Published on *University of Colorado* (https://www.cu.edu)

Using multifactor authentication (MFA) to stay safe online [1]

October 6, 2025 by ES and UIS Communications [2]

MFA helps confirm it's really you.

MFA requires two or more types of proof before letting you into an account. These proofs come from different categories:

- Something you know — like a password.
- Something you have — like your phone or an app.
- Something you are — like your fingerprint or face.

Smart MFA saves you time

Adaptive multifactor authentication, also known as Smart MFA, analyzes additional factors when a user attempts to log in and assigns a level of risk associated with that login attempt. For example:

- Where is the user who is trying to access information? Is the location different from normal?
- When are they attempting to access information? Is it during regular hours?
- What kind of device are they using? Is it different from the one they normally use?
- Are they on a private network or a public network?

Because Smart MFA learns your regular login patterns, you may see fewer prompts when everything looks familiar. But if anything unusual occurs — new device, location or time — you'll get extra verification. This helps balance security and convenience.

Is MFA worth it?

Without a doubt. Data on phishing and security incidents show that most events could have been prevented by using MFA, even when passwords are compromised. In short, MFA adds another layer of security that is unmatched by other methods.

What is MFA fatigue?

It is a type of social engineering where cybercriminals bombard a user with repeated multifactor authentication (MFA) requests, hoping that they will approve one out of frustration or exhaustion. MFA fatigue scams are becoming increasingly common, so remember that you're not alone.

Check out this real-world example of MFA fatigue leading to a security breach [3]. Stay vigilant

and always report suspicious prompts so your IT and security teams can respond quickly.

What to do if something goes wrong

- If you suspect someone else has access to your second factor (e.g. phone stolen or compromised, email breached), change your passwords and report it immediately, if it is a university account.
- Lock or freeze your accounts. A best practice is to report the incident to your financial institutions first so they may protect your debit/credit cards and bank accounts.
- Temporarily disable and replace lost/damaged factor devices.
- Review recent login activity for unusual access.

NOTE: Most personal services — email, cloud storage, banking — offer MFA. Enabling it there protects you beyond just work or school.

For more information on MFA, review the Office of Information Security's MFA webpage [4] and watch What does MFA mean [5].

cybersecurity [6], multi-factor authentication [7]
Display Title:
Using multifactor authentication (MFA) to stay safe online
Send email when Published:
No

Links
[1] https://www.cu.edu/blog/tech-tips/using-multifactor-authentication-mfa-stay-safe-online [2] https://www.cu.edu/blog/tech-tips/author/166688 [3] https://www.cu.edu/security/department-director-mfa-fatigue-approving-wrong-request [4] https://www.cu.edu/security/multi-factor-authentication-added-protection-cybercrime [5] https://vimeo.com/751302523 [6] https://www.cu.edu/blog/tech-tips/tag/cybersecurity [7] https://www.cu.edu/blog/tech-tips/tag/multi-factor-authentication