“Spam” Damaging Roles In Internet Banking Fraud

Wednesday, February 23, 2011
Fraud awareness Bulletin No.2
Virtual Banking, Cards & Loyalty Services

SPAM

The term SPAM is associated with a variety of meaning. With regards to virtual world, it refers to unsolicited emails. Most commonly received are emails about Viagra, pharmaceutical products and adult products. The subject of spam is cleverly composed to draw attention. Thankfully, with the advancement of email filtering system, spam is being ousted from user mailboxes. This has left the “spammers” with no other option except to switch their focus from direct advertisement and affiliates program to internet banking fraud.

Internet Banking

The advancement of email filtering system (such as **Bayesian spam filtering)** depends very much on the keyword being used by the spam email. The volume of spam has helped the system to improve itself as there are tremendous amount of spam emails that can be analyzed. On the contrary, this system is hardly effective in detecting internet banking spam due to the volume collected on the keyword is relatively low. The intention of any spam remains the same, that is to lure user to click on the link provided in the spam, but this time around, instead of getting affiliates commission on per click on advertisement, they wanted to infect users’ computers with virus that can steal internet banking usernames and passwords.

Staying safe online

Staying safe online is about understanding the risk in relation to information and instructions displayed on the webpage. It is about using your common sense towards what is logical and what is not

.

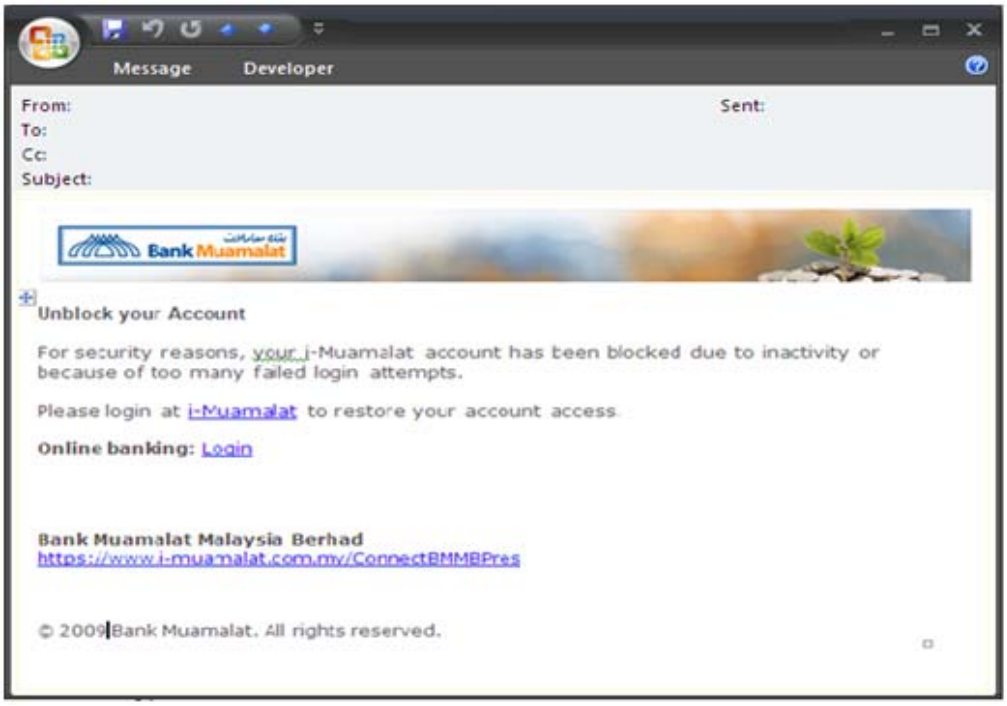
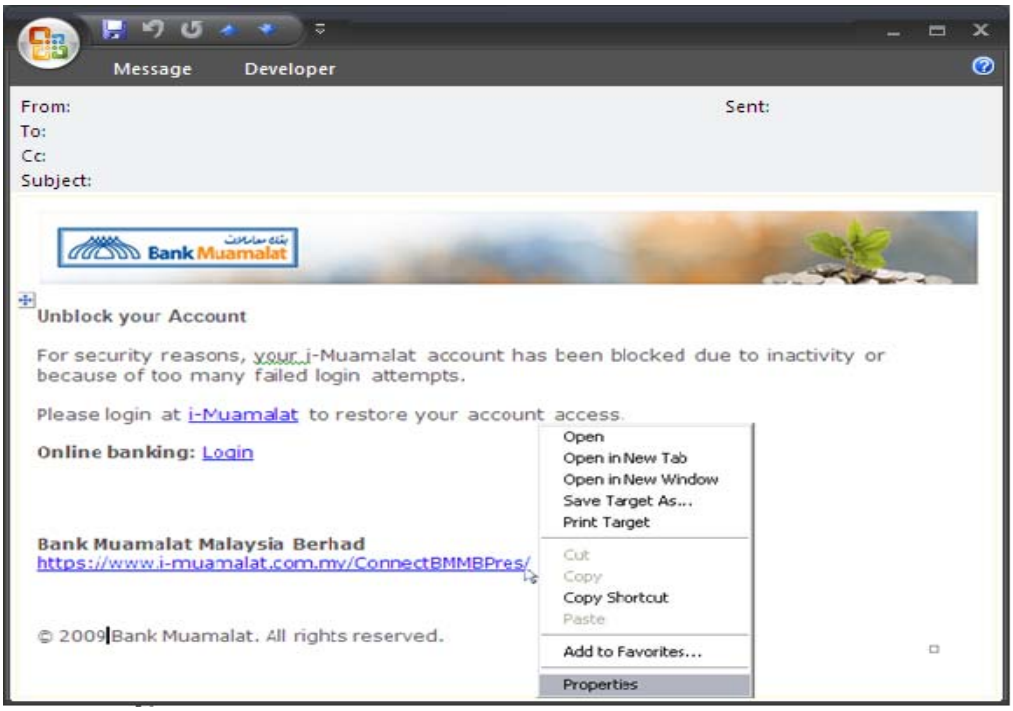


Figure 1 : Illustration of spam email

Refer to the illustration above. This kind of message is normally sent to you via e-mail. If you are not an internet banking customer of i-Muamalat, you might just ignore the e-mail. However, if you are a user, your first impression and instinct might urge you to follow the instructions as displayed. However, if you stop to think for a while maybe common sense will prevail. Is it logical that the bank would lock your internet banking ID if you had just log-in within the last few hours/days/weeks and you had never entered you password incorrectly? Secondly, is it possible that the bank knows your email address even though you have never mentioned it to them? Our advice is should you receive this kind of e-mail, it would be better to contact the bank ASAP. Never respond or follow the instructions displayed in the e-mail.

Additionally you can equip yourself with basic knowledge about the link in the email. Follow the following instructions:-

1. Move your cursor to the link and left click on the link that says login to restore your account then click on its properties as showed in the picture.



2. Upon comparing the Address (URL) to the genuine i-muamalat website, you will notice that the spam email is actually trying to redirect you to a fraudulent website

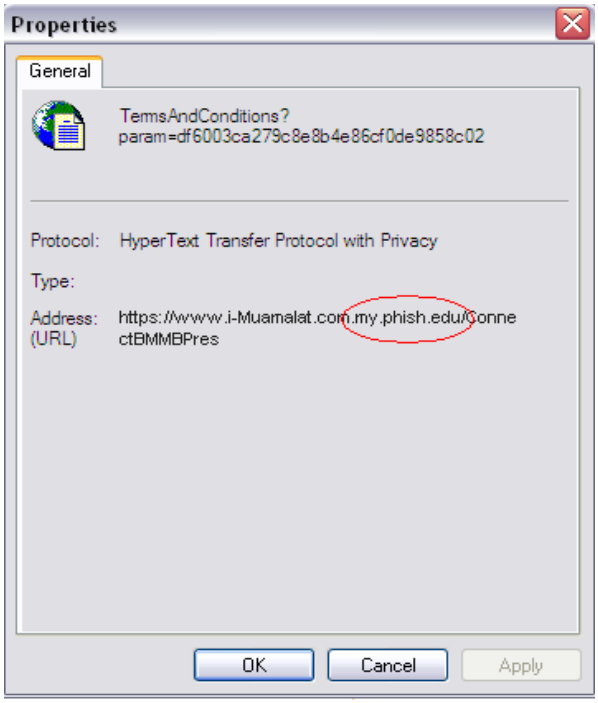


Figure 3 : Link that will redirect you to different place

In other words, the characters/words within the URL Address will tell you whether it is genuine site or not especially when there are additional names on the last dot or it is longer than the genuine address bar.

To sum all up...always be on alert and our suggestion is for you to go through the above authentication approach for "genuine" websites, especially on internet banking sites.

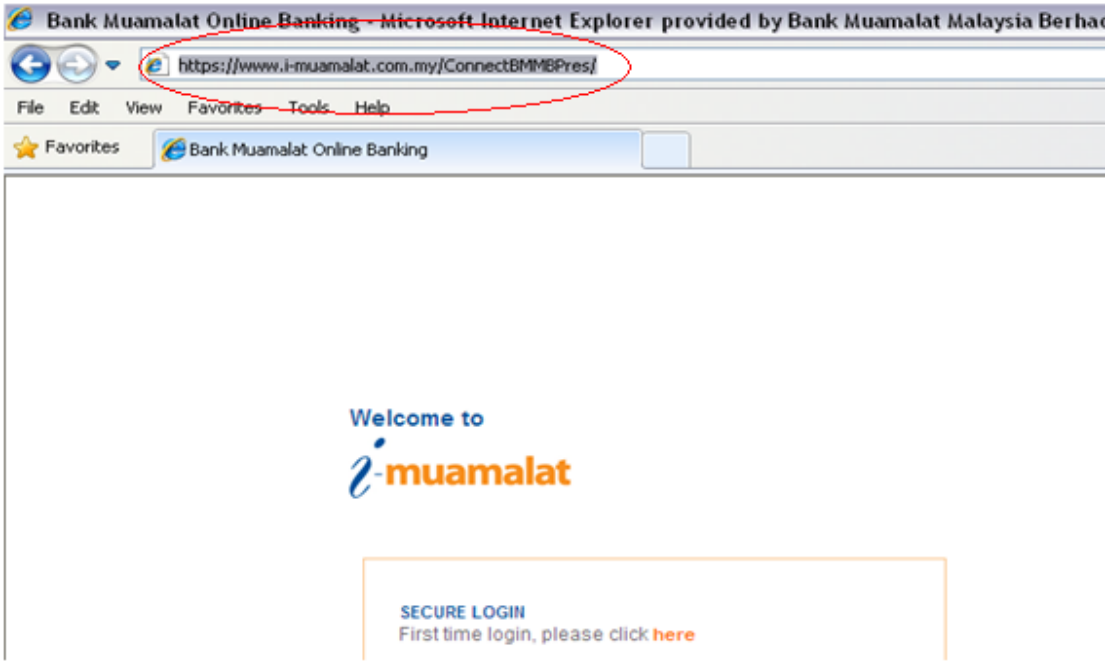


Figure 2 : Genuine i-Muamalat web address