Subject: **Cyber Security Advisory-Cautious Use of Websites Containing Ads/Redirection (Advisory No. 16)**

Recently, Israeli Cybersecurity hacking firm M/S Novoshield has targeted citizens of Qatar for probable hacking of mobile phones/devices using social media (SM) platforms (Boomsocial's Facebook page) containing fake/malicious advertisements. The Facebook page redirects users to data gathering forms including PII (E-mail ID, Phone number, etc.). The acquired PII details are further used to drop malwares through phishing emails and SM links containing malicious attachments.

2. Above in view, users are advised to avoid emails/SM engagement with M/S Novoshield, Boomsocial and all other suspicious companies asking for personal data of users, online. Users must remain cautious for malicious emails/SM links as majority of hacking attempts are conducted through phishing messages.

3. Further, guidelines for protection against phishing emails and general cyber security guidelines are attached at **Annex-A** for compliance.

Annex-A

GUIDELINES OF CAUTIOUS USE OF SOCIAL MEDIA PLATFORMS/LINKS

1. **Avoid PII Exposure**

   a. Avoid providing personal details in suspicious internet campaigns.

   b. Avoid sharing email ID with unknown persons.

   c. Always confirm the identity of the individual to/from whom email is being sent/received.

   d. Never use official email for private communication. Always use separate email IDs for personal and official correspondence.

   e. Never configure/use official email on mobile phones.

2. **Anti-Phishing Guidelines**

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

   b. Never click on unknown links and attachments.

   c. Always scan every document before opening/downloading via built-in anti-virus on mailing servers.

   d. Never install unknown and suspicious applications.

   e. Always type URLs in browser rather than clicking on links.

   f. Always open websites with https and avoid visiting http websites.

   g. Disable macros on documents (MS Excel, MS PowerPoint, MS Word etc.)

   h. Never use personal accounts on official systems.

   i. Use multi-factor authentication (MFA)/two-factor authentications where possible.

   j. Use well reputed and updated anti-virus/anti-malware.

   k. Timely update all applications and Operating Systems (PC and mobile etc).

   l. Regularly review applications permission, system, running processes and storage utilization.

   m. Use separate and complex passwords for each system, mobile, SM accounts, financial and mailing accounts etc.

3. **Anti-Masquerading Guidelines**

   a. **Administrators**

      (1) Monitor networks including file hashes, file locations, logins and unsuccessful login attempts.

(2) Use reputed firewalls, IPS/IDS and SIEM solutions.

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

(4) Restrict incoming traffic and user’s permissions to maximum extent by implementing system hardening at OS, BIOS and application level.

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

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

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

(8) Always maintain back up of critical data periodically.

(9) Regularly change passwords at administrator level.

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

b. **Users**

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

(12) Never share personal details online unnecessarily.

(13) Report any suspicious activity to Administrator immediately.

(14) Never keep critical data on online systems and store it in standalone system.

(15) Always create a back-up of critical data and store in external drives or standalone systems.

(16) Keep strong passwords on BIOS, OS level, drives (via bit locker) and documents.

4. **General Guidelines**

a. Public WiFi is more susceptible to attack as compared to private WiFi.

b. Public WiFi administrator might be monitoring network traffic and data sent online via internet packets.

c. Passwords may be stored by network administrator. Therefore, avoid using public WiFi for accessing personal/official email.

d. Regularly check and apply security updates.