CYBER SECURITY BULLETIN #6: SCAMS and FRAUDS

The rapid development in technologies may offer countless opportunities for the Philippine Army organization, but the former also offer cyber criminals many new ways to exploit the organization, scam the personnel and hurt even reputation.

All Personnel of the PA should be aware of the most common scams perpetrated online.

Cyber Plan Action Items:

1. **Train personnel to recognize social engineering**

Social engineering, also known as "pretexting," is used by many criminals, both online and off, to trick unsuspecting people into giving away their personal information and/or installing malicious software onto their computers, devices or networks. Social engineering is successful because the bad guys are doing their best to make their work look and sound legitimate, sometimes even helpful, which makes it easier to deceive users.

Most offline social engineering occurs over the telephone, but it frequently occurs online, as well. Information gathered from social networks or posted on websites can be enough to create a convincing ruse to trick personnel. For example, LinkedIn profiles, Facebook posts and Twitter messages can allow a criminal to assemble detailed dossiers on personnel. Teaching people the risks involved in sharing personal or job details on the Internet can help personnel to prevent both personal and organizational losses.

Many criminals use social engineering tactics to get individuals to voluntarily install malicious computer software such as fake antivirus, thinking they are doing something that will help make them more secure. Users who are tricked into loading malicious programs on their computers may be providing remote control capabilities to an attacker, unwittingly installing software that can steal financial information or simply try to sell them fake security software.

2. **Protect against online fraud**

Online fraud takes on many guises that can impact everyone. It is helpful to maintain consistent and predictable online messaging when communicating with your colleagues to prevent others from impersonating them.

Be sure to never request personal information or account details through email, social networking or other online messages. Let your colleagues know you will never request this kind of information through such channels and instruct them to contact you directly should they have any concerns.

3. Protect against phishing

Phishing is the technique used by online criminals to trick people into thinking they are dealing with a trusted website or other entity. The PA organization face this threat from two directions -- phishers may be impersonating someone to take advantage of unsuspecting personnel, and phishers may be trying to steal their online credentials.

Personnel awareness is the best defense against being tricked into handing over usernames and passwords to cyber criminals. Personnel should never respond to incoming messages requesting private information. Also, to avoid being led to a fake site, personnel should know to never click on a link sent by email from an untrustworthy source. Personnel needing to access a website link sent from a questionable source should open an Internet browser window and manually type in the site's web address to make sure the emailed link is not maliciously redirecting to a dangerous site.

This advice is especially critical for protecting online banking accounts belonging to personnel. Criminals are targeting 'small business' banking accounts more than any other sector.

4. Don't fall for fake antivirus offers

Fake antivirus, "scareware" and other rogue online security scams have been behind some of the most successful online frauds in recent times. Make sure your personnel read and understand the series of cyber security bulletins published for guidance. The topics are intended to be discussed repeatedly from one topic to another for better memory grasp of the personnel.

Train personnel to recognize a legitimate warning message (using a test file from eicar.org, for example) and to properly notify your cyber security team if something bad or questionable has happened. If possible, configure your computers to not allow regular users to have administrative access. This will minimize the risk of them installing malicious software and condition users that adding unauthorized software to work computers is subject for approval.

5. Protect against malware

The computing environment can experience a compromise through the introduction of malicious software, or malware, that tracks a user's keyboard strokes, also known as key logging.

Many personnel are falling victim to key-logging malware being installed on computer systems in their environment. Once installed, the malware can record keystrokes made on a computer, allowing bad guys to see passwords, credit card numbers and other confidential data. Keeping security software up to date and patching your computers regularly will make it more difficult for this type of malware to infiltrate your network.

6. Develop a layered approach to guard against malicious software

Despite progress in creating more awareness of security threats on the Internet, malware authors are not giving up. The malware research firm SophosLabs reports seeing more than 100,000 unique malicious software samples every single day.

Effective protection against viruses, Trojans and other malicious software requires a layered approach to your defenses. Antivirus software is a must, but should not be a unit's only line of defense. Instead, deploy a combination of many techniques to keep your unit computing environment safe.

Also, be careful with the use of thumb drives and other removable media. These media could have malicious software pre-installed that can infect your computer, so make sure you trust the source of the removable media devices before you use them. Don't open the auto pop ups instead manually open the thumb drive after scanning it your resident antivirus.

Combining the use of web filtering, antivirus signature protection, proactive malware protection, firewalls, strong security policies and personnel training significantly lowers the risk of infection. Keeping protection software up to date along with your operating system and applications increases the safety of your systems.

6. Verify the identity of telephone information seekers

Most offline social engineering occurs over the telephone. Information gathered through social networks and information posted on websites can be enough to create a convincing ruse to trick personnel.

Ensure that you train personnel to never disclose any information, usernames, passwords or other sensitive details to incoming callers. When someone requests information, always contact the person back using a known phone number or email account to verify the identity and validity of the individual and their request.

HELPFUL LINKS:

- Find the most updated patches for your computer and software applications: http://www.softwarepatch.com/
- Free computer security scan tools for your PC or network: http://www.staysafeonline.org/tools-resources/free-security-check-ups
- Stay on top of the latest scams, frauds and security threats as they happen: http://nakedsecurity.sophos.com/
- Additional tops to prevent against phishing: http://www.fraud.org/tips/internet/phishing.htm
- Learn how to resist phishing techniques with this interactive game: http://cups.cs.cmu.edu/antiphishing_phil/