CYBER SECURITY BULLETIN

Cyber Security Bulletin Number: 006

SPAM part 2

Unsolicited, bulk emails or as we know it as spam are annoying emails that we often receive in our inbox. Before, these kinds of emails were often used for advertisements of goods and services but in the recent years, spam emails were already used for illegal purposes. Sending of spam emails is one of the initial steps in carrying out a successful cyber crime or attack. Spams often carry malwares or links to malicious websites.

What are the implications of this? You can be subjected to fraud, identity theft, data theft or your computer can be part of the "bot net" (meaning your computer is under control to take part of an attack or crime) and worse, if your computer is connected to the Philippine Army Network (PANet), it could compromise our network.

Why? Is there something to be hacked in the PANet? Yes, of course, remember our Personnel Information System and other information systems runs through the PANet. It is the connection between our information system servers and computers that access it. No one would like that information to be divulged out in the public.

The Philippine Army email is equipped with anti-spam to detect bulk messages, spam and viruses that passes through this appliance, thus, denying it from entering our email storage (or as we know it as inbox). As per statistics, spam messages volume is increasing in our overall incoming email, undetected spam email is not part of that statistics. Undetected spam emails are delivered in to your inbox which might carry malwares or links to malicious websites.

So what? Who cares about malwares, I am not connected to the Philippine Army Network (PANet), I have my own Internet Service Provider (ISP) and I have nothing in my computer but games and videos; but I do use an email. You might want to consider that you do not want the police or NBI (or may be the FBI) to be knocking at your door because your computer has been a part of a cyber crime or attack.

How come? "Bot net", let us take for example: scenario 1: you have opened an email attachment that installed a malware that made your computer a proxy to a cyber sex den, meaning the culprit used your IP address to mask his own address with a malware. Scenario 2: your computer was one of the hundreds of computers to send bulks of traffic to a certain server to bring it down or also called denial of service attack.

So, What do I do then? The following are tips to avoid being victims of cyber crooks using spam emails:

1. Do not open or click links from un-trusted senders.
2. Do not give out your email address to the public.
3. If you are already receiving spam messages, be careful with "unsubscribe" links from questionable senders as it may deceive you from the actual intent of the link.

But, legitimate companies do have “unsubscribe” links which you can avail, check on their legitimacy by visiting their websites.

4. If you are using the Philippine Army email, do not use it in social media sites or as registration to other sites. If you are receiving spam or unsolicited emails forward it to netc_csd@army.mil.ph for inspection.

The “army.mil.ph” email is private; it is similar to corporate emails used by large companies. Corporate emails usually don’t receive spam unless users have used it unscrupulously. Start protecting yourself by securing your computer; by securing your computer you are already contributing to the security of the PANet and its information systems.