Protect Your Personal Information & Data

Secure Your Accounts

Once your computer, tablet, and phone are secure, next take steps to protect your accounts — particularly those with personal information, like your bank, email, and social media accounts.

Create and use strong passwords

That means at least 12 characters. Making a password longer is generally the easiest way to increase its strength. Consider using a passphrase of random words to make your password more memorable, but avoid using common words or phrases. For more tips, check out this Password Checklist.

Use multi-factor authentication

Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. These additional credentials fall into two categories:

- Something you have, like a passcode you get via an authentication app or a security key.
- Something you are, like a scan of your fingerprint, your retina, or your face.

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

Choose security questions only you know the answer to

Many security questions ask for answers to information available in public records or online. So, when you can, avoid questions like your zip code, mother's maiden name, and birthplace. And avoid using questions with a limited number of responses that attackers can easily guess — like the color of your first car. You can even put in random answers to make guessing more difficult. If you do that, though, you'll have to remember the answers you use.

Back up your data to protect it. Backing up your data means making an extra copy of all your files. That way, if something happens — say a virus, your device crashes, or you're hacked — you still have your files. It's important to do it once a week, so you don't lose important data, like your photos, documents, and files. If you need to restore a backup, it will only be as current as the last time you backed up.

Here are two options and a few things to consider when choosing how to back up your files.

- Save your files in the cloud. Many cloud storage services let you save files and data online. You may be familiar with some, like Google Drive, Evernote, Dropbox, OneDrive, or iCloud, but many others are out there. Many of these services come with some free storage space, and you can pay for more storage. When you save your information in the cloud, you're trusting someone else to keep that information safe. If you're thinking about using cloud storage, find out what level of privacy or security the different services offer.

Save your files to an external storage device. A USB flash drive is an affordable option that offers a moderate amount of storage. Another option is an external hard drive. It might cost a little more than a USB drive, but it can give you more storage capacity, transfer data faster, and be more reliable. You can decide which files or folders to back up, and you may schedule automatic backups.

Credit: Federal Trade Commission - www.ftc.gov