

Multi-Factor Authentication

What is Multi-Factor Authentication?

Authentication is the process by which a website or app verifies your identity, typically by using a username and password. Oftentimes, a username and password is not sufficiently secure when it comes to sensitive data, to include financial, education and medical data. Multi-factor authentication, also called two-factor authentication or two-step verification, is a process that adds at least one more step, or "factor", to verifying your identity in order to increase security around sensitive data. This step is usually a confirmation of your identity in the form of an email, text message, automated phone call, or notification on an authentication app.

Hackers and other cyber criminals are constantly looking for students and employees with unsecured data to exploit. Multi-factor authentication is a crucial step that each employee and student can take in keeping UVU safe from cyber attacks and able to achieve our educational mission.

Microsoft Authentication for Students

For students and employees accessing certain online resources such as myUVU and Microsoft apps, Microsoft multi-factor authentication will be used. If multi-factor authentication has not been set up, the next time you log into a Microsoft app with your university account, you will be prompted to set an authentication method. Either a mobile phone number or the Microsoft Authenticator app will be needed for authentication. Instructions for setting up authentication can be found [here](#).

Download the Microsoft Authenticator App



Why is Multi-factor Authentication needed?

Regent's policy now requires multi-factor authentication (Policy R345 Section 4.1.3). Hackers often target institutions by using hacked credentials to file taxes for employees, steal employee paychecks, steal from student and employee's bank accounts, and steal Social Security numbers for credit fraud. Multi-factor authentication is the most effective way of stopping this type of fraud, since you are notified of login attempts and required to verify every login to your account.

Frequently Asked Questions

For any questions not answered below, contact the [Service Desk](#) for assistance.

- I'm having trouble with multi-factor authentication. Where can I go for help?
- I do not have a smartphone or tablet. What can I do?
- When can I begin using multi-factor authentication?
- What types of devices will work with Microsoft multi-factor authentication?
- Who will be using Microsoft multi-factor authentication?
- What services will require the use of multi-factor authentication?
- I do not have mobile data on my smartphone or tablet. How can I complete Microsoft Authenticator setup?
- Can I use multi-factor authentication when not connected to the Internet? (i.e., air travel, no data, etc.)
- What if I get a login notification from Microsoft and I haven't just tried to login?
- Will UVU reimburse me for data usage or purchase a phone for me to use for Microsoft Authenticator?
- I left my device at home. What can I do to log in?
- I lost my device. What should I do?

Cybersecurity and IT Risk Management | security@uvu.edu | (801) 863-8888 | Room DX-107

STUDENT

- [ADMISSIONS](#)
- [ACADEMICS](#)
- [CAMPUS LIFE](#)
- [LOOKING TO ATTEND UVU](#)
- [CURRENT STUDENT](#)
- [ACCREDITATION](#)

EMPLOYEES

- [CAREER OPPORTUNITIES](#)
- [EMPLOYEE RESOURCES](#)
- [DIRECTORY](#)
- [PEOPLE & CULTURE](#)

COMMUNITY

- [ATHLETICS](#)
- [VISITORS & COMMUNITY](#)
- [OFFICE OF THE PRESIDENT](#)
- [ABOUT UVU / HISTORY](#)
- [ALUMNI](#)
- [INCLUSION & DIVERSITY](#)
- [ESPAÑOL](#)
- [GIVE TO UVU](#)
- [CONTACT US](#)

UTILITY

- [COVID-19 INFO](#)
- [MAPS / PARKING](#)
- [SERVICE DESK](#)
- [EMERGENCY](#)
- [POLICE](#)
- [GET HELP](#)
- [SEARCH](#)
- [ACCESSIBILITY](#)
- [TITLE IX / EQUAL OPPORTUNITY](#)