# Further information

You can find further information online that will help you secure your IT against cyber attack.

**www.cyberessentials.ncsc.gov.uk**
**www.ncsc.gov.uk/smallbusiness**
**www.ncsc.gov.uk/charity**
**www.ncsc.gov.uk/guidance/10-steps-cyber-security**

National Cyber
Security Centre
a part of GCHQ

CYBER ESSENTIALS

# Cyber security for your organisation starts here

## Five technical controls that you can put in place today, explained without jargon

National Cyber Security Centre

a part of GCHQ

# What is Cyber Essentials?

Cyber Essentials is a simple but effective, Government backed scheme, created to help you protect your organisation against a range of the most common cyber attacks.

Cyber attacks come in many shapes and sizes, but the vast majority are very basic in nature, carried out by relatively unskilled individuals.

We advise the use of five technical controls, specifically designed to prevent these attacks, which include malware, ransomware and phishing.

## The five technical controls:

CYBER ESSENTIALS

# 1 Use a **firewall** to secure your Internet connection

You should protect your Internet connection with a firewall. This effectively creates a 'buffer zone' between your IT network and other, external networks. In the simplest case, this means between your computer (or computers) and 'the Internet'. Within this buffer zone, incoming traffic can be analysed to find out whether or not it should be allowed onto your network.

## Two types of firewall

You could use a personal firewall on your internet connected laptop (normally included within your Operating System at no extra charge).

Or, if you have a more complicated set up with many different types of devices, you might require a dedicated boundary firewall, which places a protective buffer around your network as a whole.

Some routers will contain a firewall which could be used in this boundary protection role. But, this can't be guaranteed – if you can, ask your internet service provider about your specific model.

Cyber Essentials Certification requires that you configure and use a firewall to protect all your devices, particularly those that connect to public or other untrusted Wi-Fi networks.

# 2 Choose the most **secure settings** for your devices and software

Manufacturers often set the default configurations of new software and devices to be as open and multi-functional as possible. They come with 'everything on' to make them easily connectable and usable. Unfortunately, these settings can also provide cyber attackers with opportunities to gain unauthorised access to your data, often with ease.

## Check the settings

So, you should always check the settings of new software and devices and where possible, make changes which raise your level of security. For example, by disabling or removing any functions, accounts or services which you do not require.

## Use passwords

Your laptops, desktop computers, tablets and smartphones contain your data, but they also store the details of the online accounts that you access, so both your devices and your accounts should always be password-protected. Passwords – when implemented correctly – are an easy and effective way to prevent unauthorised users accessing your devices. Passwords should be easy to remember and hard for somebody else to guess. The default passwords which come with new devices such as 'admin' and 'password' are the easiest of all for attackers to guess.

So you must change all default passwords before devices are distributed and used. The use of PINs or touch-ID can also help secure your device. If you would like more information on choosing passwords, look at the NCSC's password guidance.

## Extra Security

For 'important' accounts, such as banking and IT administration, you should use two-factor authentication, also known as 2FA.

A common and effective example of this involves a code sent to your smartphone which you must enter in addition to your password.

Cyber Essentials Certification requires that only necessary software, accounts and apps are used. If you would like more information on choosing passwords, search www.ncsc.gov.uk for 'password'.

# 3 Control **who has access** to your data and services

To minimise the potential damage that could be done if an account is misused or stolen, staff accounts should have just enough access to software, settings, online services and device connectivity functions for them to perform their role. Extra permissions should only be given to those who need them.

## Administrative accounts

Check what privileges your accounts have – accounts with administrative privileges should only be used to perform administrative tasks. Standard accounts should be used for general work. By ensuring that your staff don't browse the web or check emails from an account with administrative privileges you cut down on the chance that an admin account will be compromised. This is important because an attacker with unauthorised access to an administrative account can be far more damaging than one accessing a standard user account.

## Access to software

Another simple and effective way to ensure your devices stay secure and malware-free is to only use software from official sources. The easiest way to do this is to only allow your users to install software from manufacturer-approved stores, which will be screening for malware. For mobile devices, this means sources such as Google Play or the Apple App Store.

Cyber Essentials Certification requires that you control access to your data through user accounts, that administration privileges are only given to those that need them, and that what an administrator can do with those accounts is controlled.

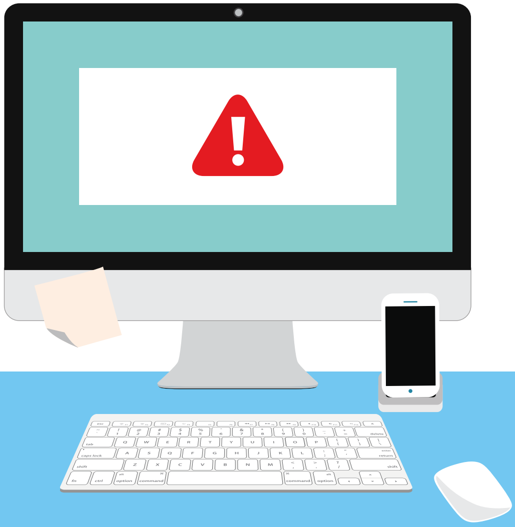
# 4 **Protect yourself** from viruses and other malware

Malware is short for 'malicious software'. One specific example is ransomware, which you may have heard mentioned in the news. This form of malware makes data or systems it has infected unusable – until the victim makes a payment.

Viruses are another well-known form of malware. These programs are designed to infect legitimate software, passing unnoticed between machines, whenever they can.

## Where does malware come from?

There are various ways in which malware can find its way onto a computer. A user may open an infected email attachment, browse a malicious website, or use a removable storage drive, such as a USB memory stick, which is carrying malware.



## How to defend against malware

- **Anti-malware measures** are often included for free within popular operating systems. For example, Windows has *Defender* and MacOS has *XProtect*. These should be used on all computers and laptops. For your office equipment, you can pretty much click 'enable', and you're instantly safer. Smartphones and tablets should be kept up to date, password protected and where possible, you should turn on the ability to track and erase lost devices. If you can avoid connecting to unknown Wi-Fi networks, this will help to keep your devices free of malware too.
- **Whitelisting** can also be used to prevent users installing and running applications that may contain malware. The process involves an administrator creating a list of applications allowed on a device. Any application not on this list will be blocked from running. This is a strong protection as it works even if the malware is undetectable to anti-virus software. It also requires little maintenance.
- **Sandboxing**. Where possible, use versions of the applications that support sandboxing. For instance, most modern web browsers implement some form of sandbox protection. A sandboxed application is run in an isolated environment with very restricted access to the rest of your device and network. In other words, your files and other applications are kept out of reach, if possible.

Cyber Essentials Certification requires that you implement at least one of the approaches listed above to defend against malware.

# **5** Keep your devices and **software up to date**

No matter which phones, tablets, laptops or computers your organisation is using, it's important they are kept up to date at all times. This is true for both Operating Systems and installed apps or software. Happily, doing so is quick, easy, and free.

## Also known as 'Patching'

Manufacturers and developers release regular updates which not only add new features, but also fix any security vulnerabilities that have been discovered.

Applying these updates (a process known as patching) is one of the most important things you can do to improve security. Operating systems, programmes, phones and apps should all be set to 'automatically update' wherever this is an option. This way, you will be protected as soon as the update is released.

However, all IT has a limited lifespan. When the manufacturer no longer supports your hardware or software and new updates cease to appear, you should consider a modern replacement.

Cyber Essentials Certification requires that you keep your devices, software and apps up to date.

# Conclusion and Checklists

Once you have taken the time to investigate and put them in place, these five basic controls will put you and your organisation on the path to better cyber security.

Cyber Essentials Certification should be your next target, but you can work towards that goal at a pace which suits you.

In the meantime, you can check how much progress you've already made by completing the handy checklists laid out below.

### 1. Use a firewall to secure your internet connection

□ Understand what a firewall is

□ Understand the difference between a personal and a boundary firewall

□ Locate the firewall which comes with your operating system and turn it on

□ Find out if your router has a boundary firewall function. Turn it on if it does.

### 2. Choose the most secure settings for your devices and software

□ Know what 'configuration' means

□ Find the Settings of your device and try to turn off a function that you don't need.

□ Find the Settings of a piece of software you regularly use and try to turn off a function that you don't need

□ Read the NCSC guidance on passwords

□ Make sure you're still happy with your passwords

□ Read up about second factor authentication

### 3. Control who has access to your data and services

□ Read up on accounts and permissions

□ Understand the concept of 'least privilege'

□ Know who has administrative privileges on your machine

□ Know what counts as an administrative task

□ Set up a minimal user account on one of your devices

### 4. Protect yourself from viruses and other malware

□ Know what malware is and how it can get onto your devices

□ Identify three ways to protect against malware

□ Read up about anti virus applications

□ Install an anti-virus application on one of your devices and test for viruses

□ Research secure places to buy apps, such as Google Play and Apple App Store

□ Understand what a 'sandbox' is

### 5. Keep your devices and software up to date

□ Know what 'patching' is

□ Try to set the operating system on one of your devices to 'Automatic update'

□ Try to set a piece of software that you regularly use to 'Automatic update'

□ List all the software you have which is no longer supported