CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology & Innovation

MEDIA RELEASE

For Immediate Release

CBMR-3-RFI-23-PhishingAdsvisory-V1
17 December 2009

Internet Users Beware: Phishing Attempts Rising

Fake internet banking websites look exactly like the originals

KUALA LUMPUR, 17 December – The number of phishing attempts is on the rise and accelerating, according to an advisory released by the *Cyber999 Help Centre of CyberSecurity Malaysia*, in Kuala Lumpur today. (available via www.cybersecurity.my or www.mycert.org.my)

The *Cyber999 Help Centre* has been receiving numerous reports from Malaysian internet users regarding phishing websites hosted overseas, that look exactly like some of the well-known local bank's e-banking websites.

These phishing websites or fake websites are used to conduct "phishing attack", which involves manipulating the weakside of human security, by masquerading as a trustworthy entity (e.g. a copycat of a familiar banking website).

The "phishing attack", also utilises a kind of social engineering tactic such as sending spam emails that look as though sent by the well-known local bank. The fraudulent email uses convincing words to trick people into clicking a link that would open up the phishing website or fake e-banking website. Because the fake website looks exactly like the original website, customers are tricked into entering their confidential information like their e-banking user-names and passwords into the fake e-banking website. This way, the "phishing attacker" could conveniently steal user-names and passwords of unsuspecting bank customers.

"Banks will never ask users to do account updates, password reset, account unlocking or anything in relation to banking via emails and URLs. If you do receive such emails and it looks like from the banks or any financial institutions, our advice is to completely ignore the emails. If you do get curious, please contact your bank for verification or contact our Cyber999 Help Centre," said CyberSecurity Malaysia Chief Executive Officer, Lt. Col. Husin bin Jazri (Retired).

CyberSecurity Malaysia regularly publishes advisories on cyber security via the corporate website www.cybersecurity.my or the National Computer Emergency Response Team's portal www.mycert.org.my. It also publishes tips on cyber security via its outreach and awareness portal www.cybersafe.my

CyberSecurity Malaysia
(726630-U)
Level 7, Sapura@Mines
No. 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia
T +603 8992 6888
F +603 8945 3205
www.cybersecurity.my

Today's phishing advisory can be accessed via this link
http://www.mycert.org.my/en/services/advisories/mycert/2009/main/detail/718/index.html

The Cyber999 Help Centre can be reached through the following channels:

E-mail	**:**	cyber999@cybersecurity.my
Phone	**:**	+603 89926969 or 1-300-88-2999 (monitored during business hours Mon - Fri 08:30 -17:30 MYT)
Fax	**:**	+603 89453442
Handphone	**:**	+60 19 2665850 (24x7 call incident reporting)
SMS	**:**	+60 19 2813801 (24x7 SMS reporting)

Some examples of the phishing emails that were sent to the Internet users are as follows:

Example 1

```
---------- Forwarded message ----------
From: Maybank <auto@securedlinks10.com>
Date: Mon, Dec 14, 2009 at 8:34 AM
Subject: IMPORTANT ACCOUNT ALERT
To:


Maybank Alert

Dear Valued Customer,

We Have Sent You An Urgent Notification Regarding Your Maybank Account And
An Unknown Transaction. View Details Below.

http://www.maybank2u.com.my/auth-account <http://www.activemm2u.com/Message.html>

Thank You

Maybank Group
```


CyberSecurity Malaysia
(726630-U)
T +603 8992 6888
F +603 8945 3205

Example 2

Plse check this email

From: CIMB Bank
To: [redacted]
Sent: Thu Dec 17 11:48:14 2009
Subject: CIMB Bank - Locked Account Information

Dear CIMB Bank user,

**Your CIMB Bank Account is currently locked,
and only after you identify on the website
the account will be unlocked and ready for use.**

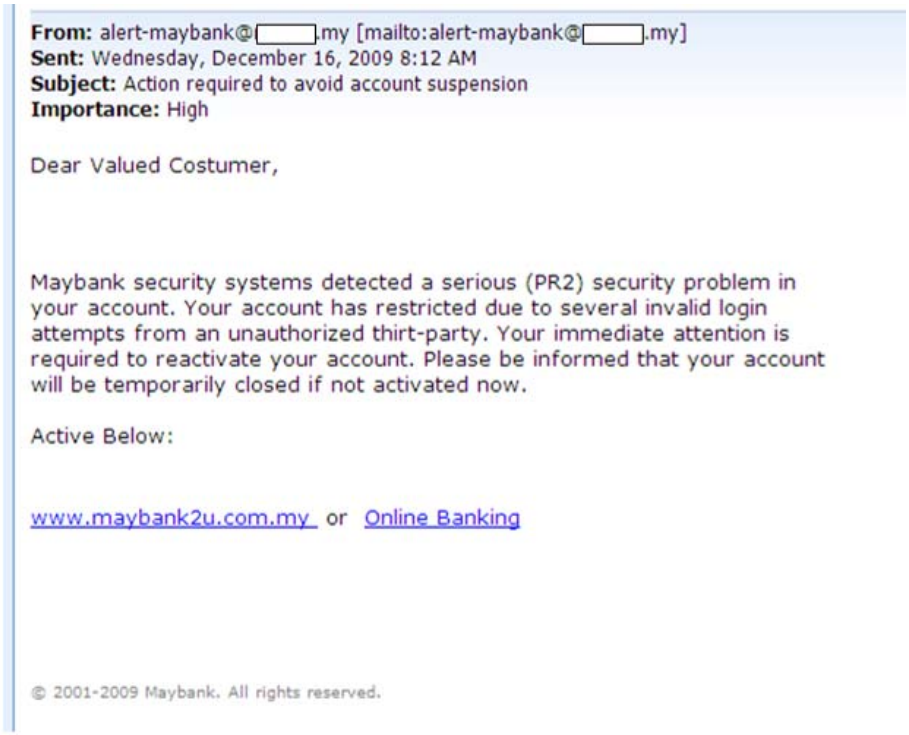
Please identify yourself by following the link given below. :

Go To CIMB Bank Online

**IMPORTANT : The identification process will be completed
only after you insert the six digit TAC Code
that will be sent to your pre-registered mobile phone
in the following minutes.**

CyberSecurity Malaysia
(726630-U)
T +603 8992 6888
F +603 8945 3205

Example 3



From: alert-maybank@[redacted].my [mailto:alert-maybank@[redacted].my]
Sent: Wednesday, December 16, 2009 8:12 AM
Subject: Action required to avoid account suspension
Importance: High

Dear Valued Costumer,

Maybank security systems detected a serious (PR2) security problem in your account. Your account has restricted due to several invalid login attempts from an unauthorized thirt-party. Your immediate attention is required to reactivate your account. Please be informed that your account will be temporarily closed if not activated now.

Active Below:

www.maybank2u.com.my or Online Banking

© 2001-2009 Maybank. All rights reserved.

About CyberSecurity Malaysia

CyberSecurity Malaysia is the national cyber security specialist centre under the purview of the Ministry of Science, Technology and Innovation (MOSTI), Malaysia. The services include:

- Digital Forensics / CyberCSI™
- Malaysia's Computer Emergency Response Team (MyCERT) / Cyber999™
- Security Management and Best Practices
- Security Assurance
- Malaysia Common Criteria Certification Body (MyCB)
- Cyber Security Training and Professional Certification
- Outreach, Awareness, and Social Responsibility Programmes
- Cyber Security Policy and Legal Research

For more information about CyberSecurity Malaysia, please visit website at www.cybersecurity.my. To report cyber incidents such as harassment, fraud or intrusion to our Cyber999™ service, you may email to cyber999@cybersecurity.my

For more information, kindly contact:

Mohd Shamil Mohd Yusoff
Office: +603 8946 0895
Mobile: +601 2249 6938
E-mail: shamil@cybersecurity.my

Sandra Isnaji
Office: +603 8946 0867
Mobile: +601 2324 5867
E-mail: sandra@cybersecurity.my