SURVIVOR'S GUIDE TO SMART HOME TECH: INTERNET OF THINGS

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 March 2024.

Many devices such as doorbells, thermostats, televisions, and speakers are now connected to the internet. This can provide access to entertainment or information without using a phone or computer, and it can allow devices in the home to be controlled remotely. These devices are often called "smart" as in smart speakers or smart TV. They are also known as IoT devices, or Internet of Things.

While internet-connected devices can be convenient, and increase access for people with disabilities, they can be misused by abusive individuals. Some of these devices can be used to monitor what's happening remotely, or to control the functions of the home like heat, alarm, locks, and lights.

This resource is written for survivors who want to understand how IoT technology might be used against them, and to explore options for increasing privacy and safety.

Safety first. Before taking the below steps, think about your safety. Some people may escalate their abusive behaviour when devices or accounts are secured, or monitoring is cut off. You can talk with a DFV practitioner about safety planning.

Trust your instincts. If it seems like someone knows too much about you, they might be monitoring your devices, accessing your online accounts, tracking your location, or gathering information about you online. If you suspect someone is monitoring you, consider using another phone or device to which they have never had access, such as a friend's phone, or a computer at a library, school, or work. Read more about phone safety and privacy.

Get more information. Navigating violence, abuse, and stalking can be difficult and dangerous. A DFV practitioner can help you figure out options and local resources and help you create a plan for your safety. You can contact 1800 RESPECT to be connected with local resources.

Mapping Smart Home Devices in Your Home

The first step is to try to create a list of all the connected devices in your home. This can be helpful if you are trying to increase your privacy or figure out if an abusive person may have access to a device. If they have commented about something you've done or said when they weren't there, for example. Or, something unexplained could be happening in your home such as the heating going up or down when you haven't changed the thermostat,

lights turning on or off, the volume on the TV changing, or alarms going off. Note that your phone could also provide the other person with a lot of access and information, and may be a simpler explanation for what's happening. Read more about phone safety and privacy.

***Important*:** Before taking any action to change someone else's access or remove the devices, you'll want to consider if it feels safe to do so, and whether you want to document what's been happening. You can get help by talking with a DFV practitioner.

Some things like TVs, doorbells, and thermostats may be easier to identify. If you or someone else can change settings or operate a device through an app, it is almost certainly internet connected. Things like refrigerators, smoke alarms, or electrical sockets may be less obvious. If you're in doubt, you can try to look up the device online, using the brand and model name or number to see if it is marketed as "smart" or connected. Remember that if you're worried the other person is monitoring your phone or computer, you may want to use a device they don't have access to. Other connected devices like cameras might be hidden, and could require more work or help from an expert to find.

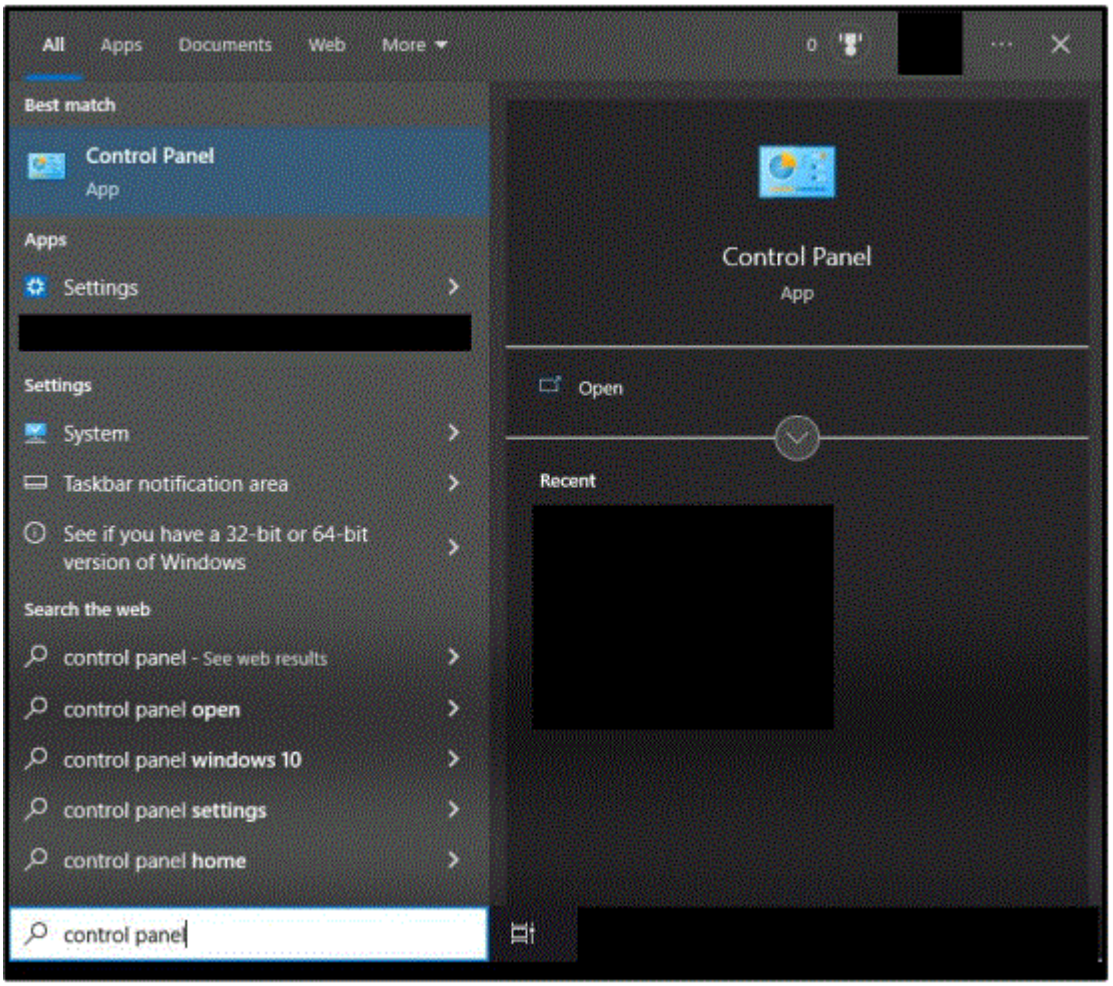
Creating a Device List Using Your Router

If you have the login information for your home wireless router – the device that provides your home WiFi access – another option for creating the list of devices is to log into your router account to view its list of connected devices.

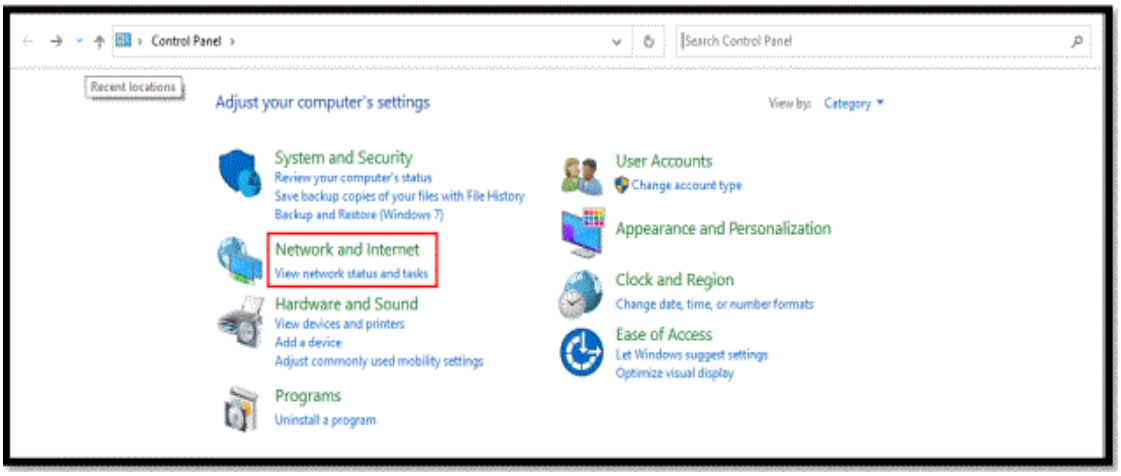
Before you can log into your router, you will need to know its IP address. In many cases, this is 192.168.1.1. If you are using a Mac, Android phone, or iPhone, you can follow the instructions listed here (your phone will need to be connected to your wireless network in order for this to work). If you are using a PC, you can find it on a PC by following the instructions below. If you already know your router's IP address, or know how to find it on your own, you can skip ahead to the paragraph that begins with "In order to do the next step, you will need the login information for your Internet Service Provider (ISP)."

[Note: view the pdf for images of each step below.]

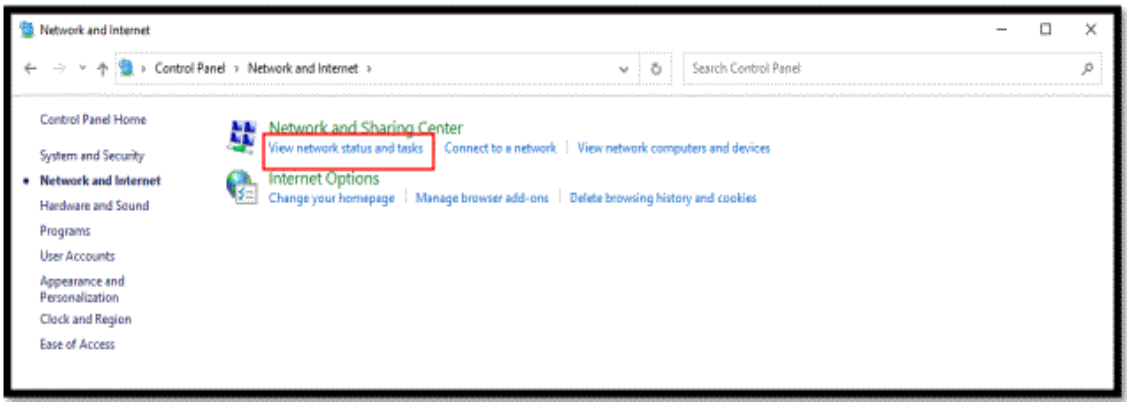
1. At the bottom left or centre of your taskbar type in "Control Panel" in the Start Menu.



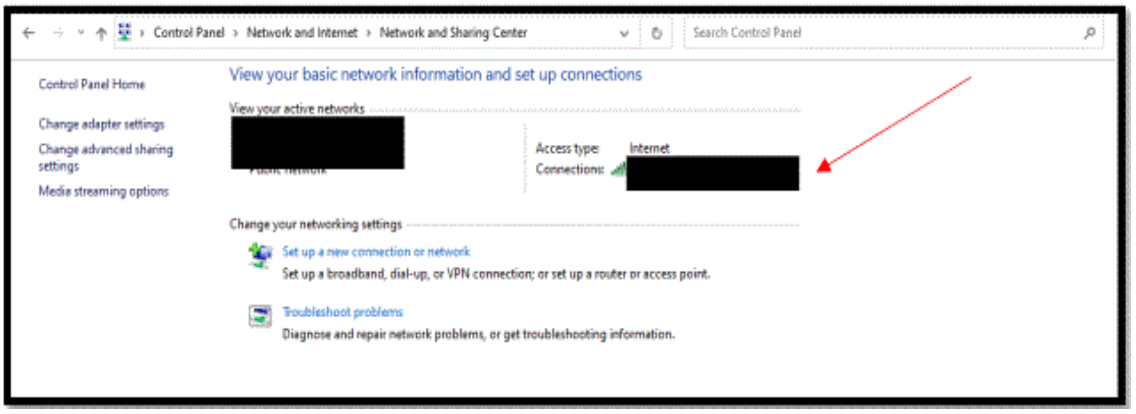
2. Click on Network and Internet.



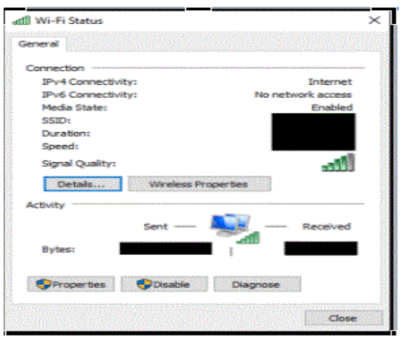
3. Click on "View Network Status and Tasks."

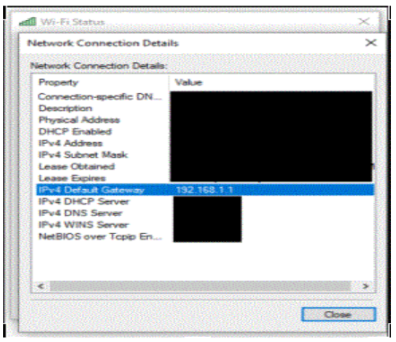


4. Select your WiFi Connection (indicated by the red arrow below).



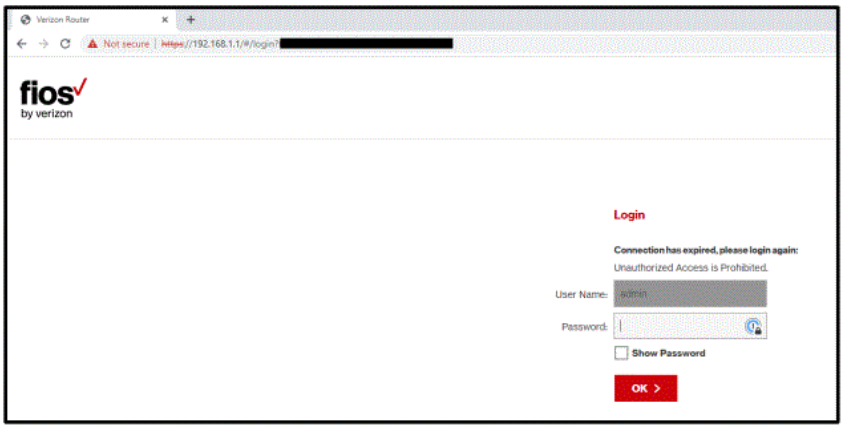
5. Once you have selected your WiFi connection, you will see a display labelled "Wi-Fi Status" (below left). Click on the "Details" button, and you will see a display labelled "Network Connection Details" (below right), which has a "Property" list and a "Value" list. Your router's IP address is the value for the IPv4 Default Gateway property. Once you have done this, you can move on to the next steps – logging into your router.



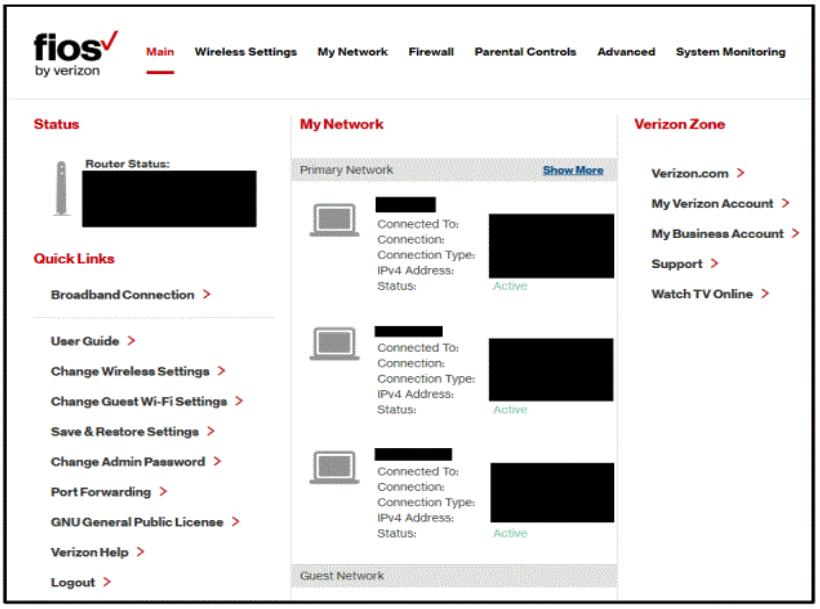


In order to do the next step, you will need the login information for your Internet Service Provider (ISP). Once you have secured this login information:

1. Go to your router's IP address in your browser, by typing the router IP address into the address bar, and log in.



This will provide you with a list of devices connected to your WiFi network, as shown in the image below this step in the pdf, under "My Network."



2. Click on a device to see more details about it. In the image above, we have hidden details about the device for privacy reasons, but you will be able to see them. The MAC address allows you to look up the manufacturer of the device, and the device name may also give you clues as to what it is, which will help in creating your list.

Using Your List of Devices

Once you have printed out or exported a list of devices, add notes about who bought or set up each device. If an abusive person added these things to your home, even if they don't live there now, they may have set up the accounts so they can monitor or control the devices remotely. Even if you purchased the devices, but the other person helped you set them up or ever shared access, they might still be able to do so.

For each device, look for information on how you can operate or change the settings. Is there a display panel that you can change options through, or do you need an app or web address to make changes? If you aren't able to find out how to make changes, you can try searching the internet with the brand and model. For now, just make note of these settings. Below we'll talk about other considerations prior to making changes.

Finally, you will want to add information about what the other person might be able to do or find out about you or your activities through the device. Does it capture video or audio? Does it create a log of activities? Can they override or change programmed settings remotely? Again, you may need to use the internet to search for information about the device.

If there are devices listed as connected to your router that you cannot identify, you can try searching online for the device. However, depending on the device this may or may be useful. You can also look up the MAC address, which will provide information about the manufacturer which could in turn provide clues as to what the device is. If you feel safe doing so, you could disconnect it. If it turns out to be a device you wanted, you can reconnect it.

Strategies to Increase Privacy and Safety

Now that you've started a list of connected devices, you have choices about what steps to take next. If you want to document what is happening, either for your own records or to share with someone else, you'll want to do that before taking any action to change settings, disconnect access, or remove devices. Depending on the device, you can take pictures of the device as you found it, take screenshots of apps or information you research about the devices online, or make notes about what you've found. It can also be helpful to make notes about anything the other person did using the device, or anything strange you noticed happening in the home, including date and time. Read more about how to document abuse.

You may want to take steps to stop the other person from having access to the devices, to change other settings, or to remove the devices completely. In some cases, abusive people will escalate their abuse when access is cut off or changes are made. You can talk with a DFV practitioner about making a safety plan. You may also choose to leave the settings or devices in place for a time in order to gather evidence or because it feels safer.

How to remove access or change settings will vary based on the device. If there is a display, you may be able to use that to make changes. Otherwise, you may need to use an

app or website. In some cases, you may need to contact the company that made the device to change the account itself.

First, find out who has access to the device, app, or account. If the abusive person still has access, any changes you make could be undone, or the person may escalate their abuse. If you feel like it's safe to do so, remove access by signing out other devices or removing users.

Next, change passwords and add security options like multi-factor authentication. Read more about passwords and multi-factor authentication.

Finally, make changes to the settings of the device, if you wish.

If you are not able to regain control of the device, and it feels unsafe to have the device operating in your home, you may consider disconnecting the power or removing the device altogether. Alternatively, if you don't recognize a device, you can disconnect it from the WiFi network by logging into your router as described in the previous section, disconnecting it through the dashboard that appears when you log in, and changing the WiFi network password afterward so that the device can only be reconnected by someone who knows the new password. Note that if you do this, an abusive person may realise what you have done – trust your instincts on what is safe.

Smart Devices, IP Addresses and your Location

If you use a device, such as a phone, for creating or logging into accounts, it is possible that the device's IP address could become public through a data breach (when someone steals and sells or publishes data from a company), and a stalker or abuser could use this information to narrow down where you live. An IP address can typically be used to trace the device to a metro area or similarly-sized rural area. In addition, if someone has access to one of your major cloud accounts like your Google or iCloud account, they may be able to see the IP addresses of all devices that have logged into that account. If you are concerned about someone locating you this way, you may want to conceal your devices' IP addresses through a VPN service, which sends your Internet activity through one of the service's computers and makes it so that to the public (outside of your home network), your IP address will appear to be that computer's address. This way, the IP address associated with your accounts will not be your own, and if there is a data breach, your real IP address will not be stolen and published.

You can protect individual devices' public IP addresses through a VPN service such as Proton VPN, NordVPN, or Private Internet Access. The paid versions of these services allow you to protect several devices at a time, and if you cannot afford to pay for a VPN service on your own, you may be able to pool money with friends (for instance, if you and two trusted friends pool money for a VPN service that allows you to protect up to six devices with the same account, you can each protect two devices). If you want to protect many devices' public IP addresses, you can add a VPN service to many types of routers, which will then protect the public IP address of every device connected to your network. Many

VPN services support this, but it can require some technical skill to set up. As of this writing, Express VPN router protection is known for being relatively user-friendly.

Summary

Controlling our privacy can be challenging with so much of our life being digital and connected. Unfortunately, abusers frequently misuse connected devices as a tactic to harass, control, or monitor. If you are experiencing this type of abuse and need more assistance, please reach out to a hotline or a local domestic violence program. If any of this content is hard to understand, you can talk it through with a DFV Practitioner and they can contact a Technology Safety Specialist at Wesnet for assistance.

Acknowledgement

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