CYBER SECURITY BULLETIN 012

HOW TO STRENGTHEN THE WEAKEST LINK IN THE SECURITY CHAIN

The guiding tenet of computer security is that an organization's overall security is only as strong as its weakest link. While organizations around the globe routinely employ traditional defences like the use of firewalls, antivirus software and sophisticated intrusion-detection-prevention systems to ensure the confidentiality, integrity and availability of data, network services and other critical information assets, they often neglect the most important and vulnerable security component: the human element. The human layer of cyberspace plays a very critical role in cyber security.

Without a license, we are not allowed to drive a car, fly a plane or practice medicine, yet we are free to surf the Internet and send and receive e-mail. While the use of the Internet doesn't have the same potential for causing harm as flying a plane without a license, the use of the Internet nevertheless has the potential to wreak havoc on an organization's networked PCs. Anyone with access to any part of the system, physically or electronically, is a potential security risk. Security is all about knowing who and what to trust. Knowing when, and when not to, to take a person at their word; when to trust that the person you are communicating with is indeed the person you think you are communicating with; when to trust that a website is or isn't legitimate; when to trust that the person on the phone is or isn't legitimate; when providing your information is or isn't a good idea.

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).

Because e-mail messages can include file attachments, malicious individuals will send infected files incorporated as attachments with a catchy subject line in the hope that recipients will open them. This was precisely the case with the infamous *AnnaKournikova worm*, the *Melissa virus* and the *Naked Wife Trojan horse*. Using the psychology of temptation, the creators of both *AnnaKournikova and Naked Wife* enticed a large segment

of the Internet population into opening the attachment, thereby activating the virus. Even the famous *"I Love You"* virus spread rapidly because the e-mail message it was attached to appeared to be a genuine sign of affection from someone the recipient knew. Another big threat is attackers posing as persons of authority such as the unit commander, Chief of Office or as PANET Network/System Administrators wherein users are unknowingly tricked into opening attached files and clicking links thinking it is from their superiors or from the IT personnel.

How to defend the Army, the Philippine Army Network and yourself

Social engineering has employed a number of ways to entice unsuspecting users into opening e-mail attachments, from pornography to phony security warnings and advice. So how do we as a military organization defend against such attacks? The only protection against social engineering attacks is through our willingness to be educated on the intricacies of the Internet. This Cyber Security bulletin aims to educate all PA personnel in cyber security and we should do our part by reading and sharing this piece of information through TI&Es, Seminars, casual conversation, in the confines of our barracks to our respective homes with our families.

Ensuring the security of our Network will certainly be enhanced when Officers and EP are motivated (but not scared) to adopt a common-sense approach to security and are trained to recognize possible security problems. If you are not certain, ask; if not contented, search the internet and ask the mighty Google for answers. In this manner, we increase our awareness and become educated. The best training doesn't present IT security as just another policy of the organization, but highlights the consequences of poor security practices. To diminish the risks posed by malicious code, the following tips are recommended to mitigate these types of threats:

1. **Close the preview pane of your e-mail program.** The preview pane is the feature that shows you the contents of an e-mail before you choose to open it. It's often displayed below the pane that displays a list of e-mails, their titles and time of receipt or transmission. It is recommended to disable the preview of html emails along with the image previews to lessen the risk of running malicious scripts from embedded in the image and attachment.

2. **Disable the *JavaScript* and *ActiveX* features of your Web browser.** *Java* and *ActiveX* were designed to run more advanced features and to use services or make changes on the computer you are using. Unless these features are explicitly required, it's safer to deactivate them to prevent malicious scripts from infecting or compromising the computer or the network.

3. **Equip your computer with an antivirus program, maintain the most current version, and select the user options that give you the most protection.** There are

several different types, not just different brands. Some antivirus programs search for specific file signatures; others monitor a computer program's activity and prohibit virus-like behaviour. There are also cost-free scans from vendors via the Internet that can scan your hard drive and removable disks. Ensure that your antivirus program will screen attached files.

4. **Save attachments to a disk before opening**. Do not open the attachment directly from the e-mail program. Save it to a disk, preferably a removable disk, and then scan the disk with an antivirus program.

5. **Do not open e-mail attachments from stra**ngers, regardless of how enticing the subject line may be. In addition to e-mails containing damaging computer viruses, there could be malicious spam. The spam plays off human curiosity. It may be an e-mail message or a redirection to another Web page. The action is often to solicit donations to organizations claiming to be charities or to barrage computers with pop-up advertising. That is why we must not use our work email in registering for anything in the World Wide Web. The PA email system must remain strictly for Army and Official Communications only.

6. **Be suspicious of any unexpected e-mail attachments from someone you do know, it may be from your Unit Commander, Chief of Office or Chief Clerk**. It may have been sent without that person's knowledge from an infected machine. The Sircam virus continues to spread by automatically e-mailing itself between users who might expect to hear from each other. Also, someone might have stolen a trusted person's such as our unit or office commanding officers or NET System Admins password and might be pretending to be that person.

7. **Verify suspicious e-mail**. In the event you receive e-mail from someone you know that has a suspicious title or attachment, contact the sender by telephone or send him a new e-mail saying that you want to verify that the questionable e-mail was intended for you.

Sowing the seeds of awareness will lead to all PA personnel taking a more proactive stance toward cyber security. If all PA personnel had the knowledge, or been instructed to automatically verify the source and content of all e-mail attachments before opening them, viruses like *Melissa* or *Naked Wife* wouldn't have been nearly as successful as they were. We as, Officers and Enlisted personnel who form part of the defences of our network and critical IT Infrastructure, must take measures to protect the Army's cyberspace, the PANET and ourselves from threats in the borderless cyberspace.

Reference:

http://www.computerworld.com/article/2580125/security0/how-to-toughen-the-weakest-link-in-the-security-chain.html