# Recording passwords securely

Our Basic section showed you how to create a strong, memorable password. However, because you need a different password for every account or service and also need to change them every few months, it can soon become difficult to remember them all. Fortunately, there are software tools to help with this ? a password manager is a software application that can generate random, secure passwords for each of your accounts and record them in a portable, encrypted password database, such as KeePass.

The password manager protects all of your passwords with a single master password so you only have to remember one thing. Of course, if you use this method, it becomes especially important that you create and remember a very secure password for KeePass, or whatever tool you choose. Whenever you need to enter a password for a specific account, you can look it up using only your master password, which makes it much easier to follow all of the suggestions above.

KeePass sits on your desktop, and it also portable, which means that you can put the database on a USB memory stick in case you need to look up a password while you are away from your primary computer.

You can learn how to set up and use this tool in the [Keepass tool guide](umbrella://lesson/keepassx).

# Tips for using password managers

There are few things to keep in mind when using password databases.

* If you lose or accidentally delete your only copy of a password database, you will no longer have access to any of the accounts for which it contained passwords. This makes it extremely important that you back up your KeePass database. Read our [Backing Up lesson](umbrella://lesson/backing-up) for instructions on how to do this.
* If you forget your KeePass master password, there is no way to recover it or the contents of the database. So, be sure to choose a master password that is both secure and memorable!
* It is also crucially important to keep your password manager itself secure. ? Some password managers will offer to store your passwords ?in the cloud,? which is to say, they will store your passwords encrypted on a remote server, and when you need them on a laptop or mobile, they will retrieve and decrypt them for you automatically. Password managers like this are more convenient, but the trade-off is that they are more vulnerable to attack. If you just keep your passwords on your computer, then someone who can take over your computer may be able to get hold of them. If you keep them in the cloud, your attacker may target that also. It's not usually a compromise you need to worry about unless your attacker has legal powers over the password manager company or is known for targeting companies or internet traffic.
* When you use a password manager, the security of your passwords and your master password is only as strong as the security of the computer where the password manager is installed and used. If your computer or device is compromised and spyware is installed, the spyware can watch you type your master password and could steal the contents of the password safe. So it's still very important to keep your computer and other devices clean of malicious software when using a password manager. You can learn more about this in the [Malware lesson](umbrella://lesson/malware).

# Two-step authentication

Many services and software tools let you use two-step authentication. Here the idea is that in order to log in, you need to be in possession of a certain physical object: usually a mobile phone, but, in some versions, a special device called a security token. Using two-step authentication ensures that even if your password for the service is hacked or stolen, the thief won't be able to log in unless they also have control of a second device, such as your phone, and the special codes that only it can create.

Two-step authentication using a mobile phone can be done in two ways: the service can send you an SMS text message to your phone whenever you try to log in which provides an extra security code that you need to type in. Alternatively, your phone can run an authenticator application, such as [Google Authenticator](https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2), that generates security codes from inside the phone itself. This will help protect your account in situations where an attacker has your password but does not have physical access to your mobile phone.

# One-time passwords

Some services, such as Google, also allow you to generate a list of one-time passwords, also called single-use passwords. These are meant to be printed or written down on paper and carried with you.

There is no way to do this by yourself if you're using a service that doesn't offer it.

If you or your organization runs your own communications infrastructure, such as your own e-mail servers, there's freely available software that can be used to enable two-step authentication for accessing your systems. Ask your systems administrators to look for software offering an implementations of the open standard ?Time-Based One-Time Passwords? or RFC 6238.

Swipe right for this lesson's checklist

Go to the Beginner lesson for advice on how to create a strong password.

[Go to Beginner Lesson](umbrella://lesson/passwords/0)

Go to the Expert lesson for advice on what to do if you think you might be forced to hand over your password.

[Go to Expert Lesson](umbrella://lesson/passwords/2)

### RELATED LESSONS/TOOLS

* [Backing Up lesson](umbrella://lesson/backing-up)
* [Malware lesson](umbrella://lesson/malware)
* [KeePass tool guide](umbrella://tool/KeePass)

### FURTHER READING

* [EFF - Creating strong passwords](https://ssd.eff.org/en/module/creating-strong-passwords)
* [Security in a Box - Chapter 3, Passwords](https://securityinabox.org/chapter-3)