

30th June 2022

Advisory on Business Email Compromise (BEC) Crime

Thank you for banking with us.

There have been increasing reports of business email compromise (BEC) frauds worldwide, where fraudsters impersonate their target companies' business partners, CEOs or CFOs, and use a variety of methods such as spoof/phishing emails, fax messages, phone calls or bogus websites to instruct companies to make remittances.

Over the years, the techniques adopted by fraudsters have increased in sophistication, from hacking of email accounts to "deepfakes" scams, which are automated phone calls using artificial intelligence (AI) to imitate the voices of a target company's senior management or colleagues in order to deceive. Through such techniques of impersonation, these fraudsters have been known to put pressure on employees of targeted companies by rushing them to change remittance instructions. Other scammers have also been known to exchange emails with their intended targets over a period of several months to gain their trust before instructing them to commit fraudulent transactions.

Hence, please be reminded of our cyber hygiene practices:

1. Be careful with external email with an attachment and or / a link is a red flag. Validate the authenticity of the email before opening any attachment or clicking on any link.
2. If the email is a spam email or unsolicited email (you're not expecting the email), be more cautious.

As your trusted banking partner, MUFG would like to remind you to remain vigilant against BEC crime. If you are asked to make a sudden and urgent remittance to a new account, please check the legitimacy of the instruction. We have included a list of security tips in an attachment entitled "BEC red flags and recommendations" on the MUFG COMSUITE pre-login page for your reference.

Lastly, if you suspect that you or your company has been subject to a BEC scam, please contact your MUFG representative immediately.

Kindest regards,
MUFG Bank (Malaysia) Berhad

Security Tips

a. Secure Login ID, Password and PIN

1. Please don't disclose to anyone on your Login ID, Password or PIN.
2. Avoid storing your Login ID, Password or PIN on the computer or leave it at any place that is easily accessible by other persons.
3. Create a Password that is a combination of characters (uppercase and lowercase), numbers, and symbols and should be at least 8 digits in length.

b. Always Keep personal information private

Please don't disclose to anyone your personal information such as your address, telephone number, social security number, bank account number or e-mail address unless you are absolutely certain that the party requesting for and collecting the information is reliable and trustworthy.

c. Keep records of online transactions.

1. Regularly check transaction history details and statements to make sure that there are no unauthorized transactions.
2. Promptly and thoroughly review and reconcile your monthly bank statements for any errors or unauthorized transactions.
3. Immediately notify us if there are discrepancies or unauthorized entries or transactions in respect of the said services.

d. Check for the correct and secure website.

1. Before conducting any e-banking transactions or sending personal information online, make sure that you have accessed the correct website. Beware of bogus or "look alike" websites which are designed to deceive consumers.
2. Check if the website is "secure" by checking the Universal Resource Locators (URLs) which should begin with "https" and a closed padlock icon on the status bar in the browser is displayed. To confirm authenticity of the site, double-click on the lock icon to display the security certificate information of the site.
3. Always enter the URL of the website directly into the web browser. Avoid being re-directed to the website, or hyperlink it from a website that may not be as secure. For MUFG Malaysia Online Banking, please key in <https://ebusiness.bk.muftg.jp/login> when to login to GCMS Plus webpage.
4. If you are remitting fund to new beneficiary, you can utilize the PDRM CCID "Semakmule Portal" (<https://semakmule.rmp.gov.my/>) to check if the owner of a bank account or phone number has any criminal records or you also can reach out to CCID Scam Response Centre at 03-26101599/ 03-26101559 to seek for immediate assistance related to Mule Accounts or any suspected fraudulent activities.
5. If possible, use software that encrypts or scrambles information when sending sensitive information or performing e-banking transactions.
- 6.

e. Protect your personal computer from hackers, viruses and malicious programs.

1. Install a personal firewall and a reputable anti-virus program to protect your personal computer from virus attacks or malicious programs and ensure that any computer you use is similarly protected.
2. Ensure that the anti-virus program is up-to-date and runs at all times.
3. Always keep the operating system and the web browser updated with the latest security patches, in order to protect against weaknesses or vulnerabilities.
4. Install up-to-date scanner software's to detect and eliminate malicious programs capable of capturing personal or financial information online.
5. Never download any file or software or open any attachment from sites or sources, which are not familiar or hyperlinks sent by strangers. Opening such files could expose the system to malicious software that could hijack your personal information including password.