Security Alert: Fraud and Scams

Sumitomo Mitsui Banking Corporation Malaysia Berhad (“SMBCMY”) would like to alert our customers to the various types of scams being perpetrated and to advise our customers to take appropriate measures to protect themselves against these scams.

What are common types of scams?

Phishing emails refers to fraudulent emails that trick the receivers into sharing personal, financial or security information.

Smishing is the attempt by fraudsters to acquire the same information using mobile phone text messages.

Impersonation scams involve the fraudster sending emails from a well-known company or organization (e.g a government agency or banks), impersonating someone in senior management from the organization or even from your own company, a government official, a supplier or creditor requesting for payments to be made, or requests to transfer money to a new account or requesting for changes to log-in and security credentials.

How to spot Red Flags of a scam?

- Asks you to click on URL links or download attachments. The URL links provided will lead you to the phishing website which closely resembles the official webpage of the organization, complete with the entity’s logo
- Emails may look ‘official’ or close to identical to emails that actual organizations send
- Replicates the logos, the layout and tone of the official emails
- Conveys a sense of urgency such as stating that your account has been compromised, or there has been third-party activity on your account, and then asks you to provide or confirm your personal or account information
- Threatens consequences such as closing or suspending your account if you do not act immediately.

How can you protect yourself?

- Do not act on an email, phone call or text message that requires you to provide personal, financial or account information (such as account numbers, answers to security questions) directly in the email, non-secure webpage or text message
- Do not open emails or accompanying attachments, or click on URL links, from unknown sources.
- Never share your user ID, password, secure token device or the answers to your security questions with anyone.
- Do not be rushed into making a quick decision in response to an 'urgent' request.
- Do not use contact numbers or links provided in the emails or by the caller – this would be fake or spoofed details.
- Do not transfer money to another account upon request.

- ✓ Do pay special attention to links and attachments.
- ✓ Always use known contact details you have on record to validate a suspicious email request purportedly from SMBCMY.
- ✓ Be vigilant as fraudsters can find your company's basic information from any public domain including social media – Do not assume the request is genuine just because they have such details
- ✓ Use only software approved by your company and follow your company's data security policies.
- ✓ Forward suspicious emails that appear to come from SMBCMY to your SMBMY Representative.
- ✓ Call your SMBMY Representative immediately if you are repeatedly prompted for log-in information.

Reminder:

- SMBCMY will NOT request for your security information to be provided directly into the email
- SMBCMY will NOT ask you to confirm, verify or refresh your account, password, email, or other information via an email
- SMBCMY will NOT send emails threatening to close your account if you do not take the immediate action of providing personal or business information
- If you receive any alerts, and you or your authorized party did not initiate the change, please contact your SMBCMY representative immediately.

Example of Actual Case

Business Email Compromise

- The fraudster was able to spoof the emails of the banker, customer and supplier to initiate a change in banking details.
- The fraudster impersonated the customer and sent a request to the bank to change the registered bank account of the supplier to another bank.
- The emails were sent from the accounts which closely resembled the official addresses of the bank and the customer. It was later discovered that the fraudster had hacked into the email of the customer and the request to change the bank account was fake.
- Upon closer inspection of the fraudsters email accounts, the email address of the bank was spoofed with the email originating from a personal g-mail account but made to look like the official business email address of the banker.

Phishing Attempt

- Customer received an email from the banker which was suspicious in nature as it contained and an attachment which the recipient was not expecting
- The customer contacted the bank's representative who confirmed that no email was sent to the customer on that day.
- Closer inspection of the email address revealed that the bank email address was spoofed

Responding to a potential Scam

- ✓ If you have received a suspicious email, letter, SMS or phone call purportedly from SMBCMY, you should immediately contact your SMBCMY Representative.
- ✓ If you suspect that you have responded to a phishing email scam with personal, financial or any credentials information, you are advised not to respond further and inform your bank.
- ✓ You can report a scam to official authorities at the following contact numbers:
  1) Commercial Crime Investigation Department Scam Response Centre at 03-2610 1559/1599
  2) BNMTELELINK at 1-300-88-5465
- ✓ Members of the public can keep themselves updated on online scams via the Commercial Crime Investigation Department's special portal (https://ccid.rmp.gov.my/semakmule/)
- ✓ Lodge a police report to facilitate an investigation.