# User and administrator accounts

People who work in offices, or who share their computers, may already be familiar with separate user accounts on their computers. Separate accounts ensure accurate authentication and accountability. How else can you track and control who accesses the files or is able to change something in your system? However, even if you are a sole trader or work in a single person company you still need at least two accounts on your computer.

When an account is created, the type of account determines what the user is able to do:

**An administrator** is someone who is in charge of the settings and controls of a computer, and someone logged into an account with administrator privileges can do pretty much anything on the computer. They can view every file on the system, including any account maintenance, billing and subscriptions, change system-wide system settings, run all installed programs, add new programs, install new hardware drivers and change the usernames and passwords of other user-accounts.

**A regular user** account cannot perform administrative tasks, they are usually limited to everyday tasks such as sending emails, creating documents and conducting internet searches. If they are able to access additional files and data, it will only be those that the administrator allows. Using a regular user account will prevent most malware and other malicious programs and apps from installing.  The malware will have the same privileges as the account you are logged in as and a user account does not have the privilege to download new software so a malware download would automatically require an administrator password. This makes your system more secure.

### ****DEFAULT ACCOUNTS****

By default, user accounts in Windows have administrator privileges, meaning they allow you to install, modify or delete software. This level of access carries security risks as unfortunately, you have the ability to do things that you never really intended to do, some of which can cause major problems with the computer.

It’s quite easy for an administrator to accidentally delete an important system file or change a setting that renders the PC unstable or un-bootable. If you work for a small business or for yourself, you might not realise that you are permanently logged on with an administrator account.

### ****ACCOUNT SEPARATION****

No one, not even home users, should use administrator accounts for everyday computer use, such as web surfing, emailing or office work. Instead, those tasks should be carried out by a standard user account.

Administrator accounts should be used only to install or modify software and to change system settings. If you’re a Windows user who has administrative rights, you should create a separate administrator account, and downgrade your regular account to standard-user account even when you’re the only person who uses the computer. (You can still perform administrative tasks by typing in the password to the admin account.)

The administrator account should only be used when a task absolutely has to be done that a standard user account is prohibited from doing. During normal use it is always best to log in to a regular user account. If more than one person will be using the same PC each user should have their own regular, separate account.

Additionally, most computers come with a ‘guest’ account enabled which allows anyone to freely access your device – you should disable it. In a similar vein, if there is an account on your computer that is no longer used, be sure to delete it.