

# Password Management

Welcome to this training lesson on **Password Management**. In this lesson, we'll look at **passwords** - how to create them, how to use them, and how to store them.

**Estimated Completion Time:** 8 minutes.

## Password Management

**Passwords.** Almost every site you contribute to, or in many cases, simply use, will require a user name and password combination for access. This includes Facebook, Twitter, Instagram, and many more. Your computer or mobile phone or tablet may also require a password.

Unfortunately, weak password security is the number one way hackers can get access to your accounts, and perhaps even your computer or mobile device.



## Password Management

**Password Strength.** It doesn't take a hacker long to determine what passwords are commonly used. Passwords such as *password1*, *password*, *12345678*, and others like this are the first ones hackers will try.

The above technique may work even if the hacker knows nothing about you. If they do - perhaps looking at your Facebook page - they may know the names of your pets, your kids, your significant others. So - clearly - do not use these as your passwords.

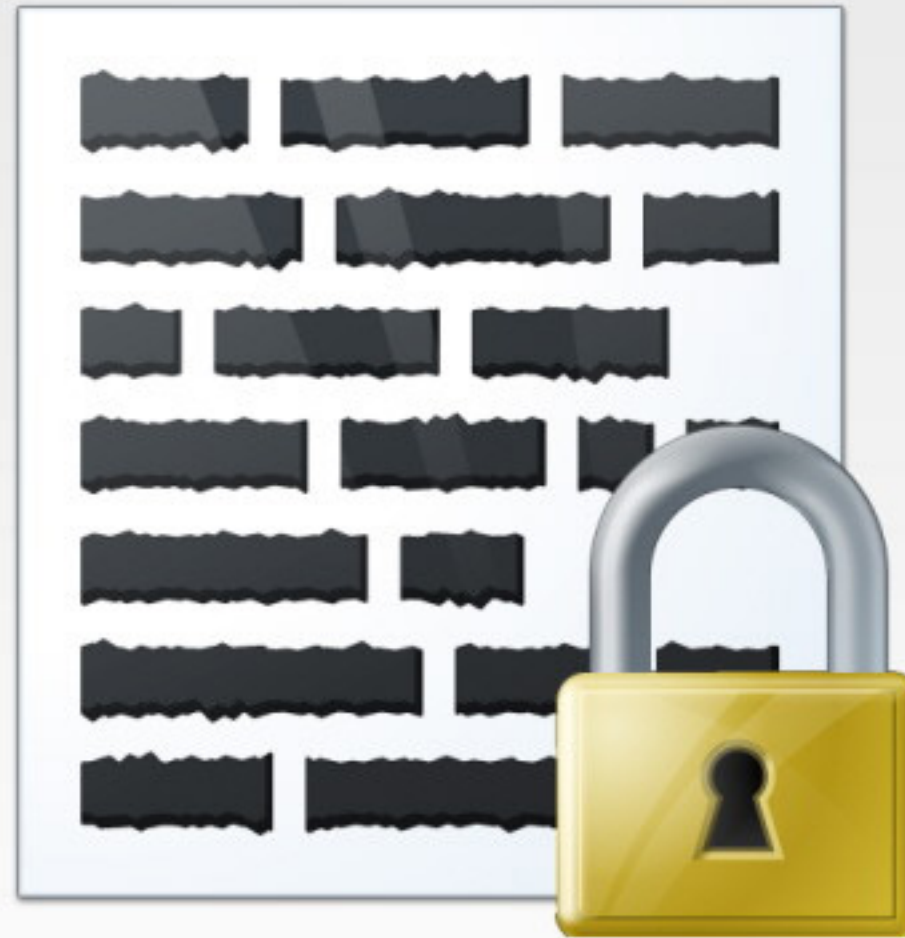




## Password Management

**Password Variations.** A common technique used by many is to replace some letters with numbers. For example, instead of *scruffy* as a password, you use *scru44y*.

While *scru44y* is probably safer than *scruffy*, it is still not all *that* safe. Hackers are aware of these sorts of tricks, and can easily employ techniques to get around them.



## Password Management

**Site Specific Passwords.** While it is important to have different passwords for different sites, don't use a password too specific for that site. Passwords like *microsoft*, *adobe*, *facebook*, *twitter*, etc, are also commonly used, and likely to be very easy to crack.



## Password Management

**Constructing a Password.** You probably already know that the more complicated a password is, the harder it will be to crack, or guess. But a password like **#jFk&#\$3j9** is a little hard to remember.

Let's look at a couple of techniques to make complex passwords a little easier to remember.





## Password Management

**Phrases.** Rather than using a single word as a password, you may try a combination of words. However, ensure these words are not a part of a common phrase, like *iloveyou*, for example.

Try a combination of words that might make sense to you, but not others. *scrapdognight*, *lowcommercenine* are some examples. Adding some numbers or special characters can also be added (and in fact may be demanded by some sites.) *scr4pdogn#ght*, for example.



## Password Management

**Acronyms.** Another technique is to take a common phrase, line from a song, or some words that make sense to you, and combine them together as an acronym. For example, a password like **Ycagwyw#1969** does not make a lot of sense (and would certainly be hard to guess, or crack), and at a glance, looks hard to remember.

However, if you are a *Rolling Stones* fan, you may remember this as the acronym for **You Can't Always Get What You Want**, released in **1969**.





## Password Management

**Don't Re-use Passwords.** It's a hard one to resist - because you don't want too many passwords to remember - but using the same password on a multitude of sites or devices is a dangerous thing.

The real problem here is that if your password becomes compromised on any site you use this password on, hackers are aware that many, many people reuse passwords. And they can try these passwords on your other sites.

If you re-use passwords, all of your accounts could be compromised if any one of the sites you use are hacked.



## Password Management

**Password Management Software.** If you have multiple passwords - and you ensure they are all different, and all very complex, you may want to use password management software.

Password management software is designed so that you only have to remember one - one very secure - password. With this one password, you can store and retrieve passwords from the software as required.

A convenient place for this software is on your phone, as an app. Especially if the passwords are only stored on your device. This makes it very difficult - if not impossible - for remote hackers to get access to.





## Password Management

**Writing Down Passwords.** If you want to write down your passwords somewhere as a memory aid, it is generally OK, as long as you take some common sense precautions.

While yes, it is true, if you write down a password (and keep it in your house, for example, rather than your wallet or purse), it is possible it can be found and used. However, it is overwhelmingly more likely that your password will be discovered online by a remote hacker. And if writing down your passwords allows you to have more secure passwords, it is probably a better option.





# Password Management

**Writing Down Passwords (2).** A few rules if you feel you **must** write down your passwords:

- Keep them in your house rather than on your person.
- Keep them hidden or out of sight.
- Don't be too obvious, as in:
  - *Facebook* - *sd45&\*934*
  - *Instagram* - *sdk34632k\**



## Password Management

**Fingerprinting.** Devices are now starting to appear with fingerprint identification. In many cases, these are still used in conjunction with passwords, but provide an added layer of security.





## Password Management

**Two Step Verification.** As a more secure method of logging into certain accounts and sites, some sites and organisations are offering what they call two step verification.

Although the process may differ a little between organisations, most make two step verification optional. If enabled, when you log into an online account with your user name and password, you'll be sent a short code by text message, to an app, by phone or email, that you will also have to key in to get access to your account.

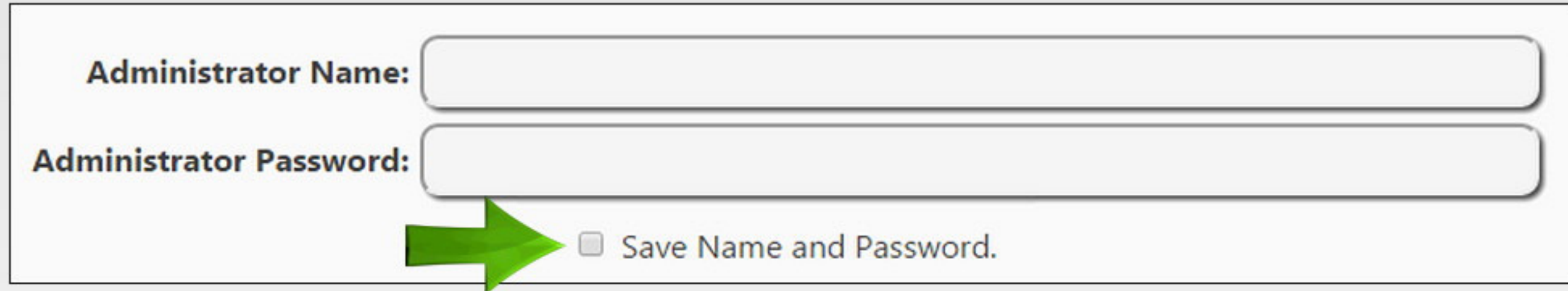
This essentially ensures that to get into your account, a hacker would require your password, **and** your phone.





## Password Management

**Letting Your Browser Store a Password.** On some sites, you'll see an option something like this:



Administrator Name:

Administrator Password:

☐ Save Name and Password.

The **Save Name and Password** option is one you should be very careful with. Yes, it can be very convenient, as you may not have to type in the name and password next time you enter this site.

However, remember that if anyone gets access to your device or computer, they also will not have to enter a name and password to enter a site.

On public computers, work computers, or friend's computers, ensure this sort of option is never selected for personal sites.

## Password Management

**Automatic Password Saving.** If the site itself does not let you store a name and password automatically, your browser may ask you if you want to save them within the browser itself. You may see a question something like this, depending on your browser:

Would you like to store your password for learningcomputing.net?

Yes

Not for this site



This does much the same thing as we discussed on the previous step. You are being asked - **do you want to save this password?** This means that the next time you enter your user name on this website, the password will be filled in automatically.

So, the same warnings apply.

## Password Management

You've now completed this training lesson on **Password Management**. In this lesson, we looked at **passwords** - how to create them, how to use them, and how to store them.