Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) adds a crucial extra layer of security to your accounts. Instead of relying only on a password, MFA requires a second form of verification, making it far harder for attackers to gain access.

How It Protects You

Stops Stolen Passwords

Even if hackers steal or guess your password, they cannot log in without the second factor, such as a code, push notification, or biometric check. This blocks many of the most common cyberattacks.

Tip: *Enable MFA on all of your important work and personal accounts.*

Stronger Methods

Not all MFAs are equal. SMS codes can be intercepted or spoofed, while authenticator apps and biometric factors are more secure. Choosing the right method increases your protection.

Tip: *Use authenticator apps or biometrics instead of SMS whenever possible.*

Code Confidentiality

MFA codes are just as sensitive as passwords. If shared with the wrong person, they can allow unauthorised access.

Tip: *Treat MFA codes as confidential and never share them with anyone.*

Suspicious Prompts

If you receive an MFA prompt or code you did not request, it may mean someone is trying to break into your account.

Tip: *Report unexpected MFA prompts immediately and do not approve them.*