**PROVE IT’S YOU**

**WHAT IS TWO-FACTOR AUTHENTICATION?**

Two-factor 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 and something you HAVE.

**HOW DOES IT WORK?**

The most popular method is a “push” notification to a smart phone. When you try to access certain systems requiring WVU Login credentials, a message appears asking you to prove you are who you say. The Duo app is free in the Apple Store, Google Play Store, Windows app store and BlackBerry World.

If you’re asked to enroll and don’t carry a cell phone, you can use a USB key that works with Chrome and Firefox or a display token that generates codes that work with any browser.

**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.

WVU must soon comply with the Payment Card Industry Data Security Standard. That affects any company or institution that accepts, stores or processes credit card payments and card holder data. Two-factor also may be required for cyber-liability insurance coverage.

**BUT ISN’T THIS AN INCONVENIENCE?**

Not really. Many people already use two-factor 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-factor authentication at work.

**WHEN IS IT COMING?**

You can sign up voluntarily starting in August 2017. WVU will begin requiring two-factor authentication in February 2018.

twofactor.wvu.edu