Survivors' Guide to the Cloud

Most phones, tablets, laptops, and other devices now require you to connect your new device to a cloud account (usually Google or Apple for phones and Microsoft for Windows laptops). Apps and other accounts you use on your devices also save information in the cloud. This includes pictures, documents, passwords, contacts, messages, and email. Depending on the devices, apps, and accounts you use, other information about you could also be saved in the cloud, including a log of your location, online activity, calls, social media posts, financial transactions, public transit or ride-sharing, and more.

What is the Cloud?

"The Cloud" refers to storing and accessing information over the internet instead of your computer's hard drive. The internet uses many computers in data warehouses across the world, connected by the internet to store content.

What Does the Cloud Mean for Safety Planning?

The biggest risk is that anyone who has access to your devices or knows your login information could view all of the information that is stored in your cloud accounts. If your cloud account is shared or linked to other people's accounts, then they may also be able to see some of your information.

However, the cloud can also be used as part of a safety strategy because you can store information for long periods of time and access it later when it's safer or share it with trusted people. This can protect information if someone damages or destroys your devices. You can also strategically create new, secure cloud accounts to increase your privacy and security (setting up a Proton Drive account or an alternative Google account from a computer the abusive person has never accessed, for example).

Here are some tips on how to minimize risks, and strategies for how to use the cloud more safely and privately.

Safety first. Before taking these steps, think about your safety. Some people may escalate their abusive behavior when 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.

Cloud Safety and Privacy Strategies

Step One: Review Access to Your Accounts

Most cloud accounts will keep a log of the devices that have access to your account. This will often be information about the kind of device, the last time it was used to access your account, and sometimes the geographic location of the device.

This log is usually in the security settings section of your account. You can review the list. If you see an unknown device accessing your account, you can take a screenshot or a picture of the list before you make any changes if you want to document what's happening. If it feels safe, you can remove access for any or all of the devices.

Step Two: Strengthen Your Account Security

After removing any unwanted access, you can secure your account. Start by reviewing any emails or phone numbers that are connected to your account, in case someone else might receive a notification that you are making changes to the account.

Next, you can change your password and set up additional security features like multi-factor authentication. Read more about Passwords, and about Online Privacy and Safety.

More Tips When Using the Cloud

- Log out of accounts and apps when you're finished using them. This is particularly important if other people have access to your phone, laptop, or other devices.
- If other people can access your cloud account, one option is to minimize the information that gets stored there. Some accounts and apps let you choose whether your information stays only on that one device, or if it is sync'd across all your devices.
- If you think someone else has access to your cloud accounts, consider logging out of cloud accounts, or opening a different browser in which you are not logged in to any cloud account, before searching for anything you wouldn't want them to know about.

Setting Up a New Phone

If you decide to get a new phone or other device because you're concerned that your old phone has been compromised or is being monitored, it is important to also create new cloud accounts and not transfer data from your old accounts or backups. If someone else has access to your old cloud account and you connect that to your new phone, they will also have access to the new phone. If you have stalkerware or other apps on your old phone, and you transfer your previous files or restore data from a backup, it could be added to your new phone. Read more about stalkerware.

You may be able to connect your old accounts to your new device if you are able to secure those accounts first. However, this may not be helpful or safe if the other person has physical access to your device, or if they threaten or coerce you into sharing your password. Review the steps above to secure your accounts.

Conclusion

The cloud, like any technology, can be a risk if misused or have great benefits to survivors. It is important to understand how someone could get access to your information through the cloud, so you can minimize safety and privacy risks. Depending on your situation, the cloud might be a helpful way to store a large amount of information (such as photos, documents, your activities) securely. An advocate can help you to balance the risks and benefits and help you decide if this tool is right for you.

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.