WIFI SAFETY AND PRIVACY: TIPS FOR FRONTLINE SERVICES AND SURVIVORS

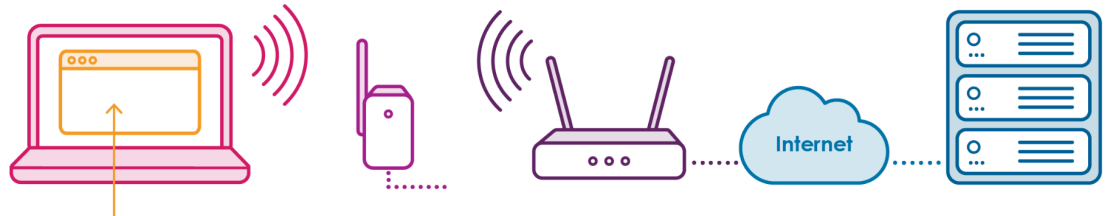
techsafety.org.au

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of January 2025.

WiFi access has become so commonplace that you can connect to many public places with networks and hotspots. But just because a network is available doesn't mean it is secure. The information below will provide you and the survivors you serve with the tools to stay safe using any WiFi network.

How WiFi Works

The following is a basic overview of the various steps involved in WiFi communication:



Browser
Your browser is software that allows you to view and send information over the internet.

Device
Your device uses its Wi-Fi connection to transmit information to and from the browser.

Eavesdropper
The data you transmit is sent over the air. It can be intercepted by anyone within range who knows the Wi-Fi password.

Wireless Router
The router receives the Wi-Fi communication from your device and sends information to and from the internet.

Internet
The internet is an interconnected system of computer networks that link devices to each other.

Destination
The information reaches the server(s) that host the website you're visiting, and those servers send back the information you requested.

WiFi Hotspots Under Your Control: A WiFi Hotspot that you have control over has the potential to be just as secure as a wired connection. In order to achieve this level of security, take the following steps:

1. Use a Strong, Private Password

Choose a WiFi password that is long. The best passwords are at least 12-15 characters long, and contain randomly placed letters, numbers, and symbols. Read more about Password Safety. Do not freely distribute this password or write it in any visible location (including on or near the WiFi Hotspot itself).

2. Adjust Security Settings

The proper configurations will make sure your WiFi Hotspot only supports the most up-to-date protocols for transmitting information:

- The only security algorithm that should be enabled is WPA2. Disable WEP and WPA.
- The only encryption method that should be enabled is AES. Disable anything related to TKIP.
- Completely disable WPS. This feature is enabled by default on most Hotspots. It allows for an alternate method of connecting without the password. It has a significant security flaw that can be easily exploited.

3. Set Up a Guest Network *(optional)*

Set up an alternate network if you have guests that need to access your internet connection. The password to this network doesn't need to be as complex or private. The name for the network should not be identifying, for your privacy and for your guests.

The steps for accessing and configuring a WiFi Hotspot are different for each device. You may need the assistance of someone with experience in making these changes.

Open/Public WiFi Hotspots

If you have serious privacy concerns or risks, it's critical to understand how to access public/open WiFi safely and when to avoid it. Any WiFi Hotspot where there is either no password or the password is publicly available should be considered an open network. Even if the network is password protected, a skilled eavesdropper will still be able to view your communications if they also have access to the password (a common example of this is in a hotel where all guests have the same password and it is not changed often). There are two ways in which browsing the internet can be safe while using a public WiFi Hotspot:

1. Use HTTPS

HTTPS adds a practically impenetrable layer of encryption between your browser and the website you're communicating with. Sites using an HTTPS connection ***can*** be trusted even while using an open/public WiFi Network. However, you must always double check that "https" is in the beginning of the web address and verify the domain name is exactly the site you are meaning to communicate with. Saving important web pages as bookmarks and always accessing these pages via those bookmarks is a great way

to assure that you are never tricked into thinking you're visiting a site that you're not. Never bypass warnings your browser displays about problems with the security certificate from an HTTPS website.

It's also important to remember that while the ***content*** of your communications with HTTPS may be private, the ***destination*** is not. Imagine you've mailed a letter to a friend using a language that only the two of you understand, but the envelope is addressed in a language everyone understands. Anyone who intercepts that letter *won't* be able to read the message inside, but they *will* be able to see who you're communicating with by reading the envelope. The same concept applies to web communications.

Activities that are generally safe when using HTTPS:

The web address/destination is typically not a secret; however, HTTPS can be trusted to protect the content. For example:

- Online banking or shopping
- Web-based email (Gmail, Yahoo! Mail, etc.)
- Social media (Facebook, Instagram, etc.)
- Any other web service that requires a username and password to view information

Activities that are NOT private with HTTPS:

The information in the web address/destination gives away what information is being viewed:

- Search engines (Google Search, Bing, etc.)
- Online mapping (Google Maps, Mapquest, etc.)
- Any website that you wouldn't want an eavesdropper to know you've visited

The line between web page "content" and "destination" can be a blurry one. When in doubt, always assume your information is not private. Wait until you're using an internet connection you have full control over before proceeding.

2. Use a Virtual Private Network (VPN)

An easy way to avoid most every privacy risk related to using WiFi is to subscribe to a virtual private network (VPN). A VPN will encrypt 100% of the internet traffic sent from your computer and deliver it to an alternate server elsewhere. Once the information has reached that alternate server, it is decrypted and sent to its final destination. The

VPN makes it look as if the requests you sent were coming from that alternate server and keeps your IP address and location anonymous.

A VPN provides the following benefits:

- Encrypts all web traffic (HTTP and HTTPS) as it passes over WiFi
- Disguises both the web content ***and*** destination as it passes over WiFi
- Masks your originating IP address from the website you're visiting. This prevents the website from tracing your IP address back to your general geographic area.
- More information about VPN's is available from the Electronic Frontier Foundation's Surveillance Self-Defense tool, and a guide to VPN's is available from reputable reviewers such as Tom's Guide.

Other Safety Tips

1. Keep Software Updated

It's extremely important to promptly install all updates to your operating system, browser, anti-virus program, and anything else on your computer, tablet, or device related to the internet or security. Without these updates, your computer is vulnerable. New threats are constantly being found, and these updates help protect against them but only when they are current. It can be helpful to think about updates like repairs to a leaky roof - if you don't mend them as soon as possible, things could get dire quickly, and your roof could cave in.

2. Use Anti-Virus/Anti-Spyware Software

While not perfect, antivirus/anti-spyware software is still an important tool for stopping malicious content before it can even reach your browser.

Most computers come pre-loaded with anti-malware and anti-spyware applications. These applications will typically only be free for an introductory period and should not be relied upon after the trial period has expired. You can also download a variety of free antivirus programs.

Anti-malware apps are available for cell phones, but they do not provide as significant a benefit as their computer counterparts.

Thoroughly vet any anti-virus program before installation. Malware can commonly be disguised as an antivirus program or computer scanning tool to trick you into installing it.

3. Use Privacy Screens

A low-tech way to prevent someone from looking over your shoulder to view the information on your devices is to use a privacy screen. Privacy screens are shaded filters you put on top of your laptop or tablet screen to prevent someone from looking over to see what you're doing.

4. Manage WiFi Network History

Most mobile devices and computers store a list of WiFi networks you've signed on to. Review the list and remove any that feel unsafe to keep. You may not want to delete the whole list because that might be a heads-up to someone physically monitoring your devices. Also, it could be inconvenient to wipe the entire list because it probably includes the WiFi you most frequently connect to (including passwords).

What DFV Practitioners/Frontline Workers and Survivors Can Do

For victims of domestic violence, stalking, and sexual assault, and their DFV Practitioners, there are a few more options for increasing security:

1. Safety Plan

For some survivors of abuse, securely and safely accessing the internet is important. It's important to have a safety plan around technology's safe use and update those safety plans regularly. Share this WiFi safety information with survivors so they can make informed decisions regarding their internet usage.

2. Know Your Devices

Most devices have settings that help increase security. Both advocates and survivors should know how to change, modify, and turn off the settings on their devices. For more information about various device settings and features, visit techsafety.org.au.

3. Trust Your Instincts

Always trust your instincts. If you think a particular network, website, or service isn't reputable, be cautious about using it. If you must use it, don't share sensitive information while doing so.

The Bottom Line

Survivors have a right to access information freely without fear for their safety. The internet is a wonderful tool, and safe access is important for survivors to feel empowered and independent. However, survivors and DFV practitioners should be aware of the risks and know how to manage those risks. With these tips and strategies,

survivors and support workers can reduce the vulnerability of their devices and personal information being compromised over any WiFi network.

Special thanks to Steven Jenkins of EmpowerDB for providing content expertise on this handout.

Acknowledgement

This handout has been created by Wesnet under licence from the National Network to End Domestic Violence.