*IOSR Journal of Research & Method in Education (IOSR-JRME)*
*e-ISSN: 2320–7388,p-ISSN: 2320–737X Volume 2, Issue 3 (Jul. –Aug. 2013), PP 33-41*
*www.iosrjournals.org*

# Phishing: Educating the Internet users – a practical approach using email screen shots

Lalitha Muniandy[1], Dr. Balakrishnan Muniandy[2]
[1](School of Arts & Science/ Tunku Abdul RahmanCollege,Malaysia)
[2](Centre for Instructional Technology & Multimedia/UniversitiSainsMalaysia,Malaysia)

***Abstract*:***Phishing is an attack targeting human component in cyber security. It becomes a common phenomenon in recent years. The modern phishing attacks evolved to become more sophisticated and difficult to detect even by IT savvy users. Various techniques deployed in security awareness training to curb the phishing attacks with no avail. In this conceptual paper we propose a mandatory training or education programs for home users by using email screen shots.*

***Keywords-*** *phishing, security, awareness, training, email screen shots*

## I. Introduction

According to [1] although information security is about people, but often the counter measures weighed on technical aspects. [2]claimed that human factor is the most important factor in computer security. This fact is acknowledged by many researchers, when it has been repeatedly stated that human is the weakest link in any computer security systems ([3],[4],[5],[6],[7]). The weakest link in computer security – the human must be educated to ensure they are fully protected while using the Internet – the information super highway to reduce the monetary, information, and data loses.

According toKevin Mitnick, the most notorious hacker turned author and security consultant, "*I was so successful in that line of attack that I rarely had to resort to a technical attack. Companies can spend millions of dollars towards technological protections and that's wasted if somebody can basically call someone on the telephone and either convince them to do something on the computer that lowers the computer's defences or reveals the information they were seeking"* ([5]).

According to [1], the act of human manipulation to obtain confidential information or performing an action is known as social engineering. [8]stated that phishing is a type of social engineering skills. According to [3], phishing is a form of social engineering attack.There are three primary techniques of phishing: URL manipulation, Web site forgery, and phone phishing. During a phishing attack one or a combination of these phishing techniques will be used in launching the attack ([6]). In this conceptual paper, we are going to discuss phishing technique based on URL manipulation."*In URL manipulation, attackers send an html embedded e-mail message, or a hyperlink whose HTML code opens a forged Web site*" ([6]).

## II. What is phishing?

[4]stated phishing attacks is launched by a conman by sending an email message to someone, usually pretending as a legitimate organization or person. Often the email message contains the instructions that need to be followed by the unsuspected victim, eg: clicking on hyperlink, opening an attachment, etc. When the unsuspected victim follows the instructions, the victim is either trick into providing confidential information or allows malicious programs installed on victim's computer. Any of these actions will lead to identity theft, loss of data, fraud, etc. "*The word phishing is a variation on the word fishing: bait is thrown out knowing many will ignore it yet some will be tempted into biting.*" – ([3]).

## III. The evolution and current state of phishing emails

According to [9], the initial phishing emails written poorly with spelling errors and bad sentence structure. But the modern phishing emails evolved into something that is difficult to identify even by a technology savvy and knowledgeable user. The current phishing emails written in a more convincing way with no or less spelling mistakes and better sentence structure and added with the necessary logos and graphics that will result in a more genuine look as the legitimate organization. [9]also claimed that fake web sites are designed similar in the appearance to the legitimate web sites, hence; make it impossible to be detected. As a result, the numbers of phishing scams are skyrocketing and made phishing as one of the most well organized online crimes. Phishing attacks also mainly launched due to financial gain. A small number of victims for spoof email will result enormous financial gain for the perpetrator. As a result of high monetary gain the Banking and Financial sectors attract the most number of phishing attacks.A spoof email is a falsified email with the sender

intentionally modified portions of the email, for example, sender's information and the content of the email to make it appear as though it came from a legitimate organization.

[3], claimed that in a week a single attacker is responsible for sending 5 billion email messages. The author further stated that the numbers of users responding to phishing attacks are extremely high. Citing some controlled tests conducted by researchers [3] claimed that 28 percent to 50 percent of users were tricked in entering their personal information.

Malaysian Computer Emergency Response Team (MyCert) categorized phishing in fraud incidents. According to [10], the reported fraud incidents comprising of phishing, job scams, fraud purchase and Nigerian scam. The reported phishing incidents involved foreign as well as local brands. See Fig. 1 for the number of incidents reported to MyCert from year 2006 to 2012. For the first quarter (January to March) of 2013, a total of 1,116 cases have been reported to MyCert by Malaysian Internet users.

According to [11], citing a report published by Trusteer (a Tel Aviv-based browser security company) in December 2009, found that every year from a total of 1 million bank users, 4,700 bank customers becomes victims of phishing scam by revealing the online banking information. Although the successful phishing attacks consists of only 0.47% but monetary loses are in the range of $2.7 million to $9.4 million for each year.

Phishing email from a poorly written message had transformed into one of the sophisticated attacks with appropriate subject line, logo, background and colour that represent a legitimate organization and a proper sentence structure with less or no grammatical errors. As a result, even highly alert users face problems in detecting or categorizing a phishing email. The "look and feel" of these email messages resembles an email message from a genuine organization.

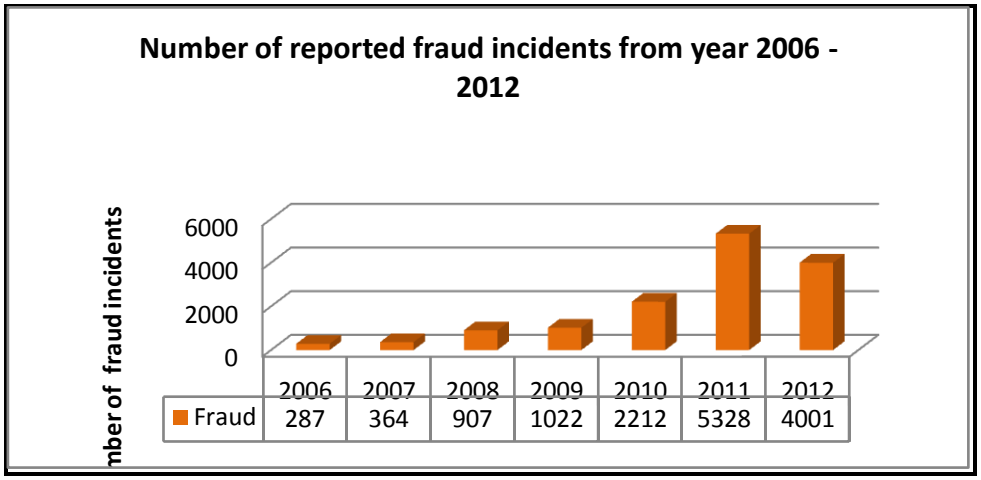



**Figure 1: Graph shows the number of fraud incidents reported in Malaysia from year 2006 to 2012.**
(Source: Based on data compiled from [10])

## IV. Educating the users in detecting phishing attacks: a practical guideline using actual phishing email screen shots

Many researchers claimed that education for users in creating awareness regarding security issues is important to curb the rising phishing attacks. There are a few simple precautions that can be used by users when they received phishing emails. First, if the users received an email and if it is not addressed to the customer, and instead addresses in general (for example: "Dear customer"), most probably it is a bulk email sent to a large number of users ([12],[13]). Second, most legitimate organization will proofread emails sent to its customers as email with grammar errors or poor sentence structure often brought down the image of the organization. If a user receives an email with poor language or grammatical mistakes, most probably it is a type of scam or a phishing email. Third, users should always understand that legitimate organizations usually do not request for personal information or confidential information through email ([12],[9]).

According to [13] and [9], web sites which required user to enter confidential and private information should start with https instead of http. Furthermore, in the browser status bar one can see a padlock sign or yellow lock sign. But a user must aware that the existence of the padlock or yellow lock sign and https does not guarantee that an email is not part of phishing game. They further claimed that users should be suspicious about emails requesting for users' immediate or urgent actions. [12], [13] and [9] also claimed that it is important for the users to know the correct hyper link or URL address of the legitimate organization and avoid clicking on the hyperlink embedded in the email to enter the requested information. Users should always open a new browser window and type the legitimate web address.

[13]acknowledged that phishing involves social engineering to trick users in responding to the email messages or to click and view an email message. As such the users must be aware of these social engineering tricks and able to protect themselves. The following are some of the other ways a user should take note to recognize phishing emails: (i) a link to web site provided in an email message should not have @ sign in the middle of the address. (ii) Phishing emails often use the legitimate organization's logo and appearance to convince the users that the email comes from a legitimate organization. Users must be aware that the existence of logo and appearance of a legitimate organization does not guarantee that email originated from a genuine organization and (iv) Legitimate organization never send an email message with attachments or pop-up box as it is considered as tools used by phishers; As such, user must always practice caution while dealing with emails.

Users must be trained to recognize phishing emails from legitimate emails. We believe that a practical approach is more appropriate to educate the users in recognizing phishing emails. During training, users must be exposed to real phishing emails and they must be trained on various techniques that can be used to recognize these phishing emails. The following are a few examples of phishing emails targeting the Internet users. The screen shots are some examples of phishing emails received by us or someone known to us.

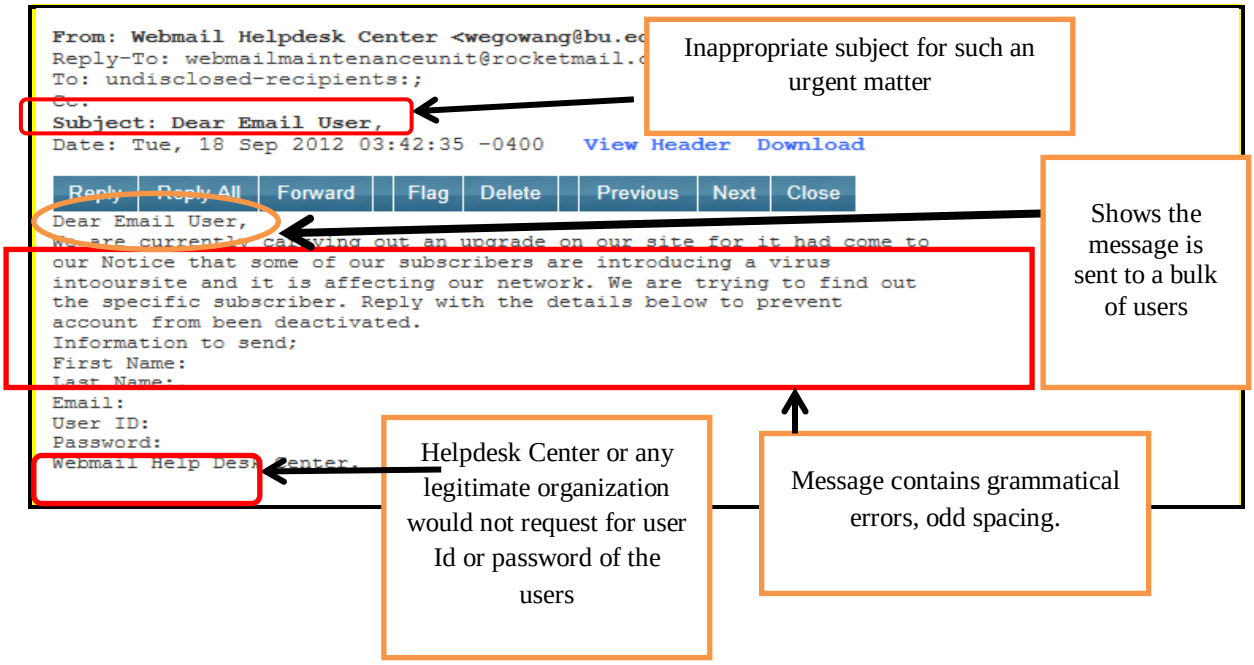



**Figure 2: Sample email screen shot 1**


**Figure 3: Sample email screen shot 2**

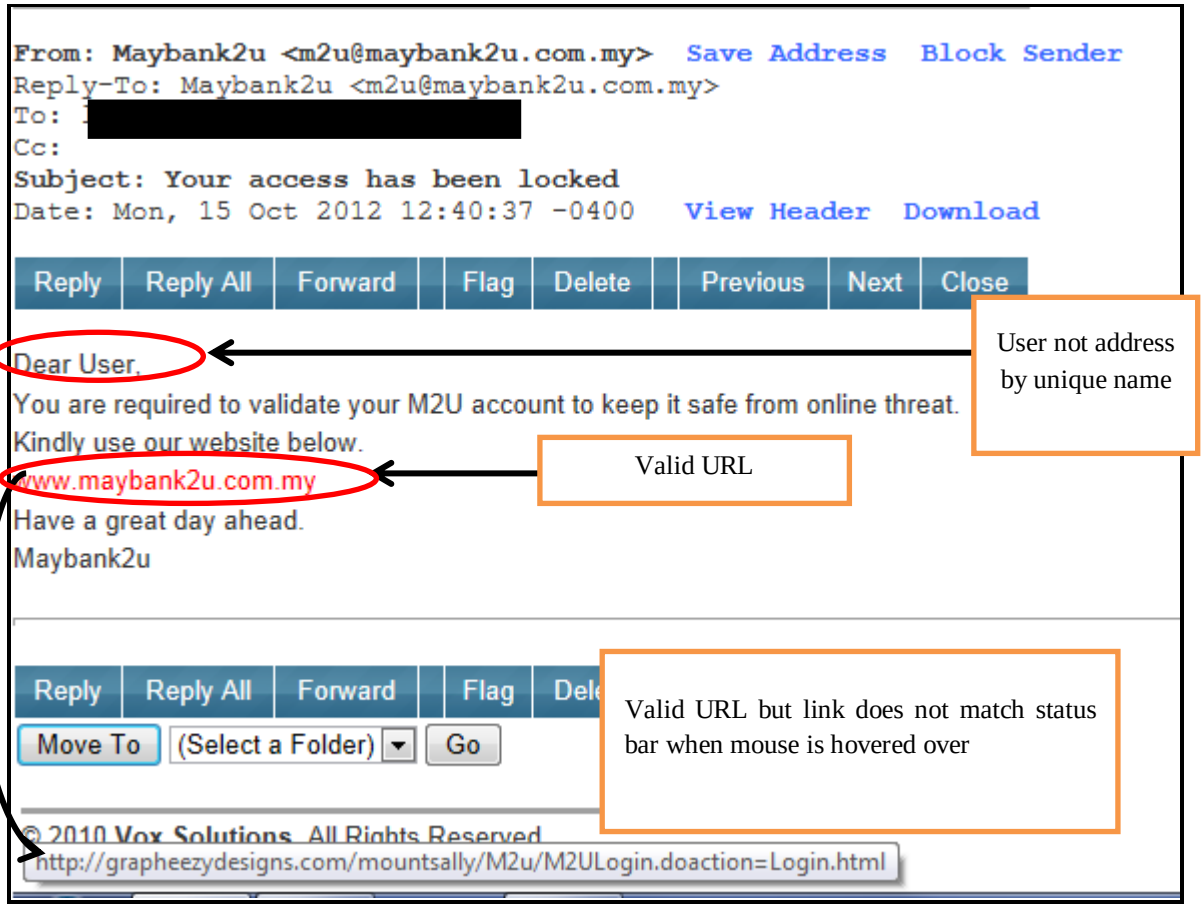



**Figure 4: Sample email screen shot 3**

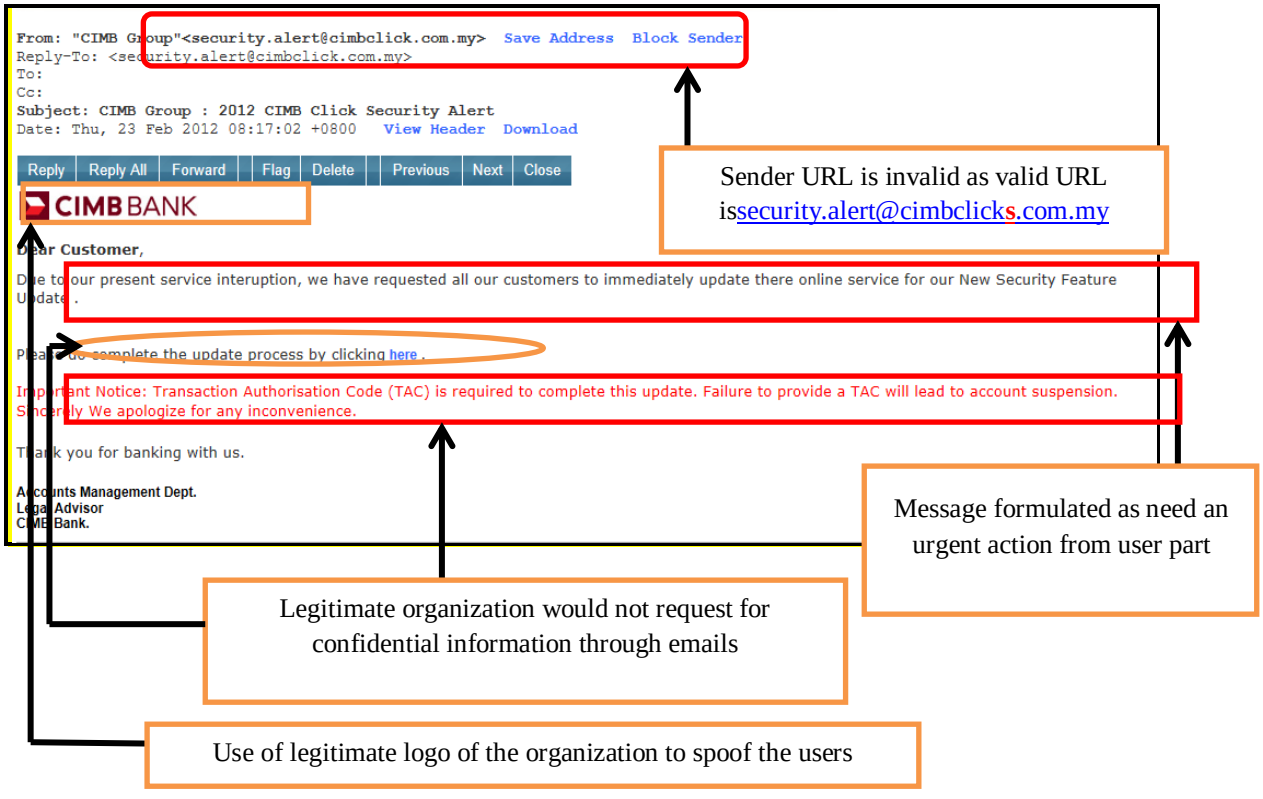
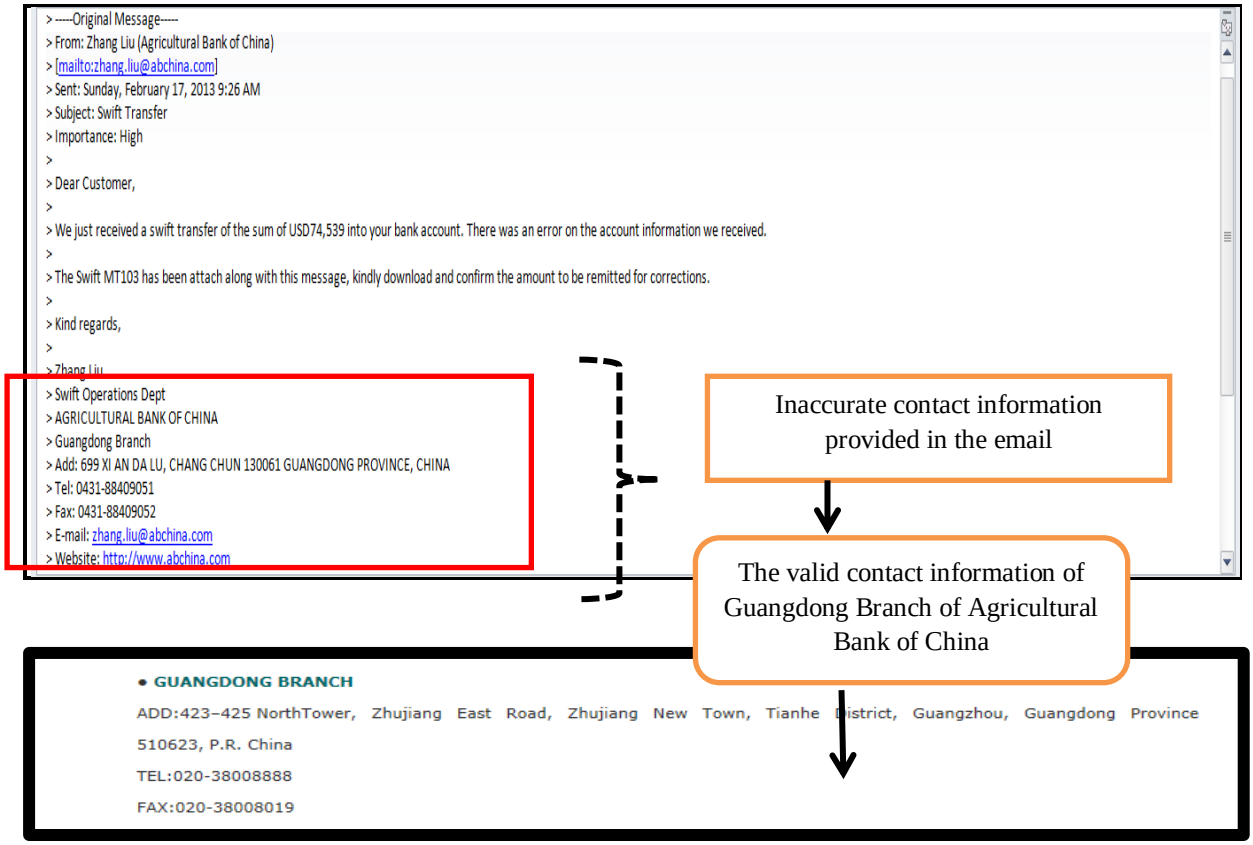



**Figure 5: Sample email screen shot 4**




Source :http://www.abchina.com/en/about-us/about-abc/network/domestic-branches/ - Retrieved May 2, 2013

**Figure 6: Sample email screen shot 5**

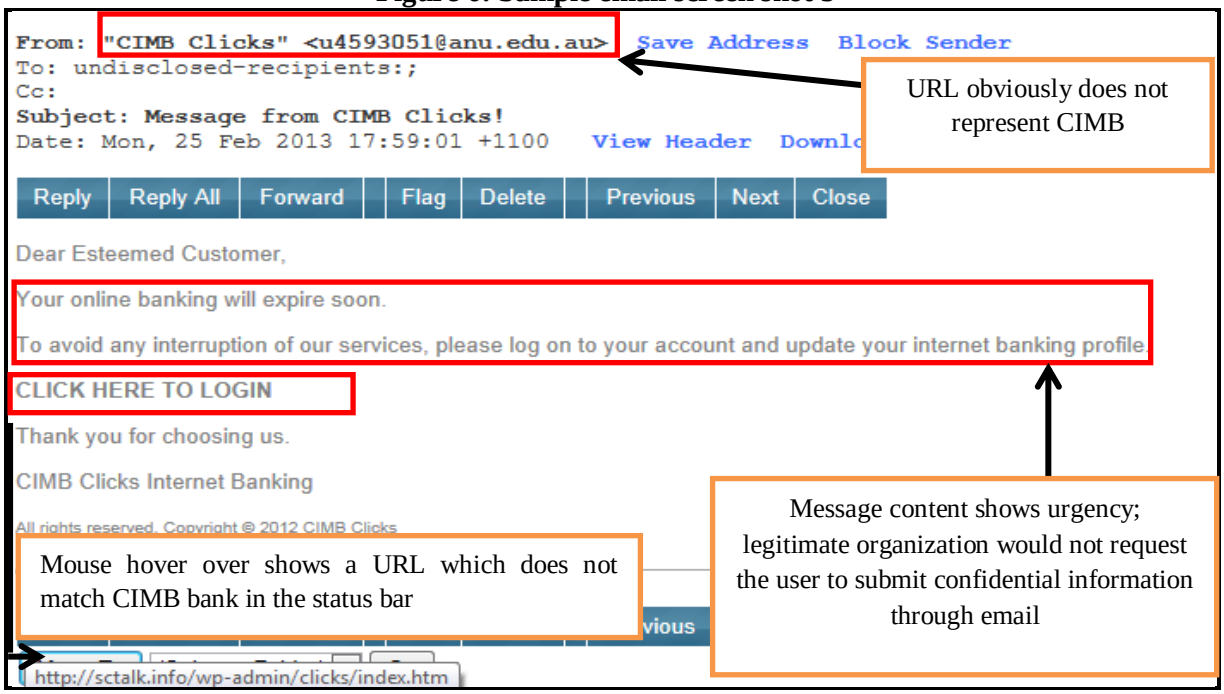



**Figure 7: Sample email screen shot 6**

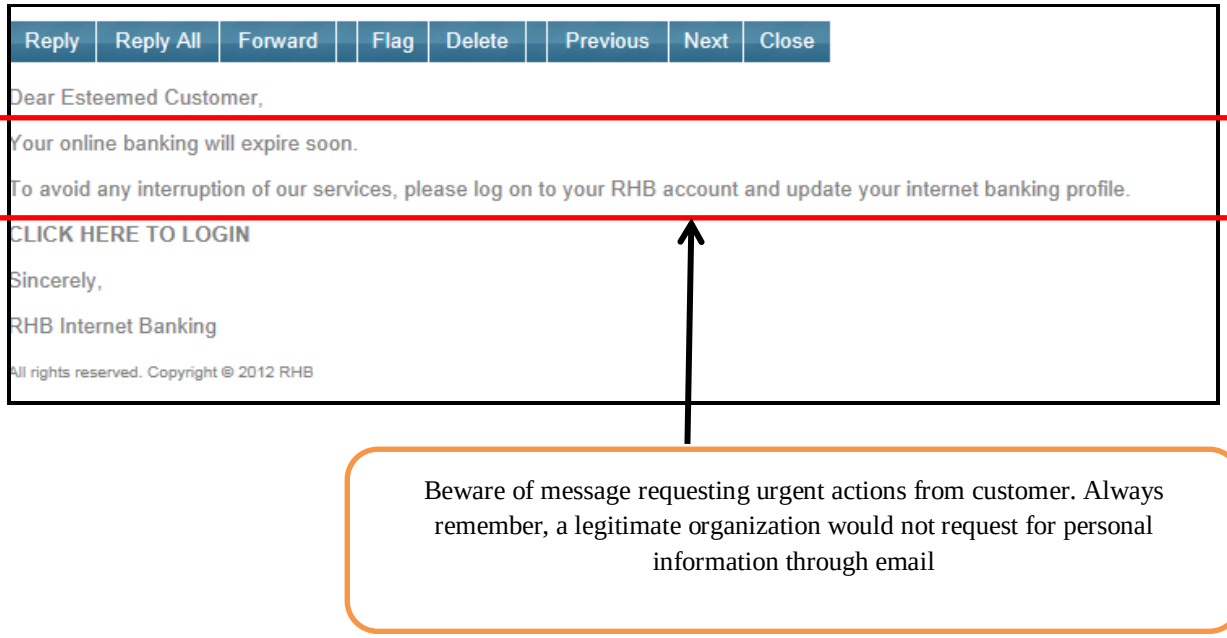



**Figure 8: Sample email screen shot 7**

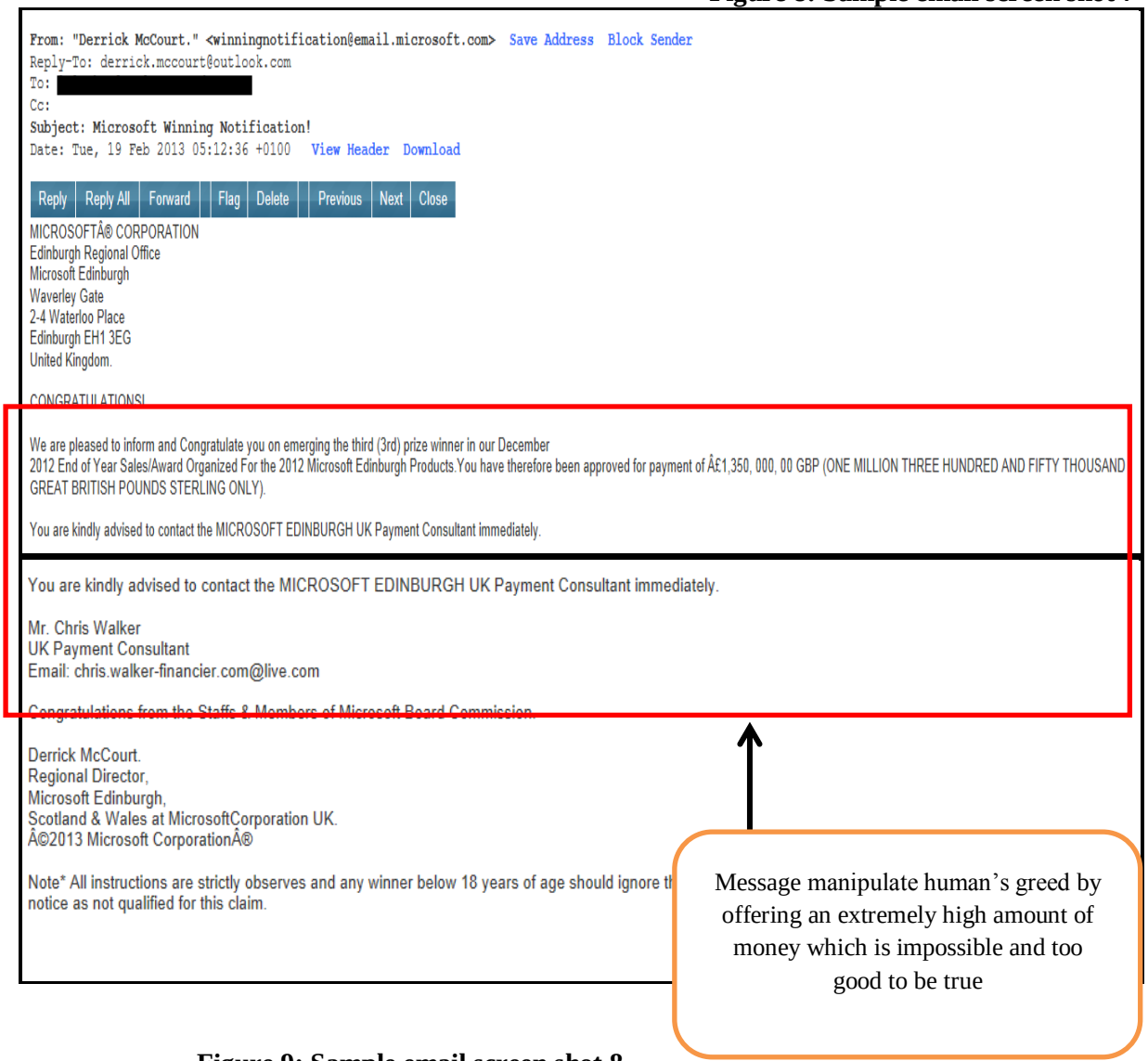



**Figure 9: Sample email screen shot 8**

## V. Discussions based on email screen shots

The email screen shots presented in section 4, ascertain the factors that mentioned by several researchers in educating the Internet users about phishing emails. Based on the eight screen shots in the preceding section, generally there are some aspects that must be considered by an Internet user before taking any actions that will put the user in a disadvantage position. First, beware of emails requesting for confidential information by a perpetrator claiming to be from a legitimate organization. It is known fact that legitimate organization would not request the user to submit the confidential information directly in the email or by clicking a hyperlink to enter the requested information. If a user could not ascertain the source of the email, immediately access the home page of the organization and contact the responsible person through the information provided in the "contact us" link. As discussed in the preceding section, majority of the phishing attacks are launched on banking industry. As an online banking user, users must read the safety and security information on the homepage regarding online danger and possible types of attacks that can be launched on Internet users who are also using online banking. Refer to the Fig.10 below.


**Figure 10: Screen shot from CIMB clicks**

(Source : http://www.cimbclicks.com.my/internet-safety.html - Retrieved May 7, 2013)

Next, as an email user, beware of emails that request for urgent or immediate action *(Refer Fig. 10*). Legitimate organization would not send a threatening email forcing the user to perform an action or request the user to provide some confidential or personal information through email. The user should contact the relevant party before providing or even replying to these kinds of emails. User should always read and understand the safety and security information provided on the homepage of the legitimate organization. If there are any queries users should always contact the relevant parties based on the information provided on the genuine homepage of the organization. Users should never attempt to contact the legitimate organization based on the contact information provided in the email.

Users should also be aware of the logos, background graphics and contact information such as address, telephone number and email addresses of the legitimate organization. One should always understand that an email with legitimate organization's logo or background does not guarantee that the email message must originate from the organization itself. The use of seemingly legitimate logos, URL and graphics may be employed to mislead the customer. Always double check the contact information provided with the contact details given by the legitimate organization. Before clicking on the hyperlink always roll over the mouse on the hyperlink. This technique will reveal the real URL address assigned with the hyperlink.

Finally, users should check spelling, sentence structure, grammatical errors and spacing in the email message. Legitimate organization would not send email message to bulk of the users, especially for urgent matters. If the email really originated from a legitimate organization it will address the user with the name of the user. Yet, email messages addressing the user by name still does not guarantee that email message must be originated from a legitimate organization as it can be part of spear phishing. Users must ensure that the subject line is appropriate for the email content. Moreover beware of email message claiming that someone offering a large amount of money. Basically, these type of messages targeting one of the negative aspects of human – greed. Always remember there is nothing free and nobody in the whole world will ever voluntarily give money to some strangers.

## VI. Effective methods of phishing training

Many organizations use various types of training programmes to educate Internet users about phishing emails. As we stated in earlier sections, phishing emails target financial institutions as it involved huge monetary transactions. Financial institutions can become pioneer in providing phishing education for its Internet home users.

According [15], all users can be trained to detect suspicious looking emails although sometimes it takes considerable time in the training process. [16]claimed that the content of training materials play important role in facilitating people to learn and reproduce knowledge. They concluded that people able to make better decisions if testing is performed with the same or similar training situation and materials. Due to the above reasoning we believe that phishing training will be more effective if it is conducted using real phishing emails by showing the ways to detect it as a spoof email.

[17], agreed that education and awareness are important in educating users about phishing simply because an automatic system which will detect phishing activities on Internet with full accuracy does not exists to date. Education still plays an important role in educating the user but it is only effective if the users really read the training material. In order to encourage the users to read the training materials, it must be fun, interactive and up-to-date. This would be our rationale to make it mandatory (or force) forall users to read the training content and it will be the responsibility of the financial institutions to constantly change the content of the training materials by publishing latest information and design the training materials so that it is fun and attractive for the users.

According to [18], end user awareness training is considered as the most valuable security approach among the 1,029 business technology and security professionals who took part in *Information Week 2013 Strategic Security Survey*. The survey respondentssuggest that testing is important to ensure that users understand the training material after a training session. 64% of respondents claimed that email as frequently used media in security awareness training. This is followed by PowerPoint(52%), interactive test/quiz (50%), newsletters (41%), video (39%), social media (6%), mouse pads or other tchotchkes (4%) and other (9%). However, they claimed that the delivery method used in training is less significant compared to the message that needs to be delivered to the users.

We propose that the financial institutions should design its homepage in a way that 'force' the users to read their phishing training material before they go through with their usual banking transactions. Education for home users is important and it should be made mandatory. Financial institutions should display the latest incidents, show the methods that can be used by users in detecting phishing emails using some real phishing emails (as we did in *section 4*), and publish latest statistics about phishing incidents and add any other useful information for users about phishing. After training materials are presented for users, the users should be tested to determine the users understanding level of security issues. Testing can be done by sending spoof emails to users to check their knowledge and alert level on phishing emails. Based on the past researches, if the training material is accepted and well read by the users, then the message regarding security issues can be disseminate successfully to users and subsequently the phishing related incidents can be reduced significantly.

## VII. Conclusion

Phishing is a type of social engineering. The perpetrator launches the attack targeting the human's weak point. Education to create awareness among users is important in curbing the phishing attacks. Although only a small percentage of users fall for phishing scam but the monetary losses are really great.Technical countermeasures employed for social engineering attacks to protect users are inefficient as it targets human weak point. Users must be educated to protect themselves and they must beware of the existence of phishing techniques. Education for users apparently becomes more important as people from all life and age groups using Internet and emails in their everyday lives.

We suggest users be trained using a practical approach by exposing them to real phishing emails. They must be educated on the various techniques to recognize a phishing email and they must possess the knowledge to validate an email. Although a vast amount of emails circulating in the Internet sphere can be categorized as

phishing emails, but the number of reported incidents are far from the truth. This shows the awareness among the users are still very lowand education and training is the only way to improve the users' awareness regarding the phishing emails. Selecting an appropriate training style and content also very important in ensuring the message is successfully delivered to customers.

Most of the past researches suggest that training and education for end users are important in protecting the end users from human manipulations to illegally access into an information system. Education or training must be conducted in a similar or same situation that can simulate the real life scenarios. The choice of training method is less important compare to the training content in user education and awareness training. Training materials must be presented as attractive, fun and with up-to-date information to successfully engage the users during training session.

## References


[1] Mann, I, *Hacking the human – social engineering techniques and security countermeasures* (England : Gower Publishing Limited, 2008).

[2] Schneier, B, *Schneier on security.* (Indianapolis: Wiley Publishing Inc, 2008).

[3] Ciampa, M, *Security awareness: applying practical security in your world* (Boston: Course Technology, 2010).

[4] Howard, D., & Prince, P, *Security 2020. Reduce security risks this decade* (Indianapolis: Wiley Publishing, Inc, 2011).

[5] Schneier, B, *Secrets and lies.* (Indianapolis: Wiley Publishing Inc, 2004).

[6] Whitman, E.M., &Mattord, J.H, *Principles of information security* (3rded.). (Canada: Thomson Course Technology, 2009).

[7] Mitnik, D. K., & Simon, L.W, *The art of intrusion – The real stories behind the exploits of hackers, intruders & deceivers.* (Indianapolis: Wiley Publishing Inc., 2005).

[8] MosinHasan, NileshPrajapati, SafvanVohara, Case study on social engineering techniques for persuasion, *International Journal on Applications of Graph Theory in wireless ad hoc networks (GRAPH-HOC), 2(2),* 2010, 17-23.

[9] TusharVisheshSrivastava. (2007). Phishing and Pharming – The Deadly Duo.*SansInstitute*.Retrived April 20, 2013, from http://www.sans.org/reading_room/whitepapers/privacy/phishing-pharming-evil twins_1731

[10] MyCERT. Retrieved April 30, 2013 from http://www.mycert.org.my

[11] SPAMfighter. *Victims of Bank Phishing Fewer, but Financial Losses Enormous.*Retrieved May 5, 2013 fromhttp://www.spamfighter.com/News-13591-Victims-of-Bank- Phishing-Fewer-but-Financial-Losses-Enormous.htm

[12] Gerald Goh Guan Gan, Tan Nya Ling, GohChoonYih and Uchenna Cyril Eze, Phishing : A growing challenge for Internet banking providers in Malaysia, *Communications of IBIMA, 5(17),*2008, 133-142.

[13] Ciampa, M, *Comptia security + 2008 in depth* (Boston: Course Technology, 2009).

[14] Cimb Clicks. Retrieved May 7, 2013 from http://www.cimbclicks.com.my/internet-safety.html

[15] Bowen, M.B, RamaswamyDevarajan, Stolfo, S. (2012). Measuring the Human Factor of Cyber Security. *Homeland Security Affairs, IEEE 2011 Conference on Technology for Homeland Security: Best Papers*, 2012. Retrieved May 2, 2013 from http://www.hsaj.org/?article=supplement5.2\

[16] PonnurangamKumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong. (2004). Lessons From a Real World Evaluation of Anti-Phishing Training. Retrieved June 1, 2013, from http://www.cs.cmu.edu/~ponguru/eCrime_APWG_08.pdf

[17] Steve Sheng, PonnurangamKumaraguru, Alessandro Acquisti, Lorrie Cranor and Jason Hong. (2009). Improving Phishing Countermeasures: An Analysis of Expert Interviews. Retrieved June 1, 2013, fromhttps://www.cs.cmu.edu/afs/cs.cmu.edu/Web/People/jasonh/publications/ecrs-ecrime2009-interviews.pdf

[18] InformationWeek reports. (June 2013). *2013 Strategic Security Survey.*Retrieved June 1, 2013 from reports.informationweek.com