British Assessment Bureau


# Cyber Essentials Handbook

# Table of contents

39% of UK businesses reported a cyber attack in 2022.

Out of the businesses that identified an attack, the most common was Phishing (see page 15).

Out of the 39%, around 1 in 5 identified a more sophisticated attack such as denial of service, malware and ransomware.

Cyber attacks are becoming more prominent in the world we live in, with companies looking for cost-effective and efficient ways to protect their data.

Cyber Essentials provides the evidence that you have actions in place to protect your business from cyber attacks.

## Cyber Essentials helps you to guard your organisation against cyber attacks.

# Cyber Essentials

## What is Cyber Essentials?

Cyber Essentials is an effective, government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

## Why should you get it?

There is a multitude of benefits for Cyber Essentials, they are, but are not limited to:

- Reassure customers that you are working to secure your IT against cyber attack
- Attract new business with the promise you have cyber security measures in place
- You have a clear picture of your organisation's cyber security level
- Some government contracts require Cyber Essentials certification

CYBER ESSENTIALS

# 6 Steps
## to success

## 1. Firewall

**Two types of firewall**
You should protect your Internet connection with a firewall. This effectively creates a ‘buffer zone’ between your IT network and other, external networks. The two main types are:

- **Dedicated boundary firewall** which protects their whole network.
- **Personal firewall** on your internet connected laptop or computer.

## 2. Settings

**Check the settings**
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.

# 3. Passwords

**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 are an easy and effective way to prevent unauthorised users accessing your devices.

**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.

# 4. Access

**Administrative accounts**
Check what privileges your accounts have - accounts with administrative privileges should only be used to perform administrative tasks.

**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.

We would love to have the opportunity to help you with your ISO certification or even just help you and your team to learn about ISO 27001.
Either way, we're keen to hear from you:

# 5. Protect

**Designed to cause harm**
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 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. These should be used on all computers and laptops.
- **Allowed list** can also be used to prevent users from installing and running applications that may contain malware. The process involves an administrator creating a list of applications allowed on a device.
- **Sandboxing** is an application run in an isolated environment with restricted access to the rest of your device and network. In other words, your files and other applications are kept beyond the reach of malware, if possible.

# 6. Up to date

**Keep devices up to date**
No matter which phones, tablets, laptops or computers your organisation is using, it's important that the manufacturer still supports the device with regular security updates and that you install those updates as soon as they are released. This is true for both Operating Systems and installed apps or software. Happily, doing so is quick, easy, and free.

**Lifespan**
However, all IT has a limited lifespan. When the manufacturer no longer supports your hardware or software and new updates cease to appear, you must replace it with a supported product if you wish to stay protected.

# Cyber Essentials Certification

To start your process contact us for a Cyber Essentials quote.

Cyber Essentials Certification requires that you implement at least one of the three malware defence approaches which are:

- Antivirus.
- Only download Apps from manufacturer approved stores.
- Apps and programs can be run in a ‘sandbox’. This prevents them from interacting with, and harming, other parts of your devices or network.

## Next steps

**Identify requirements**
Assess the status quo using the six steps to success (also referred to as critical security controls).

**Develop a cyber security policy**
Identify existing weaknesses in your security and determine where you are now and where you need to be. Create a set of initiatives to address the high-priority risks and control gaps.

**Plan and implement**
The gap analysis focuses on identifying a set of actions and best practices for implementing and administering improvements and testing success.

**Complete and submit a self-assessment questionnaire for the audit**
Whether you can complete your self-assessment questionnaire independently, we can offer Cyber Essentials, Cyber Essentials Plus or a package of both to suit your budget, timeframe and level of experience.

Get a Quote

CYBER ESSENTIALS

# Cyber Essentials Plus Certification

Cyber Essentials Plus is awarded to organisations when the evidence provided in **their basic Cyber Essentials** self-assessment is audited through a series of vulnerability tests. You **MUST** complete Cyber Essentials Plus within 3 months of your Cyber Essentials completion.

We offer a Cyber Essentials & Cyber Essentials Plus package or Cyber Essentials Plus service on receipt of a valid Cyber Essentials certificate. Our experienced assessors will work in partnership with you and offer pragmatic support to help you achieve certification quickly, whilst minimising impact on your internal resource.

**Key Cyber Essentials PLUS Benefits:**

- Reassure your stakeholders that the IT security measures you have put in place to safeguard your services and data meet the UK Government benchmark and have been externally audited
- Displaying the Cyber Essentials Plus mark provides you with a competitive advantage when attracting and retaining customers
- Cyber Essentials Plus is a key requirement for Government, Defence and Critical National Infrastructure sector contracts
- A growing number of Commercial sector organisations are now stipulating that their supply chain has Cyber Essentials Plus in place.

The Cyber Essentials Plus audits can be conducted 100% remotely whilst individuals work from home.

**Get a Quote**

CYBER ESSENTIALS PLUS

# Jargon Buster

## A

### Adware

Adware (short for advertising software) is unwanted software whose sole purpose is to display adverts to generate money for the author. Whilst adware doesn't often do damage, it is normally installed either without the user's permission or through deceptive means.

### Antivirus

Antivirus software tries to find and neutralise any viruses or malicious software (Malware) that may be on computers or smartphones. Example products include Kaspersky, McAfee, and AVG.

### Authentication

Authentication is the process of confirming that you are whom you say you are, for example by using a password (something that only you should know). Other methods include biometric checks such as a fingerprint scan, or proximity cards at doors.

## B

### Biometrics

Biometrics are a way of proving your identity (see Authentication above) based on a physical aspect of yourself. Examples include fingerprint recognition, facial recognition, iris scans, and gait (or walking) analysis. Other methods are being developed too, such as your typing pattern which, it has been suggested, could one day remove the need for passwords.

### Botnet

A botnet is a collection of (often thousands of) computers that a criminal has under their control. They're often used to send out spam emails, to attack websites as part of a DDoS (Page 12) attack, or sometimes (with their combined computing power) to crack passwords. Computers join botnets without the owner even knowing, normally after being infected with a virus such as through a phishing email.

# Jargon Buster

**Browser**
An internet browser is software that you use to access the internet. Common browsers include Microsoft Edge (or previously Microsoft Internet Explorer), Apple Safari, Mozilla Firefox, Opera, and Google Chrome.

**Brute force**
Brute force is the process of trying every possible password combination until the correct one is found, from "**a**" all the way up to "**zzzzzzzzzzz**" (and beyond!).

## C

**Cloud computing**
The "Cloud" has become a very popular term in computing over recent years. Essentially it means a remote computer doing many of the tasks that you typically used to do on your home computer, for example using it to backup data or to run software such as Google Docs. Many companies are using the cloud too, using it to host data and services that they would typically keep on their own powerful in-house computers.

**Cookies**
Cookies (not the edible type!) are small text files that are stored in your browser and which are key to the normal working of the internet. They help websites to remember who you are, what pages you looked at when you last visited, or to keep track of your shopping basket.

**Cryptography**
Cryptography is a special branch of mathematics that scrambles data into unreadable forms. This might not sound useful but is in fact fundamental to many aspects of the internet today. It's used for keeping data private, checking that data has been transmitted correctly, and verifying identity, and it can help ensure that people or computers can't deny carrying out certain actions. Both encryption and hashing are forms of cryptography.

# Jargon Buster

## D

**Denial of Service attack ("DoS" or "DDoS")**

A Distributed Denial of Service attack ("DoS" for short) is when an attacker bombards a website with so much traffic that it buckles under the strain & stops working. These attacks are often carried out by multiple computers as part of a botnet, leading to the term Distributed Denial of Service attack (or "DDoS"). Criminals will often use these attacks as part of a blackmail campaign to extort money from companies who rely on their website being up and running or to mask other hacking activity at the same time. A DDoS attack, despite what is often reported in the media, is not a form of hacking since it doesn't involve breaking into websites; it simply involves overwhelming them with too much traffic.

**Dictionary Attack**

A Dictionary Attack is a method used by hackers to find passwords, by running down a list of dictionary words until a match is found. They'll often combine words in common pairs too (such as "ManchesterUnited"), make common letter substitutions (such as a 1 for i), or add numbers to the end. Modern computers allow billions of passwords to be tried each second, making it possible to find the most common passwords in fractions of a second.

## E

**Encryption**

Encryption is the process of converting a piece of data into an unreadable format that can only be recovered with the knowledge of a secret key. It's a form of cryptography that uses some complex mathematics to ensure it's unbreakable. Encryption is used in many parts of our daily lives, from making sure that our online banking can't be intercepted to protecting conversations over email or Skype. Common encryption algorithms include RSA and AES.

# Jargon Buster

## F

### Firewall

A firewall is a piece of software (or within large organisations, a physical device itself) that can analyse the internet traffic flowing into and out of your computer to try to detect (and stop!) anything that's unauthorised.

## H

### Hash

A hash is an output from a special mathematical process which jumbles data up in an unrecoverable manner. The hashing process has several key properties, such as being repeatable (the same input always gives the same output) and non-reversible. Hashes have many uses in computing, for example, to store, to compare files to see if they're identical, as well as other uses in security. A typical hashing algorithm is SHA-256.

### HTTPS

You might see HTTPS appearing in the address of a website that is encrypting your data as you send it (the "s" in https stands for "Secure"). If you're logging into a website or sending any sensitive data, such as credit card information, you should always check first that the site uses https (and not just http without the s).

## I

### Internet

The internet is a global computer network connecting millions of computers to each other and allowing information to be shared. Borne out of research done in the 1960s by the US military, it has since come to define modern life today. No single organisation owns or runs the internet, however, many organisations play key roles such as ICANN, the Internet Architecture Board (IAB), as well as your internet service provider (ISP). Email, the web, and many of the apps that you use on your phone all sit on top of and make use of the internet.

# Jargon Buster

## K

### Keylogger

A Keylogger is an (often malicious) program that silently records all the keys you type on your keyboard, including any passwords you might type. Keyloggers can exist either as a form of malware, or (for more sophisticated and targeted attacks) as a physical device that's plugged into your keyboard.

## M

### Malware

Malware is an all-encompassing name for different types of malicious software. There are many different forms of malware, all with different purposes and methods of spreading. They include viruses, worms, ransomware, rootkits, keyloggers, spyware, adware and trojans, amongst others. Despite its name, antivirus software will catch all types of malware - not just viruses.

## P

### Password

A password is a series of letters, numbers, and symbols, that should only be known to one person and which is used to verify their identity. They are the most common form of authentication in use today but have many weaknesses, such as being easy to steal (for example by viruses) and not always being easy to remember (especially when you have a lot to remember).

### Password hash

A password hash is, as the name suggests, a hash of a password. It's the output of a mathematical process that scrambles the password such that it can't be recovered, but it still allows for checking that a user has entered the correct password. Examples of dedicated password hashing algorithms include PBKDF2 and bcrypt.

# Jargon Buster

**Password manager**
Password managers are used to store your passwords in a safe and secure place, so you don't have to remember them all. They can automatically create super-strong passwords, log you into websites, and store other details such as payment options as well.

**Phishing**
Phishing is a form of social engineering that tries to deceive users into entering their login details into a spoofed website (such as one that imitates their bank or one claiming to be from a shop you've bought from), or that spreads viruses through infected attachments. These attacks normally arrive by email but can also come via a text message or phone call.

## R

**Ransomware**
Ransomware is a vicious and aggressive form of malware that has become more popular in recent years. When activated on your computer it makes all files unreadable and, in some cases, destroyed until a ransom fee is paid.

**Rootkits**
A rootkit is a type of malicious software (malware) that tries to avoid detection by burying itself in your computer to do damage unnoticed. Despite its name, anti-virus software will look for and try to catch all types of malware including rootkits - not just viruses.

## S

**Social Engineering**
Social Engineering is also referred to as conning/fooling someone. These types of attacks can include but aren't limited to, phishing emails, attackers blagging their way into company offices to steal documents, as well as fraudsters on the phone.

# Jargon Buster

**Spear-phishing**
Spear-phishing is a highly targeted phishing attack. Whilst most phishing emails are sent to hundreds of thousands of people at a time, spear phishing emails are highly personalised by the criminals who have spent time researching their victims. These types of attacks are often sent to high-ranking business members asking for an invoice to be paid or as an attachment.

**Spyware**
Spyware (short for spy software) is a form of malware that spies on a computer user without them knowing. This often views your login details, websites you visit as well as your payment information if you buy something.

**SSL**
You might occasionally see websites claiming to be secure because they use "SSL". This is a method by which websites encrypt data as it's sent between your browser and the website, keeping it safe from prying eyes. Websites that use ‘http’ at the beginning of their web address often have this. SSL is an old technology that has been replaced by something called TLS, however, the use of SSL has become so common that the acronyms SSL and TLS are often used together.

## T

**TLS**
See SSL

**Trojan**
A trojan is a type of malicious software that acts as if it’s a normal piece of software. Examples include fake antivirus programs or malicious online games. Trojans can do all sorts of damage, from encrypting all your data and only releasing it for a ransom fee, to stealing data such as passwords, and financial information. Despite its name, anti-virus software will catch all types of malware including trojans - not just viruses.

# Jargon Buster

## V

**Virus**

A virus is a type of malicious software ‘malware’ that can do damage to your computer or steal information, such as credit card details. They often get onto your computer through infected emails or unsafe websites.

**Virus Definitions**

Virus Definitions (sometimes called Virus Signatures) are a way an antivirus can work out if you have a virus or not. It is seen as a ‘Virus Fingerprint’ helping the antivirus find the viruses.

## W

**WiFi**

WiFi is a technology that allows you to connect your devices to the internet. As well as being common in homes, restaurants, airports, hotels and other public places, WiFi is something very common in the modern world.

**World Wide Web (or "web")**

The web, as we know it today, is a series of websites allowing us to discover almost limitless information, purchase products, or do online banking. It is one of the most used aspects of the internet, and from the first website going live on August 6th 1991 (saved for posterity at info.cern.ch it has since exploded to around 2 billion websites today.

**Worm**

A worm is a type of malicious software ‘malware’ that can automatically spread from computer to computer, dropping off viruses and trojans as it goes. Worms can spread incredibly quickly - in 2003 the SQLSlammer worm infected 75,000 computers in just 10 minutes! Despite its name, anti-virus software will catch all types of malware including worms - not just viruses.

## Head Office

30 Tower View,
Kings Hill,
West Malling,
Kent ME19 4UY

## Contact Us

salesteam@british.assessment.co.uk

0800 404 7007

## Website

british-assessment.co.uk



British Assessment Bureau