Cyber Security Bulletin Number: 017

10 Steps for Safe Web Surfing

The internet change our lives forever. We now live through infinitely complex virtual networks connecting disparate people globally. Interconnectivity almost made impossible things possible and spawned greater knowledge because of its borderless character and "open-free" services. It equally threaten us on the existence of criminals who use technology as their instrument to conquer privacy and confidentiality, destroy the integrity of our digital assets and freely manipulate data and informations dictating its availability causing superfluous suffering to people globally.

The Philippine Army's Information and Communications Technology owe its life to the connectivity that the internet brings. And the reality of web surfing activities of our personnel is a common site in the workplace- personal or work related, they are interwoven to make the individual's online habit. Different online habits should be guided accordingly by observing policies, following reminders from cybersecurity bulletins, TI&Es, forums, seminars and stakeholder's engagement.

These cybersecurity bulletin – **10 steps is to make the Web work for you and not against you** – is yet another reminder for our personnel that security in cyberspace is a continuous undertaking that every personnel should not be short of:

1. **Education** – Educate yourself about the types of scams on the Internet so that you are better equipped to defeat them. Read up on the latest phishing scams, for example, and learn how to recognize them.

2. **Use a firewall** – Firewalls monitor traffic between your computer or network and the Internet and are your first and best line of defense. Most operating systems come with a firewall, but it won't help you if you don't activate it.

3. **Click with caution** – When checking e-mail or instant messaging, be careful not to click on links in messages from people you don't know. Such links could connect to phony websites designed to solicit personal information, or they could download Trojan horses or other malware designed to steal personal information. Even if the message is from someone you do know, it could still contain a computer virus; check with the sender if you have any concerns about the validity of the message.

4. **Surf safely** – When browsing the Web for financial institutions or other sites, take steps to avoid fraudulent sites that ask for personal information. Most legitimate sites don't ask for such information, but instead require registration ahead of time. Use a search engine that corrects misspellings so that you navigate legitimate sites and avoid landing on a fake webpage. Creating fake sites with a similarly spelled address is a fairly common scam known as "**typosquatting**."

5. **Practice safe shopping** – Shopping online or planning vacations via the Internet can be a terrific tool for consumers, but be careful when you're on sites you've never used before. When on the checkout page, look for the lock symbol or some other indication, such as the prefix "**https**," that the page is encrypted or scrambled. Use a credit card instead a debit card; if the site turns out to be fraudulent, your credit card company may reimburse you for the charges. Evaluate the site's security and privacy policies regarding the use of your personal data.

6. **Use regularly updated security software** – Use security software that updates automatically and often to provide maximum protection from viruses, spyware and other cyber threats, which also are being constantly updated. Conduct regular malware scans of your computer, and update your operating system and browser with the manufacturer's latest security patches.

7. **Secure wireless networks** – Don't let your home network's wireless router be a welcome mat for hackers. Enable the firewall on your router and regularly change the router's administrative password. Check the support section of your ISP's website or your router manufacturer's website for instructions on how to take these precautionary steps. And make sure your router has a strong encryption, such as WPA or WPA2.

8. **Strong passwords** – While short, simple passwords may be easier to remember, they're also easier for hackers to crack. When banking online or accessing other sites that may reveal personal or financial information, use passwords with at least 10 characters and include combinations of letters, numbers and symbols. Change passwords regularly.

9. **Common sense** – Cybercrime continues to accelerate and it's being fueled by common mistakes people make when online, such as responding to spam or phishing scams or downloading attachments from people or sites they don't know. Use common sense and caution; limit posting of personal information online; and be careful about clicking on links or prompts to download software.

10. **Be skeptical** – Many victims of scams may have thought they were cyber savvy and let their guard drop long enough for a cyber-thief to strike. Back up data regularly in case a virus infects your computer, and monitor accounts and credit reports to make sure your identity has not been stolen.

Application of this 10 steps at least assure us of safety in our web browsing activities. However, we need to religiously apply this 10 steps and engage subject matter experts or technical guys on how we can better secure our digital assets and maintain its confidentiality, integrity and availability. We need to develop a proactive habit in cybersecurity- at the workplace and at home.