University of CINCINNATI

Multi-Factor Authentication

Beyond Passwords: MFA Explained

Multi-Factor Authentication (MFA) is like having a second lock on your digital door. It's not enough to just have a password; MFA double-checks it's really you by asking for an additional form of proof. This extra step makes it much harder for hackers to break in.

The Why & What of MFA...

99.9% Effective: Blocks nearly all unauthorized attempts.
Breach Barrier: Prevents 80% of security breaches.
Instant Alerts: Know immediately if there's unauthorized access.
Quick and Impactful: Takes seconds, adds robust security.
Identity Verified: Confirms you are you.
Brute-Force Resistant: More than just a password.
Data Protection: Safeguards personal and financial info.
Secure Recovery: Easier account retrieval.
Community Safety: Your security helps everyone.

MFA TIPS + TRICKS

Opt-In Everywhere: Always activate MFA on accounts that offer it.

Authenticator Apps Over SMS: Use an authenticator app for greater security compared to SMS.

Update Recovery Info: Keep your backup phone number and email current.

Duo is the University of Cincinnati's official provider for Multi-Factor Authentication

When it comes to security, 2 steps are always better than 1.

For any Cyber Security questions, please visit the Office of Information Security or email us at infosec@uc.edu