Dubai Financial Services Authority

By Email

27 March 2026

To: Senior Executive Officers (SEO) of DFSA Authorised Firms; Senior Officers (SO) of Registered Auditors; Money Laundering Reporting Officers (MLRO) of Designated Non-Financial Businesses and Professions (DNFBPs); and Principal Representatives of Representative Offices.

Dear SEO's,

Subject: Elevated Cyber Threat levels

The DFSA has observed recently events involving elevated cyber-attacks towards critical infrastructure and hybrid operations targeting technology service providers in the region.

In particular, we observed:

- threat actors conducting low-impact cyber operations, focusing on Distributed Denial-of-Service ('DDoS'), privilege users credential harvesting, and website defacements adversarial activity directed at financial institutions within the region.
- opportunistic exploitation of unmitigated vulnerabilities in internet-facing assets.
- surge in financial fraud, specifically e-mail and QR code-based impersonation attacks targeting both the organisation and its client base.
- hybrid operations targeting regional cloud services infrastructure.

In that regard, the DFSA would like to remind all Authorised Firms, Registered Auditors, DNFBPs, and Representative Offices to:

- maintain vigilant monitoring and conduct impact assessments within your specific operational environment. Recent intelligence indicates that low-level cyber incidents are frequently amplified to align with broader geopolitical narratives.
- notify the DFSA of any material security incident without delay, no later than 72 hours after becoming aware of such event, via the Cyber Incident Notification form as required in Rulebook GEN 5.5.19 for authorised persons. The notification form can be located on the DFSA ePortal.

Level 13, The Gate, PO Box 75850, Dubai, UAE
Telephone: +971 (0)4 362 1500
Fax: +971 (0)4 362 0801
Email: info@dfsa.ae

Dubai Financial Services Authority

- register with the DFSA Cyber Threat Intelligence Platform ('TIP') to receive and share timely cyber threat intelligence within the DIFC and the wider financial services community. The registration form can be found on the DFSA ePortal. Registered firms should engage in proactive threat hunting and share threat intelligence to enhance the collective cyber resilience and situational awareness of the DIFC community.

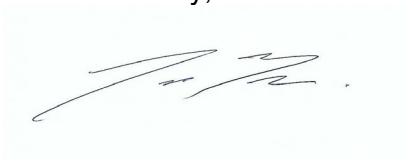
- conduct a review of your cyber risk management framework to evaluate its operational effectiveness. For Authorised Persons, in compliance with the Rulebook GEN 5.5 (Cyber risk management).

- prioritise risk mitigation efforts focused on identity and access management controls and the security of internet-facing assets.

- validate incident response processes through scenario-based simulations tailored to the current threat landscape.

If you have any questions, please contact us using the DFSA Supervised Firm Contact Form found on the DFSA ePortal.

Yours sincerely,



Justin Baldacchino
Managing Director, Supervision

CC: Compliance Officers of DFSA Authorised Firms
Audit Principals of DFSA Registered Auditors

Level 13, The Gate, PO Box 75850, Dubai, UAE
Telephone: +971 (0)4 362 1500
Fax: +971 (0)4 362 0801
Email: info@dfsa.ae