Multi Factor Authentication (MFA)

Multi-factor authentication (MFA) is the process of needing more than one piece of information to login to a secure website or service. In traditional systems, all you need to know to gain access to an IT system, is a username and password, data that can easily be hacked or stolen.

MFA introduces a second component, often a PIN code that can only be generated by a mobile phone or an access token, meaning that for a malicious user to gain access to a system, they would need to steal not only your password information, but also your mobile device – making it signicantly harder to hack. MFA isn't really new; we've been doing it at cashpoints for decades – to get money from your bank you have always needed both your password (your PIN) as well as the associated bank card.

The three stages of MFA

There are generally three recognised types of authentication factors:

Something you know:

Usually passwords or PIN numbers and the more complicated the better, but anything you need to remember falls into this category.

Something you are:

Use of a biometric feature, such as ngerprints, facial recognition or voice recognition. If you're using a mobile app as part of your MFA, the fact that the device itself needs to be unlocked using a thumb print or facial recognition,has added an additional factor in the process to access your data.

Something you own:

Using a code that is sent to a separate device to the one you're logging on to, covers off the third factor. In most cases, MFA involves the sending of a time limited code as either a text message or mobile app on a mobile device enrolled by your organisation to receive the code.

So, by implementing an MFA system that requires a code to be inputted before access to a database for example, your users need to know their login details, their password, use their thumbprint to open their phone and have the enrolled phone in their possession. A true Multiple Factor process of authenticating access.

ramsac
the secure choice

Why are organisations using MFA

Passwords are such a weak link when it comes to security, users often use the same password over multiple systems, they are often not complicated enough and not changed frequently enough.

Increasingly, more and more businesses are storing information in the cloud, Office365, SharePoint, Box, Google Drive etc are all fairly common place, and whilst previously users needed a VPN to access company data, access is now much more straight forward. This has led to a signicant increase in cybercrime with criminals focussed on stealing email addresses and passwords.

When users so frequently use similar passwords, you could soon find that a data breach with a national online retailer for example, exposes information about you that a criminal could easily then use to gain access to your organisations cloud file storage. With passwords as the only security measure hackers find it easy to impersonate the victim, and organisations are left vulnerable to a cyber-attack.

With MFA there is a signicant decrease in the chance of user (and, subsequently, an organisations) data being compromised. By adding additional authentication measures cybercriminals (even when they have the right password) cannot get past the extra levels of security.

What to consider when implementing MFA

Needs Analysis
It is vital for an organisation to understand the way that all users work and access data prior to choosing a multi-factor authentication method.

User training and adoption
User training is important to ensure users understand the new way of working and do not have a negative experience when using MFA. This can be difficult to manage as passwords are still present and now in addition to managing these, users have to manage the extra security measures. But by explaining the importance behind the additional security measures, cybersecurity awareness across the organisation will also increase.

Time and resources
MFA implementation takes planning and training because you need to ensure you have not only researched the needs of the organisation but also the most appropriate solution for your organisation and how best to roll this out. It's important to test your chosen solution with a selection of users before rolling out to your wider organisation, to ensure that everyone can continue to access files without too much inconvenience.

Back up plan
Your MFA solution should be factored into your business continuity plan. For example, what if a user loses his or her phone or token? Is there a way for users to gain emergency access?

For more information on ramsac's cybersecurity solutions and how you can protect your organisation

Call: **01483 412 040** Email: **info@ramsac.com** Visit: **www.ramsac.com**

ramsac
the secure choice