Precautions on Fraudulent Activity

Fraudulent websites

1) A fraudulent website is a fake website which looks genuine by using similar graphics and website address to those of the legitimate website with the purpose for them to collect your user login information to access your bank accounts in an unauthorized way.
2) To avoid going into any fraudulent Internet COMSUITE website, you should access COMSUITE by inputting the COMSUITE website address (i.e. https://ebusiness.bk.mufg.jp/, https://ebusiness.bk.mufg.jp/j/) in the address bar of the browser. You can also bookmark the COMSUITE website address and confirm every time when you use the bookmarked page to access COMSUITE. You are strongly urged NOT to access COMSUITE through any hyperlinks embedded in any emails or Internet search engines. Be alert any suspicious fraudulent websites that are published in the public.

Email Security Alerts

1) The Bank will never send you an email containing an embedded link, and request you to enter secret information. Remember not to click on the embedded link and input any sensitive information that might help provide access to your accounts, even if the page appears legitimate.
2) Remember that the Bank will never ask you for any of your password(s) by email, by phone, by written requests or by any other means.
3) If you believe that someone is trying to commit fraud by pretending to be the staff, an email or the website of the ‘MUFG Bank’, please contact the Account Officer responsible for your account immediately.