GENERAL

Protect data and be alert to online cyber threats

21 May 2021

By: Irman Khalil, Centre for Information and Communication Technology and Mimi Rabita Haji Abdul Wahit, Corporate Communications Unit, The Office of The Vice-Chancellor

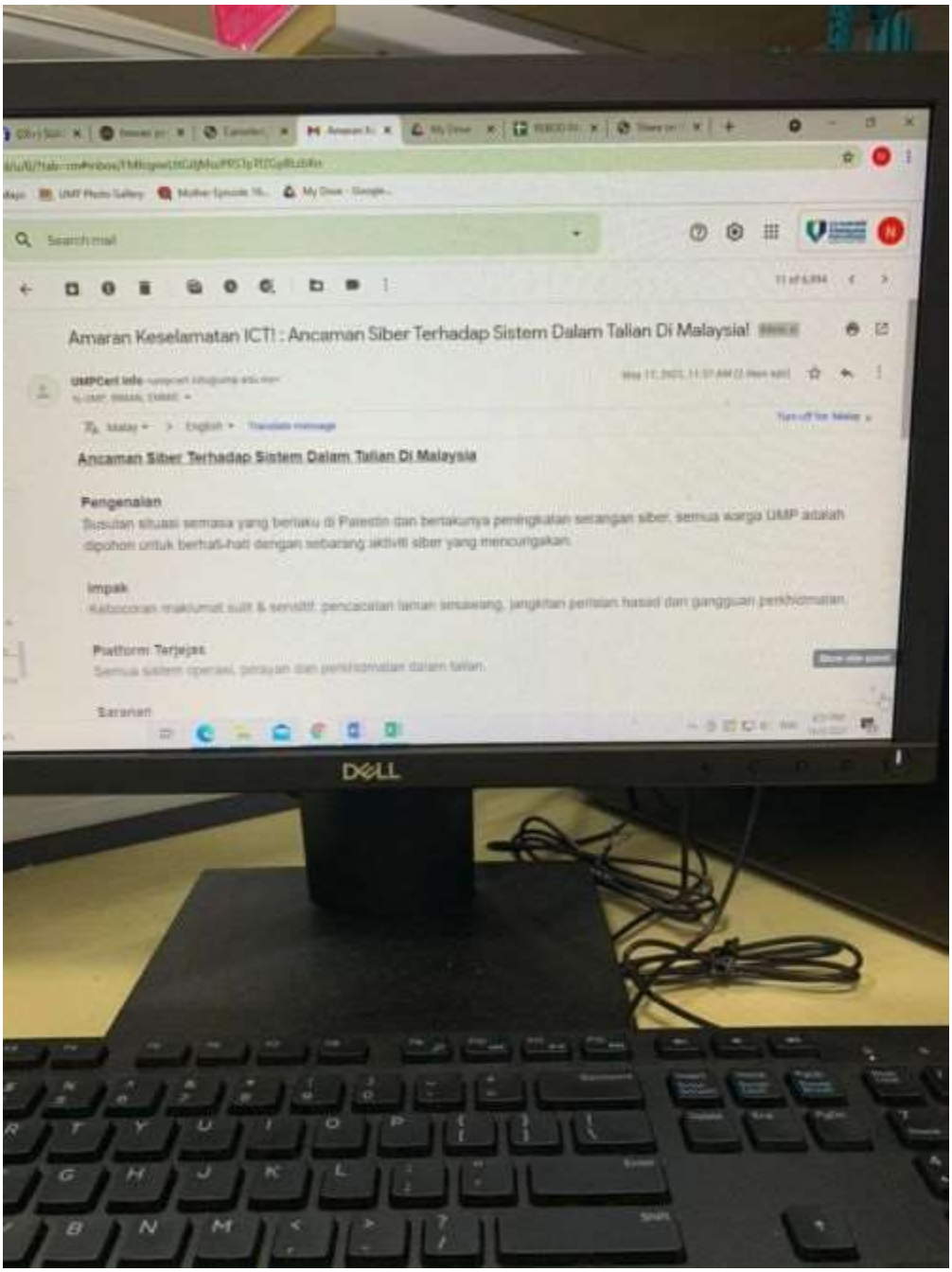
Translation by: Dr. Rozaimi Abu Samah, Engineering College/Faculty of Chemical and Process Engineering Technology

PEKAN, 18 May 2021 - Universiti Malaysia Pahang (UMP), through the Centre for Information and Communication Technology (PTMK), advises university residents to always ensure that all internet-

related applications are updated and upgraded and always be careful with emails and links from suspicious sources.

It can result in leakage of confidential and sensitive information, web defacement, malware infection and service disruption.

The cyber threats in Malaysia began following the tense situation in Palestine, leading to a series of hacktivist campaigns that attacked the social media accounts of Israeli figures, leaders and celebrities with insulting comments with the hashtags #shameonIsrael and #IsraelKoyak.



Based on the National Cyber Security Agency (NACSA) alert issued on 16 May 2021, there has been an increase in responses from the Israeli side targeting Malaysian organisations.

Every organisation must take appropriate action to avoid becoming a victim of this attack, resulting in disrupting the organisation's operations.

According to Irman Khalil, the Acting Director of PTMK, some groups hack Israeli-owned websites and databases, resulting in hundreds of websites and databases being hacked and hijacked.

"As users, we need to ensure that the passwords for internet applications are strong and secure and the use of 2-step factor authentication is also highly encouraged for email and social media accounts.

"In addition, organisations are advised to be vigilant and take action on updating critical ICT assets with the latest security patches (patch updates), be alert with suspicious emails and links with/or without attachments and ensure antivirus for computers personal and laboratory computers have been updated and are working well," he said.

He also advised users never open links from untrusted sources that could lead to cyber attacks, computer virus infections or theft of identity or account information.

"Switch off all workstations before leaving the office, whether personal computers or laboratory computers, and perform updates and upgrades to all internet applications.

"Users must also disconnect the computer network (personal computers and laboratory computers) from the internet if not in use and ensure that the passwords for system, faculty and department portals are strong and secure.

"This includes administrators of UMP faculty and department social media accounts (Facebook, Twitter, Instagram and others) who are required to make two-factor authentication on their respective social media accounts," he said.

Among the expected cyber attack methods in response to such attacks are intrusion, hacking attempts, distributed denial-of-service (DDoS), website defacement and malware infection.

Intrusion activity is an attempt to enter a website illegally to do damage or steal certain data.

Hacking attempts is an activity that aims to cause damage to a website.

A DDoS attack is a method of disabling a network or server with a high amount of traffic affecting the memory resources and hardware processors.

Website defamation involves intruders acting to do damage to the existing website.

One of the popular methods is to change the website's front page to inappropriate writing or pictures.

While malware is a programme developed to access a system, damage data, steal data and others.

There are many types of malware such as viruses, trojans, spyware and ransomware.

The university prohibits its citizens, whether staff or students, from engaging in cyber intrusion activities using the UMP network.

They must report any anomalies in their network and environment to UMPCERT via email umpcert@ump.edu.my.

NACSA has also issued guidelines for organisations in dealing with cyber attack situations, including recommendations for users and system and network administrators.

Self-service cyber security measures have also been issued by the Malaysian government, which consists of ten simple steps:

1. Use a password
2. Update security software
3. Keep your information protected
4. Be aware of your cyber environment
5. Observe your ethics on the internet
6. Beware of cyber criminals
7. Think before you click
8. Lodge a report
9. Be alert
10. Comply

Source: National Cyber Security Agency (NACSA) https://www.nacsa.gov.my/individuals.php