Army Vision: By 2028, a world-class Army that is a source of national pride.

H E A D Q U A R T E R S
P H I L I P P I N E A R M Y
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR
COMMAND AND CONTROL COMMUNICATIONS, AND CYBER SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB 29 December 2016

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #78

Public Wi-Fi Security 101: What Makes Public Wi-Fi Vulnerable to Attack And How To Stay Safe

Nowadays, free public Wi-Fi is widely and readily available in larger cities- airports, restaurants, coffee shops, libraries, public transport, hotel rooms, you name it. Of course, we all know jumping on a free Internet connection can be a convenient way to access online accounts, catch up on work, and check emails while on the go. However, the security risks should not be forgotten. While the best way to protect your information is to avoid accessing sensitive information or performing sensitive transactions when connected to public Wi-Fi, there are additional measures you should be aware of.

According to the 2013 Norton Report, 68% of public and unsecured Wi-Fi users fell victim to cybercrime hence, it's only smart to take practical measures to keep you and your devices protected.

Why is public Wi-Fi vulnerable to cyber-attack?

The average free public Wi-Fi isn't secure and just because you may need a password to log in, it doesn't mean your online activities are encrypted. Various reasons make public Wi-Fi susceptible to attack. One issue has to do with the encryption protocol used by some wireless networks. Another reason has to do with the possibility of joining a rogue Wi-Fi hotspot.

Some wireless networks may use older standards for encryption, which can cause security problems. Wireless Encryption Protocol (WEP), one of the first encryption schemes for wireless networking devices, was found to be weak and easily susceptible to being cracked. Wi-Fi Protected Access (WPA) was intended to replace WEP as the standard for wireless networking devices, but it too was found to have weaknesses. Given their flaws, users are especially at risk when connected to a wireless network that uses these encryption protocols. In fact, tools like Aircrack-ng, available online, are built to perform brute force attacks to crack weak keys on networks using WEP or WPA.

Another issue that can arise when attempting to use free public Wi-Fi is the risk of joining a rogue Wi-Fi hotspot. In such case, an attacker creates a rogue hotspot with the intent to unleash man-in-the-middle (MITM) attacks on unsuspecting victims that join their rogue network. This type of attack allows an attacker to intercept the communication between you and the servers of the websites you visit, allowing them to read, insert, and modify messages.

With pre-built kits that can perform MITM attacks, even minimally skilled hackers can easily eavesdrop and monitor your online traffic to capture valuable information, such as login credentials, credit card numbers, and social security numbers.

Signs you may be logged on to a rogue Wi-Fi

Devices are known to probe for known Wi-Fi networks, and attackers can use this to their advantage. An attacker's rogue Wi-Fi hotspot can pretend to act as your home network or as a public network that you might come across at a coffee shop. Instead of connecting to a real public Wi-Fi hotspot, your device ends up connecting to the attacker's rogue hotspot and now the attacker is sitting between you and the actual Wi-Fi network, so they are able to see your online traffic. Another tactic that can be used is to create a public Wi-Fi network called "Free Wi-Fi" and wait for victims to join. Naturally, lots of people will try to connect, especially if free Internet service is being offered.

If you're away from home, say at a coffee shop, and all of a sudden your computer shows that you're connected to your home network. Chances are someone could have caught your computer's broadcast request. In some cases, if you're browsing a website that you know should be encrypted (HTTPS) such as your bank or your favorite social networking site, but the page is rendering in HTTP, then someone

might be performing a man-in-the-middle attack and serving you the HTTP version of the site in order to capture your login credentials.

Measures you can take to stay protected on public Wi-Fi

Generally speaking, as a precaution, you shouldn't engage in any sort of sensitive web browsing, such as accessing your bank account or entering payment details when connected to public Wi-Fi. Consider these additional safety measures to keep your information protected:

1. Never use public Wi-Fi networks to access sensitive information. If you need to get online to browse for directions or do something else that is less sensitive, you can do it. But if you're trying to pay your bills or buy something. It can wait. If it's a dire situation, or if you regularly use public Wi-Fi, using a Virtual Private Network (VPN) is a must. You can find a variety of trusted VPN services online, but if you want a good service you'll have to pay. Be sure to choose one from a reputable security provider.

2. If you need to use public Wi-Fi to do work and if your company offers VPN access use it. VPN creates a private network for you to shuttle information back and forth, adding an extra layer of security to your connection.

3. Only browse websites that start with HTTPS and avoid websites that start with HTTP while on public Wi-Fi. Websites that start with HTTPS are encrypted, adding an extra layer of security and making your browsing more secure. If you connect to an unsecured Wi-Fi network, and use regular HTTP instead of HTTPS, your traffic is visible if hackers are snooping around in the network.

4. You should also consider installing an extension like **HTTPS-Everywhere** to force all websites you visit to connect using HTTPS. Electronic Frontier Foundation is a recommended option: https://www.eff.org/Https-everywhere (link is external)

5. Configure the wireless settings on your devices to not automatically connect to available Wi-Fi hotspots. This ensures that you do not unknowingly connect to public networks. You can do this by turning off the "Connect Automatically" feature on your computers so they don't auto-connect and search for known Wi-Fi networks. Doing this will prevent your computer from broadcasting to the world that it's trying to connect to "Home Wi-Fi" network and allow an attacker to spoof that.

6. Consider using a privacy screen if you must access sensitive information in public areas—hackers are anywhere and they aren't afraid to use any means necessary to access your information.

7. Lastly, treat and protect your mobile devices such as smart phones and tablets with the same precautions you would your laptop or desktop computer when you join a Wi-Fi network.

Reference:

Cybersecurity Bulletin #78

This was cross posted from:
https://community.norton.com/en/blogs/norton-protection-blog/public-wi-fi-security-101-what-makes-public-wi-fi-vulnerable-attack-and

DO YOU WANT TO KNOW MORE? TALK TO US.

POC: LTC JOEY T FONTIVEROS (SC) PA – Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-6281057. Email: fontiverosjt@army.mil.ph.