

Tips for Using Video Sharing and Hosting Sites

With more people being home due to social distancing, watching videos on YouTube, TikTok, Facebook, and other activities, means that we can access fun as well as informational content like never before. While video content on these platforms can open doors to new information and resources, survivors of violence who watch should be aware of the related risks that come with watching videos in these spaces.

Here are some considerations for survivors around watching, interacting with, or sharing videos.

1. Delete browsing history

Web browsers on computers and mobile devices often store and save information about the sites you've visited and the videos you have watched. It is important to remember if you think your computer, tablet, or phone is being monitored, be thoughtful about deleting your browsing history because it can reveal the sites you visit and may identify what you have viewed. Periodically delete history, cookies, temporary internet files, saved forms, and passwords from your web browser if safe to do so.

You may also consider using browsers and search engines that are built with privacy in mind. Privacy forward browsers that do not track your activities, and work to keep other third parties like advertisers from tracking your activities include Firefox, Epic, Tor, and Brave, and privacy forward search engines include Startpage, DuckDuck, and Swisscows. Be mindful that you may have to install these browsers to your device.

2. Use Private Browsing, when safe

When searching for videos, or looking at videos that you want to keep private, you may also want to consider using an Incognito/In-Private Browser. Private browser windows keep history and cookies from being stored once the window is closed. It also means that any accounts you are logged into in the regular browser window will not be logged into in the private window.

Using these private browsing options can limit what data is tracked and stored. It is important to note that the websites you visit may still be visible if you don't close the window once you are done viewing. Visit our handout on <u>Internet Browsing Privacy Tips</u> to learn more. Use our <u>Online Privacy and</u> <u>Safety Tips</u> for more information on how to maintain safety and privacy in online spaces.

3. Log out of accounts

Some video-focused social media platforms give you the option of creating an account. Accounts you are logged into often store information on videos you have viewed and what you have searched for. When you create an account, the sites often store specific data about what you have viewed and what you have searched for. They often will also make suggestions about future videos you may want to watch based on that history. If you want to keep that information out of your account so that others can't access it, or so someone else who uses your account doesn't get video suggestions that may reveal private information about you, or view videos without logging into the account. Likewise, these accounts, such as YouTube or TikTok, may be linked to other accounts on your phone, such as your Google or iTunes account. This could lead to information you do not want to be shared, shared, and backed up.

4. Beware of the comments

Many times, video sharing services such as TikTok, YouTube, or Vimeo may allow users to post comments under videos. If you choose to share a comment for a video, viewers may view or access your username and profile. If you have concerns about this, be mindful of what videos you comment on. While many times comments can be empowering, some use comments to troll, attack and harass users. Take caution when posting comments, and learn about the site's policies for reporting harassment.

5. Consider using a safer device

If you think that someone is monitoring your computer, tablet, or mobile device, try using a different device or using a different browser that the person hasn't had physical or remote access to in the past, and doesn't have access to now (like a computer at a library or a friend's phone). This can hopefully give an option for video viewing that cannot be monitored by this person.

6. Check privacy and account settings

Every platform has privacy and account settings that give users the ability to lock down their accounts to viewers, limit the types of videos that are shown, and ways to increase password or account security. Some platforms offer many different options for securing and ensuring privacy settings are engaged, others offer limited ability to make changes. When using YouTube, Vimeo, or any other video sharing site, ensure that your settings are secured to your desired level, and check these settings frequently. If you don't know how to find these settings, use a search engine to search for an account, privacy, or security settings on your desired platform.

7. Trust your instincts

Abusers, stalkers, and perpetrators are often very determined to maintain control over their victims, and technology is one of many tools they use to do this. If it seems like the person knows too much about you, they could be getting that information from a variety of sources, like monitoring your devices, accessing your online accounts, tracking your location, or gathering information about you online.

For more strategies and tips on online accounts, browsing safely, and using safe internet, visit our <u>Tech Safety Blog</u> for helpful information around technology use.

© 2020 National Network to End Domestic Violence, Safety Net Project. This product was supported by cooperative agreement number 2017-VF-GX-K030, awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this product are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

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