An Introduction to Multi Factor Authentication

P3M WORKS

Multi Factor Authentication (MFA) is an approach adopted by organisations that requires users to present a combination of two or more credentials to verify their identity to be granted access. It is also known as 2FA.

Three main types of MFA methods:

1) **Something you know (knowledge)**
   Often a password or a PIN.

2) **Something you have (possession)**
   Can be a cryptographic identification device, token.

3) **Something you are (Inheritance)**
   The biometrics of a person like their fingerprint, voice recognition or face scan.

Why should organisations enable MFA?

- Reduces the possibility of a brute force attack being successful.
- Helps your organisation take appropriate measures to secure your system.

Two ways to enable MFA:

- Text message (SMS) or Email: Usually a code will be sent to the users registered phone number or email address which will then be used to login. However, this method is the weakest form of MFA.
- Authenticator Application: A *trusted* authentication app for smartphones will generate a One-Time Passcode (OTP) which refreshes every 30 or 60 seconds. Authentication apps can also ask users to 'approve' access for a login request.

Authentication apps:

- Google Authenticator
- Microsoft Authenticator
- VIP Access

"**MFA can block over 99.9%** of account compromise attacks. With MFA, knowing or cracking the password won't be enough."
- Microsoft.com

CASE STUDY

In September 2022, Uber announced that their internal system had been accessed by an unauthorised entity. The initial access happened when an employee, unknowingly, allowed access by accepting a two-factor authentication (2FA) request.

The employee is reported to have received many notifications to allow the attacker to gain access to the systems, therefore allowing the attacker to move freely around Uber's internal network.

MFA is only useful if you are the sole user approving requests or having access to OTPs. Cyber awareness training should be conducted regularly to ensure employees are not making the same mistake.

UWE Bristol University of the West of England

Delivering Workforce for the Future on behalf of:

WEST OF ENGLAND Combined Authority

European Union
European Social Fund