NNEDV

# Steps to Increase Privacy & Safety Online

There are several ways that we can increase privacy and safety -- *and* stay connected.

**Safety first.** Before taking these steps, think about your safety. Some people may escalate their abusive behavior when they become aware that your passwords, accounts, or devices are secured. You can talk with an advocate about safety planning.

**Trust your instincts.** If it seems like someone else knows too much about you, they might be monitoring your devices, accessing your online accounts, tracking your location, or gathering information about you online. *If you suspect someone else is monitoring you, consider using another phone or device such as a friend's phone, or a computer at a library, school, or work.* Read more about phone safety and privacy.

**Get more information.** Navigating violence, abuse, and stalking can be difficult and dangerous. Advocates can help you figure out options and local resources and help you create a plan for your safety. You can contact a national helpline to be connected with local resources.

## Online Privacy & Safety Tips

*Sharing with Social Media*

- Social media is designed to be social, and information is often public by default. Some sites let you choose who can see your profile or posts. Use the privacy settings tools and guides, which many social media sites offer, to meet your privacy needs.

- Be cautious about connecting social media accounts or using one account to sign on to another - it makes it more difficult to lock down your privacy.
- When you take photos or create videos to post on social media, be aware of any information in the background that someone could use to find your location, such as street sign names, address numbers, license plate numbers, or business names.
- Regularly review who is in your "friends" or "followers" list, and be aware that your friends' friends may be able to see your profile and posts.
- Read about Online Dating and Online Gaming.
- Read about Video Sharing Sites.
- See our guide to Facebook.
- **Bonus:** Read the privacy policies of apps and sites to find out who has access to your information and how they can get it. Many sites and apps will sell your information or share information if they receive a subpoena or court order; this can be important for survivors who have or may have legal cases with an abusive person.

*Talk to Friends & Family*

- Talk to friends and family about limiting what they post about you.
- Ask employers, community groups, sports teams, volunteer organizations, or other groups you're involved in to not share your personal information online.

*Data Brokers & Removing Content from the Internet*

There may be different types of information about you on the Internet that you would like to remove because they are "sensitive" – impacting your life in some way or endangering your safety – such as your home address or intimate images of you. You may also find inaccurate information. Depending on the sensitivity of the information, it may be best to leave it alone. Many survivors prefer to leave inaccurate information online to obscure the accurate information that is also available. If the information you find on the web is abusive or potentially dangerous, you can contact the website and ask them to remove the information. Read more about your options for removing sensitive content from the Internet.

Companies called data brokers are one very common way in which individuals' personal information gets disseminated on the Internet. Data brokers gather your personal information from the Internet and public sources. This may include your current and previous addresses and other contact information, as well as information about your age, social connections, education, work, and more. In some cases, older paper records may be digitized and become searchable on the web. Read more about data brokers and how to opt out of them so that they no longer display your information online.

*When You Sign Up for New Accounts*

- Create email addresses and usernames that don't include identifying information, such as your full name.
- Create more than one email account. You can use separate email accounts for job searches, social groups, online dating, and more.
- You can even go one step further and use a service that "masks" your account address, so that when you're asked to enter your email address, it uses a proxy email address.

- Use different usernames when creating different online accounts.
- Use a different profile photo for each separate account profile. You can also consider using a picture that isn't a photo of you.
- Be cautious about sharing personal information beyond what's required to create an account or set up a profile. Sometimes sites don't make it obvious that the information is optional, so look to see if it's required.
- Click "no" when sites or apps offer to check your contact list, Facebook friends list, or any other source of information about your contacts, to help connect you with your friends already on their site.
- Opt--out of having your profile be publicly searchable.

*Make Your Passwords Stronger*

- The best passwords are at *least* 12 characters long.
- Use different passwords for each account, and use a secure password manager to keep track of them.
- Don't share your passwords with anyone without a specific reason that you're comfortable with. It can be a sign of abuse when someone demands that you give them your password. You have a right to privacy. If you feel unsafe, reach out for help.
- Use additional security options like multi-factor authentication. One example of how this works is that when you log in to an account, you also receive a verification code on your phone or in your email.
- Read more about Passwords.

*Private Web Browsing*

- Most web browsers give you an option to browse privately, which means that once you close the browser window, the websites you visited won't be saved in the browser history. However, if you bookmarked or downloaded anything, that can still be seen.
- You can also regularly delete history, cookies, temporary internet files, and saved forms and passwords from your web browser. NOTE: If you are worried that someone is monitoring your web browsing, deleting all of this information at once could alert the person monitoring your web browsing, which could be a safety risk.
- Read more about Internet Browser Privacy Tips.

*Be Careful with Wireless Networks*

- Consider using a VPN (Virtual Private Network) when using public Wi-Fi. You can also use one at home, or even install one onto your home router, if you want to hide your location from websites you visit.
- Change the default password for your home wireless network.
- Read more about WiFi Security.

*Minimize Location Sharing*

- Adjust the settings on your devices, apps, and accounts to limit or turn off location sharing.
- Don't include location in your pictures. You can turn off the option to save or share location in the settings of your camera and photo sharing apps.
    - Read more about Location Tracking.

Connecting online can help decrease isolation. Following these tips can help you be online, while also minimizing safety risks and keeping your personal information private and secure.

 Supported by US DOJ-OVW Grant #15JOVW-21-GK-02216-MUMU. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.