CYBER INCIDENT MANAGEMENT: NATIONAL AND REGIONAL LESSONS LEARNED

HARME MOHAMED

21 OCTOBER 2015

MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION

- MCMC is both the developer and the regulator for the C&M industry, established based on:
  - Malaysian Communications and Multimedia Commission Act 1998 (MCMCA 1998)
  - Communications and Multimedia Act 1998 (CMA 1998)
- In terms of network security MCMC derives its powers from:
  - Section 3(2)(j) of the CMA 1998 provides for the national policy objective to ensure the information security and network reliability and integrity.
  - Section 16(1)(c) of MCMCA 1998 requires SKMM to regulate all matters relating communications and multimedia activities not provided for in the communications and multimedia laws.

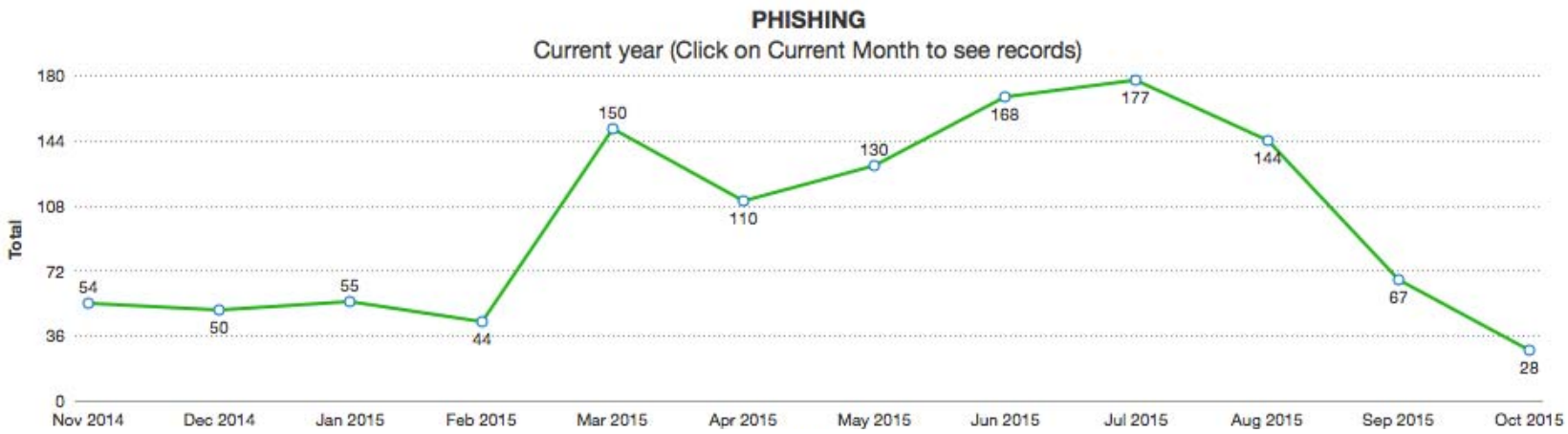
MCMC: NETWORK SECURITY CENTRE

http://snsc.skmm.gov.my

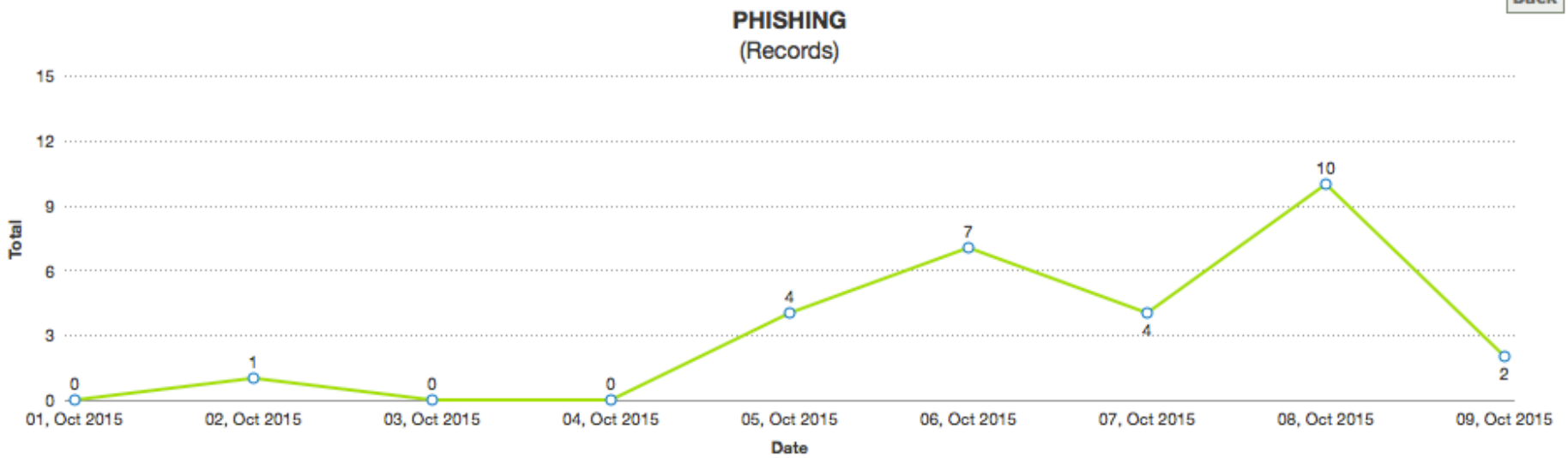
INDUSTRY COLLABORATION TO COMBAT ONLINE BANKING PHISHING

- To collect phishing emails and website locations to help people avoid becoming victims of online banking phishing scams.
- Collaborate with Internet Banking Task Force (IBTF), Malaysian ISPs and the global CERT community to take down all phishing sites.

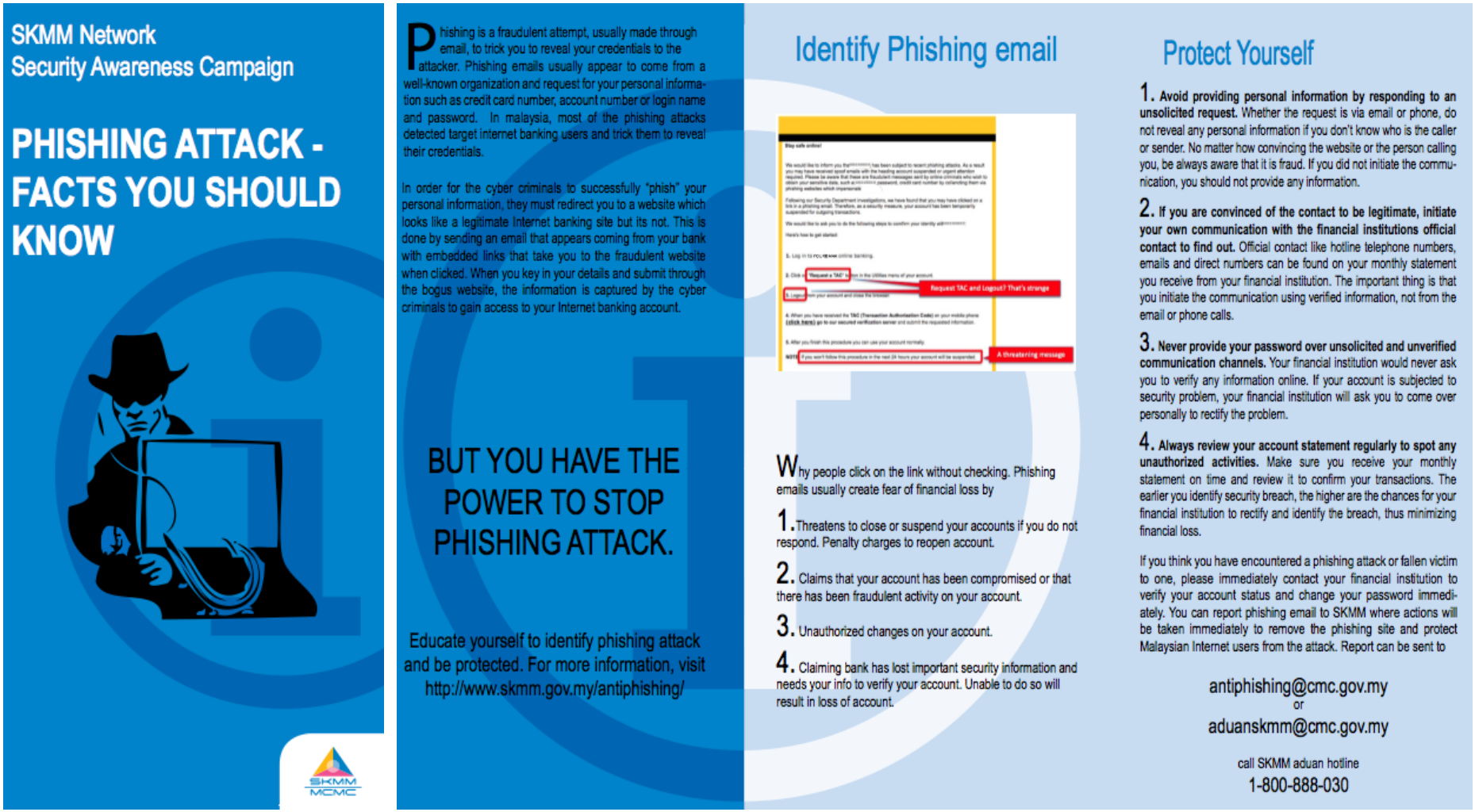
PHISHING INCIDENCE: OCT 2015



Back



ANTI-PHISHING BROCHURE



SKMM Network
Security Awareness Campaign

PHISHING ATTACK - FACTS YOU SHOULD KNOW

Phishing is a fraudulent attempt, usually made through email, to trick you to reveal your credentials to the attacker. Phishing emails usually appear to come from a well-known organization and request for your personal information such as credit card number, account number or login name and password. In malaysia, most of the phishing attacks detected target internet banking users and trick them to reveal their credentials.

In order for the cyber criminals to successfully "phish" your personal information, they must redirect you to a website which looks like a legitimate Internet banking site but its not. This is done by sending an email that appears coming from your bank with embedded links that take you to the fraudulent website when clicked. When you key in your details and submit through the bogus website, the information is captured by the cyber criminals to gain access to your Internet banking account.

BUT YOU HAVE THE POWER TO STOP PHISHING ATTACK.

Educate yourself to identify phishing attack and be protected. For more information, visit http://www.skmm.gov.my/antiphishing/

Identify Phishing email

Request TAC and Logout? That's strange

A threatening message

Why people click on the link without checking. Phishing emails usually create fear of financial loss by

1. Threatens to close or suspend your accounts if you do not respond. Penalty charges to reopen account.
2. Claims that your account has been compromised or that there has been fraudulent activity on your account.
3. Unauthorized changes on your account.
4. Claiming bank has lost important security information and needs your info to verify your account. Unable to do so will result in loss of account.

Protect Yourself

1. **Avoid providing personal information by responding to an unsolicited request.** Whether the request is via email or phone, do not reveal any personal information if you don't know who is the caller or sender. No matter how convincing the website or the person calling you, be always aware that it is fraud. If you did not initiate the communication, you should not provide any information.
2. **If you are convinced of the contact to be legitimate, initiate your own communication with the financial institutions official contact to find out.** Official contact like hotline telephone numbers, emails and direct numbers can be found on your monthly statement you receive from your financial institution. The important thing is that you initiate the communication using verified information, not from the email or phone calls.
3. **Never provide your password over unsolicited and unverified communication channels.** Your financial institution would never ask you to verify any information online. If your account is subjected to security problem, your financial institution will ask you to come over personally to rectify the problem.
4. **Always review your account statement regularly to spot any unauthorized activities.** Make sure you receive your monthly statement on time and review it to confirm your transactions. The earlier you identify security breach, the higher are the chances for your financial institution to rectify and identify the breach, thus minimizing financial loss.

If you think you have encountered a phishing attack or fallen victim to one, please immediately contact your financial institution to verify your account status and change your password immediately. You can report phishing email to SKMM where actions will be taken immediately to remove the phishing site and protect Malaysian Internet users from the attack. Report can be sent to

antiphishing@cmc.gov.my
or
aduanskmm@cmc.gov.my

call SKMM aduan hotline
1-800-888-030

IASP CYBER DRILL

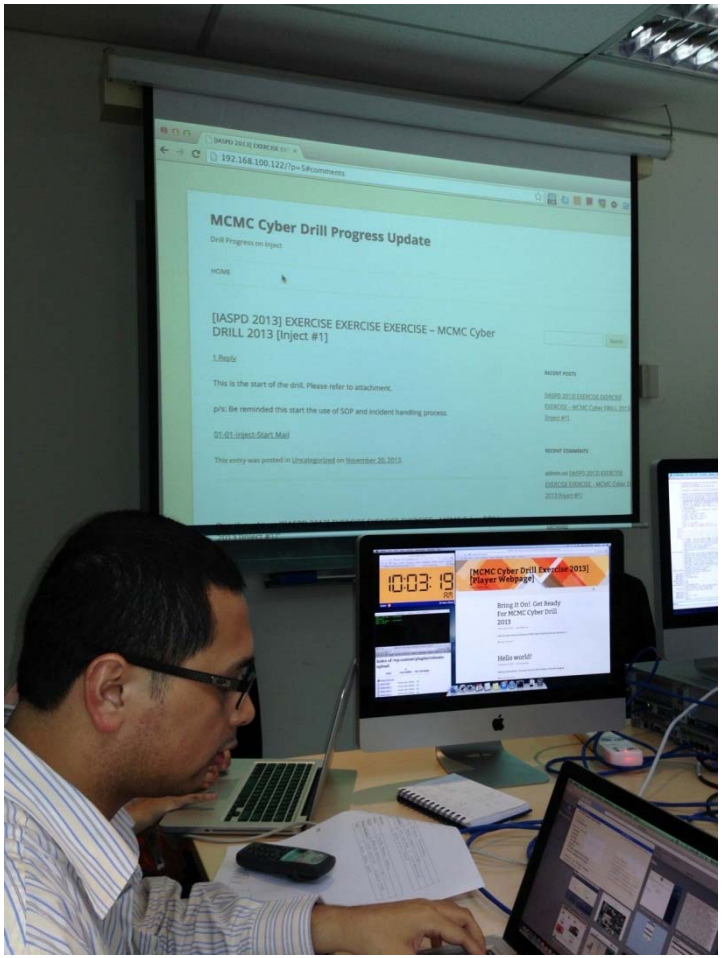
IASP CYBER DRILL

- Organized by Network Security Center of Malaysian Communication and Multimedia Commission
- The IASP Cyber Drill is a simulated coordinated process where mock threats are handled by the IASP's Computer Emergency Response Team (CERT) with SNSC as the coordination entity:
  - First IASP Cybre Drill in July2012
  - Second IASP Cyber Drill in November 2013
  - Third IASP Cyber Drill in November 2015
- Participated by 10 ISPs
- Focused on
  - Communication efficiency
  - Standard Operating Procedures

OBJECTIVE

- Initiative from Network Security Center to measure the gap of licensees under MCMC
- Reports of the drill will be made available to all the players for them to take measures to better equip/improve in handling incidents, malware propagations and advance persistent threat

2013 IASP CYBER DRILL



Coordination Team

THANK YOU