

# 8

## Ways to Stay Safe on the Internet



The internet is a powerful tool for those experiencing domestic violence and can be an essential resource to access help. Here are eight tips for staying safe on the internet and ways to protect yourself, your devices, and your personal information online.

1

### Avoid using shared computers or devices

- **Computers and digital devices store information about the websites you visit.** This includes the bills you pay, the purchases you make, and the emails you send, all of which can be retrieved.
- Practice **safe browsing methods** like using a virtual private network (**VPN**) to prevent abusive partners from **tracking your internet history**. Or use safe spaces such as a library, shelter, or workplace should you need to research legal issues, housing options, or relevant topics.

2

### Protect your passwords

- **You never have to share your passwords.** Shield valuable information, such as your passwords, by keeping them private.
- **Memorizing your passwords**, adding **encrypted passwords** to your phone or email, and **changing your passwords** can increase your safety and online privacy.

3

### Be protective of your personal information

- **Once your information is online, it's no longer under your control.** Protect phone numbers, addresses, handles, and personal details – such as birth certificates, schools you attended, employers, and photos with landmarks – as this information makes it easier for anyone to reach you.
- **Check your social media settings to ensure your privacy settings are secure**, and **disable others' ability to tag you** in their photos or posts.

4

## Customize your privacy settings

- Often digital platforms such as social media allow users to control how their information is shared and who can access it.
- [Customize these settings](#) in the privacy section of the website or app.

5

## Safeguard your digital identity

- Your digital identity helps establish who you are online. It protects your privacy by verifying your identity when logging into websites or making purchases.
- Sharing your digital identity can expose you to risks such as [identity theft](#), fraud, and even [cyberstalking](#). Be cautious about what and where you post online.

6

## Manage your search & browsing history

- Your [history can never be erased](#) from a computer or a device, even in “private” or “incognito” mode.
- Protect your digital privacy by [deleting your phone number](#) and clearing your internet browsing history after using digital devices.
- Ensure your web browser is up to date. Use the latest version and security features.

7

## Limit what you share

- Many people are willing to share images privately with their partners, only to have them break their trust and later threaten to distribute those images publicly. These images or videos are often used as retaliation or blackmail by a current or former partner.
- Intimate images shared with your partner could be used as [revenge porn](#), where nude or sexually explicit photos or videos are shared without your consent.
- If you find yourself in this situation, use this [Google form](#) to request removing your images from search results.

8

## Create a digital safety plan

- Digital abuse uses technology and the internet to bully, harass, stalk, intimidate, or control a partner. It's often a form of verbal or emotional abuse conducted online.
- You are not alone. Technology is a powerful tool, and The Hotline's 24/7 advocates can help you create a [digital safety plan](#).