

Cybersecurity Questions to Ask Your IT Provider



NRCC

CybercrimesResource.org



**National Network to
End Domestic Violence
SAFETY NET PROJECT**

TechSafety.org

This project is supported by Grant No. 15JOVW-24-GK-02960-MUMU awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the Department of Justice.

September 2026.

When it comes to discussing cybersecurity with vendors who provide information technology (IT) services, program managers, directors, and other decision-makers may not know where to begin. Here we recommend a number of questions relevant to victim service providers, with explanations of why these questions are relevant. Some questions are listed multiple times, as they fall within multiple categories.

The purpose of this guide is not to overwhelm you or make you an IT expert. It is to provide you with vocabulary, ideas for what to check, and an understanding of why you would want to do those checks. You do not need to read the whole guide at once – it is structured so that you can look up topics as needed. The table of contents can help you find what you are looking for or give you ideas about what to look for.

Note: If your program is housed within a multi-service agency, or co-located with other agencies (for example, a Family Justice Center), some of your technological infrastructure may be shared. Your agency may not be able to make some decisions about IT policies. In this case, it is important to understand what the policies are, and to advocate for the needs and requirements of victim service providers.

When to use this guide

Scroll down for a full table of contents. Consider using this guide and its sections at the following times:

- Onboarding: [Databases, Encryption, and Cloud](#), [Email](#), and [Wireless](#)
- Offboarding: [Access Management](#)
- Engaging new collaborators outside of the organization: [Collaboration Tools](#)
- Getting new technology or assessing a vendor: Entire guide
- Looking at emergency management planning: [Incident Response and Disaster Recovery](#)
- Annual review: Leadership should review the **entire** guide annually

Table of Contents:

1. Databases, Encryption, and Cloud	4
<i>Can the tech company that provides our database access survivor data (information about a survivor that can identify them)?</i>	<i>4</i>
<i>Does the database use zero-knowledge encryption?</i>	<i>4</i>
<i>What cloud-based services do we use? Why did we choose them?</i>	<i>4</i>
<i>Can the tech company that provides our file storage and collaboration tools (such as Dropbox or Google Drive) access the contents of our documents?</i>	<i>5</i>
<i>Do we back up our systems? Where? How are the backups protected?</i>	<i>6</i>
<i>Do we use Simple Mail Transfer Protocol Secure (SMTPS) and other secured email protocols? If not, have we considered it?</i>	<i>6</i>
<i>What security protocol do our wireless networks use?</i>	<i>7</i>
<i>Do we have any guidance available for staff and volunteers on wireless network security when working remotely?</i>	<i>8</i>
2. Collaboration Tools	10
<i>How do we manage our Zoom (or other remote conferencing tool such as Microsoft Teams or Webex) data?</i>	<i>10</i>
<i>Can the tech company that provides our file storage and collaboration tools (such as Dropbox or Google Drive) access the contents of our documents?</i>	<i>10</i>
3. Access Management	11
<i>How do we ensure that only people who need information or resources have access to them?</i>	<i>11</i>
<i>Do we use a Zero Trust methodology?</i>	<i>12</i>
<i>What resources and data can our consultants access?</i>	<i>12</i>
<i>What are our IT policies and procedures when someone leaves the organization?</i>	<i>12</i>
4. Incident Response and Disaster Recovery	13
<i>What is our incident response and disaster recovery plan? How often is it updated?</i>	<i>13</i>

<i>Do we back up our systems? Where? How are the backups protected?</i>	
<i>How long do we keep them?</i>	13
<i>Do we have cybersecurity plans in place in case of physical security incidents in shelter/transitional housing?.....</i>	14
5. Data Lifecycle and Asset Management	14
<i>How do we dispose of data once we no longer need it?</i>	14
<i>How do we manage our Zoom (or other remote conferencing tool such as Microsoft Teams or Webex) data?.....</i>	15
<i>What kind of data does our website collect from people who use it?....</i>	15
<i>Do we have an assets inventory?</i>	16
6. Housing.....	17
<i>Do we have cybersecurity plans in place in case of emergencies in shelter/transitional housing?</i>	17
<i>What security protocol do our housing wireless networks use?.....</i>	17
7. Data Breach Prevention.....	17
<i>Do we have a process for automatically installing updates on work devices?</i>	18
<i>Do we use a Zero Trust methodology?.....</i>	18
<i>Email</i>	19
• <i>Do we use Simple Mail Transfer Protocol Secure (SMTPS) and other secured email protocols? If not, have we considered it?.....</i>	19
• <i>Do we have regular anti-phishing training and testing? How are the staff doing?.....</i>	20
• <i>Do we use a secure email gateway? What does it protect against?</i>	20
<i>Wireless internet network.....</i>	21
• <i>Does our router have the latest updates?.....</i>	21
• <i>Do we have an inventory of on-premises IoT (Internet of Things / “smart”) devices connected to our wireless network?.....</i>	21
• <i>What security protocol do our wireless networks use?.....</i>	22
• <i>Do we have any guidance available for staff on wireless network security when working remotely?</i>	23

1. Databases, Encryption, and Cloud

Can the tech company that provides our database access survivor data (information about a survivor that can identify them)?

Does the database use zero-knowledge encryption?

In order to maintain confidentiality, survivor data should be stored in a database where only authorized employees of your agency can access it. Ideally, not even the employees and contractors of the tech company that provides the database should be able to access survivor data. This can be achieved by a type of data encryption called *zero-knowledge*, *client-side*, or *no-knowledge encryption*. While most online services are encrypted in some way, zero-knowledge encryption is not the default for most databases or online file storage.

To learn more about what encryption is, how it is relevant for your program, and what to consider when selecting a database, see our [Encryption Basics for Programs](#) and [Selecting a Database](#) resources. To learn more about confidentiality and how it intersects with technology, you can browse through our [Confidentiality Toolkit](#). To learn more about how encryption may be relevant for other types of program information, go to [this question and answer](#).

What cloud-based services do we use? Why did we choose them?

There are a variety of services that allow people and organizations to store data offsite on large computers owned by a tech company and accessible online (i.e. “in the cloud”). These computers are in data warehouses located throughout the world. Cloud-based services allow users to access their data from different devices and locations. It is important to have an inventory of your organization’s devices and accounts for both administrative and cybersecurity purposes.

Some of these services (e.g. Google Cloud, Microsoft Azure, Amazon Web Services) are more aimed at large organizations working with large amounts of data, though they may also be used by smaller organizations. Some may be more user-friendly for individuals or smaller organizations (e.g. Google Drive, Dropbox). If your agency uses a database that contains survivor data, it probably stores those data in cloud-based storage.

You may already know what cloud services your organization uses (for both survivor and non-survivor data). In that case, it can still be worth learning about why they were chosen and what benefits they offer over other options.

Can the tech company that provides our file storage and collaboration tools (such as Dropbox or Google Drive) access the contents of our documents?

This is a little different from the question about [survivor data storage](#) in that these might be different tools. For example, you might be using Google Drive for document collaboration and using EmpowerDB to store survivor data.

You should not store any confidential survivor data online other than in a database designed and intended to store confidential survivor data. However, there still might be sensitive information (such as your agency's financial information or personnel files) that is not confidential survivor data. With most common general-purpose storage and collaboration tools, by default, the tech company can access the data (though would generally not do so without a need). This may or may not be something you are comfortable with as an organization. There are options such as [Cryptomator Hub](#) that allow organizations to create virtual "vaults" with zero-knowledge encryption within the general-purpose storage (such as Google Drive, Dropbox, or OneDrive) that they are already using.

To learn more about what zero-knowledge encryption is, see our [Encryption Basics for Programs](#) resource.

Do we back up our systems? Where? How are the backups protected?

Backups can be very important. If, for example, if one of your computers was infected with a virus that made it impossible to access the data on it, a backup could be used to restore the data. If your computer equipment was damaged in a natural disaster, backups stored in “the cloud” could be used to get the information and software that you need onto new computers.

However, backups can also be a vulnerability. They may have old survivor data on them that you had deleted on the current system. Old backups could have security vulnerabilities that have since been fixed. If they are being stored in the cloud, the storage may or may not have proper [encryption](#). Therefore, while backups are important, backup *management* is also important. Organizations need to have policies about backup retention (how long backups are kept) and secure deletion to make sure old backups are gone.

Do we use Simple Mail Transfer Protocol Secure ([SMTPS](#)) and other secured email protocols? If not, have we considered it?

Like other types of information that are sent between computers, email has a standardized set of formatting rules that it must follow in order to travel successfully between those computers. For email, one of these sets of rules is called SMTP (which stands for Simple Mail Transfer Protocol).

When email was invented, the concept of the internet was still new and not widely known among the general public. There was much less concern about cybersecurity than there is now. SMTP was not

created with security in mind. So SMTP is vulnerable to hackers who might be looking for easy targets. For example, a hacker could forge spam or phishing emails to look like they came from your staff members' email addresses. This could lead to many problems – even survivors being scammed by phishing emails that look like they came from your organization. *SMTPS (Simple Mail Transfer Protocol Secure)* adds a layer of security to SMTP in order to prevent these attacks.

However, it is important to remember that using SMTPS does not necessarily make email safe. Email is a vulnerable technology for a number of reasons, including the way people use email. Some survivors may prefer to use email to contact providers even given its shortcomings, but confidential survivor data should not be sent over email directly between providers. One common alternative is using ID numbers for survivors, such as “Have you sent the grocery cards for #1111 yet?”

What security protocol do our wireless networks use?

You have probably encountered wireless (Wi-Fi) networks that require passwords and ones that do not. You may also have encountered wireless networks that are somewhere in the middle (for instance, hotel networks that do not require a password but do require you to enter a name and room number in a hotel web portal before you get internet access).

Passwords help make your wireless networks more secure. But there are different qualities of security, based on both when the protocol was created (newer versions are more secure than older ones) and what kind of user the protocol was created for such as (e.g. general use, personal home networks, small offices with simple IT infrastructure, or enterprise for offices with a more complex IT infrastructure).

In this screenshot from a home wireless network, the security protocol used is called *WPA2-Personal*. You can see what security protocol you have by looking at the properties of your Wi-Fi network.

Properties

SSID: [REDACTED]

Protocol: [REDACTED]

Security type: WPA2-Personal

Network band: [REDACTED]

Network channel: [REDACTED]

Link speed (Receive/Transmit): [REDACTED]

IPv4 address: [REDACTED]

IPv4 DNS servers: [REDACTED]

Manufacturer: [REDACTED]

Description: [REDACTED]

Driver version: [REDACTED]

Physical address (MAC): [REDACTED]

Copy

The most secure protocol for wireless networks at the time of this writing is WPA3. The next most secure is WPA2. You should use at least WPA2 if your devices can communicate with it. Older devices may need to use an older protocol. Whether you use a Personal or Enterprise version will depend on the rest of your IT infrastructure.

Do we have any guidance available for staff and volunteers on wireless network security when working remotely?

Staff and volunteers who are working remotely – whether that’s from their own homes, from a courthouse as they accompany a survivor to a hearing, or from a hotel as they travel to a conference – will be connected to different wireless networks than staff who are working

on your premises. These staff may need separate guidance on wireless network security. At home, staff may benefit from similar tips to the ones Safety Net [provides for survivors](#). The same considerations for Wi-Fi security that apply on premises, [as discussed above](#), may apply to staff members' home networks. It could be useful as well to provide special guidance to staff who travel or need to work from different sites, who must connect to networks whose security they do not control.

A virtual private network (VPN) is software that allows a remote device to connect to another computer through the internet, as if the device were physically or wirelessly connected to it. VPN connections usually require a login and a password, and may require a secondary method of authentication. If a VPN connects to your office's network, the remote device would be able to access the office's printers, file storage, and other devices connected to the office network. VPNs can also be used to maintain privacy, and some VPN services will connect the remote device to that VPN service's computers in a specific city or country. To internet service providers, it will appear that the remote device is in the city or country that the VPN service connects it to. This can hide the remote device's actual location from internet service providers and websites, and can be used to avoid location-based content restrictions and surveillance. VPN connections are also more difficult to hack-into than other types of internet connections.

If your program uses an internal VPN – a network that users on or off site must log into in order to access your internal resources – to connect to your office network, this provides some level of security for the staff member's *connection* even if the actual wireless *network* the staff member is connected to is completely public. It makes it harder to technologically eavesdrop than would be the case ordinarily on a public network. In that case, it may be most important to have strong

password policies for that internal VPN. If your program does not use an internal VPN, staff can still use a reputable consumer VPN. Some examples (not a comprehensive list) include Proton, Mullvad, Nord, and Private Internet Access.

2. Collaboration Tools

How do we manage our Zoom (or other remote conferencing tool such as Microsoft Teams or Webex) data?

Remote conferencing and messaging tools (such as Zoom, Microsoft Teams, or Webex) are useful or even vital. However, they may be storing usage data – such as chat transcripts, recordings, or meeting transcripts – either in the cloud (accessible through a web portal), on users’ devices, or both. These tools usually have settings that allow organizations and individuals to control at least some of what data is stored and where it is stored. These tools often add features and settings, so it can be useful to go over them. Safety Net has [guidance](#) for this as relates to Zoom (as of mid-2025). In particular, organizations should be careful of settings that allow AI readers to follow users into the room without the user realizing it.

Can the tech company that provides our file storage and collaboration tools (such as Dropbox or Google Drive) access the contents of our documents?

This is a little different from the [question](#) about survivor data storage in that these might be different tools. For example, you might be using Google Drive for document collaboration and using EmpowerDB to store survivor data.

You should not store any confidential survivor data online other than in a database designed and intended to store confidential survivor data. However, there still might be sensitive information (such as your

agency's financial information or personnel files) that is not confidential survivor data. With most common general-purpose storage and collaboration tools, by default, the tech company can access the data (though would generally not do so without a need). This may or may not be something you are comfortable with as an organization. There are options such as [Cryptomator Hub](#) that allow organizations to create virtual “vaults” with zero-knowledge encryption within their general-purpose storage.

3. Access Management

How do we ensure that only people who need information or resources have access to them?

This relates to two important concepts from cybersecurity: *role-based access control* and the *principle of least privilege*. Both of these make use of the idea that if someone's account doesn't have access to information, it makes it harder for an unauthorized person to use their account to access that information. This way, even if someone accidentally downloads malware or falls for a phishing scam and an unauthorized person gets access to their account, the unauthorized person only gets access to a limited amount of information.

Role-based access control is the idea that people should only be able to access the organizational resources needed to be able to do their jobs. For example, an advocate does not need access to personnel files or clients' therapy session notes, and a benefits administrator does not need access to confidential survivor data.

The principle of least privilege says that people should only have the *privileges* that they need. This is subtly different than role-based access control. As an example of least privilege, neither the advocate nor the benefits administrator, in the example above, should be able to make a cybersecurity change for the entire organization. There are

some things that only IT administrators should have “privileges” to do. This also means that *service provider* staff who do not need that level of privilege should not have it.

Do we use a Zero Trust methodology?

Zero Trust is an organizational cybersecurity methodology that takes into account the sophistication of modern cyberattackers. Its motto is “trust no one, verify everything.” The rationale behind this motto is to “keep as much protection as possible even if someone’s device or account is accessed by an unauthorized person.” The [principle of least privilege](#) is part of Zero Trust methodology. You can learn more about Zero Trust by reading [Microsoft’s overview](#).

What resources and data can our consultants access?

This is another piece of [role-based access control](#). Consultants’ roles rarely require them to be able to access all of an organization’s resources, or even all of the resources of the team they’re working with. They only need to be able to access the resources for the projects they work on. This kind of compartmentalization should be easy for an internal or external IT provider to implement using modern tools.

What are our IT policies and procedures when someone leaves the organization?

Once someone leaves the organization, they should no longer have access to the organization’s systems (unless they are still doing consulting work for you, in which case they should be treated like [consultants](#)). This is true whether they left on good or bad terms. Either way, extra accounts and devices that someone could use to get into your organization’s systems are a security liability. In addition to being unnecessary, their passwords and other security features

are probably not being updated anymore, which will make them an even greater extra risk over time.

Some specific questions that you may consider:

- How long does it take before the former employee can no longer access their old accounts (e.g. because IT has changed their passwords)?
- How long does it take before the old accounts are deleted?
- What are the procedures for collecting any devices that the former employee used for remote work?
- What are the procedures regarding logins on work-related outside platforms (such as Canva) where the former employee signed up using their work email or phone number?

4. Incident Response and Disaster Recovery

What is our incident response and disaster recovery plan? How often is it updated?

Your ability to access and protect survivor and other data can be affected by incidents (such as a cyberattack) and disasters (such as natural disasters, terrorism, or a very severe cyberattack). It is common practice in cybersecurity to have procedures and plans in place for incident response and disaster recovery.

Do we back up our systems? Where? How are the backups protected? How long do we keep them?

Backups can be very important. If, for example, one of your computers gets infected with a virus that makes it impossible to access the data on it anymore, a backup could be used to restore the data. If your computer equipment was damaged in a natural disaster, backups stored in “the cloud” could be used to get the information and software that you need onto new computers.

However, backups can also be a vulnerability. They may have old survivor data on them that you had deleted on the current system. Old backups could have security vulnerabilities that have since been fixed. If they are being stored in the cloud, the storage may or may not have proper [encryption](#). Therefore, while backups are important, backup *management* is also important.

Do we have cybersecurity plans in place in case of physical security incidents in shelter/transitional housing?

“Incidents,” in this case, could refer to a variety of circumstances. The incident could be a break-in, an abuser showing up at a survivor’s transitional housing, a situation where law enforcement needs to enter the building, or any other entrance or attempted entrance of someone to whom survivors have not released data. If there is program-administered tech on site, it should have adequate security protections, including against unauthorized physical access.

5. Data Lifecycle and Asset Management

How do we dispose of data once we no longer need it?

In most cases, data doesn’t disappear permanently when you click a “delete” button. There may also be traces of data, including confidential data, on a computer or other device, that are not obvious to you. Paper files also need proper disposal, so that someone cannot, for example, reassemble pieces to recreate the original document.

The University of California at Irvine has helpful [guidance about how to dispose of different kinds of data](#). Do not worry if you don’t understand all the terms in this guide. It is included here as something your IT provider could adapt to your needs.

How do we manage our Zoom (or other remote conferencing tool such as Microsoft Teams or Webex) data?

Remote conferencing and messaging tools (such as Zoom, Microsoft Teams, or Webex) are useful or even vital. However, they may be storing usage data – such as chat transcripts, recordings, or meeting transcripts – either in the cloud (accessible through a web portal), on users’ devices, or both. These tools usually have settings that allow organizations and individuals to control at least some of what data is stored and where it is stored. These tools often add features and settings, so it can be useful to go over them. Safety Net has [guidance for this as relates to Zoom](#) (as of mid-2025). In particular, organizations should be careful of settings that allow AI readers to follow users into the room without the user realizing it.

What kind of data does our website collect from people who use it?

Organizations do not always realize how much information their website is collecting or sending to others. Technological “building blocks” may have activity trackers built in – some online font packages, for example, send information about user activity to the company that makes them. The creators of website components often assume that website owners want to collect IP addresses or information about users’ browsers. Even common features such as social media “like” buttons, post display widgets, and anti-bot captchas, may be sending user information back to their developers. A 2022 [investigation](#) by The Markup found that out of 50 tested telehealth startups’ websites, 49 were sending user information – sometimes including sensitive information like names, phone numbers, specific pages, and questionnaire answers, to advertising and social media companies like Google, Facebook, and TikTok.

There are simple ways to do an initial scan of your website.

- The Electronic Frontier Foundation's [Privacy Badger](#), which blocks third-party (outside companies') tracking behavior on websites, can tell you in real time how many potential trackers it is blocking and what they are.
 - This can also be useful for advocates to discuss with survivors. It can help survivors and advocates avoid trackers when they are searching together, or putting sensitive information into webapps that automatically send it to advertising companies.
- The Markup's [Blacklight](#) tool can scan both desktop and mobile versions of your website for whether it contacts well-known advertising technology companies. Blacklight is not perfectly accurate, but can give you a good idea of what adtech might be in your site.

Do we have an assets inventory?

A (technology) assets inventory, in IT and cybersecurity, is a listing of all the different devices and accounts that an organization has, and their status (for instance, is a particular laptop currently assigned to a staff member? Does the organization still use a particular social media account?). It may rate them – for instance, on a 1-5 scale – in multiple ways. One common way is importance to the organization and its functions (including, in this case, the maintaining of survivor confidentiality). Another way is the risk that it would pose if the asset (a device or account) were compromised. Including both ratings in the list helps determine what to prioritize. Having a list, the inventory, makes it possible to track the organization's technology assets, as well as to better assess whether they should be deleted/disposed of.

For privacy reasons, the assets inventory should not include the personal devices of shelter/transitional housing residents.

6. Housing

Do we have cybersecurity plans in place in case of emergencies in shelter/transitional housing?

“Incidents,” in this case, could refer to a variety of circumstances. The incident could be a break-in, an abuser showing up at a survivor’s transitional housing, a situation where law enforcement needs to enter the building, or any other entrance or attempted entrance of someone to whom survivors have not released data. If there is program-administered tech on site, it should have adequate security protections, including against unauthorized physical access.

What security protocol do our housing wireless networks use?

If your organization houses survivors in a shelter, congregate transitional housing, or other setting where the organization provides Internet access to survivors, those sites will have their own wireless networks. These should also use WPA3 or WPA2 security protocols, [as described earlier](#).

If the organization houses survivors in scattered sites where survivors have control over the wireless network, the organization should not dictate how survivors set up their own networks. Survivors in these sites, just like survivors in the general community, may benefit from our [Wi-Fi safety & privacy tips](#) resource.

7. Data Breach Prevention

Remember that prevention of data breaches starts with staff understanding confidentiality, and being empowered to push back if asked for confidential information. For more information about confidentiality, please see our [confidentiality toolkit](#). It also requires using

[appropriate tools](#) to store your data, and having appropriate policies on data minimization, [data retention](#), and [data disposal](#).

It is still, however, useful to have technological measures in place to prevent data breaches. Many modern cyber attackers are not necessarily looking for the “juiciest” or most lucrative targets. Instead, they target as many people/organizations as possible, hoping that there will be at least a few successes. Alongside technological measures, it is useful for staff to be aware of common technological threats like phishing and how to avoid them.

Do we have a process for automatically installing updates on work devices?

Installing updates to operating systems, apps, and other technology, can be very inconvenient. It’s also very important, especially for security updates. In the cybersecurity world, people are constantly testing products looking for security flaws, and many companies pay “bounties” to those who can prove to the company that they have discovered one in a product. Tech companies create and release updates in part in order to fix security flaws that *have already been discovered*. If the updates are not installed, that makes a user an easier target for hackers.

Do we use a Zero Trust methodology?

Zero Trust is an organizational cybersecurity methodology that takes into account the sophistication of modern cyberattackers. Its mantra is “trust no one, verify everything.” The rationale behind this mantra is “and thereby keep as much protection as possible even if someone’s device or account is accessed by an unauthorized person.” The [principle of least privilege](#) is part of Zero Trust methodology. You can learn more about Zero Trust by reading [Microsoft’s overview](#).

Email

- *Do we use Simple Mail Transfer Protocol Secure (SMTPS) and other secured email protocols? If not, have we considered it?*

Like other types of information that are sent between computers, email has a standardized set of formatting rules that it must follow in order to travel successfully between those computers. For email, one of these sets of rules is called *SMTP (Simple Mail Transfer Protocol)*.

When email was invented, the concept of the Internet was still new and not widely known among the general public. There was much less concern about cybersecurity than there is now. So SMTP is vulnerable to hackers who might be looking for easy targets. For example, a hacker could forge spam or phishing emails to look like they came from your staff members' email addresses. This could lead to many problems – even survivors being scammed by phishing emails that look like they came from your organization. *SMTPS (Simple Mail Transfer Protocol Secure)* adds a layer of security to SMTP in order to prevent these attacks.

However, it is important to remember that using SMTPS does not automatically make email safe. Email is a vulnerable technology for a number of reasons, including the way people use email. Some survivors may prefer to use email to contact providers even given its shortcomings, but confidential survivor data should not be sent over email directly between providers. One common alternative is using ID numbers for survivors, such as “Have you sent the grocery cards for #1111 yet?”

- *Do we have regular anti-phishing training and testing? How are the staff doing?*

Phishing is one of the most common ways that people's accounts get compromised. The best password in the world doesn't matter if you enter in into a fake login screen by accident. Even very savvy people can fall for phishing scams – especially as generative AI tools increase their sophistication – and phishers take advantage of how rushed people are and how many things they might be juggling.

There are products that allow IT departments and providers to run fake phishing campaigns and assess how well staff are spotting and avoiding phishing scams. These can also help identify people who may need additional training. The purpose is not to shame or punish them, but to provide extra support. If your IT provider is not already using these sorts of training tools, they may want to consider it. If you have only one IT staff member and/or a very low budget, there are free and freemium small-business phishing trainings available.

- *Do we use a secure email gateway? What does it protect against?*

Most of us are familiar with spam filters. These filter out spam and sometimes offer basic protection against viruses. A secure email gateway protects against other potential email threats, like phishing and [ransomware](#). It may also be able to protect against bad *outgoing* emails – for instance, if a staff member's email address is being spoofed in order to send malware to others.

Wireless internet network

- *Does our router have the latest updates?*

Often, people forget that routers are also devices! Routers can have security flaws just like software can. Traditionally, routers have often been overlooked in cybersecurity. The industry is getting better about this. However, tech companies do not always push updates to routers regularly in the way that they do to other types of devices like phones. This can leave routers – and through them, whole networks – vulnerable to cyberattacks. Searching phrases like “how to check router firmware” and “check for router updates,” along with the type of router you have, can help figure out whether the router is up-to-date, and provide update instructions if it is not. An outside IT provider/consultant should know how to do this. They may also be able to tell you when it is better to buy a new router.

- *Do we have an inventory of on-premises IoT (Internet of Things/“smart”) devices connected to our wireless network?*

In order to be effective, your IT provider needs to know what devices need security protections. They also need to be able to identify if an unauthorized device logs onto the network.

An inventory helps to make sure that cybersecurity and other technology policies and procedures are being applied to *all* program devices. This means not only laptop/desktop computers, tablets, and phones, but other internet-connected devices, especially those that connect to the program’s wireless network. Examples include routers, smart home devices, cameras, any kind of smart lock or doorbell.

For privacy reasons, the assets inventory should not include the personal devices of shelter/transitional housing residents.

However, it may make sense to have separate wireless networks for residents and for visitors.

- *What security protocol do our wireless networks use?*

You have probably encountered both wireless (WiFi) networks that require passwords and ones that do not. You may also have encountered wireless networks that are somewhere in the middle (for instance, hotel networks that do not require a password but do require you to enter a name and room number in a hotel web portal before you get Internet access).

Passwords help make your wireless networks more secure. But there are different qualities of security, based on both when the protocol was created (newer versions are more secure than older ones) and what kind of user the protocol was created for (in general, personal for home networks and small offices with simple IT infrastructure, enterprise for offices with a more complex IT infrastructure).

In this screenshot (on the next page) from a home wireless network, the security protocol is WPA2-Personal. You can see what security protocol you have by looking at the properties of your WiFi network.

Properties

SSID:

Protocol:

Security type:

WPA2-Personal

Network band:

Network channel:

Link speed (Receive/Transmit):

IPv4 address:

IPv4 DNS servers:

Manufacturer:

Description:

Driver version:

Physical address (MAC):

Copy

The most secure protocol for wireless networks is WPA3. The next most secure is WPA2. You should use at least WPA2. Whether you use a Personal or Enterprise version will depend on the rest of your IT infrastructure.

- *Do we have any guidance available for staff on wireless network security when working remotely?*

Staff and volunteers who are working remotely – whether that’s from their own homes, from a courthouse as they accompany a survivor to a hearing, or from a hotel as they travel to a conference – will be connected to different wireless (WiFi) networks than staff who are working on your premises. These staff may need separate guidance on wireless network security. At home, staff may benefit from similar tips to the ones Safety Net provides for survivors. The same considerations for WiFi security that apply on premises, as

[discussed above](#), may apply to staff members' home networks. It could be useful as well to provide special guidance to staff who travel or need to work from different sites, who must connect to networks whose security they do not control.

If your program has an internal VPN – a network that users on or off site must log into in order to access your internal resources – this provides some level of security for the staff member's connection even if the actual wireless network the staff member is connected to is completely public. It makes it harder to technologically eavesdrop than would be the case ordinarily on a public network. In that case, it may be most important to have strong password policies for that internal VPN.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.

© 2026 National Network to End Domestic Violence, Safety Net Project.