MULTI-FACTOR AUTHENTICATION

A Short Guide to MFA and its Benefits

MULTI-FACTOR AUTHENTICATION

Have you noticed how often security breaches, stolen data, and identity theft are consistently front-page news these days? Perhaps you, or someone you know, are a victim of cyber criminals who stole personal information, banking credentials, or more. As these incidents become more prevalent, you should consider using multi-factor authentication, also called strong authentication, or two-factor authentication. This technology may already be familiar to you, as many banking and financial institutions require both a password and one of the following to log in: a call, email, or text containing a code. By applying these principles of verification to more of your personal accounts, such as email, social media, and more, you can better secure your information and identity online!

WHAT IS IT?

Multifactor authentication (MFA) is defined as a security process that requires more than one method of authentication from independent sources to verify the user's identity. In other words, a person wishing to use the system is given access only after providing two or more pieces of information which uniquely identifies that person.

IT ie

Unit 35, Finglas Business Centre, Jamestown Road, Finglas Dublin 11, D11 EP86

hello@it.ie

(01) 8424114

HOW IT WORKS

There are three categories of credentials: something you either know, have, or are. Here are some examples in each category.

SOMETHING YOU KNOW

- Password/Passphrase
- PIN Number

SOMETHING YOU HAVE

- Security Token or App
- Verification text, Call, Email
- Smart Card

SOMETHING YOU ARE

- Fingerprint
- Facial Recognition
- Voice Recognition

WHAT ARE THE BENEFITS OF 2 FACTOR AUTHENTICATION?

Reduce fraud & identity theft

It is very likely that at least one of your online accounts has been compromised. To check simply enter any email address into this very useful and free online tool- Have I Been Pawned. Don't be surprised if at least one of your email addresses has been subject to a compromise. Having 2 forms of verification greatly reduces the chances of a hacker gaining access to your online services including your business networks and the valuable data that you are responsible for.

INCREASED PRODUCTIVITY

Remote and hybrid working is the future of work for many businesses, and it has been shown to increase productivity. The danger with remote working is that it also opens up your organisation's networks to potential compromise where remote workers don't have stringent security tools and practices in place. Having MFA in place gives you the confidence to allow your workers to work away from the office and mitigate the chances of a data breach. MFA alone will not prevent a breach but combined with other tools such as email filtering and good cybersecurity practices by

COMBAT PASSWORD FATIGUE

The average computer user has anywhere between 60 and 80 passwords. With so many passwords to remember, many users resort to using the same password on multiple accounts or variants of the same password. Adding MFA safeguards against password fatigue and adds an extra buffer that ensures that cybercriminals cannot hack even

LOWER SECURITY MANAGEMENT COSTS

2FA authentication reduces the amount of time your employees will spend on helpdesks for password resets that can be costly in terms of helpdesk expenses and employee productivity.

WHEN SHOULD IT BE USED?

We strongly recommend that wherever MFA is available, it should be implemented without delay.

CONTACT IT.IE

If you would like to know more about 2FA and how to protect your systems, get in touch with us and we'll be happy to help. Email hello@it.ie and we'll get right back to you.especially