MFA Explained for Non-Technical UK Business Owners

Why Passwords Alone Are No Longer Enough

- Digital technologies are the backbone of every modern company today, from email to cloud storage to software for accounting.
- However, too many businesses rely solely on usernames and passwords as their only way to secure these systems. Passwords alone cannot adequately protect your business account any more.
- Too often, employees use the same password across different websites and online services. This means that when one of those services gets compromised, hackers will attempt to take advantage of the stolen information by trying to log into your business system.
- Another common way for hackers to steal passwords is through phishing emails. A hacker sends an email that looks legitimate but actually takes you to a fake website where you enter your username and password. Once a criminal has that password from you, they can log into your company's system just as you would.
- If that happens, the hacker could complete have access to your company's email account, steal files, commit forensic fraud and gain the trust of your clients and vendors.
- By implementing Multi-Factor Authentication (MFA), organisations are providing a greater level of security to their online accounts.
- Organisations with MFA enabled make it significantly more difficult for an attacker to gain unauthorised access to their systems.

What MFA Actually Means

Multi-Factor Authentication (MFA) refers to a type of security measure, in which an account can only give access based on showing multiple layers of authenticity, (meaning, that an individual can't just log into an account via a password).

In addition to entering your password when you want access, the system will also verify your identity by requiring another kind of verification.

Typically, security analysts have broken authentication into three branches:

1. What You Know

This is generally memory-based identification; examples include:

- Passwords
- PINs
- Security questions

This is the most typical form of authentication used by traditional log-in systems, in order to gain access.

2. What You Have

This is a physical, identifying device that you own. Examples of this type of device include:

- A mobile device (ex, a smartphone)
- An app used for authentication
- A physical security token
- A device that receives your verification codes.

In this situation, the company that you're trying to log in to, must see before you log into your account, that you have this type of device.

3. What You Are

This is a biometric measure of authentication. Examples of this type of identification include:

- Fingerprint scans
- Facial scans
- Voice scans

Most types of "smartphones" and "laptops" on the market at this time already support these types of authentication.

By combining these two types of authentication with each other, the security of your log-in is greatly increased.

If someone tried to hack into your account by using just your password, they would not be successful because they would have no other way to authenticate who they are using your password.

How MFA Works (Simple Explanation)

MFA has a simple process.

Let’s take an example to illustrate the process.

- The employee enters his/her username and password.
- Then the system requests another piece of verification.
- A notification pops up on the employee's mobile device or Authentication App.
- The employee approves the login or enters a separate verification code.
- The employee is granted access to his/her account.

Typically, this second factor of identification takes only minutes to complete.

Despite the short amount of time it takes to use MFA, it dramatically decreases the likelihood of someone gaining unauthorised access to your account.

For example, if someone were to successfully steal your password, they could not log into your account without also having your second factor of identification.

Passwords vs Two-Factor Authentication vs MFA

Many people confuse these terms, but they do have some key differences.

Password-Only Logins

This is the traditional method people have used to access computers/phones for many years.

If someone enters a correct password, then he/she can gain access to that machine or phone.

However, this is a very weak protection against unauthorised access, particularly if someone gets their hands on your password.

Two-Factor Authentication (2FA)

Examples of this could be:

- an internal password
- a code sent to my phone.

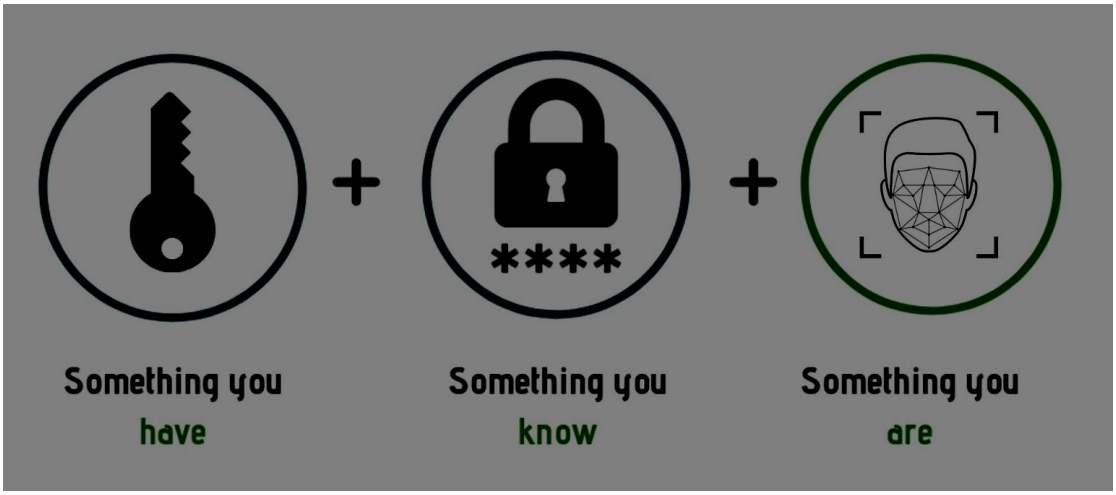
The vast majority of online applications, have the option of using this type of two-factor check.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) are systems that use two or more authentication methods.

Most Multi-Factor Authentication (MFA) today use two steps, but the terminology allows for other means of authentication, such as biometrics or security keys.

In daily normal business use, 2FA and MFA are often used synonymously.



Why MFA Is Essential for Modern Businesses

Small and Medium Enterprises are more frequently targeted by cyber criminals.

This is due to the fact that SMEs typically hold sensitive information, but don't always have the same level of security resources as larger corporations.

Email accounts are only one example of how easy it is for criminals to gain access to an SME's email system. Once the hacker accesses an employees email account, they can perform many different actions, including:

- Monitoring communications
- Sending fake emails
- Requesting payment from other customers

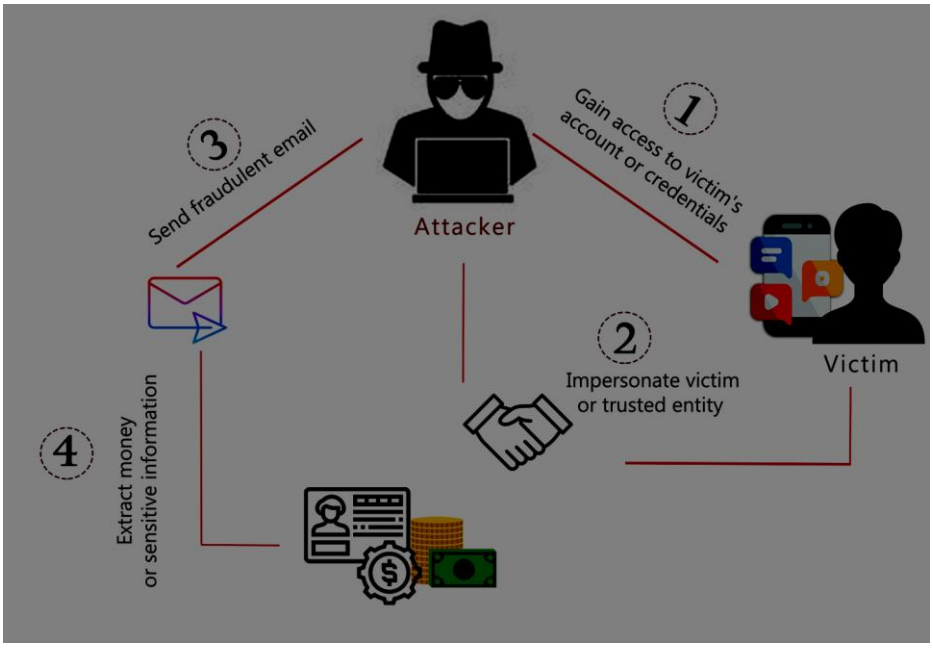
- Resetting other system passwords.

Multi-Factor Authentication significantly lowers the possibility of a successful attack.

Even if an employee password has been breached, the hacker will still need to obtain a secondary method of verification.

This simple and effective security measure will help protect a significant proportion of the most common types of cyber attacks.

MFA can also demonstrate and provide assurance to UK-based business continuity and expose UK companies to civil liability if the MFA is not implemented.



Common MFA Methods Explained Simply

MFA can be used in a number of ways by companies throughout industries.

Most platforms allow companies the flexibility to choose what works best for them and their employees.

Authentication Applications

An authentication app is a program that generates one-time login codes or provides users a means to approve requests from the user wanting to log in.

When the employee attempts to log in, the app will send a notification that they need to verify the request.

These apps are widely used and provide a high degree of security.

SMS Verification

Some systems send a single-use code via SMS.

In order for the user to log in, they enter this code.

This method is simple, but might not be as secure as an app because sometimes SMS text messages can be intercepted before they arrive at the intended device.

Email Verification

Some systems send a verification code to an email address.

This is often used as an (admin) backup method of authentication.

Hardware Security Keys

A hardware security key is a small physical device that is used for identifying yourself to gain access to an administrator-level account when logging onto a device.

The employee either connects the device to the device they are logging on to or taps it against their phone for identification purposes.

These keys are very secure and are typically used only for administrative account access.

Biometric Authentication

Biometric authentication is a form of authentication that uses factors associated with a person's physical being (e. g., fingerprints or facial recognition).

Many modern day smartphones and computers now have an integrated form of biometric authentication.

Biometric verification methods are typically faster and easier to use than traditional methods of authentication.

Common Mistakes Businesses Make with MFA

Some examples of common errors are:

- Not creating MFA for all employees
- Not securing administrator accounts with MFA
- Allowing staff to bypass MFA
- Not offering alternative methods of authentication
- Employees approving suspicious requests for logins
- Using weaker authentication methods where stronger methods are available

Companies should communicate with their employees to remind them that verification codes should not be shared with anyone.

MFA Setup Checklist

- Identify critical business systems
- Enable MFA on email accounts
- Enable MFA on cloud platforms
- Protect admin accounts
- Select authentication method
- Training of employees to use MFA

Accounts That Should Always Use MFA

- Business Email Accounts
- Admin Accounts
- Cloud Platforms
- Financial Software
- Remote Access Tools

FAQs

1. **Is MFA user friendly for employees?**

Most employees are able to adapt quickly. It usually only takes several seconds longer than normal to log in.

2. **Does MFA slow down employee productivity?**

MFA should minimally impact productivity due to the additional login step, but it will greatly increase your company's overall security.

3. **Is my organisation safe by using SMS as the MFA method?**

Using SMS as your MFA method is definitely better than no MFA, but the best methods remain the authentication app and/or security key.

4. **What happens should an employee lose their mobile device?**

Most systems offer a backup authentication option or can reset via an administrator.

5. **Should all business accounts have MFA?**

All accounts that store business data or allow access to systems should be required to follow the MFA process.

About This Guide

The **Computer Support Centre** put together this multi-facotr Authentication (MFA) document aimed specifically at non-technical business owners in the UK. The goal of this document is to explain MFA in a manner that is straightforward and practical so that both business owners & managers understand how MFA protects their business systems from the cyber threats that exist today, and also to detail what steps can be taken to implement it across common company systems such as e-mail, cloud systems, financial software, remote access applications, etc.

This MFA document contains many simple examples, and practical checklists that will allow organisations to take concrete steps to boost their cyber security, and ultimately minimise the chance of unauthorised access to company information.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
 https://computersupportcentre.com

Conclusion

In the current digital landscape of business, depending on just a single form of authentication, such as passwords alone, isn't sufficient any more to secure sensitive information and/or systems. Cyberthieves frequently focus their efforts on targeting small and mid-sized businesses due to their lack of proper security systems.

Multi-Factor Authentication (MFA), provides an extra level of protection since in order for you to successfully authenticate to an account, you will have to provide at least two different types of proof that you are who you say you are (e.g., a password alone isn't enough). When using MFA, it decreases the chance for unauthorised access due to the second type (or more) of identification method.

Enabling MFA on critical systems (like email, cloud services, financial software, and admin accounts), will improve the overall security profile of an organisation tremendously. Installing MFA is an easy yet highly productive method to help safeguard company data, maintain customer confidence, and support a safer work environment day-to-day for staff and customers alike.