# CYBER SECURITY BULLETIN

**Cyber Security Bulletin Number: 005**

## Basic Cyber Security Best Practices

**Secure your computer.** Be sure to have a firewall installed.on your computer. Operating System like windows has built-in firewall be sure it is enabled. Use spyware and adware protection software. This software is designed to protect you against spyware or malware, which can extract private information from your computer without your knowledge. Set these programs to auto-update to avoid missing a critical update.

**Use strong passwords on all your accounts.** Use a minimum of eight characters and a mix of special symbols, letters, and numbers. Use separate passwords for each account, so that if one account password is breached, an attacker will not automatically have access to all of your other accounts. Do not re-use your work password on other systems.

**Secure your online transaction.** When submitting your sensitive information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission. Also be sure that "https" appears in the website's address bar before making an online transaction. The "s" stands for "secure," and indicates that communication with the webpage is encrypted.

**Don't reveal too much personal information online.** The less information you post, the less data available for a cyber criminal to use in a potential attack or scam.

**Protect your laptop, smartphone, or other portable devices when traveling.** Just as your wallet contains lots of important and personal information that you wouldn't want to lose, so too do your portable devices. Don't let them out of your sight! Never store your laptop as checked luggage. In addition, make sure you have strong passwords on these devices in case they are lost or stolen.

**Be aware that public computers and public wireless access are not secure.** Cyber criminals can potentially access any information you provide, such as credit card numbers, confidential information, or passwords. Don't conduct any sensitive transactions at the local free Wi-Fi site.

**Understand if and how location data is used**. Check to see if GPS location data is being stored when you upload pictures to your social media site from your mobile device, and disable it if you don't want the world to know exactly where the picture was taken.

**Do not e-mail sensitive data.** Beware of emails requesting account or purchase information. Delete these emails. Never e-mail credit card or other financial/sensitive information. Legitimate
businesses don't solicit sensitive or confidential information through email.

**Dispose of information properly.** Before discarding your computer or portable storage devices, you need to be sure that the data contained on the device has been erased or "wiped." Read/writable media (including your hard drive) should be "wiped" or destroyed.

By securing our own information, we secure others’ and the Philippine Army as well. Cyber security is our shared responsibility.

Reference: *www.msisac.cisecurity.org*