CMSGu2023-08

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on the safe usage of public Wi-Fi

CERT–MU

Mauritius

August 2023

Issue No. 1

Version 1.0

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to guide the public at large in making safe use of public Wi-Fi or hotspots.

1.2 Audience

The target audience for this guideline is the public in general.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document’s content, the targeted audience and the document’s structure.

Section 2 presents a background on public Wi-Fi.

Section 3 provides some potential attacks that can occur on public Wi-Fi.

Section 4 describes some signs you may be connected to an unsafe Wi-Fi network.

Section 5 explains how you can use public Wi-Fi with less risks.

Section 6 concludes the document.

2.0 Background

Public Wi-Fi networks are ubiquitous, providing internet access in various public places such as cafes, airports, and libraries. This service has become an essential part of modern life, allowing users to stay connected while away from their homes or offices. A public Wi-Fi network is inherently less secure than a personal, private one, because we do not know who set it up, or who else is connecting to it. The issue with public Wi-Fi is that there is a tremendous number of risks that come along with these networks. While business owners may believe they are providing a valuable service to their customers, chances are the security on public Wi-Fi is non-existent.

3.0 Types of attack on public Wi-Fi

3.1 Man-in-the-middle attacks

This is a form of eavesdropping. When a computer makes a connection to the internet, data is sent from point A (device) to point B (service/website), and vulnerabilities can allow an attacker to get in between these transmissions and “read” them. So what you thought was private no longer is. Scammers may also carry out a MITM attack using phishing emails. In these emails, they'll impersonate a trusted source to trick you into sharing your private information.

3.2 Unencrypted networks

When using an encrypted network, the information sent between your device and the Wi-Fi router is in a “secret code.” Because of this, nobody can see the information without a key. Most Wi-Fi routers have encryption turned off by default and must be turned on when setting up the network. If you connect to an unencrypted network, it is much easier for a scammer to get a hold of your web traffic and use it for nefarious activities like MITM attacks. While the public Wi-Fi network you want to use may be encrypted, there is no sure way to tell if this has happened.

3.3 Malware distribution

Software vulnerabilities are one of the ways that attackers can embed malware onto your computer without you even knowing. A software vulnerability is a security hole or weakness found in an operating system or software program. Hackers can exploit this weakness by writing code to target a specific vulnerability, and then inject the malware onto your device.

3.4 Wi-Fi snooping and sniffing

Cybercriminals can buy special software kits and even devices to help assist them with eavesdropping on Wi-Fi signals. This technique can allow the attackers to access everything that you are doing online, from viewing whole webpages you have visited (including any information you may have filled out while visiting that webpage) to being able to capture your login credentials, and even hijack your online session.

3.5 Malicious hotspots

These trick victims into connecting to what they think are legitimate networks because the names sound reputable. Assuming you are staying at a hotel named “Goodnyght Inn” and wish to connect to the hotel’s Wi-Fi. While trying to connect, you see a list of available networks, including “GoodNyte Inn”. You may think you are selecting the correct one when clicking on “GoodNyte Inn,” but it might not be a genuine network. (Note the capital N.) Instead, you could have just connected to a rogue hotspot set up by cybercriminals who can now view your personal information.

4.0 Signs you may be connected to an unsafe Wi-Fi network

- **“HTTPS” sites render as “HTTP”**

  If you are trying to connect to a secure website and notice that the page is loading as an “HTTP” site instead, you may be connected to a rogue Wi-Fi hotspot. This could mean that someone is trying to steal your information using a MITM

- **The network name matches a trusted network**

  In some cases, a hacker may set up a fraudulent Wi-Fi network to impersonate an existing network. An example of this is seeing duplicate network names or being connected to your “home network” even if you’re away from home.

- **The name is generic**

  Certain rogue networks may show up in a highly populated area with vague names such as “Free Wi-Fi,” hoping to lure in users. In most cases, legitimate public Wi-Fi networks such as ones at coffee shops will have a more specific name that is displayed in their place of business.

5.0 How to safely use public Wi-Fi?

- **Avoid Public File Sharing**

  Make sure you turn off file sharing before accessing public Wi-Fi. If you keep file sharing on, your folders may be accessible to anyone connected to the same public network, allowing a hacker to get their hands on your private information without your permission.

- **Avoid accessing sensitive information**

  Avoid conducting sensitive transactions, such as online banking or shopping, on public Wi-Fi networks. If you must do so, use a trusted cellular network or a VPN to add an extra layer of security.

- **Use a Virtual Private Network (VPN)**

  A VPN encrypts your internet connection, making it harder for hackers to intercept your data. It creates a secure tunnel between your device and the internet. There are many reputable VPN services available that offer both free and paid plans.

- **Stick to "HTTPS" websites**

  Only browse websites that include an **SSL certificate** while on public Wi-Fi. A website has an SSL certificate when the URL begins with "HTTPS." Website addresses that start with "HTTPS" are encrypted, adding an extra layer of security and making your browsing more secure. If you connect to unsecured Wi-Fi networks and use "HTTP" instead of "HTTPS" addresses, your traffic could be visible to anyone else on the network.

- **Use two-factor authentication**

  When you are using public Wi-Fi, cyber snoops could gain access to your passwords. One way to enhance your protection is by enabling two-factor authentication on any services that offer it. When enabled, this ensures that even if someone gains access to your password while you are using public Wi-Fi, they still will not be able to access your accounts. Usually, you will receive a second login step, a call or a code on your smartphone, for instance, that you will use to log in to your account.

- **Remember to log out**

  When you are done browsing, be sure to log out of any services you were using. Also, check your settings to make sure your device will “forget the network” and not automatically reconnect to that network again if you are within range without your permission. This can help minimize the time your device is connected to a public network.

- **Use antivirus software**

  Using antivirus software is another great way to stay safe while using public Wi-Fi. With antivirus software installed, you can use public Wi-Fi networks knowing you are protected against cybersecurity threats such as computer viruses and spyware.

- **Keep your firewall enabled**

  If you are using a laptop, keep your firewall enabled while on public Wi-Fi. A firewall acts as a barrier that protects your device from malware threats. Users may disable the Windows firewall because of pop ups and notifications and then forget about it. If you want to restart it on a PC, then go to the Control Panel, “System and Security” and select “Windows Firewall”. If you are a Mac user, go to “System Preferences”, then “Security & Privacy”, then “Firewall” tab to enable the feature.

- **Adjust your connection settings**

  Configure the wireless settings on your devices to not automatically connect to available public hotspots. You can do this by turning off the “Connect Automatically” feature on your devices so they do not auto-connect and search for known Wi-Fi networks. Doing this can prevent your computer or device from broadcasting that it is trying to connect to your “home Wi-Fi” network and allow an attacker to create a bogus network with the same name.

6.0 Conclusion

Public Wi-Fi hotspots can be a convenient way to access the internet when you are out, have poor reception, or are travelling overseas. Similar to other technologies online, there are risks involved when using them They can be accessed by anyone, and are often free and unsecured. These hotspots can be an attractive target for cybercriminals, who may try to use them to steal your passwords or sensitive information. As such, it is important to be aware of the risks, and to develop secure habits when making use of these hotspots.

7.0 References

- https://us.norton.com
- https://cybersecurity.wa.gov
- https://www.aura.com
- https://www.cyber.gov.au