



Network Security Portal:

Educating and raising awareness on Internet security

Harme Mohamed, Director of Security, Trust & Governance Department expounds on the latest project by the National Security Centre.

Today, there are an estimated 1.7 billion Internet users globally, and it is estimated that consumers spent more than \$2.8 billion on online shopping worldwide in 2008. The Internet has shifted key financial and personal information to the hands of Internet users at home, as more and more commerce are transacted online by this group of Internet users – such data may now be kept in personal computers or even mobile phones instead of large data centres owned by corporations. As a result, securing online transactions has become more complex and challenging – it is no longer sufficient to only secure information contained in large data centres, consumers at home also need similar kind of protection.

According to a cyber security report released by Symantec on September 2009 (<http://bit.ly/46kCzF>), nearly 10,512,000 identities are stolen every year, averaging one identity theft every three seconds. The seriousness of the situation becomes apparent when one compares this rate to crime rates in some of the largest cities in the world. New York City sees a crime once every three and a half minutes and Tokyo, one crime in every two and a half minutes.

Cyber crime is highly profitable. In March 2009, US telecommunications company, AT&T's chief security officer, Edward Amoroso and a panel of security experts told a US Senate Commerce Committee that revenues from cyber crime are running up to USD1 trillion annually, even exceeding drug-related crimes (<http://bit.ly/9D303e>).

While e-commerce in Malaysia has yet to see the level of acceptance seen in the US or Europe, local Internet users should not be oblivious to Internet threats. Today, Internet users face Internet threats in the form of crimeware – malicious software stealthily distributed by cybercriminals with the purpose of secretly extracting information and gaining money from Internet users. Crimeware may take the form of viruses, worms, Trojans, Botnets or other malicious programmes. In addition, cyber crime allows perpetrators to hide behind the anonymity of the Internet, making it difficult for law enforcers to prosecute them compared to offline crimes.

It is therefore paramount that an Internet user, whether using a personal computer or a mobile device, to know what these threats can do and the ways to overcome them. Hence, SKMM's Network Security Portal was born.

SKMM Network Security Portal

To ensure that Malaysian Internet traffic is secure, SKMM has established the SKMM Network Security Centre (SNSC) that has a dedicated team to monitor Malaysian Internet traffic for network threats in collaboration with Malaysian ISPs. The SNSC serves as the national Internet network thermometer to provide overall understanding of macro cyber threat level with the involvement and cooperation of both public and private sectors.

The SNSC security professionals monitor the ISPs' networks 24 x 7, all year round, checking on any known threats and anomalies. The threat monitoring will generate early warning of massive attacks or malicious propagation. This is to ensure continued protection of networks and ICT systems of ISPs and other key organisations from security infringements.

Started early 2009, the SKMM Network Security Portal is designed to raise awareness and provide valuable network security related information to home users, organisations and service providers that use the Internet for their various activities. The portal is divided into two main sections - one section focuses on information for home users and organisations and the other on information for service providers. The Portal aims to be a one-stop centre to engage and empower Internet users, by providing information on how to protect themselves when they are on the Internet.

For example, it educates home users that their home computers are a popular target due usually to lack of security measures that have been put in place as compared to computers in their workplace. The Portal lists several simple ways home users can begin to protect their computers. It stresses the importance of good online practices such as using anti-virus software, not opening junk emails, installing firewalls, creating strong passwords and only downloading files from trusted sources.

As for the section for service providers, the information is much more technical and in-depth. Here it is more about sharing and providing relevant information to the ISPs, for them to provide a secure Internet environment to users. While ISPs also have their own monitoring systems, the portal has distinct advantage because it compiles and distributes information gathered from the real-time traffic monitoring of ISPs in Malaysia. The portal provides significant information that are relevant to service providers.

The portal also contains real time security alerts. These alerts provide timely information about current security issues regarding vulnerabilities, exploits and patches found from various resources on the Internet. The security alerts provide steps and actions to home and corporate users.

There are also statistics to show the network occurrence for the last 24 hours. Data for the statistics is collected from the SNSC. Statistics include the following:

Top 10 Attacks

This shows top 10 network attacks for the last 24 hours. Internet traffic was scanned against SNSC's vulnerabilities databases.

Top 10 Ports

This shows the top 10 TCP/UDP ports that had been targeted by attackers.

Top 5 Countries

This shows top five countries' attackers targeting Malaysia's network. Currently, sources of the majority of attacks are local, followed by the United States, Republic of Korea, China and United Kingdom.

The portal has also uploaded two advisories, one regarding Nine-Ball and one about the Win32/Conficker. B worm. It also has files for best practices from US-CERT (United States Computer Readiness Emergency Team) and NIST (National Institute of Standards and Technology). Lastly, there are articles on cyber security tips on common security issues for technical and non-technical computer users.

SKMM Anti-Phishing Portal

Complementing the SKMM Network Security Portal, SKMM has established the SKMM Anti-Phishing Portal in cooperation with banking and financial institutions in Malaysia. This Portal disseminates information related to Phishing and Phishing activities in Malaysia.



 The Network Security Portal team at work

Apart from network security threats, Malaysians are also faced with Internet fraud or generally known as Phishing - a fraudulent attempt, usually made through email, to steal your personal information. Phishing emails usually appear to come from a well-known organisation, requesting for Internet users' personal information such as credit card number, account number, login names and password. Often times Phishing emails/attempts appear to come from sites, services and companies with which Internet users do not even have an account.

In order for cybercriminals to successfully "Phish" financial personal information, they must get users to go from an email to a website. Phishing emails will almost always tell users to click a link that takes them to a site where their personal information is requested. Legitimate organisations would never request this information via email. In Malaysia, most Phishing attempts involve Malaysian financial institutions. Emails sent usually cite that the financial institutions were experiencing problems with their computer systems and requests their Internet clients to resubmit their personal information for verification purposes.

The Anti-Phishing Portal aims to educate users on how to detect Phishing attempts and protect themselves against these type of threats. The portal lists several precautionary steps to avoid getting phished. Internet users should never respond to any emails that:

- Require users to enter their personal information directly into the email or submit them online.
- Threaten to close or suspend users' accounts if they do not respond.
- Claim that users account has been compromised or that there has been fraudulent activity on the users' account and requests the users to enter, validate or verify account information.
- State that there are unauthorised charges on the users' account and requests their account information.

- Claim that the bank has lost important security information and needs users to update their information online.
- Require users to enter their card number, password, user ID or account numbers into an email, pop-up window or non-secure webpage.

Phishing victims should file a report with SKMM. The reports will be used to identify the owners of Phishing sites and SKMM will act to take down the offensive sites by issuing instructions to relevant parties. Swift action to take down Phishing sites are crucial in preventing further damage to Malaysian Internet users. SKMM will instruct the ISPs to reroute the Phishing sites to SKMM's Anti-Phishing Portal to alert Internet users that they have visited a Phishing site. On average, SKMM receives three to four phishing reports every day. SKMM's phishing portal also has examples on how phishing websites look like, thus raising awareness amongst Internet users.

Conclusion

The setting up of the National Security Centre coordinates not only the Commission's efforts towards securing the nation's information and network systems but will also effectively coordinate with similar efforts in Malaysia. At the same time, SKMM's Network Security Portal aims to heighten awareness of Internet security and be a one-stop shop for Malaysians to get up-to-date information on network security. www.skmm.gov.my

Harme Mohamed is Director,
Security and Trust & Governance Department, SKMM.
He can be reached at harme@cmc.gov.my

