NNEDV
NATIONAL NETWORK
TO END DOMESTIC
VIOLENCE

norton™

Securing Devices & Accounts

Table of Contents

Introduction

For survivors of abuse, privacy is closely related to safety. Privacy planning can also feel overwhelming and tricky, as most of us have many devices and accounts and the ways abusive people can get access to information can seem endless. However, it is possible to increase your privacy and security of your devices and accounts in ways that can make it a lot harder for an abusive person to misuse technology as a tactic of abuse, such as tracking your activity or finding your location.

To make the process easier, let's first break down the areas where we can increase privacy and security to 1) our devices, 2) accounts, and 3) the Internet. This resource will walk through common privacy and security considerations for devices, accounts, and using the Internet specifically with the lens of what you may need at different times: when living with or in close proximity/relationship with an abusive person, or when relocating/fleeing/no longer with the abusive person.

Shared devices and accounts are common. In relationships where abuse is happening, an abusive person may pressure or force you to share passwords, accounts, or devices. This can be a tactic of abuse and control. Abusive people may also break your devices, or limit access, in order to isolate you. This may include computers, phones, tablets, smart home devices, and connected cars. It can also include assistive technology used by people who are d/Deaf, or who are living with disabilities or chronic illnesses.

In situations where you've ended a relationship or you're being stalked, the abuser/stalker may try to get information about any new devices and

accounts you have, to surveil you remotely, or to use information that they already had about existing devices and accounts (such as passwords) to interfere with your use of technology or your activities.

Because of this, people experiencing abuse often need guidance on how to use the Internet as safely as possible, increase the security for devices and accounts, create new secure accounts, and/or get new secure devices. The level of access an abusive person has to devices and accounts is a key piece of both risk assessment and safety planning. In this resource, we talk about ways to do these things, keeping in mind both situations where someone lives (or is in close contact) with an abusive person (Access Level High), and situations where they do not live with or have close contact with the abusive person (Access Level Low). Since device settings are a potential issue in both of these situations, this resource begins with some suggestions about device settings.

Devices: Tips for Settings

- It can be helpful to disable any features that you are not using on your devices. For example, if you are not using a phone's location feature at the moment, you can disable location. If you are not using Bluetooth, you can disable Bluetooth.

- Devices that have auto-update features turned on will have stronger security, as this ensures that they're receiving the latest fixes for newly-discovered security flaws. How to do this depends on the device, but it is usually an option in a "Settings" app. Many devices have a search bar that allows users to search for specific apps or settings.

- If it is possible for you to disable 2G (a version of cellular network service) on your phone, and you live in a location where 5G, 4G, or 3G service are reliable, disabling 2G is a good security choice. This article explains how to disable 2G and why you may want to. "G" stands for "generation," and each generation of cellular network technology is more secure and less vulnerable to monitoring than the previous one.

Access Level High:
If you are still living with the abusive person or are in close contact

The next few sections will refer to "safer" devices. The reason that we use the word "safer" here rather than "safe," is that there is no such thing as perfect security or safety.

Devices: Regular Checkups
If you are able to do so, it is important to regularly check phones and tablets to see whether they have been rooted (someone has the ability to administrate the phone or tablet's operating system) or jailbroken (someone has removed the limitations that the phone's or tablet's manufacturer put in place, for example by making it possible to install apps on an iPhone that do not come from the Apple Store). For more information, read our guide to checking whether a device has been rooted or jailbroken.

Devices: Consistent Access to Safer Phones
For many people, it is important to have regular access to a phone that the abuser/stalker cannot monitor. Some options for this include:

- A pay-as-you-go phone, ideally purchased in cash (see the "Using the Internet: Options for Safer Purchases" section for other options if you

cannot use cash, and to learn about other things you may want to consider as you use your pay-as-you-go phone).

- A phone provided through a domestic violence or other program.
- An old phone that has had a factory reset, or a cheap refurbished phone with a new SIM card. The SIM card is the smart card inside of the phone that allows you to have a phone number and a subscriber account. You can learn more about SIM cards and their uses in tech safety and privacy planning, in the "Accounts: Dedicated Email Addresses and Phone Numbers" section.
    - If you purchase a cheap refurbished phone, one that has been "unlocked," meaning the device is not tied to a particular cellular service carrier, will allow you to use whatever brand of SIM card you want with it. This may allow you to pay less for data, and also makes it more difficult for an abusive person to guess information about your carrier and your subscriber account.

Devices: Transmissions and Safeguards

Many of our devices are designed to send information to, and receive it from, other devices. For example, wireless earbuds may receive information from your mobile device. Your mobile device may exchange information with a wireless router, for example when you connect to the guest WiFi at a café. This can be useful, but abusive people with access to your tech may also be able to change your settings or monitor your activity. For example:

- If you turn on your mobile device's Bluetooth to listen to music through your wireless earbuds, without making sure that Bluetooth visibility is disabled or restricted to paired devices only, an abusive person with Bluetooth enabled can see your phone's Bluetooth MAC address, and use that to track and follow you.

- Your device's GPS location service can be essential as you walk to an unfamiliar location, and a GPS tracking app can help you find a lost device, but someone with access to your accounts might be able to monitor your location remotely using these same features.
- An abusive person may be able to view your recent connections to WiFi networks if they physically go through your phone or if they've installed stalkerware.

You can manage these risks by using tech strategically. For example:

- Regularly check if Bluetooth is enabled on your devices, and only use it when you want to connect to another wireless device.
- Regularly check whether GPS location is enabled on your device, and only enable it when you need it to navigate.
- Check browser privacy settings and learn about other tools for safer browsing.
- Have sensitive conversations in a safer place, using safer devices.
- Know the settings on your devices, so you can regularly check if someone has changed them.
- Learn how to check your devices for stalkerware and spyware, or for rooting/jailbreaking.

Another option is using a *Faraday bag* that blocks all signals from going in or out in order to prevent hacking, remote monitoring, and data theft. There are discreet, attractive options that look like ordinary phone protectors, belt bags, and more.

Accounts: Separate, Secure Email Accessed Through Safer Devices

As part of safety planning while living with or being in close contact with an abusive person, it can be helpful to have a separate secure email account that the abusive person doesn't know about. This can include other types of accounts for messaging and calling. You can create a new encrypted

email account for free through services like Proton, and protect it with a strong password. Most people have trouble thinking up strong passwords and even more trouble remembering them – one way to get around this is to use a pass*phrase*, which is a string of unrelated words that you can remember (because it's easier for most people to remember words than random characters), like "instant fashion blue newspaper" or "prizes cats trumpet sunny." If you have trouble thinking of good words to use in your passphrase, you can use a passphrase generator.

Once you have a secure account, use devices that you're sure the abusive person has not compromised to log into it – such as a safer alternate phone or a library computer. No matter how strong your passphrase is, if the abusive person is able to open the account from your device, or monitor your device's activity, they may be able to access your account.

Using the Internet: Options for Safer Purchases

If you need extra privacy in making purchases, there are multiple options. The most anonymous option is a no-fee prepaid debit card, paid for in cash. If you don't need quite that level of privacy, cannot safely get to a store to buy a prepaid card, or cannot safely store a physical card, you may want to create an account with a service like Privacy.com, and use it to legally create virtual cards in alias names. You will have to provide your legal identifying information to Privacy.com. If you are concerned about your device activity being monitored, you might want to use a safer device (see below).

If you have purchases to make that you don't want the abusive person to know about (especially if you are planning on leaving), it might be best to strategically use a safer device. Some examples of possible safer locations and devices:

- A safer phone provided by a domestic violence program

- A library computer (be aware that some libraries use software from outside companies such as LexisNexis that sell patron usage data to other companies or government agencies – see our resource on data brokers to learn more about how this works – and be cautious about creating or logging into accounts that you don't want the abusive person to learn about while logged into library computers under your real name)
- A friend's device
- A device at a drop-in program or day shelter
- A university workstation
- A pay-as-you-go phone purchased with cash, using a public WiFi network, such as that of a coffee shop you don't normally go to.
    - Remember not to connect tools for safer purchasing to accounts you think an abusive person may have access to. For example, if an abusive person may have access to your usual Amazon account, and you enter a card that you obtained to make purchases more anonymously, that uses an alias name (which you can get entirely legally through services like Privacy.com, or MySudo for iOS) as a payment method, the abusive person will be able to see the information that you entered for the card, including the alias name that you may have been trying to keep private from them. If you need to make purchases from services like Amazon using your safer payment tools, you may want to use your secure email account to register for other safer shopping accounts.

Access Level Low:

If you are no longer living with or physically around the abusive person

If the abusive person is not able to physically access your device, they may try to gather information about you or monitor your activity (on or off your devices) by accessing your accounts. This section will focus on ways to increase account security and privacy.

If you need more information about safer devices, you may find it helpful to read the devices sections of the previous chapter, even if you no longer live with the abusive person.

Devices: What Should You Get?

If feasible, consider getting new devices as part of your relocation safety plan. Unfortunately, there is sometimes a tradeoff between affordability and security. Newer-model phones usually have security features that older models lack, and manufacturers usually only provide security "patches" (updates to fix newly-discovered security problems) for newer models of phones. If you are concerned about an abusive person accessing or interfering with your devices using hacking techniques, you may want to choose a relatively new model of phone (which will also help protect you more generally against cyberattacks). However, if you believe that an abusive person already has access to your existing devices and would not *need* to use high-tech means that take advantage of older devices' weaker security, your first priority may be getting new devices at all, which may make affordability the most important factor.

If you cannot afford new devices, you still have some options:

- Getting devices from a community program that provides services to survivors of domestic violence.
- Upgrading a slightly older device's operating system to a newer version (ask the company that made the computer or phone, through phone or web-based support or at an in-person service center!).
- Buying a new SIM card for an older phone.

- Buying a refurbished phone and a SIM card of your choice.

Note: If you connect your new devices to existing accounts before removing others' access to those accounts, changing your passwords, and enabling multi-factor authentication, an abusive person may be able to access the new devices. If you load backups of your old devices into the new ones, this may reinstall stalkerware or spyware.

Accounts: Getting Phone and Internet Service

If you were on a family plan for phone service with an abusive person, you will still be on it after you are no longer with that person, unless someone removes you. If you remain on the shared plan, that person may be able to access sensitive information about your phone usage. The Safe Connections Act of 2022 allows survivors of abuse to remove themselves from family phone contracts without any termination fees.

If you cannot afford service for your phone, you may qualify for help from the US government's Lifeline program.

For information on family plans in situations where there are children involved, see the section on co-parenting and children's technology.

Accounts: Checking Access and Removing Unwanted Access

Most phones and tablets require you to connect a Google, Apple/iCloud, or Amazon account in order to use them. These accounts can store large amounts of data about you, and someone with access to them can learn a lot about your activities. For this reason, it can be useful to check what devices are signed into your account, and remove any unwanted ones. All

of these companies provide instructions on how to do this (Google; Apple; Amazon).

Once you have removed unwanted access to your accounts, change your passwords and enable multi-factor authentication (you can find more information about this in our password security resource). If you do not, an abusive person may be able to use the old passwords to regain access.

Accounts: Password Managers and Password Updates

As part of "disconnecting" from an abusive person, you may want to consider updating your passwords, especially if they may have had access to your accounts. Even if you don't think they had access, it can still be helpful to update your passwords regularly, because they may have appeared in data breaches (such as when a hacker steals user information from a website in order to sell it), and if they have, the abusive person may be able to discover them. HaveIBeenPwned allows you to find out, for free, whether an email address or phone number has appeared in many data breaches. If you learn that one of your accounts was compromised through a data breach, not only should you update your password for that account, you should update it for any other account that used that same password, and not use that password again.

Most people have trouble thinking up strong passwords and even more trouble remembering them – one way to get around this is to use a pass*phrase*, which is a string of unrelated words that you can remember (because it's easier for most people to remember words than random characters), like "instant fashion blue newspaper" or "prizes cats trumpet sunny." If you have trouble thinking of good words to use in your passphrase, you can use a passphrase generator.

Another helpful tool is a password manager. A password manager is a virtual vault that holds your usernames and passwords for different accounts, and can generate strong passwords, so that you don't have to come up with or remember them. See our resource on password safety for more information.

Accounts: Multi-Factor Authentication

Many apps' and websites' security settings include an option to turn on multi-factor authentication (MFA). With MFA turned on, you have to present two or more pieces of evidence that you are an account's owner, to log into the account – most commonly, a password and some other form of evidence, such as a verification code sent to you in a text message. If someone does obtain your password for an account, MFA provides an extra layer of protection for that account. Another example of MFA is the use of a debit card to buy groceries – the card itself is one piece of evidence, and then you have to enter a PIN, which is a second piece of evidence that protects your account in case a thief tries to use the debit card.

Having any method of MFA provides more security for an account than does having no MFA. However, some methods provide more security than others. For instance, a verification number sent by text message, phone call, or email, could be intercepted by a hacker or by an abusive person with access to your email account or mobile device, and an abusive person may know the answers to your security questions, so security researchers often consider these to be weaker methods of MFA. There may be accounts that only allow you to use one of these methods, but there are many that allow you to use stronger methods instead.

One increasingly common method of MFA is the use of a third-party authentication app. There are many options for authentication apps, but you may get stronger protection from having one that is not connected to

an existing account like your Google or Microsoft account, in case an abusive person has access to that account. 2FAS is an example of a simple third-party authentication app that can be used for accounts on many popular apps and websites, and has video tutorials explaining how to use it with different accounts.

Here is an outline of how to set up this form of MFA:

1. Install the authentication app on your mobile device.
2. Open security settings on the individual accounts that you use (like Instagram, Snapchat, or Gmail) and turn on MFA (sometimes called "two-factor authentication").
3. Choose the option for using an authentication app (usually called something like "Use authentication app") and follow the instructions.

Another option for MFA is a YubiKey or other hardware authenticator. This is a small device that you can connect to a computer or mobile device to prove that you are the rightful owner of your accounts. There are several varieties, and the company that makes YubiKeys has a quiz to help you select the one that best fits your needs. A hardware authenticator can be a very good form of protection, because an abusive person who has compromised your mobile devices or some of your online accounts still cannot access your hardware authenticator. However, if there is a high risk of the abusive person stealing the hardware authenticator or forcing you to give it to them, or of you losing it, it may not be the best option for you.

Sometimes when people are trying to secure their accounts, they forget about accounts and passwords that they no longer use (for instance, someone who created several social media accounts in high school with the same insecure password, and has not used any of those accounts in several years). However, those accounts may still have information or access that is

useful for an abusive person to have (such as the ability to easily message your family and friends, or the name that you used prior to a gender transition). The apps' user data, including email addresses, username, and passwords, may have been stolen and published by a hacker at some point – an unfortunately common occurrence – which could make it easier for an abusive person to find and access these old accounts. This means that when possible, you may want to either close these accounts or protect them with a strong password and MFA.

If you aren't sure how to find old accounts, you can search your current and past email addresses on a tool like Epieos, that will find many accounts for you. You can try looking through your email inbox(es) for old account verification emails, or use a tool like WhatsMyName to find accounts linked to a particular username that you often used. You can also go to HaveIBeenPwned and enter email addresses or phone numbers that you have used, to see what data breaches they appeared in, because this may remind you of old accounts (if your present or past email address appeared in the 2008 MySpace data breach, then you had a MySpace account back then!). Once you find the accounts, if you don't remember your old passwords, try going through the apps' "forgot password" processes. Once you're able to access an account, you can search online for updated info on how to delete it, or contact the app's customer support.

Accounts: Caution About Syncing Contacts

Many apps offer options to connect your account with your contacts. You may have seen this called "Find My Friends," "Sync My Contacts," "Upload My Contacts," "Upload My Address Book," or a similar option. This feature is meant to make it easier for people who know each other to find each other on the app. However, using it could also inadvertently share your

information with the abusive person. To increase privacy, be cautious about syncing contacts or linking your accounts from different apps together.

You can also make sure contact syncing features are turned off in the settings. Apps regularly change their settings menus and privacy features, so this guide does not attempt to explain how to turn them off for every app. In general, if you search the name of the app and "turn off contact syncing," the information that you need will be in the first few results. If you can't find it that way, you can try to find a menu with a title like "settings" or "privacy" within the app, search the name of the app and "privacy settings," or look in the app's help section.

Accounts: Dedicated Email Addresses and Phone Numbers

One useful practice for increasing privacy is to create one or more email addresses or phone numbers to use only when signing up for apps. If you only use them to sign up for apps and don't give them out to other people, then an abuser/stalker is unlikely to have them in a contacts list. Creating new email addresses, using services like Gmail or Proton, is straightforward and free. You can create a phone number that will be usable for many apps, using a Voice over Internet Protocol (VoIP) service - a technology that allows you to make calls over an Internet connection - like TextNow, MySudo, Burner, or Google Voice. However, some apps require a "real" phone number and will not accept a VoIP number. Here are some options for situations where you cannot use a VoIP number:

- If possible, avoid providing a number in the first place (one trick for this is to only sign up for apps using their mobile versions (instead of through their site on your computer) - this sometimes makes it less likely that they'll require a phone number from you). If you can use either a phone number or an email address to sign up, use an email address only.

- If you do have to provide a real number, there are services that allow you to cheaply purchase a temporary non-VoIP number for app verification (try searching "use real number for verification").
- You can purchase low-cost SIM cards – the smart card inside of your phone that connects a subscriber account with the phone itself, and allows you to have a phone number and make calls. Swapping your usual SIM card with a different one, or putting a new SIM card into an old phone, when you need a cellular phone number with which to verify accounts, will mean that you can verify them with a number that the abuser/stalker/harasser does not know about. If you put a new SIM card in your regular phone, you can then take it out and put your old one back in as needed. If you put it in an old phone, this can serve as a long-term second phone.
- For a little more expense but greater reliability, you can buy a cheap, prepaid second phone.

Accounts: Hiding Location when Setting Up Accounts

Many people share information about their location when online without even realizing it. For example, a dating site may use data provided by your mobile device's GPS or detected by your browser, to pinpoint which potential matches are closest to you. An app may record and store the IP addresses (the "address" of any device connected to the Internet) that you use to log in to your account. Unfortunately, an abuser or stalker may be able to take advantage of the ways in which our devices share location information. Although most people can't use IP addresses to pinpoint an exact location, if someone gets access to the IP address of one of your accounts, it could allow them to identify the city or town that you're in.

There are, however, simple ways to hide this information while you create and use your accounts. These steps can help increase your privacy from

both broad privacy risks, such as scams, as well are purposeful misuse by abusive people.

Using the Internet: Virtual Private Network (VPN) Services

A VPN service hides your IP address from websites that you visit while your device is connected to one of their servers, by replacing your IP address with their own. Both free and paid VPN services exist. Most free VPN services are not recommended because they sell data to other companies, but ProtonVPN is an exception, though the free tier is slower than the paid tier. There are many high-quality paid services – some of them include:

- NordVPN (allows protection of up to six devices)
- Private Internet Access (allows protection of up to ten devices)
- The paid tier of ProtonVPN (allows protection of up to ten devices)
- ExpressVPN (relatively easy to install on a router, which protects smart home devices)

Using the Internet: Location Guard

Location Guard is a browser extension (Firefox; Chrome; Microsoft Edge) that will add "noise" when you give a website permission to access your location, so that your location appears to be in a slightly different place than it actually is. For extra privacy, you can set it to use a fixed location that is further away.

Accounts, Devices, and Using the Internet: Co-Parenting and Children's Technology

It can be challenging to "disconnect" from an ex-partner, and children's technology or co-parenting issues can make it even more complicated. Access to technology is important in the contemporary world, and child survivors, like adult survivors, deserve to be able to use technology and can use technology strategically to increase their safety.

Many adult survivors are aware that remaining on a family data plan with an abusive person can be a privacy risk, as the abusive person may be able to impose controls on devices in the plan or monitor devices' usage. This is also the case if children remain on a family data plan with an abusive person. In some cases, it may not be safe for children to be entirely removed from the previous family plan (for instance, because the abusive co-parent may escalate, or because children's visits with the co-parent could lead to that co-parent gaining access to the new plan). In these situations, it may be useful for them to have new devices on a different plan, associated with new, secure email accounts (see the "Accounts" sections of this document), and to only use the older devices when visiting or communicating with the co-parent.

Children, especially young children, may not understand safety concerns about a co-parent. However, children can learn about technology safety and privacy in age-appropriate ways. Cybersecurity company TrendMicro has a "Cyber Academy" of short videos and conversation guides about Internet safety, aimed at children ages 7-10 – given that survivor parents often want to learn cybersecurity and Internet safety basics themselves, it can be even more fun and educational for parent and children to go through these together. For even younger children, Internet Matters has links to online safety activities that parents and children ages 0-5 can do together (as well as links to activities for older age groups).

Children's visits with a co-parent can present other technology safety issues. You may want to check children's luggage, clothing or other possessions, and gifts from the co-parent, for devices that could be used for tracking or monitoring (such as GPS trackers, lost device finders like AirTags or Tiles, phones that you don't recognize as belonging to the child, or lost

pet finders) before returning home. If you drive to a child hand-off location, you may want consider leaving your devices at home, making sure their location features are turned off or that they are in Faraday bags, and checking your car for tracking devices at a rest stop before returning home. In some custody situations, a judge may order parents to use a special app for all communication between each other, that allows the communication to be documented and monitored by the court. These apps can be helpful in compartmentalizing necessary communication with an abusive person. However, if you use them to share photos, videos or other files (which may be required by the court), make sure that you remove metadata (data describing a file, that can include the location where it was created, the service provider of the phone used, or other information that could compromise your privacy) from them before uploading them, as not every app removes metadata from files automatically.

The creation of this resource was made possible with generous support from Norton. Opinions, findings, and conclusions or recommendations expressed in this guide are NNEDV's.

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

In partnership with
norton