Cybersecurity

This FAQ aims to provide further guidance and practical examples for the implementation of the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (Guidelines).

1.1 Two-factor authentication (2FA)

Q1: What should an internet broker consider when selecting its 2FA solution?

A: 2FA is a principle-based requirement for authentication. An internet broker is free to select 2FA (including in-house developed) solutions which best align with its security infrastructure and are suitable for achieving its risk mitigation objectives.

In particular, an internet broker should assess and evaluate, with the assistance of solution providers or technical consultants where needed, the features, limitations and vulnerabilities of each 2FA solution being considered, and put in place compensating controls as appropriate. For example, an internet broker that deploys a short message service (**SMS**) for transmitting one-time passwords (**OTP**) should advise its clients against forwarding OTPs received from their mobile devices to other devices.

Given that 2FA solutions may become obsolete and ineffective over time due to technological advances, an internet broker should make reasonable efforts to keep abreast with the latest development and enhance its 2FA solution or implement compensating controls as needed.

Q2: Can "dual-password" model (eg, a password is used for system login and another password is required for order placement or two separate sets of passwords are required for system login) fulfil the 2FA requirement?

A: No, dual passwords only constitute a single factor in the authentication process, i.e., "what a client knows". Hence, it does not fulfil the 2FA requirement.

1.2 Implement monitoring and surveillance mechanism

Q3: Can you cite some examples of how an internet broker can detect unauthorised access to clients' internet trading accounts??

A: An internet broker may monitor (i) logging into multiple client accounts from the same IP address; and (ii) change of IP address for accessing the same client account from one country to another country in a short period of time.

1.3 Prompt notification to clients

Q4: Are internet brokers required to notify clients of each system login if clients already receive notifications of irregular logins (i.e. through a device which is not customarily used by the client)?

A: Our requirement is for internet brokers to notify clients promptly of each system login. But we accept that an internet broker could allow clients to opt-out from notifications of each system login provided that:

- the internet broker has the capability to identify irregular logins and promptly notify clients of irregular logins;
- the internet broker has provided adequate risk disclosures to clients who have acknowledged that they understand the risks involved in opting-out from notifications of each system login; and
- the clients have not opted out from trade execution notifications.

1.4 Data encryption

Q5: Is Demilitarised Zone (DMZ) considered as part of an internal network for the purpose of the data encryption requirement?

A: Yes, DMZ is considered as part of an internal network for the said purpose.

1.6 Stringent password policies and session timeout controls

Q6: How often should an internet broker remind its clients to change their passwords?

A: Internet brokers would generally be expected to remind clients who have not changed their passwords for more than 90 calendar days.

Q7: What controls can internet brokers implement on invalid login attempts?

A: Internet brokers may, among other things, implement the following controls:

- account lockout;
- exponential back-off between successive failed login attempts; and
- brute-force attacks detection with appropriate responses.

The above list is not exhaustive and internet brokers can choose to implement any controls they deem appropriate.

2.8 System and data backup

Q8: Can "remote backup server" qualify as an "off-line medium" used for the system and data backup?

A: Yes, the term "off-line medium"[1] refers to tape or any other kind of medium, such as remote backup server, which is securely segregated from the production system.

[1] As referred to in paragraph 2.8 of the Guidelines and paragraph 1.2.6(b) of Schedule 7 to the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission