



User Access Control	What are the Cyber Essentials controls?
	<ul style="list-style-type: none"> Use a standard user account for day-to-day activities Administrative accounts must be controlled and limited to those who need them Multi-factor authentication needs to be set up on all cloud services
<p data-bbox="229 815 932 864">www.ncsc.gov.uk/cyberessentials</p> 	

Control who can access your data and services and what level of access they have.

Separate accounts for each user with no shared accounts

People who work in jobs where they have to share a computer or a till are familiar with needing to log on with a password or code to their own account. Separate accounts ensure accurate authentication and accountability. How else can you track and control who has been doing what?

Separate user and admin accounts for different tasks

When an account is created, the type of account determines what the user is able to do. There are two main types of accounts.

An administrator is someone who is in charge of the settings and controls of a computer. They can view every file on the system, including any account maintenance, billing, and subscriptions. Someone using an administrator account can also 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 (admin 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. This is because 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. In this instance, a malware download would automatically require an administrator password. This makes your system more secure.

It's worth noting that even if you are a sole trader or work in a single person company you still need at least two accounts on your computer.

Default accounts

By default, user accounts in Windows and Mac 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 or Mac 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.

Delete accounts that are not used

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.

Account creation and tracking processes

An account creation process can help your organisation keep track of staff accounts, recording and approving account permissions for starters and movers and disabling or removing accounts for leavers. It might be that only once someone has signed their paperwork and received clearance (if appropriate) they are issued with a computer account.

A specific set of rules can be created around administrator accounts. Clarify and record who has administrator accounts and ensure that these accounts are not used for emails and web browsing. This rule applies to third parties with administrative accounts providing support services to your organisation. It is often necessary to use a combination of policy and staff training to achieve this requirement.

The value of passwords

Stealing personal information such as usernames and passwords, bank account details and credit card numbers is incredibly profitable for criminals. They can send fraudulent emails from your account, make fraudulent purchases from your credit card, use your identity to take out loans and open new accounts and go on to launch other attacks against you. Criminals also profit from disrupting or re-routing websites, illegally tracking users and selling stolen credentials to other criminals. With the rise of online accounts, criminals have realised that they need to get hold of passwords to gain access to accounts and they have become very proficient at password harvesting. The master plan for many cyber criminals is to discover as many passwords as they can in the shortest amount of time and then use computers to try matching passwords and usernames on as many accounts as they can at the same time. According to Breach Alarm, 1 million passwords are stolen every week.

There are several factors that will help prevent your password from being guessed or stolen.

Strong unique passwords

A default password is a standard pre-configured password allocated to a device by the manufacturer for its initial set up. It is not difficult to find out the default passwords for many devices with a simple internet search. Attackers will use a default username and password combination and try to connect to one of your devices, even though it is within your internal network. Simply by changing the default password (and username if possible) you have immediately made a hacker's job much harder.

One password for one account

Do you have a username and favourite password combination that you tend to use on most of your accounts to make life easier? If just one of your accounts becomes compromised (and you might never know) your username/ password combination can be stolen. Attackers have lists of compromised username/passwords combinations and this enables them to try and access any account where that combination works. If you use different passwords for different systems, one compromised password does not mean that attackers can then get onto all your systems.

Sharing is not caring

Sharing usernames and passwords is not a good idea. If one of the users did something which was not allowed, it would not be possible to determine who it was or even if it was an authorised user. When organisations want to share user accounts the software or the processes can be changed to achieve the same result safely without actually sharing accounts. This makes the organisation more secure.

Password processes

The following ways can help your employees create stronger, more secure passwords:

- Educating people on how to avoid common or discoverable passwords, such as a pet's name, common keyboard patterns or passwords they have used elsewhere. This could include teaching people to use the password generator feature built into some password managers
- Encouraging people to choose longer passwords. This can be done by promoting the use of three or more random words to create a password [How to create passwords using three random words](#)

- Providing usable secure storage for passwords (for example a password manager or secure locked cabinet) with clear information about how and when it can be used. [How to use a random generated password from a password manager](#)
- Not enforcing regular password expiry
- Not enforcing password complexity requirements

Keep passwords safe from brute-force attacks

Brute force attacks use computers to target a login page where they try many different combinations of characters until the correct combination is found to crack the password. Depending on the length and complexity of the password, cracking it can take anywhere from a few seconds to many years.

Using a long password is a good way to protect your data from a brute-force attack. A password that is created by a password manager or three random words can be used to achieve this.

Implementing **at least one** of the following measures can help protect your passwords against brute-force password guessing:

- Using multi-factor authentication
- 'Throttling' the rate of attempts. This means the time the user must wait between attempts increases with each unsuccessful attempt. This should permit no more than 10 guesses in 5 minutes or the minimum that the device allows
- Locking accounts after no more than 10 unsuccessful attempts or the minimum that the device allows

Password policy

Make the rules clear by having a password policy that details the process for creating passwords for all work accounts. This applies to everyone in the organisation including contractors.

A password for a work account must include **one** of the following:

- Using a password of at least 8 characters long (with no maximum length) and multi-factor authentication
- Accounts protected by a password alone need to ensure that the password has at least 12 characters (with no maximum length)

- A minimum password length of at least 8 characters with no maximum length restrictions and use automatic blocking of common passwords using a *deny list.

*An automatic deny list will block users from using passwords that are on a pre-configured list of common passwords that have been breached. Organisations can create a deny list from a file of the [100,000 most commonly breached passwords](#) compiled by the NCSC.

Additionally:

- Have an established process to change passwords promptly if someone knows or suspects their password or account has been compromised
- Enable MFA on all administrator accounts and all accounts (user and administrator) that are accessible from the internet (cloud services)

Turn on multi-factor authentication

Multi-factor authentication (MFA) requires the user to have one or more types of credentials in addition to a password, before being able to access an account. Businesses have a choice of several different methods that they can use for multi-factor authentication.

- **A trusted device:** MFA techniques that use a trusted device can rely on the knowledge that a user possesses a specific device (e.g a company computer) to prove they are who they say they are. Organisations can configure cloud services to only accept authentication attempts from within their trusted enterprise networks. This ensures that users can only authenticate if they are either directly connected to that trusted network or have remote access to it over a virtual private network (VPN). In addition, or as an alternative to using a VPN, remote workers would be able to access online services only on trusted devices that are managed by the organisation.
- **An application:** An authenticator app generates a single-use password that changes every minute. Alternatively, an app can receive push notifications that prompts the user to confirm or deny that they are currently trying to log in to a named service.
- **A physically separate token:** These techniques use the knowledge that a user has a physical security token, which proves they are who they say they are. Some types will require the user to unlock them before use, others just require proof of possession.

Examples of physically separate tokens are [FIDOuniversal2nd factor](#) authenticators such as YubiKey, Smartcards that are unlocked by a PIN code, and devices such as RSA tokens and chip-and-PIN card readers which generate a single-use code each time a user logs in.

- **A known trusted account:** These techniques send codes to a registered email address or phone number.

The service sends an SMS message containing a single-use code or makes a voice call in which a single-use code is read out to the phone number registered for that user. An SMS message is not the most secure type of MFA, but still offers a huge advantage over not using any MFA. Alternatively, the service will email a single-use code to an address registered for that user. A code for the user to type in is preferable to a clickable link, as it is difficult for a user to distinguish between a legitimate email and a phishing email.

Turn on multi- factor authentication.

Whether an attacker acquires your password via a phishing attack, stolen credentials from another breach or manages to crack it using a brute force attack, if you have MFA enabled, this will be your safeguard. As soon as the account asks for the MFA, the attacker will be thwarted and unable to access. It makes sense to turn on MFA for as many accounts as you can where available.

Based on studies conducted by Microsoft, your account is more than 99.9% less likely to be compromised if you use MFA.

The five controls of Cyber Essentials are:

- **User Access Control**
- Security Updates
- Secure Configuration
- Malware Protection
- Firewall and Routers

Help and support

There are over 300 specially trained cyber security companies around the UK who are licensed to certify against the Government's Cyber Essentials Scheme. They can offer help and support in preparation for the assessment. [Find one near you.](#)

For questions and feedback about the Cyber Essentials scheme, contact IASME at info@iasme.co.uk or Tel: 03300 882 752