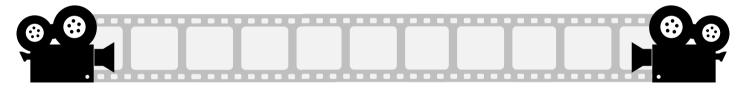# NOW SHOWING
ENABLING MULTI-FACTOR AUTHENTICATION

In computer security, an authentication factor is anything you use to authenticate yourself with a system. Using a password is the most common type of authentication. With multi-factor authentication (MFA), you use two or more different factors to log in.

One example is a password and a verification code sent to your smartphone. This is an extra layer of security, so even if one of your factors is stolen, the hacker doesn't have access to the other authentication factor. This stops them from accessing your account.

As more and more organizations implement MFA to strengthen their security practices, you may encounter different types of authentication factors. There are three different types that you may be asked to provide:

- **Something you know** — Passwords and security questions
- **Something you have** — A verification code on your phone or a key card
- **Something you are** — Biometrics, like your fingerprint

The more factors you use, the better your security. Having a combination of authentication factors is an even better way to keep your data protected.

INFOSEC

SECURE YOUR SCREEN

E-TECH