Republic of the Philippines
National Police Commission
NATIONAL HEADQUARTERS, PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City
E-mail: acg@pnp.gov.ph

ACG-CYBER SECURITY BULLETIN NR 196

ACG-CSB 092320196

Reference Number ACG-CSB 092320193

Beware of Bluesnarfing

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 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

Bluesnarfing is the use of Bluetooth connection to steal information from a wireless device, particularly common in smartphones and laptops. Using programming languages that allow them to find Bluetooth devices left continuously on and in discovery” mode, cybercriminals can attack devices as far as 300 feet away without leaving any trace.

Once a device is compromised, hackers have access to everything on it: contact, emails, passwords, photos, and any other information. To make matters worse, they can also leave victims with costly phone bills by using their phone

When an attack is happening, the victim can be completely in the dark, unaware that their high-value data is leaking into cyber-criminal hands. Unfortunately, there's no way to completely prevent bluesnarfing. However, there are many ways to decrease chances of becoming a victim.

hacker can synchronize their own system with their targeted victim’s device, in a process known as pairing. If the firmware on a device is unsecured or improperly implemented, an attacker may be able to gain access to and steal all the files whose names are either known or guessed correctly. They may also be able to gain access to any services available to the targeted user.

RECOMMENDATION

All PNP personnel as well as the public are advised to follow the tips in order to avoid the dangers of Bluesnarfing , to wit:

- Switching your Bluetooth to “non-discovery” mode

- Using at least eight characters in your PIN as every digit adds approximately 10,000 more combinations required to crack it
- Never accept pairing requests from unknown users
- Require user approval for connection requests (configurable in your smartphone's security features)
- Avoid pairing devices for the first time in public areas

For additional information, please refer to the following websites:

- https://en.wikipedia.org/wiki/Bluesnarfing
- https://www.techadvisory.org/2017/06/bluesnarfing-what-you-need-to-know/
- https://www.inpixon.com/blog/bluesnarfing
- https://www.finjanmobile.com/what-is-bluesnarfing/

POINT OF CONTACT

Please contact PMAJ JOSEPH ARVIL L VILLARAN, Police Communication Relation officer thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 7230401 local 3562 for any inquiries related to this CYBER SECURITY BULLETIN.