MESSAGE FORM

(INSTRUCTION: FILL-UP BOXES INSIDE DOUBLE LINES ONLY)

FOR COMCEN/SIG USE

PRECEDENCE ACTION/PRECEDENCE INFO
"PRIORITY"

FM: CG, PA

TO: All Unit Commanders
Attn: G6/Signal Officer/IS Officer

INTERNAL: All G-Staff, Personal, Special & Tech Staff, C, AOC/SAGS/XA

INFO: CSAFP
Attn: J6

GROUP:
22 December 2015

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 2212-32-2015

1. References:

   a. Command Guidance, and;
   b. VAPT and PANET Monitoring Result

2. As per above references, forwarded is the Cybersecurity Bulletin number 039 with topic regarding **PUBLIC WIRELESS THREATS.**

3. ITR, all concerned G6/Signal Officers/Information System Officer/NCOs are reminded to include this information as part of TI & E on all of its subordinate units as part of enhancing the Cybersecurity Awareness of the Philippine Army.

4. For information and widest dissemination.

DRAFTER'S NAME AND TITLE	**PHONE NR:**
MAJ JOEY T FONTIVEROS (INF) PA Chief, CMB, OG6, PA	6630
RELEASER'S NAME AND TITLE	
COL VENER ODILON D MARIANO GSC (SC)PA AC OF S FOR CEIS, G6, PA	

HEADQUARTERS
PHILIPPINE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB 22 December 2015

CYBER SECURITY BULLETIN

Cyber Security Bulletin: #39

PUBLIC WIRELESS THREATS

A wireless-enabled laptop can make you more productive outside your office or home, but it can also expose you to a number of security threats. This article describes some of the security threats you face when using a public access point.

Evil Twin Attacks

In an evil twin attack, the attacker gathers information about a public access point, then sets up his or her own system to impersonate the real access point. The attacker will use a broadcast signal stronger than the one generated by the real access

point. Unsuspecting users will connect using the stronger, bogus signal. Because the victim is connecting to the internet through the attacker's system, it's easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, addresses, and other personal information.

Wireless Sniffing

Many public access points are not secured, and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted "in the clear," malicious users can use "sniffing" tools to obtain sensitive information such as passwords, bank account numbers, and credit card numbers.

Peer-to-Peer Connections

Many laptop computers, particularly those equipped with 802.11-type WiFi wireless networking cards, can create ad hoc networks if they are within range of one another. These networks enable computer-to-computer connections, a situation that creates security concerns you should be aware of. An attacker with a network card configured for ad hoc mode and using the same settings as your computer may gain unauthorized access to your sensitive files. You should note that many PCs ship from the manufacturer with wireless cards set to ad hoc mode by default.

Unauthorized Computer Access

As is the case with unsecured home wireless networks, an unsecured public wireless network combined with unsecured file sharing can spell disaster. Under these conditions, a malicious user could access any directories and files you have allowed for sharing.

Shoulder Surfing

In public wireless areas, the bad guys don't even need a computer to steal your sensitive information. The fact that you may be conducting personal business in a public space is opportunity enough for them. If close enough, they can simply glance over your shoulder as you type. Or, they could be peering through binoculars from an apartment window across the street. By simply watching you, they can steal all kinds of sensitive, personal information.

Safe Wireless Networking in Public Spaces

Accessing the internet via a public wireless access point involves serious security threats you should guard against. These threats are compounded by your inability to control the security setup of the wireless network. What's more, you're often in range of numerous wireless-enabled computers operated by people you don't know. The following sections describe steps you can take to protect yourself.

Watch What You Do Online

Because you're likely to have an unsecured, unencrypted network connection when you use a public wireless access point, be careful about what you do online—there's always the chance that another user on the network could be monitoring your activity. If you can't connect securely using a VPN (see "Connect Using a VPN" below), then consider avoiding

- online banking
- online shopping
- sending email
- typing passwords or credit card numbers

Connect Using a VPN

Many companies and organizations have a virtual private network (VPN). VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends, and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

Disable File Sharing

File sharing in public wireless spaces is even more dangerous than it is on your home wireless network. This is because you and your wireless-enabled laptop are likely to be even closer to other wireless computers operated by people you don't know. Also, many public wireless networks feature peer-to-peer networking in which other computers will attempt to connect directly to yours. To leave file shares open in this kind of environment is to invite risk. To prevent attackers from gaining access to your sensitive files, you should disable file sharing when connecting to a public wireless access point. Consult the help file for your operating system to learn how to disable file sharing.

Be Aware of Your Surroundings

When using a public wireless access point, you should be aware of what's going on around you. Are others using their computers in close proximity to you? Can others view your screen? Are you sitting near a window through which someone, using binoculars, could get a view of your screen? If any of these conditions exist, your sensitive data might be at risk. Consider whether it is essential to connect to the internet. If an internet connection is not essential, disable wireless networking altogether. If you do need to connect, use caution and follow the steps noted above.

DO YOU WANT TO KNOW MORE? TALK TO US.

POC: MAJ JOEY T **FONTIVEROS (INF) PA** – Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-628-1057.

Reference:

https://www.us-cert.gov/sites/default/files/publications/Wireless-Security.pdf