MEDIA RELEASE

31 March 2015
FOR IMMEDIATE RELEASE

CYBERSECURITY MALAYSIA ALERTS INTERNET USERS ON CYBER BLACKMAIL SCAM

Seri Kembangan (31 March 2015) – CyberSecurity Malaysia, a technical cyber security and specialist centre under the Ministry of Science, Technology and Innovation (MOSTI) today issued an alert on "Cyber Blackmail Scam".

Cyber Blackmail Scam occurs when perpetrator connects with the potential victims through social media mainly Facebook and Tagged by portraying themselves as beautiful, sexy woman purportedly from the Philippines, Japan or Korea. Perpetrator will then ask the victim to video chat with "her" using Skype application and uses attractive words to lure the victim. The perpetrator actually use pre recorded webcam videos to fake their real identity, to look like they are genuinely engaged in conversation online with victim. While in conversation online, the perpetrator will record unpleasant video of the victim without the victim's knowledge and use it to extort the victim further by threatening to make it public at Youtube, social networking sites or direct it to the victim's family or friends.

"We had been observing an increase number of cyber blackmail scam incidents which involves blackmailing and extorting victims for money in this first quarter of 2015. Between January till March this year, 25 incidents of cyber blackmail scam had been reported to Cyber999 help centre compared to 21 incidents in Q1 2014 and more users may fall into victims if proper mitigations are not in practice." said Dr. Amirudin Abdul Wahab, Chief Executive Officer of CyberSecurity Malaysia.

A total of 121 incidents on cyber blackmail scam were reported to Cyber999 Help Centre in 2014.

CyberSecurity Malaysia
(726630-U)
MS ISO/IEC 17025 TESTING SAMM NO. 456 (MySEF LABORATORY)
MSC MALAYSIA Status Company
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

Dr. Amirudin said “Malaysians Internet users continue to be victims, being threatened to have their unpleasant videos or compromising videos released on Youtube and social networking sites if they do not pay the amount requested by perpetrator, within a certain period of time.”

Based on Cyber999 statistics, victims are mainly teenagers to middle aged man. “We suspect the perpetrators are male foreigners operating the scam from various locations. The scam uses social networking sites like Facebook, Tagged and online video chats such as Skype to carry out their activities.” added Dr. Amirudin.

Apart from victims in Malaysia, the scam also affects victims globally in which they are threatened, extorted and has impacts on their reputation. Malaysian Internet users are advised to be precautious with whom they friend or get to now on Internet.

Some of the recommendations are:

- Internet users are advised to adhere to best practices and ethics when they are online on social networking sites and online chatting:
- Internet users should be very precautious with whom they friend with and must not fulfil all unnecessary requests from other users while they are online:
- Be alert and suspicious of unusual activities on the net and immediately report it to relevant authorities:
- As preventive measure, configure your Skype to restrict communication with your contact list only by doing the following: *Go to* > *Tools* > *Options* > *Privacy* > *Only Allow IMs, Calls etc from People on my Contact List* > *SAVE*
- Always make sure your software and systems are up-to-date, and that you are using up-to-date security software:
- Be aware that anything you do on the internet, including video and voice calls, can be recorded and manipulated for malicious purposes:
- Never use your webcam to video call someone you do not know.

For further enquiries, please contact CyberSecurity Malaysia through the following channels:

- E-mail: cyber999@cybersecurity.my or mycert@mycert.org.my
- Phone: 1-300-88-2999 (monitored during business hours)

- Fax : +603 89453442
- Mobile: +60 19 2665850 (24x7 call incident reporting)
- SMS : CYBER999 REPORT EMAIL COMPLAINT to 15888
- Web: http://www.mycert.org.my
- Twitter: http://www.twitter.com/mycert
- Cyber999 Mobile Apps: IOS Users or Android Users

  (Business Hours : Mon - Fri 09:00 AM - 18:00 PM MYT)

For more information and preventions against the scam is available at: https://www.mycert.org.my/en/services/advisories/mycert/2013/main/detail/944/index.html

~ end ~

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

For additional information, please visit our website at http://www.cybersecurity.my.

For general inquiry, please email to info@cybersecurity.my
Stay connected with us on social networks: facebook/ CyberSecurityMalaysia, twitter/cybersecuritymy, youtube/cybersecuritymy, instagram/CyberSecurity_Malaysia.

For further enquiries about this document, please email: media@cybersecurity.my or call +603-89926888, Mohd Shamil Mohd Yusoff (ext: 6978) or Sandra Isnaji (ext: 6977)