Two-Factor Authentication (2FA)

What is two-factor authentication?

2FA adds a **second layer of security** to your account. This method is used to prove that the user accessing the account is who they say they are.

What benefits does 2FA provide?

Hackers may obtain your usernames and passwords, such as after a data breach or on the dark web.

With 2FA, even if a hacker has your information, they won't be able to access your account without proving the second layer of security.

How does 2FA work?

Traditionally, we enter our username and password to access an account.

With 2FA, you are required to provide another piece of information, either:

Something you **know**:
E.g., one-time PIN, security questions

Something you **have**:
E.g., physical devices

Something you **are**:
E.g., fingerprint, facial recognition

SCHOOL OF
INFORMATION
UNIVERSITY OF MICHIGAN

Two-Factor Authentication (2FA)

How do I get started?

1. Check whether a service you use (e.g., Facebook, Twitter, or online bank accounts) offers 2FA protection. You can often find this in the settings, or by visiting websites that provide this information like 2fa.directory.

2. Follow the steps to activate 2FA in the service's settings. You may be prompted to choose an authenticator app on your phone. Examples include **Duo Security** or **Google Authenticator**.

Google Authticator

3. Once it is enabled, follow the on-screen instructions on the authenticator app to connect it to your account.

Enter your password

Enter code from phone

That's it. You're signed in!

SCHOOL OF INFORMATION
UNIVERSITY OF MICHIGAN