



# PROTECT YOURSELF WITH MORE THAN A PASSWORD

## What is two-step authentication?

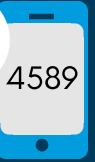
Two-step authentication is a second layer of security besides your password for any kind of login. It means you have to confirm your identity in two ways - with something you know (your password) and something you have (a code sent to your phone).

1

\*\*\*\*\*

2

4589



65938



The Division of IT uses Microsoft two-step authentication to ask individuals for a second confirmation of their identity at login, using a physical device in their possession.

## How does it work?

The device may be a smartphone or tablet using the free Microsoft Authenticator app, a text message sent to your phone, or an automated voice call to landline or cell phone.

## Why do we need it?

Passwords alone aren't good enough anymore when it comes to protecting your personal information, and our systems and networks. Two-step authentication helps protect your information with more than a password.



## Isn't this an inconvenience?

Not really. Many people already use two-step authentication systems for online banking and shopping. Even social media sites may ask you to confirm your identity when you're trying to log in from a new device or location. If you try to use your credit card to buy gas, you may be asked to enter your ZIP code. That's two-step authentication at work.