MARCH 2017

Public Wi-Fi Hygiene

THINGS TO CONSIDER

IAN LOE

Table of Content

Ian Loe

DN: email=ian@ianloe.net
Date: 2017.03.09 21:51:57 +08'00'

Introduction

As we are becoming a more connected society, the need for internet access on the go is becoming more important. Many people would look for a public Wi-Fi access when they are out and about. In May 2016, Symantec (a leading cybersecurity firm) conducted an online survey of 1025 people to find out what users are doing on public Wi-Fi.

> From the report, 57% of consumers think their information is safe when using public Wi-Fi connections. And only 49% think that they are responsible for securing their own information. 18% believe that the Wi-Fi provider is responsible for protecting their data and another 18% believe it is the website operators who are responsible.
>
> Common activities on public Wi-Fi include logging into a personal email account (55%), logging into social media (54%) sharing photos and videos (38%) and 20% have used it to access their banks or perform some financial transactions.

[1]

But behind some of these "free" Wi-Fi access lurks some malicious intent. This paper will cover some of the basic hygiene you should adopt when using public Wi-Fi connections.

Background

Many people are using free Wi-Fi access without a second thought about the security of the connection. Most would trade privacy or security for convenience and are not fully aware of the consequence. The biggest threat would be that your data, traffic and identity could be stolen and majority of users are not doing enough to protect themselves.

Problem Statement

With the lax protection in most public Wi-Fi, many users are putting their data and devices at risk. Encryption is usually employed to keep network traffic private and prevent snooping. For example, the Wi-Fi network at home is usually set up with some encryption like WPA2, so that even if your neighbour at home is within range of your Wi-Fi network, they cannot see the web pages you are viewing. This wireless traffic is encrypted between your device and your wireless router or access point.

When you connect to an open Wi-Fi network like one at a shopping centre, restaurant or airport, the network is usually unencrypted. This is usually indicated by the lack of a padlock symbol (next to the network name on your device or you do not have to enter any password when connecting to the network. Your unencrypted network traffic is then clearly visible to everyone in range. Even with a secure banking application with the data encrypted, they may be able to know which bank you use.

[1] Norton Wi-Fi Risk Report – Global : https://www.slideshare.net/NortonSecurity/norton-wifi-risk-report-global

There are also many rogue access points that are mimicking a legitimate Wi-Fi connection to fool you into connecting to them. The biggest threat with this is the ability for the hacker to position himself between you and the connection point. So instead of connecting directly to the Wi-Fi hotspot, information will be sent to the hacker, who then relays it on.

Hackers can also use an unsecured Wi-Fi connection to distribute malware. If you allow file-sharing across a network, the hacker can easily plant infected software on your computer. Some ingenious hackers have even managed to hack the connection point itself, causing a pop-up window to appear during the connection process offering an upgrade to a piece of popular software. Clicking the window installs the malware.[2]

Recommendations

I would highlight some areas to be aware of to improve your security while looking for and connecting to public Wi-Fi hotspots.

Be careful of fake (rogue) Wi-Fi hotspots

There are many hackers out there that use a fake (honeypot) Wi-Fi hotspot to collect information about the user. These rogue Wi-Fi hotspots often use the same SSID as legitimate hotspots (e.g. Wireless@SG, etc.) or use a name associated with the location (e.g. yourlocalcoffeeshopfreewifi, etc.)

These rogue Wi-Fi hotspots often attempt to capture your credentials with a spoofed login screen (as shown in figure 1 below) and often would just collect the information and pass the traffic straight to the internet so users may not realize the webpage was a fake. This is especially hard to detect in a foreign hotel.

Figure 1: Fake Hotel Login Screen

[2] http://usa.kaspersky.com/internet-security-center/internet-safety/public-wifi-risks#.WL--Thid5Bw

The other use of these rogue Wi-Fi hotspots is to infect your device with a malicious malware in the form of an update program or a fake "Terms of Service" link that will download and execute a malware.

At minimum, make sure your device is protected by the latest anti-virus or other end point protection software.

Be careful of Wi-Fi hotspots that ask for your phone number

There are some Wi-Fi hotspots around the world that ask for your phone number and then send you an SMS with the access code. These kind of hotspots can be used to conduct targeted attacks on the user.

Here is a possible scenario that might be played:

1. User connects to a rogue hotspot and enters the phone number.
2. User continues to use the connection to perform a few actions (check email, check bank balance, etc.)
3. Although the mail or banking app is secure, the hacker can still see who you are connecting to, therefore will know which email service you use or which bank you use.
4. Hack sends a spoof SMS (e.g. shown in Figure 2) which can carry a malicious link that might inject a malware or send you to a fake website.

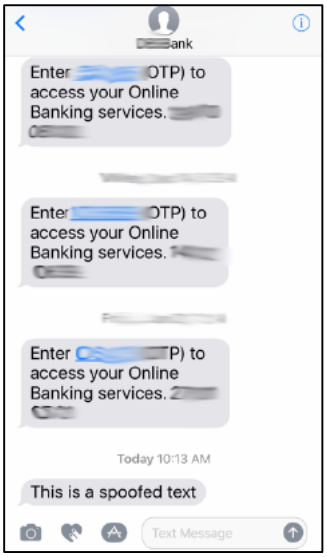

Figure 2: Fake SMS

Choose an encrypted hotspot over an open hotspot

This is true especially at airports, some airline lounges offer encrypted Wi-Fi hotspots (those that need a password to join the network). These networks are preferred over the typically free airport wide hotspots. But do pay attention that it is not a rogue Wi-Fi hotspot.

Use of VPN

Virtual Private Networks (VPN) is a private tunnel that encrypts the traffic between end-points. The use of a VPN service will help secure your traffic from eavesdropping but do note that the VPN used should be of a reputable source. I recommend you do some research on the VPN vendor before signing up for any service. An alternative is to host your own VPN service, which is an extension from my previous paper "Protection of Home Networks"[3].

[3] "Protection of Home Networks: A Suggested Approach" I. Loe, 2007 – https://ianloe.com/resources/Protection-of-home-networks-Ian-Loe.pdf

However, do note that even with the use of a VPN to encrypt the traffic, there is still a vulnerability – this occurs at point of connection. The VPN cannot connect until you are connected to the Internet, and the VPN connection is not instantaneous. Sometimes before you can connect to the Internet, the Wi-Fi Hotspot will direct you to a captive portal to manually accept some "Terms of Service" agreement.

During this period before your VPN connection is established, your device might be trying to connect to some services. For example, you could have an email client or chat service that tries to connect automatically, and this traffic is out in the clear for all to see, including potentially the login credentials.

Even if your software attempts to use HTTPS, it could be vulnerable to attacks like SSLStrip[4], which tricks the software into using open HTTP anyway. This vulnerability window might be very small, but that is enough to expose valuable information like login credentials.

Configure software firewall

If you are using a public Wi-Fi from your computer, there are a few more protection actions you could employ.

The idea is to block all inbound and outbound connections on your public networks (or zones) with the exception of a browser that you use to connect to captive portals. That browser should be one you only use for this purpose.

You should also set up a profile/zone for VPN traffic where inbound / outbound traffic is less restricted (you should always block all outbound connections by default and then allow connections as needed) This approach will ensure your email and other programs do not send unnecessary data out before the VPN is connected.

Conclusion

Although there might be a need to get connected on the go, it pays to be vigilant on who you are connecting to, how you are connected and what you are doing online over that connection.

Paying attention to basic security hygiene can save you from a lot of trouble later.

Remember: Only the paranoid survive ☺

[4] Video demo on how to strip SSL: http://www.irongeek.com/i.php?page=videos/sslstrip