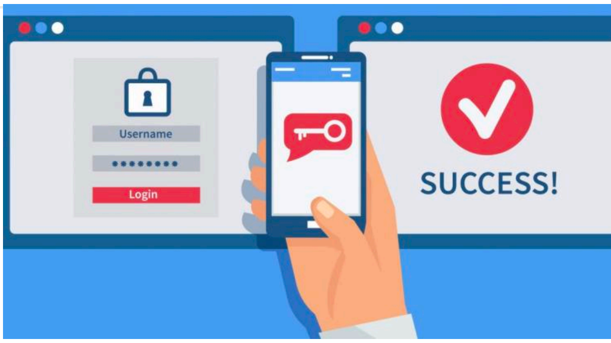
LEVEL-UP YOUR LOGIN: SET UP MFA



Multi-Factor Authentication (MFA) is like having a second lock on your digital door. Beyond merely requiring a password, MFA adds a crucial layer of verification by demanding an additional form of identification.

This added verification reduces the risk of security breaches by 80%.

WHAT & WHY: THE CASE FOR USING MFA

MFA is a layered defense system for your accounts. You need more than just a password to gain access; you'll also need to provide an additional form of identification, such as a code sent to your phone or a fingerprint scan.

Why is this so vital? Because even if an attacker cracks your password, they will still need to beat the second layer of security, making their job significantly more difficult. If you're looking for effectiveness, MFA blocks 99.9% of unauthorized access attempts, providing a robust shield against cyber intruders.

To get the most out of MFA...

USE AUTHENTICATOR APPS: Ditch SMS for an authenticator app. They are generally more secure and don't require cell service to function.

UPDATE RECOVERY INFORMATION: Ensure your backup contact methods (like a secondary email or phone number) are current.

ENABLE ON IMPORTANT ACCOUNTS: Don't just set up MFA on your work email. Use it for all crucial accounts including bank, personal email, and cloud storage.

REVIEW SECURITY SETTINGS: Periodically review the MFA settings on your accounts to make sure no unauthorized devices or methods have been added.

QUESTIONS ABOUT MFA?

To learn more and/or report suspicious behavior, email the Office of Information Security at infosec@uc.edu.

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