MEDIA RELEASE

07 January 2014

FOR IMMEDIATE RELEASE

CyberSecurity Malaysia alerts the public of Cyber Flings turning into Blackmail Scam

KUALA LUMPUR (07 January 2014) – CyberSecurity Malaysia, the national cyber security specialist agency under the Ministry of Science, Technology and Innovation (MOSTI), recently alerted the public to be wary of 'cyber flirts', as there is a rising trend in cyber blackmail scam.

Victims are mainly teenaged boys to middle aged man. The perpetrators are suspected to be of foreign nationals, most probably males with some female accomplices creating a scam hub in various locations including in Malaysia. The scammers use social networking sites like Facebook, Tagged and online video chats such as Skype as the platform to carry out their activities.

The scam has become a global issue and has become quite serious where people are losing their money and reputation. Victims are asked to pay ranging from RM500 to RM5000.

"Only four incidents of cyber blackmail scam were reported to our Cyber999 Help Centre in 2012, but by mid 2013 we saw an upward trend, which made us very worried. We referred the issue to the Royal Malaysia Police (RMP) for further investigation so the culprits can be dealt with accordingly. By end of 2013 the number rose to 73, which is 18.5 times more. This huge increase in incidents triggered the alarm. We also believe there are more incidents out there that are not reported to us. Hence, we released an alert on 25th December 2013 to warn the public. Malaysians are advised to be extra careful and not to entertain online seductions from women that they get to know only in social media, but have never really known them in person." Said Dr. Amirudin Abdul Wahab, Chief Executive Officer of CyberSecurity Malaysia.

Based on the analysis of about 80 reported incidents, CyberSecurity Malaysia found a similar pattern of the modus operandi of a typical cyber blackmail scam. The perpetrator would usually create a profile on Facebook or Tagged, portraying herself as a beautiful, sexy woman purportedly from the Philippines, Japan or Korea. She would then identify a man as his potential victim and befriend that man on Facebook or Tagged. The

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
www.cybersecurity.my

perpetrator would flirt with the victim and lure the victim for an intimate video chat with her using Skype. During the video chat, the perpetrator would take off her clothes and seduce the victim to perform unpleasant act, while she secretly records the victim's acts. The perpetrator would later play the video chat footage to the victim and blackmail him to remit a certain amount of money via Western Union or a third party bank account; otherwise his video footage will be circulated in Facebook and YouTube.

What to do if you are a victim of such a scam:

- Discontinue and refrain from communicating with the perpetrator. Ignore and disregard all calls, SMS or messages from the perpetrator.
- Remove the perpetrator from all your social media friends or contact list or put her into your 'blocked' list.
- Make all your social networking accounts private so the perpetrator will not be able to reach you and your friends.
- Keep all relevant data such as chat logs, screenshots, emails as evidence for reporting and prosecution purposes.
- Paying the scammers is never encouraged as it may further propagate the scam.
- Lodge a police report at a nearby police station together with evidence for the police to further investigate.
- Report to CyberSecurity Malaysia's Cyber999 Help Centre for further assistance by emailing to cyber999@cybersecurity.my or by calling 1-300-88-2999 (monitored during business hours). In case of emergency outside the regular working hours, send SMS text message to +60 19 2665850.

Our general advice to Internet users:

- Be aware that anything you do on the internet, including video and voice calls, can be recorded and manipulated for malicious purposes.
- Internet users are advised to adhere to best practices and religious or social ethics when they are online on social networking sites and online chat forums.
- Internet users should be very precautious with whom they 'friend' with and must not fulfill 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.
- Never use your webcam to video call someone you do not know.

~ The 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 www.facebook.com/CyberSecurityMalaysia and www.twitter.com/cybersecuritymy

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