks in the realms of leading cyber threat such as phishing and malware development. To prevent the menace of such AI-enabled exploitation, extreme caution, due diligence and due care is to be practiced on a proactive basis. In this regard, guidelines are provided in ensuing paras for sensitization.

2. **ChatGPT-Malicious Capabilities**. Following is a non-exhaustive list of ways malicious actors can use ChatGPT:-

a. **Malware Generation**. Malware generation by ChatGPT is no longer a mere theoretical possibility. Its use is already gaining traction and is under discussion in various Dark Web forums.

b. **Phishing Emails**. ChatGPT has demonstrated capability to generate extremely convincing phishing and spear-phishing emails, which carry the possibility and probability of slipping through email provider's spam-filters.

c. **Scam website**. With the lowered bar for code generation, ChatGPT can help less-skilled threat actors effortlessly build malicious websites such as masqueraded and phishing-landing pages. For example, malicious actors with zero to little skill can clone an existing website with ChatGPT and then modify it, build fake e-commerce websites or run a site with scareware scams etcetera.

d. **Disinformation Campaigns**. With ChatGPT, users have access to software that is able to write extremely convincing prose, generate thousands of fake news stories and social media posts in a fraction of time.

3. **Guidelines/Preventive Measure**

a. **Prevention against Phishing Emails**

(1) Never open unknown, unanticipated and/or suspicious emails, links and attachments.

(2) 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.

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

(4) Use well-reputed and trusted antivirus/antimalware in all computing devices.

(5) Never use personal accounts on official devices.

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

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

(8) Always type URLs in the browser rather than clicking on links.

(9) Always open websites with HTTPS and avoid visiting HTTP websites.

b. **Anti-Masquerading Guidelines**

(1) **Administrators**

(a) Restrict incoming traffic and user permissions to the maximum-possible extent, by implementing system hardening at OS, BIOS and Applications level.

(b) Unauthorized storage media (such as USBs) be blocked via system hardening.

(c) Format removable media frequently to avoid lateral propagation of malware to the extent possible.

(d) Monitor network activity by (at-least) employing checks via file hashes, file locations, logins as well as unsuccessful login attempts.

(e) Use reputed and trusted Anti Malware, Anti-virus, Firewalls, IPS, IDS, SIEM solutions.

(f) Use separate servers/routing for offline LAN and online networks.

(g) Allow internet access to specific users on need basis and restrict data usage/applications rights.

(h) Verify software and documents before downloading via digital code-signing technique.

(i) Implement MFA in mailing systems administrator controls and other critical systems.

(j) Always maintain back-up of critical data periodically.

(k) Regularly change passwords at administrator level.

(l) Regularly patch and update all OS, applications and other technical equipment.

(m) In order to reduce the attack surface of malicious code execution; it is advisable that the user should always login with the account having standard user privileges.

(2) **End-Users**

(a) Always re-verify trusted users who have sent email/attachment via secondary means (call, SMS, verbal) before downloading.

(b) Report any suspicious activity to the Administrator immediately.

(c) Never store critical data on online systems, rather store it on standalone systems.

(3) **Guidelines for ChatGPT users**

(a) When using ChatGPT, be mindful of the information shared. Avoid sharing sensitive or confidential information, such as passwords, financial information or personal details.

(b) Use caution with links and attachments. ChatGPT may provide links or attachments as part of its answers, but it's important to exercise caution before clicking on them. Always verify the source of the link or attachment and beware of suspicious/unknown sources.

(c) Official phones MUST NOT be used for ChatGPT.

(4) In case of encountering a security issue while using ChatGPT, please report it immediately to Open AI.

c. **Prevention against Disinformation Campaigns**

All Government Departments to undertake following actions as preventive measures: -

(1) Awareness campaigns and trainings be regularly arranged.

(2) Always try to verify information from multiple sources.