waystone | Compliance Solutions

Phishing Detection and Prevention: Key Takeaways from the SFC Circular

Leo Wong August 18, 2025

As phishing scams continue to impact clients and markets in 2025, the Securities and Futures Commission (SFC) issued a circular in May titled, "Phishing Detection and Prevention." The circular, directed at licensed corporations (LCs), addresses the growing number of attacks that have resulted in client financial losses.

It outlines standards for detecting and preventing phishing attempts, along with reminders of Code of Conduct obligations to report incidents to the SFC. Recent phishing SMS messages containing malicious hyperlinks have led to unauthorized transactions and potential market manipulation, prompting the SFC to stress the need for proactive measures for client protection and market integrity. These guidelines support LCs in strengthening their risk management and enhancing operational resilience.

Why It Matters

Phishing remains a major cyber security threat to Hong Kong's financial sector, driven by the rise in digital client interactions. The SFC's February 2025 cyber security review identified weak monitoring systems and insufficient client education as key vulnerabilities. For LCs, inadequate phishing defenses risk can result in significant client losses, regulatory fines, reputational harm, and even potential license suspension.

With rising fraudulent SMS scams luring clients to fake websites, the SFC's circular underscores the need for robust controls to prevent unauthorized access and potential market misconduct. Strengthening compliance not only mitigates these risk but also reinforces investor trust amid evolving digital threats and heightened regulatory scrutiny on AML and operational resilience.

Expected Standards for Phishing Detection and Prevention

The SFC's circular reinforces its cyber security expectations for licensed corporations to protect clients from phishing scams, building on previous regulatory guidance.

The circular outlines the following key standards:

- **Avoid Hyperlinks in Communications:** LCs should refrain from sending emails or SMS messages containing hyperlinks to websites or apps for transactions to prevent redirection to malicious sites.
- **Safeguard Sensitive Information:** LCs must never request login credentials or one-time passwords through hyperlinks. Clients should be clearly informed that such requests will not be made and advised to avoid unverified sites.
- **Client Education:** Regularly issue cyber security warnings about phishing and encourage reporting suspicious messages to police if defrauded.

- **Strengthen Monitoring Systems:** Implement robust surveillance to detect unauthorized access to trading accounts, per Schedule 7 of the Code of Conduct, with automated pre-trade controls and post-trade monitoring for manipulative activities.

LCs must promptly notify clients of phishing incidents and assist affected individuals in reporting cases to relevant authorities. These steps align with broader SFC cyber security requirements, which also include maintaining up-to-date anti-malware tools and conducting regulatory phishing simulations to test and enhance internal defenses.

Notifications to the SFC

The circular reinforces LCs' reporting obligations under the Code of Conduct. LCs must immediately notify the SFC in the event of:

- Any material failure, error, or defect in trading, accounting, clearing, or settlement systems (Code of Conduct, paragraph 12.5(e)).
- Any suspected material breach of market misconduct provisions under Parts XIII or XIV of the Securities and Futures Ordinance, including details and supporting documents (paragraph 12.5(f)).

Timely reporting enables the SFC to investigate potential market manipulation arising from unauthorized transactions, thereby protecting the integrity of Hong Kong's financial markets.

Strengthening Internal Controls and Governance

The SFC's circular underlines the importance of phishing prevention for licensed corporations (LCs), aligning with Code of Conduct requirements for robust risk management and client disclosures.

To meet these expectations, LCs are encouraged to:

- Conduct gap analyses to identify weaknesses in current controls
- Update internal policies and procedures
- Enhance staff training on phishing red flags
- Integrate monitoring tools, especially for digital trading platforms where phishing intersects with AML obligations.

Engaging external consultants perform mock reviews can help uncover hidden vulnerabilities, while also supporting senior management oversight responsibilities. These proactive measures can help reduce the risk of incidents, regulatory inspections, and potential enforcement actions.

How Waystone Can Help

Waystone provides a comprehensive suite of Corporate Compliance Solutions tailored to support businesses expanding into or operating within Hong Kong. Our team is committed to strengthening compliance framework, so you can concentrate on growing your business with confidence.

To learn more about our Corporate Compliance Solutions, please reach out to your usual Waystone representative or our APAC Compliance Solutions via below.

Contact Us →