MULTI-FACTOR AUTHENTICATION

Mitigation strategy to limit the extent of cyber security incidents

Secure your on-line data

Multi-factor authentication (MFA) is a key aspect of the Essential Eight. Multi-factor authentication relates back to Confidentiality and Integrity in the CIA triad and is designed to keep your online data secure. Correctly configured multi-factor authentication is considered bulletproof for protecting accounts. MFA normally involves you entering your username and password then using another factor to complete the login. The factors are *something you know, something you have, something you are.* The Essential Eight recommends setting up multi-factor authentication for VPNs, RDP, SSH and other remote access utilities, and for all users when they perform a privileged action or access an important data repository. The reason for this is that stronger user authentication makes it harder for adversaries to access sensitive information and systems.

WHAT ARE THE MULTI-FACTORS?

To gain access to data or an account, when MFA is enabled, the user is required to identify themselves through any combination of at least two of the following factors

- **Something you know** – such as a username and a password.
- **Something you have** – often this is the user's nominated portable device (mobile phone etc.), but could be a FOB or a swipe card.
- **Something you are** – Most common is your fingerprint but could be voice recognition or retina scan.

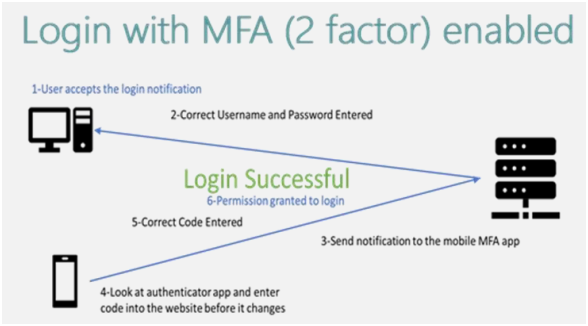
A good example: You log into your bank account with a username and password; the bank sends a text message with an authentication code to your separate device (phone); you enter the code and only then do you gain access to your account.

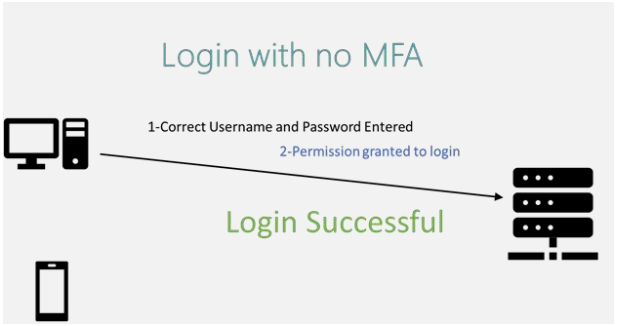
MULTI-FACTOR AUTHENTICATION

Mitigation strategy to limit the extent of cyber security incidents

GETTING THE RIGHT MIX OF MFA

Why not just implement all factors immediately? Two reasons, expense and usability. Make the system too usable and security will suffer. Make the system too secure and usability will decrease leading to user dissatisfaction. Higher security usually means higher I.T. costs.





The Essential Eight maturity level three for MFA requires the following strategies:

- Multi-factor authentication is used to authenticate all users of remote access solutions.
- Multi-factor authentication is used to authenticate all privileged users and any other positions of trust.
- Multi-factor authentication is used to authenticate all users when accessing important data repositories.
- Multi-factor authentication uses at least two of the following authentication factors: passwords, universal 2nd factor security keys, physical one-time password tokens, biometrics or smartcards.

LEARN MORE

Go to the Cyber Security Business Connect and Protect portal www.loyalit.com.au/cybersecurity and see our videos, Q&A sessions and podcasts on this and other topics.

LOYAL I.T. SOLUTIONS

PROFESSIONAL. RELIABLE. LOYAL.