



TOP COMPLIANCE (Pty) Ltd

Your Business' Safety Is Our Concern

QSE B-BBEE - Level Four

www.topcompliance.co.za

June 2019

Why you should never connect to a public Wi-Fi

There may come a time when your only option is an unsecured, free, public Wi-Fi hotspot, and your work simply cannot wait. If that's the case, understanding the risks of public Wi-Fi may prevent you from falling victim to an attack.

Security is no longer a one-machine affair. You need a security suite that helps protect all your devices: Windows PC, Mac, Android smartphone or your iPad.

When considering whether to connect to the public Wi-Fi network at coffee shops, malls, restaurants, and hotels. Two simple words of advice: don't and **don't**. The flaw discovered in WPA2, the encryption standard that secures all modern Wi-Fi networks, launched the possibility that anyone near you could easily access your information if you use a Wi-Fi network. This includes information that was understood as being encrypted.

Despite numerous warnings, headlines, and efforts to educate, many people still don't understand why connecting to free Wi-Fi is an incredibly dangerous situation regardless of what you are doing online. While you may think 'okay, I'm not checking my personal email or logging into my bank account, I'm just checking the sports scores,' remember anything you do on a public Wi-Fi network is NOT secure. Any information you share or access on these networks is as good as gone.

If you find yourself in a situation where you absolutely must connect to Wi-Fi (first, ask if you REALLY need to connect) here are a few suggestions to improve your safety:

1. Do not touch any of your personally identifiable information (PII)

If you use information over a public Wi-Fi network, you are not treating it like it is valuable. Therefore, if you must use a public Wi-Fi network, avoid touching any PII including banking information, ID numbers and home addresses at all costs.

2. Use virtual private networks (VPN) instead

A VPN allows you to create a secure connection to another network over the Internet. VPNs can be used to access region-restricted websites, shield your browsing activity from prying eyes on public Wi-Fi and more. They are an excellent alternative to public Wi-Fi networks. While they do cost some money, the peace of mind and additional security is well worth it. While employees are on the go and need to access Wi-Fi networks to do their jobs, the company's data is at a high-risk if they use a public network.

3. Use SSL connections

You can still add a layer of encryption to your connection when browsing the internet, be sure to enable the "Always Use HTTPS" option on websites that you visit frequently, including any and all sites that require you to enter any type of credentials (most websites that require an account or credentials have the "HTTPS" option somewhere in their settings).

4. Invest in an unlimited data plan

Most of the time, individuals find themselves hastily connecting to public Wi-Fi networks to save themselves from overage charges on their cell phone accounts. But your cell phone is just as likely to be attacked as your laptop, if not more. Investing in an unlimited data plan will not only eliminate your need for accessing insecure Wi-Fi networks, it will

also often allow you to use your mobile device to create a personal internet “hotspot,” meaning a VPN connection would not even be necessary.

5. Turn off sharing

When connecting to the internet at the airport, university etc, do you really need to have file sharing turned on? File sharing is usually easy to turn off from the system preferences or control panel, depending on your operating system.

6. Man-in-the-Middle attacks

One of the most common threats on these networks is called a Man-in-the-Middle (MitM) attack. Essentially, a MitM attack is a form of eavesdropping. When a computer makes a connection to the Internet, data is sent from point A (computer) 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.

7. Unencrypted networks

Encryption means that the information that is sent between your computer and the wireless router are in the form of a “secret code,” so that it cannot be read by anyone who doesn’t have the key to decipher the code. Most routers are shipped from the factory with encryption turned off by default, and it must be turned on when the network is set up. If an IT professional sets up the network, then chances are good that encryption has been enabled. However, there is no sure way to tell.

8. Malware distribution

Software vulnerabilities are also ways that attackers can slip 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.

9. Snooping

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 accounts.

10. Malicious hotspots

These “rogue access points” trick victims into connecting to what they think is a legitimate network because the name sounds reputable. For example, you are staying at the Goodnuyt Inn and want to connect to the hotel’s Wi-Fi. You may think you’re selecting the correct one when you click on “GoodNyte Inn,” but you haven’t. Instead, you’ve just connected to a rogue hotspot set up by cybercriminals who can now view your sensitive information.

How to stay safe on public Wi-Fi

Don’t:

- ***Don’t*** allow your Wi-Fi to auto-connect to networks
- ***Don’t*** log into any account via an app that contains sensitive information. Go to the website instead and verify it uses HTTPS before logging in
- ***Don’t*** leave your Wi-Fi or Bluetooth on if you are not using them
- ***Don’t*** access websites that hold your sensitive information, such as such as financial or healthcare accounts

- **Don't** log onto a network that isn't password protected

Do:

- **Do** disable file sharing
- **Do** only visit sites using HTTPS
- **Do** log out of accounts when done using them
- **Do** use a VPN to make sure your public Wi-Fi connections are made private

<https://www.csoonline.com/article/3246984/why-you-should-never-ever-connect-to-public-Wi-Fi.html>
<https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html>

Please go visit our NEW online store for all your first aid, personal protective equipment, signage and legal posters.

<https://www.topcompliance.co.za/index.php/products>



Our contact details:

Training, Audits and Retail:

Pat: 082 442 8521 (07h00 – 16h30)

p.wessels@topcompliance.co.za

Website: www.topcompliance.co.za

Public courses

For all the dates this year

8 & 9 June	Pretoria	Level 1 first aid - FULL
10 June	Pretoria	SHERQ Rep – legal Liability - FULL
8 July	Pretoria	SHERQ Rep – legal Liability
11 & 12 July	Midrand	Level 1 first aid - FULL
15 & 16 July	Pretoria	Level 1 first aid
17 & 19 July	Pretoria	Level 2 & 3 first aid
30 July	Pretoria	Basic firefighting & EAP
5 Aug	Pretoria	SHERQ Rep – legal Liability
19 Aug	Pretoria	Basic firefighting & EAP
22 & 23 Aug	Pretoria	Level 1 first aid

Corporate and Private training courses as below:

First Aid Courses:

First aid: Level 1

First aid: Level 2

First aid: Level 3

First aid: Level 1 & 2

First aid: Level 2 & 3

First aid: Level 1, 2 & 3	
Child and infant CPR & choking	
Adult CPR & choking	
Adult CPR & choking and AED	
Occupational Health and Safety Courses	
OHS Act & SHERQ representative	
The Occupational Health + Safety Act - responsibilities of management	
Food facility health & safety course	
Basic ladder safety	
Fire Fighting and Prevention Courses	
Basic firefighting	
Basic firefighting with emergency action planning	
Basic firefighting with fire extinguisher practical	
SKILLS PROGRAMS	
First Aid Level 1,2 & 3 - HW/SP/1601190 – NEW REQUIREMENT	
US 119567	Perform basic life support and first aid procedures
US 120496	Provide risk-based primary emergency care/first aid in the workplace
US 376480	Provide first aid as an advanced first responder
First Aider - HW/SP/1202005	
US 119567	Perform basic life support and first aid procedures
US 120496	Provide risk-based primary emergency care/first aid in the workplace
US 13915	Demonstrate knowledge and understanding of HIV/AIDS in a workplace, and its effects on a business sub-sector, own organisation and a specific workplace.
First Aid (Basic) - HW/SP/150795	
US 119567	Perform basic life support and first aid procedures
US 9964	Apply health and safety to a work area
Health, Safety and Fire Combination - HW/SP/1510179	
US 9964	Apply health and safety to a work area
US 119567	Perform basic life support and first aid procedures
US 120331	Demonstrate knowledge pertaining to fires in working places
Workplace SHE Rep - HW/SP/1510182	
US 9964	Apply health and safety to a work area
US 259639	Explain basic health and safety principles in and around the workplace
First Aid and Safety Representative - HW/SP/1510183	
US 9964	Apply health and safety to a work area
US 119567	Perform basic life support and first aid procedures
Safety Incident Investigation and inspections - HW/SP/1511233	
US 259617	Conduct investigation into workplace safety, health + environmental incidents
US 259619	Conduct workplace Occupational Health and Safety (OHS) inspections
First Aid and Firefighting - HW/SP/1511239	
US 120496	Provide risk-based primary emergency care/first aid in the workplace
US 13961	Demonstrate knowledge and use of hand operated firefighting equipment
Fire and Rescue Skills Programme - HW/SP/1604338	
US 252250	Apply firefighting techniques
US 119567	Perform basic life support and first aid procedures
Emergency First Aider - HW/SP/1605377	
US 119567	Perform basic life support and first aid procedures

US 120496	Provide risk-based primary emergency care/first aid in the workplace
Safety Management - HW/SP/1601159	
US 9964	Apply health and safety to a work area
US 259639	Explain basic health and safety principles in and around the workplace
If you no longer wish to receive these emails, please reply to this message with “Unsubscribe” in the subject line or simply click unsubscribe. <u>Please send from the email address you wish to unsubscribe.</u>	