Hardware | Cloud | **Cyber Security** | Software | Support | Disaster Recovery | Monitoring | Networks | Remote & Communication | Pricing

Why do we need MFA? It's too much like hard work.

Multi-Factor Authentication (MFA) might seem like an extra step, but it plays a crucial role in enhancing security. Here's why MFA is essential and worth the slight inconvenience:

Enhanced Security:
The primary purpose of MFA is to provide an additional layer of security. Even if someone obtains your password, they won't be able to access your account without the second factor, which could be something you have (like a phone or a hardware token) or something you are (like a fingerprint or facial recognition).

Protection Against Phishing:
Phishing attacks, where attackers trick individuals into revealing their passwords, are prevalent. With MFA, knowing the password alone isn't enough.

Defence Against Password Attacks:
Attackers use various methods, like brute force, dictionary attacks, or credential stuffing, to crack passwords. MFA ensures that even if they succeed, they can't gain access.

Mitigate Stolen Data:
If there's a data breach and usernames and passwords are exposed, accounts with MFA are less likely to be compromised.

Regulatory Compliance:
Many industries have regulations that require enhanced security measures, including MFA, especially when handling sensitive data.

User Peace of Mind:
For users, knowing that there's an extra layer of security can provide peace of mind, especially if they're dealing with financial transactions or sensitive information.

Flexibility:
MFA can be implemented in various ways, from SMS codes to biometrics, allowing organisations to choose the method that best fits their needs and their users' preferences.

Adaptive MFA:
Some MFA systems can adapt their checks based on risk. For example, if a user logs in from a new location or device, the system might request MFA, but for regular logins from a known device, it might not.

Missing Link Q&A Information Sheet
Subject: Hardware
Topic: The Evolving Role of Servers: Do I Still Need One?

Date: August 2023
Version: 1

Conclusion

While MFA does introduce an extra step, many systems are designed to be as user-friendly as possible. For instance, some allow "remembering" trusted devices, so you don't need to use MFA every time. Others use smartphone apps or biometrics, which can be quicker than entering a password.

In today's digital age, with cyber threats continually evolving, MFA is a small but significant step towards ensuring that our online accounts and data remain secure.

Missing Link have a range of MFA technologies, so depending on your requirements or risk tolerance we have a solution to suit your needs. If you would like to discuss this or any other related topic, then please contact myself or one of the Missing Link team on info@mlinkuk.com or call 01257 473445 and we will happily guide you through all the pros and cons associated to such a technology.

Contact Information

Phil Heyworth
Commercial Director

E: phil@mlinkuk.com
T: 01257 473445
DDI: 01257 478278
M: 07768 330703
W: mlinkuk.com

Missing Link Q&A Information Sheet
Subject: Hardware
Topic: The Evolving Role of Servers: Do I Still Need One?

Date: October 2023
Version: 1