



Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City



ACG-CYBER SECURITY BULLETIN NR 223

ACG-CSB 102521223

Reference Number ACG-CSB 102521223

UNDERSTANDING THE SECURITY RISK OF PUBLIC WI-FI

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and not classified as “**Restricted**” pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

SUMMARY

The quarantine restrictions are easing out and thousands of people head out for the holiday season, and as they go to places of convergence, its likely they can connect to public Wi-Fi. The spread of this easily accessible Wi-Fi has enabled people to do everything from checking emails, mobile banking or as simply as web browsing.

In unsecured public Wi-Fi, users maybe joining an open network in which creates an opportunity for the hackers to get unrestrained access to unsecured devices.

The hackers are either setting up an open Wi-Fi connection in crowded areas or join an unsecured Wi-Fi connection to exploit unsecured devices. In this set up, the hacker has access to every piece of information you are sending out in the internet such as emails, credit card information, personal details, and contacts. Hackers can also use unsecured Wi-Fi connection to distribute malwares that can cause damage to your device.

RECOMMENDATION

All PNP personnel as well as the public are advised to follow the tips below in order to avoid the security risk of **PUBLIC WI-FI**:

- Don't send any financial information on public networks. Credit card and banking information should be done on secure networks or at home.
- Don't automatically connect to free Wi-Fi. It could be a fake network set up by scammers.
- Don't do online shopping on a public network. That may allow hackers access to your credit card numbers.

For additional information, please refer to the following websites:

- <https://www.forbes.com/sites/johnwasik/2016/11/20/how-to-avoid-wi-fi-scams-during-the-holiday-shopping-season/?sh=1fdc839f3aa7>
- <https://www.teckrr.com/did-you-know-about-the-new-free-wifi-hotspot-scam/>

POINT OF CONTACT

Please contact **PCPT MARK GERALD A NORBE** Police Community Relations Officer thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 723 0401 local 7483 for any inquiries related to this CYBER SECURITY BULLETIN.