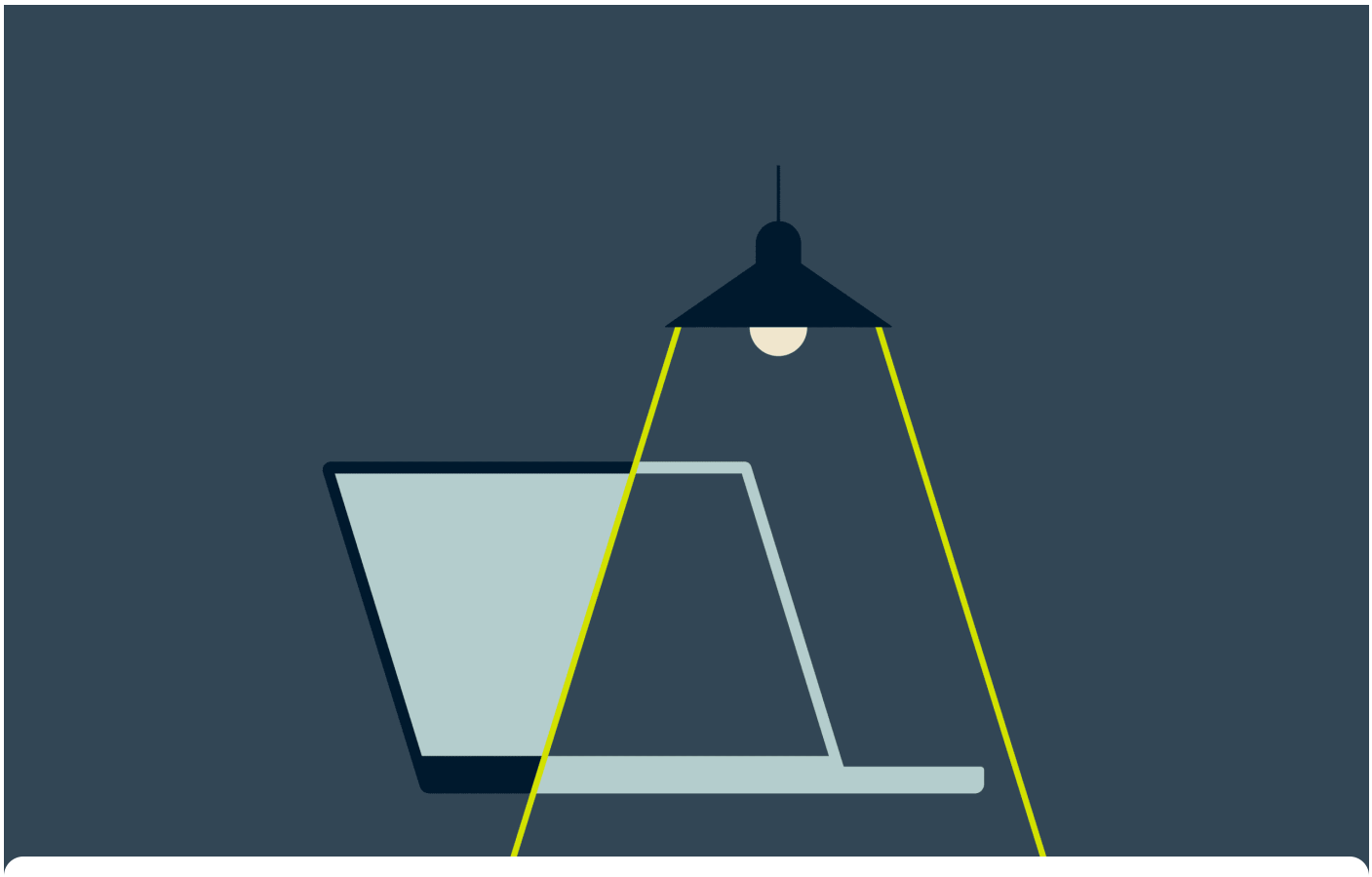
Tech safety for survivors of domestic violence

Research 05.09.2025 23 mins

Written by
Lexie



Domestic violence is about the abuse of power and control, which can take many forms. Often, technology can serve as a major tool of control and oppression, online and off.

Survivors are not responsible for or in control of their abuser's actions, but learning about how technology can be used against them can, in turn, help them take back control and take precautions to protect themselves. This guide provides tips on how to better secure and control technology, assert your autonomy in the digital realm, and work towards establishing safety and security.

The focus of this guide is specifically on technology-related coercive control and abuse. For urgent assistance, please contact a domestic violence organization. If you're in the U.S., call the National Domestic Violence Hotline at 1-800-799-SAFE (7233) or visit **thehotline.org**. For resources in other countries, see this **global directory of helplines**.

Before you start reading, if you believe someone is monitoring your devices, either visit this page from a device the person has no physical or remote access to, like a public computer, or use your **browser's** incognito (or "private") window.

Read more: What is incognito mode, and is it safe?

Jump to...

Domestic violence situations can present a unique set of digital security challenges that may not be covered by other help resources.

For example, most people can reasonably assume that nobody has tampered with their phone or computer. Tampering with devices is expensive and difficult, even for attackers like criminal organizations, hackers, and government agencies, in part because it usually requires physical access to your device. But in situations of domestic abuse, you often cannot confidently trust your own hardware and devices, because it's likely that you share a home with your abuser, which means they have access to your belongings.

In addition, a controlling partner may attempt to gain access to your online accounts—such as your email, social networks, online banking, and more—through coercion or deception.

Being able to gain confidence that your devices are not compromised and to assert control over your online activity is an important step in regaining your digital autonomy.

Who might benefit from this guide

Use this guide if...

- You’re experiencing technology-enabled domestic abuse
- You suspect someone might be spying on your computer or phone activity
- You fear you may be targeted by someone in your home or family
- You want a safe way to communicate with people you trust
- You’re helping someone experiencing technology-enabled domestic abuse increase their safety

This guide will show you how to protect yourself from online surveillance so you can securely maintain contact with others and seek help privately.

Part 1: Be able to trust your devices

To use your device safely, you need to know that you can trust it. Your device may be a phone, laptop, or desktop computer, or it may be a car or television. To be able to trust your device, it is best to keep it hidden and prevent anybody from finding out about its existence. In the case of your car, hiding its existence is close to impossible, so you may not be able to have full confidence in its safety.

Some devices are easy to modify physically while others are not. For example, it's easy to attach a GPS tracker to your car but hard to make modifications to your iPhone, because an iPhone is more difficult to open and has no spare space inside it for extra parts.

Here's what to look for if you suspect someone has tampered with your phone: loose parts, missing screws, or scratches where parts are glued together. When in doubt, err on the side of caution and assume your device isn't safe.

How to tell if someone has bugged your phone, computer, or other devices

There is no surefire way of knowing if someone has tampered with your devices or if someone is using your devices against you.

There are, however, a few signs that may indicate that something is wrong:

- Your device has been taken from you for a period of time
- Your device behaves differently from how you expect it to
- Your abuser discourages you from using other devices or leaving your device at home
- Your abuser knows things that you would not expect them to, like whom you've spoken with, where you've been, or the contents of an email
- You receive notifications that someone has been accessing your accounts without your knowledge or consent

Make sure you can trust your phone

Smartphones offer reasonable protection by default, but anyone with access to the device can compromise your phone's security. If you set up your phone by yourself with a good passcode, and if nobody else has had access to your device, then you can probably assume it is secure.

If you did not set up your phone by yourself, your abuser could be using your phone to track you. They may have installed **stalkerware** (a type of **spyware**) onto your phone that allows them to track your location and monitor your activity without your knowledge. "Bugging" your phone requires physical access to the device, but it can be done in less than an hour. This process, called **rooting**, removes security features and safeguards pre-installed by your phone's manufacturer.

Rooting allows any software to be installed on your phone, invisible to the untrained eye. This

Restore your phone to factory settings

When you're not sure if someone has installed tracking software onto your phone, restore your phone to its factory settings. For most devices, including Android phones and iPhones, performing a factory reset will usually return the device to a safe state. In rare cases, you may need to reinstall the software on Android phones from scratch. This is slightly more complicated, but **guides** are available online if needed.

After you've reset your phone to its factory settings, set it up with a strong passcode (a long, random one that you use nowhere else, or a number with at least six unique digits) and make sure you enable device encryption. Don't use your phone's integrated fingerprint or face scanner, because that may enable someone to unlock your device without your knowledge, such as by using your finger while you are sleeping. With a strong passcode and encryption enabled, you can now trust your device again.

Make sure you can trust your computer

Like smartphones, you can probably trust your laptop if you set it up by yourself, are the only one with access to it, and encrypt the hard drive. Full-disk encryption protects your data if someone tries to access the computer without your password. On Windows, this is done through **Device Encryption** or **BitLocker**, and macOS offers **FileVault**. Most modern PCs and laptops also include simple reset options that can return the system to factory settings.

Watch out for keyloggers

In general, it's much easier for someone to tamper with the hardware of a desktop computer than with a laptop. The external mouse and keyboard make it easy to attach a physical **keylogger** to your machine. A keylogger is a device which records all your keystrokes and makes it possible for someone to see any sensitive data you have typed, such as your passwords, addresses, and correspondence.

To ascertain if a physical keylogger is connected to your computer, follow the cable of your keyboard to the point where it reaches your computer. If there's a little device (similar to a

If you're not in a position to trust your own computer or smartphone, you can find a trustworthy computer at the library. The library also has facilities to let you make copies and scans of your documents, and library staff are helpful and well trained in helping you secure your documents online and communicate with others even if you don't have access to a trusted computer at home.

Semi-trust your device

Even if you can't fully trust your device, chances are your abuser isn't a super hacker who can deploy sophisticated malware and fiddle with your hardware to keep you under their control.

In this case, here are simple measures you can take to use your computer safely and privately:

- **Keep important files on USB drives** and hide the USB drives in safe places. For additional security, consider encrypting the drive and setting a password (this functionality is built into both **Windows** and **macOS**).
- Conversely, **use cloud storage** services that are password protected, use two-factor authentication, and have strong encryption and privacy policies.
- Browse the internet in an incognito window. This prevents your browsing history and cookies from being stored on your device.
- Use a VPN (Virtual Private Network) to encrypt your internet connection and hide your IP address, making it much harder for anyone to track what you do online.
- Use strong passwords.

You can also keep a copy of the **Tor Browser** on a USB stick and use it to surf the web privately. At the end of this article, you'll find an introduction to **TAILS**, which is an operating system that runs from a USB stick to protect your data and online activity—even on untrusted computers.

motion sensors. These devices often have poor security; it is easier to be out of view or earshot of these devices when you need privacy.

Make sure you can trust your car

Physical modifications to your car, like hidden GPS trackers, might be difficult to spot if you're not a car expert. Some **abusers may also use connected-car apps** to remotely track location, lock or unlock doors, or even control certain functions of the vehicle. You could hire a car mechanic to check for tampering, but doing so can be expensive, not to mention dangerous if your abuser has an eye on your whereabouts and financial activity. Trusting your car can be difficult. An abuser's knowledge of your car's make, model, and license plate may also make it easier for them to look for you.

Hitching a ride with someone is a good alternative to using your own car. Taxis, buses, and trains are also good options, as long as you pay with cash. Paying with cash eliminates any financial trail for your abuser to follow.

Trusting your device is a powerful step to achieving personal autonomy, because it allows you to keep your device on you without compromising your privacy, and enables you to install messaging apps so you can communicate securely with people you trust (more on this below).

Part 2: How to secure your files, data, and important information

Save your files to the cloud

If you have a device you can trust, it should be easy to keep your files and data safe from your abuser. Online storage services like Google Drive, iCloud, OneDrive, or Dropbox let you save your files online in the cloud. Even if you lose access to your device, you'll still be able to access your files from another phone or device.

Remember to protect your online storage account with a strong password that only you know, or else your files in your cloud storage account may become vulnerable to theft or snooping.

Use two-factor authentication

To protect your data and accounts in the cloud from unwanted access, make sure that you alone have exclusive access to your email address, and that you are the only one who knows the password. If you have a device that you trust, and know your abuser doesn't have access to it, **two-factor authentication** will help prevent them from accessing your account. If you aren't able to trust and secure your device, then don't use it.

When setting up recovery options, add ones you control, such as a recovery phone number or email address that only you can access. Google lets you add a **recovery phone or email** to regain access if you get locked out, while Apple offers **Recovery Contacts** for the same purpose. Avoid using a number or account that your abuser may know. Consider supplying the email or phone number of a trusted friend if necessary.

Some services, like Google, also let you generate a set of **backup codes** to use if you lose

If you can't trust your device, you can still store data safely, although it's harder to keep your files secret. Secret USB sticks will do the trick—as long as you hide them somewhere safe.

Better still, store your files on USB sticks with secret partitions; if your abuser were to get ahold of one of these partitioned USB sticks and plug it into a computer, the USB stick would appear to be broken rather than revealing all of your files. If you are tech-savvy or have a tech-savvy friend, you can encrypt your USB stick or create an encrypted hidden volume with the free program **Veracrypt**.

Scan your most important records

Scan, photograph, or make copies of all your important documents, such as birth certificates, marriage certificates, immigration papers, your children's documents, school diplomas, passports, visas, credit cards, medical records, court filings, police reports, insurance papers, and driving licenses. These records will make it easier for you to get these documents back in case your abuser takes them away from you. Without these documents, you may face difficulty if you want to leave the country, work, vote, or drive a car, and, in some cases, receive basic medical treatment.

If you don't have access to a scanner or photocopier, head to your local library or use a free screening app like **Adobe Scan**.

Secure your social media presence

Similar to your cloud storage or email, you will need to secure your social media accounts from intrusion. Make use of two-factor authentication, and make sure the email you provide at signup is secure.

Your abuser may use your social media presence to surveil you. Review the privacy settings of each of your accounts, and consider withdrawing location permissions from apps altogether. You may want to set your account to private or only create accounts under pseudonyms.

You also need to be careful not to share sensitive information on social media, such as ticket numbers, identification documents, or details that reveal your exact location, like street signs.

Part 3: How to protect your communications from surveillance

Maintaining secure communications with your friends is far easier if you have a trusted device. Without a trusted device, you will need to take extra precautions to maintain the privacy of your chats and phone calls. Use the following tips if you don't think you can trust your phone.

Encrypt your chats

Always choose encrypted communications over unencrypted ones. The encryption features in apps like **WhatsApp, Telegram, Signal, and Viber** make it impossible for anyone who takes over your account to read your past chats.

In some apps, you can set your messages to "self-destruct" after a set amount of time, so even if someone gains access to your device, they won't see your past message exchanges.

Read more: How to use disappearing messages on chat apps

Beware of phone metadata

In the case of your phone, the numbers you call may appear on your bill. The person who pays your phone bill can access even more detailed information, such as when you called which number, for how long, and, in some cases, your location at the time of the call. If the person trying to obtain your call information is close to you or has family ties with you, they may be able to obtain a lot of your metadata from your mobile phone provider.

They will also be able to forward all incoming calls to your phone to another number, which means they could receive your phone calls and texts, including those used for security

To keep the information associated with your phone activity out of the hands of your abuser, you can ask your mobile provider to add a “high risk” flag to your account by calling their customer support. Better yet, you can obtain a prepaid SIM card that you pay for with cash and keep it somewhere safe for your secret communications.

Protect your email account

Protect your email account as you would your cloud storage. If you have a phone that you're sure only you can access, secure your email with two-factor authentication, ideally using an authenticator app or passkey rather than SMS, which can be intercepted.

Many email providers allow you to review when and where your email account was recently accessed. Gmail’s Last Account Activity also shows sign-in times and IP addresses. If you have reason to suspect that someone is looking at your emails, you may wish to review these logs. As such, your email address is an important tool to keep in touch with old friends and family.

Abusers often use financial dependence as a way to gain power and control. Ensuring you have access to and control over your own finances is an important step in the path towards independence.

Securing your bank account

If you have a bank account in your own name, you already have a powerful tool of financial independence–and you should be sure to secure it. Protect your bank account by making sure it stays in your name. Ask your bank what it would take for a family member to take over your account, so you have some idea of how easy or difficult it might be for your abuser to gain access to finances. Usually, this process requires someone to produce a death certificate or a letter of attorney, which are not easy to obtain or forge. You can also ask your bank to add a “high risk” flag to your account, raising the barrier to anyone trying to obtain information about your account or take your account over.

Avoid online and phone banking

Conducting your banking activities over the phone or internet leaves you vulnerable to anyone trying to impersonate you to access your account. If you do not have access to a computer or phone that you can trust, you can visit your bank in person and request that they permanently disable phone and internet banking for you. Some banks also now offer **customer-controlled kill switches** that let you block digital access temporarily until you have a safe device.

Hide your credit cards

Credit cards are much more difficult to manage if you can’t keep them secure; all someone needs to abuse your cards are the numbers on the front and back. By providing just the name and a few digits from your card number, anyone can cancel your card. To make things worse, there is no way to “uncancel” a card once it is canceled.

Credit cards are also difficult to hide if you want to use them regularly. If you see fraudulent charges on your card, you can call your bank in the hope they will reverse the charges, but this only works a few times and will inevitably hurt your credit score. In a case like this, it

Money in a joint account is not yours. While you might be able to withdraw money from it, your transactions may be limited, subject to review, and most definitely allows the other signatory to see what you spend your money on and which ATMs you use.

If you are pressured to have your monthly income sent to your joint account against your will, you may wish to explore an arrangement with your employer that slowly gives you back agency, such as arranging to have your raises or unexpected bonuses paid to you in cash or cheque.

Open your own bank account

Depending on where you are, you may be able to open a bank account in your own name and keep it a secret from your abuser. Because many banks will ask for "proof of address" to open an account—like an electricity bill—you will need to have a trusted partner or family member who can provide you with an address. Once your own bank account is open, you will be able to deposit savings into the account or use the associated debit card for private transactions.

Use cash and other bearer assets

Without your own bank account, there are still a few ways you can achieve some financial autonomy, save for the future, and spend money without letting those around you know. Cash immediately comes to mind, though it can be hard to store. Putting away $10 every week might not raise much suspicion, but it will accumulate to a respectable emergency stash after just half a year. Keep in mind, however, that cash stored at home isn't insured the way bank deposits are, so it can be lost to theft or disasters.

Gold is also an option, especially for long-term savings. Significantly large sums of gold will take up very little space, and unlike paper cash, it does not degrade over time. Gold can also come in the form of jewelry or be incorporated into other daily objects like watches, which often makes it easier to attribute ownership, for example in court.

Cryptocurrencies like **Bitcoin** allow you to spend money online relatively anonymously. Unlike cash or gold, it is possible to store Bitcoin online where it is harder to steal and easier to hide

without any of these transactions appearing on your credit card or bank statement. But note that Bitcoin is highly volatile and not a reliable long-term investment.

Part 5: How to use TAILS to secure your computer activity

TAILS (The Amnesic Incognito Live System) is an operating system (like Windows) that runs from a USB stick on any computer. You can use TAILS to keep your files secure, browse the web on untrusted computers, and store your Bitcoin.

Using TAILS is not a cure-all. For example, if you lose your USB drive or your USB drive gets stolen, you also lose all your files. But with little technical knowledge, TAILS grants you access to an operating system you can trust, even if you can't trust the computer you load it onto.

Get a TAILS stick

A TAILS stick is a USB stick with special software installed on it. Since TAILS requires very little storage, this stick can be very small and relatively easy to keep secret. TAILS can be installed on any USB stick of at least 8 GB, and you can configure it with a persistent volume to save files and settings. **Making a TAILS stick** and configuring it with a persistent volume is not difficult, but it does require some technical knowledge. If you're not comfortable creating a TAILS stick on your own, then your local library, the computer club at the **neighborhood school**, a community college, or domestic violence support groups might be able to help you out.

Start the computer

TAILS works with almost any computer. To start it, restart the computer and press the key that opens the Boot Menu right after it turns on, which is F12, Esc, or F9 on many PCs. You can then choose to "boot from USB." On Macs with Intel processors, hold the Option (⌥) key at startup to select the USB drive. Note that TAILS does not work on newer Macs with Apple processors.

TAILS stick, so make your password strong and keep your password to yourself.

Read more: Create strong and memorable passwords with just dice

Use the TAILS stick

TAILS comes with a word processor, spreadsheet software, browser, Bitcoin wallet, and many other useful applications. You can use TAILS to maintain your entire digital life while keeping your activity a secret from others. If you want to save files and settings across sessions, you can create Persistent Storage on the USB stick. This is an encrypted area protected by a passphrase, and anything you choose to keep there is automatically encrypted.

Things to keep in mind

Although TAILS will protect you from malicious software installed on the computer you are using, it will not protect you from things like physical keyloggers. Your TAILS stick is also at risk of loss and theft. As long as you've set a good password on your stick, your data is secure. However, if someone discovers that your USB exists, they could still try to coerce you into revealing the passphrase. You might want to keep a backup stick around, especially if you are keeping valuable stuff on your TAILS drive.

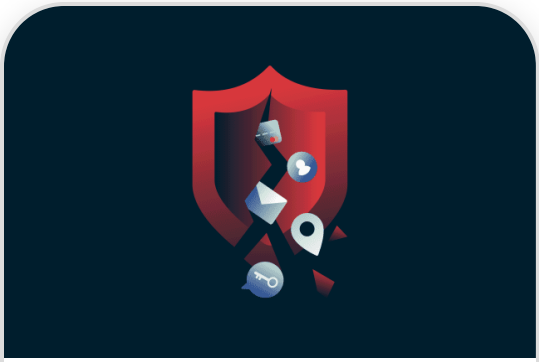
We hope this guide has helped empower you to turn technology into a powerful shield that enables you to plan for your own safety, and to protect and ultimately liberate yourself. ***If you are in immediate danger, call the police for help.***

Lexie

RELATED POST MORE FROM THE AUTHOR

18 top tips to protect your online privacy in 2026

Keith Fong 9 mins



What is doxxing, and how can you stay safe online?

Jennifer Pelegrin

21 mins

Is your car s you?

Lexie

Comments

Lawyer Sonia

2024-02-16 08:56:04

This insightful article sheds light on the crucial intersection of technology and safety for survivors of domestic violence. It offers invaluable guidance on securing digital privacy and protecting oneself from potential risks online. A must-read resource for anyone navigating the complexities of technology

munications from surveillance | Part 4: How to establish financial independence

Programs

Tottenham Hotspur

Brooklyn Nets

Partner with Us

Affiliates

Influencers

Get Help

VPN Setup Tutorials

FAQ

Contact Us

Buy VPN

Learn More

What is a VPN?

What Is My IP?

Hide My IP

Top 5 VPN Uses

Blog

Privacy Policy

Terms of Service

Cookie Preferences