ADGM
أبوظبي العالمي

14 April 2025

Notice No.: FSRA/FCCP/33/2025

To: Senior Executive Officers (SEO) and Principal Representatives (PR) of FSRA's Authorised Persons and Recognised Bodies.

Dear SEO/PR,

RE: Cybercrime Prevention - Avoiding Phishing Attacks

In line with the Financial & Cyber Crime Prevention ("FCCP") department's commitment to keep FSRA Authorised Persons and Recognised Bodies informed of inherent and emerging cybercrime threats, this notice aims to raise awareness of the risks posed by phishing attacks.

The Growing Threat of Phishing

Financial institutions have become prime targets for cybercriminals seeking to exploit digital vulnerabilities for malicious purposes. Social engineering tactics such as phishing, have become one of the most prevalent cyber threats affecting firms and are often the first step in gaining unauthorized access to sensitive data.

A typical phishing attack involves the distribution of fraudulent emails or social media messages that solicit sensitive information. These communications often contain malicious file attachments or links to deceptive websites designed to capture credentials, potentially granting unauthorized access to device sensitive data. Once this information is compromised, it can lead to data breaches, further hacks, and identity theft, which serve as the foundation for larger financial crimes.

Given the sophistication of modern phishing tactics and the advancement of artificial intelligence, phishing attacks are becoming harder to detect. We encourage FSRA Authorised Persons and Recognised Bodies to remain vigilant and exercise caution when handling unsolicited communications.

***Recommended practices to reduce the risk* and safeguard your organisation against phishing attacks**:

➢ **Establish comprehensive awareness and training programs**
Firms must establish an enterprise-wide cybersecurity awareness program. Employees represent a significant cybersecurity risk, as inadvertent actions such as clicking on a link in a phishing email can lead to severe security breaches. Therefore, firms must ensure that cybersecurity awareness programs are implemented regularly to educate employees on recognizing and responding to phishing threats.

Recognising red flags; tips to identify possible phishing scams:

- Verify how the email is addressed. Generic terms like 'valued partner; 'friend' or 'colleague' rather than personalized salutations, may indicate a phishing scam.
- Check the misspelling of the sender's email domain.

- Be cautions of emails that create a sense of urgency, such as requests for immediate action within a specific timeframe.
- Watch out for emails that appear to originate from a high-ranking person within the organisation, particularly those requesting payment to a particular bank account.
- Pay attention to spelling, grammatical, or punctuation errors. Phishers may also attempt to create convincing emails using logos and graphics.

➢ **Encourage internal reporting**
Employees are encouraged to report internally and ask for help if they think they have received a phishing email. Immediate actions such as malware screening and password changes should be taken if a successful attack is suspected.

➢ **Review your digital footprint**
Limit the amount of sensitive information shared publicly on your organisation's website and social media accounts. Attackers often exploit publicly available information about your organisation and employees, sourced from websites and social media. Be mindful of the information shared online, as it could be exploited/leveraged by cybercriminals for more convincing phishing attempts.

➢ **Reinforce Standard Operating Procedures**
Ensure employees are familiar with standard operating procedures for communication and transactions, both internally and with external partners. This includes recognizing common channels of communication, verifying requests through trusted methods (e.g., phone calls for financial transactions), and being aware of typical timelines for actions.
Fostering this awareness can help employees identify suspicious or unexpected requests. Empowering them to question the authenticity of request can prevent costly mistakes.

➢ **Implement Two Factor Authentication (2FA)**
Firms are strongly encouraged to enable two-factor authentication to enhance account security. 2FA requires users to provide a second form of verification, such as a one-time code sent to a mobile device or generated via an authentication app, in addition to their password. This added layer of protection significantly reduces the risk of unauthorised access, even in cases where login credentials have been compromised.

➢ **Adopt the principle of ‘least privilege’ in account configuration**
Firms are advised to configure user accounts in accordance with the principle of least privilege, granting employees only the minimum level of access necessary to perform their job functions. Limiting access rights could reduce the potential impact of a successful phishing attack and strengthen the organisation’s overall security posture.

➢ **Back up data**
All businesses, regardless of size, are expected to perform regular backups of critical data. Backups should be recent, securely stored in a location isolated from the main network and readily accessible for restoration in the event of data loss or compromise.
Integrating backup practices into the organisation’s routine operations and regularly testing both backup and recovery procedures are essential for ensuring effective and timely execution when required.

Your cooperation and vigilance in adhering to these measures are crucial to maintaining the integrity, security, and stability of the ADGM and wider UAE's financial system.

For any further clarification, Authorised Persons and Recognised Bodies are required to reach out by email to fccp-cybercrimeprevention@adgm.com.

Sincerely,

Financial & Cyber Crime Prevention