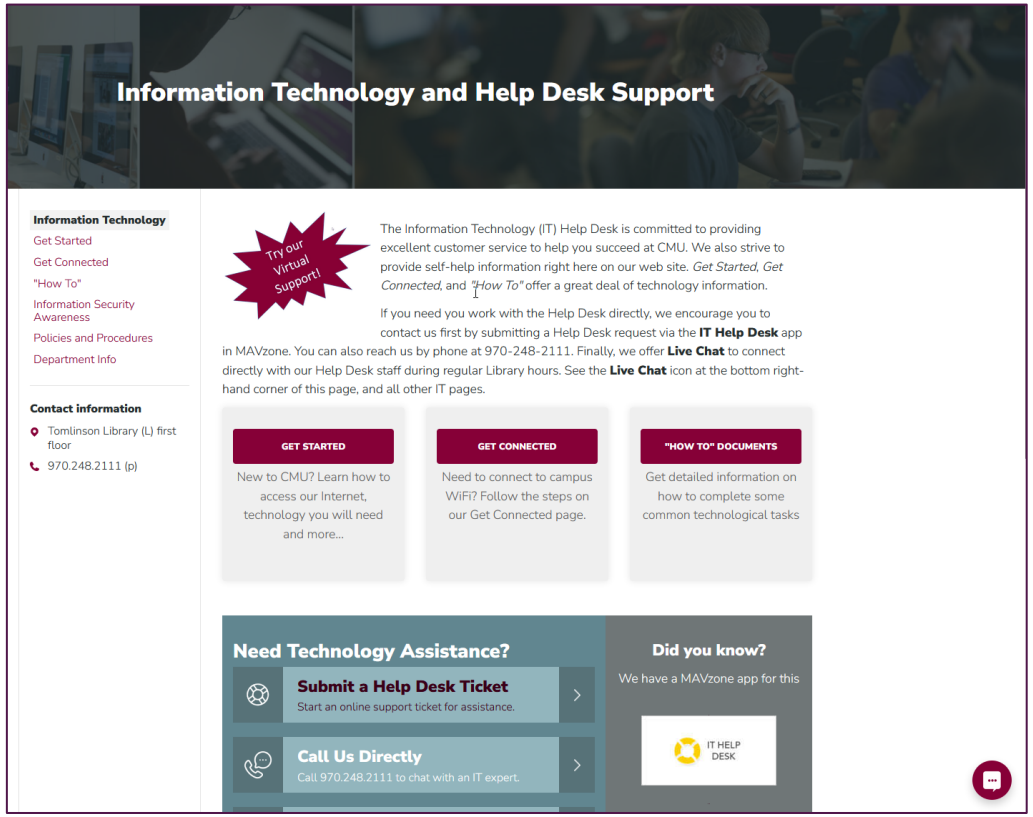
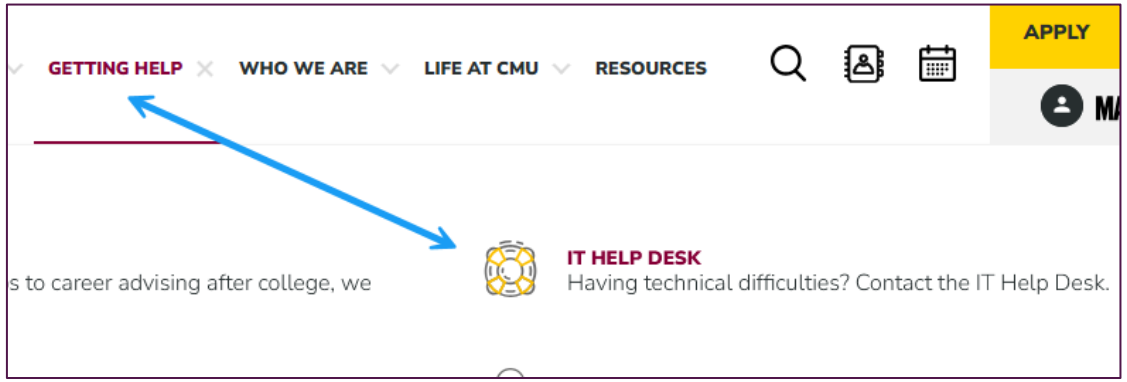
COLORADO MESA
UNIVERSITY
Information Technology at CMU

Introducing Information Technology

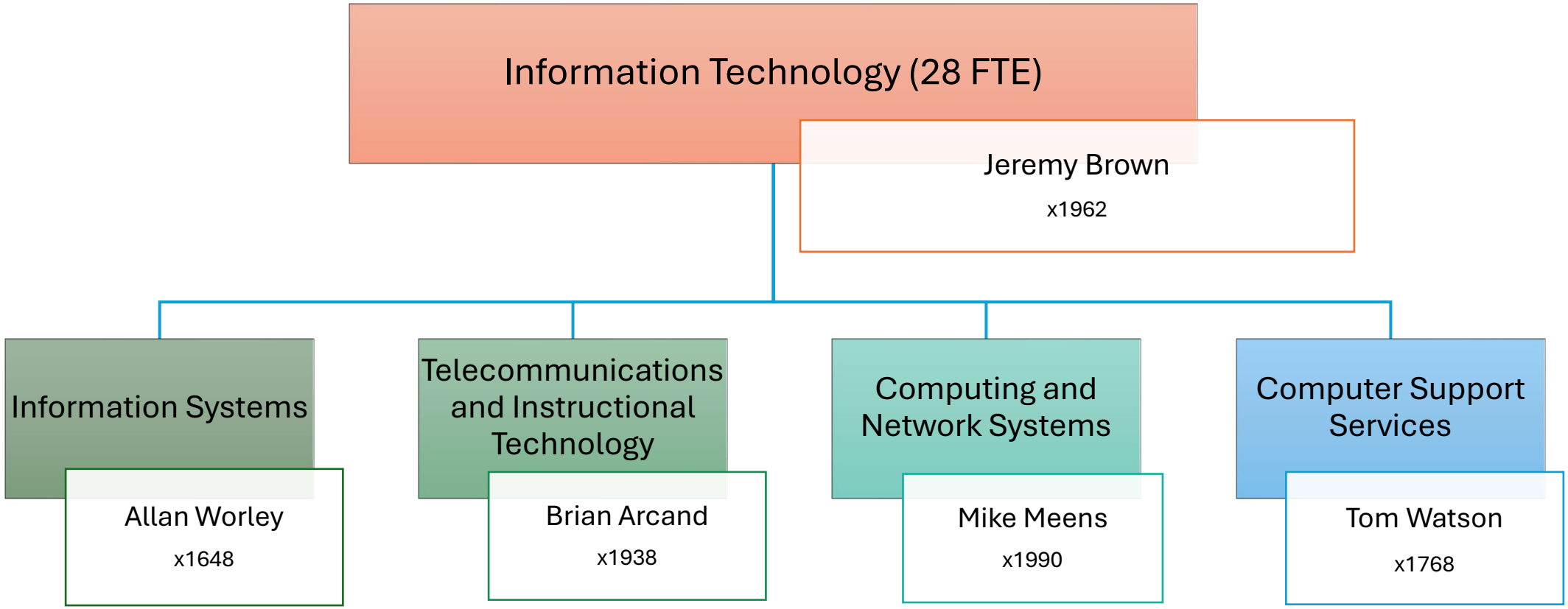
Information Technology is committed to supporting the technology needs of faculty, staff, and students as they apply to supporting the mission of CMU. A great way to get to know our department is to visit our IT page, www.coloradomesa.edu/it.



Alternately, from www.coloradomesa.edu, click Getting Help, then IT Help Desk.



Information Technology



- Banner SIS
- Enterprise SW
- MAVzone Portal
- MAVprint

- Media Services
- Classroom AV
- Phone System
- Infrastructure

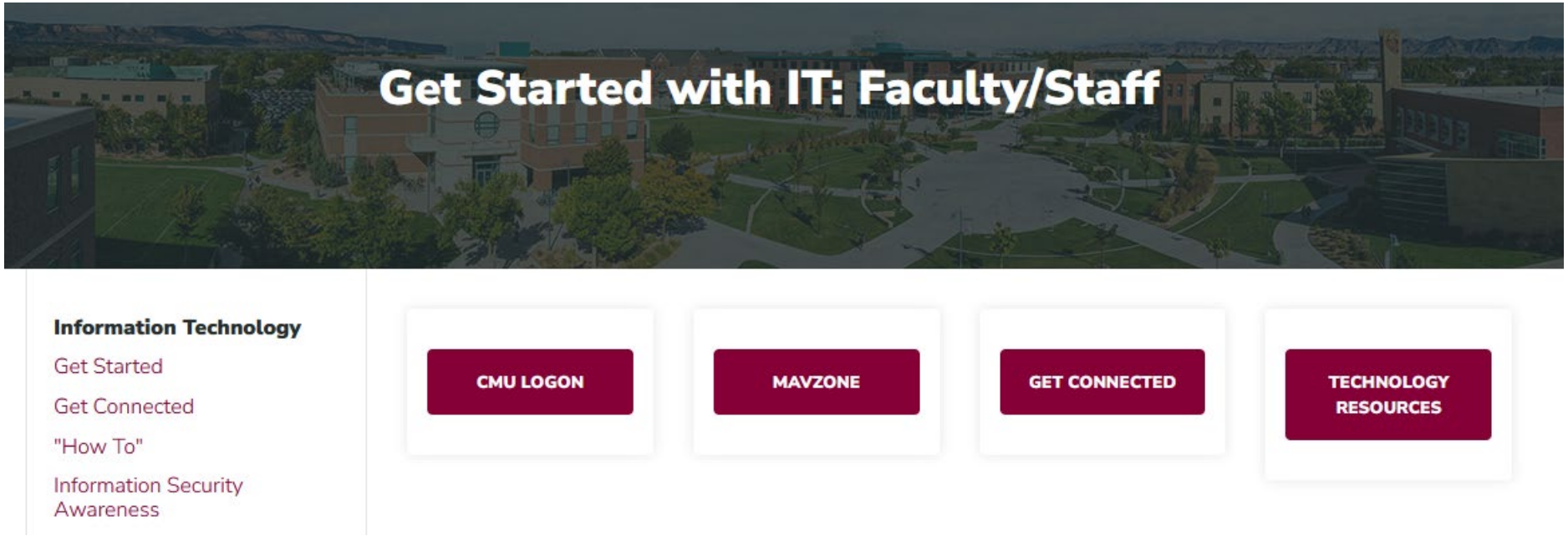
- Servers & Storage
- Networks/Wireless
- E-mail
- Security

- Help Desk
- Computer Techs
- Desktop Support
- Software

Get Started: Faculty/Staff

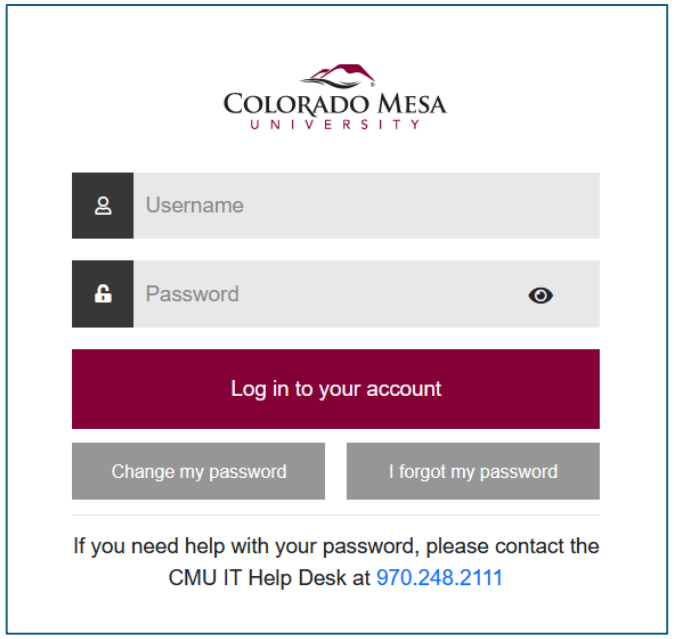
As a new employee of CMU, you'll want to check out the Get Started page for Faculty/Staff, https://www.coloradomesa.edu/it. Click **Get Started**, **Faculty/Staff**, **Technology Resources**. Topics include:

- CMU Logon; Changing, Resetting Passwords, Securing Your Computer
- MAVzone; Campus Portal for all users
- Get Connected; Connecting your WiFi devices, and synchronizing CMU Mail on your Smart Phone
- Technology Resources; Details on technology for use at CMU



Logging In

Your CMU login is used to login to any campus computer and to access the campus portal, MAVzone. Go to www.coloradomesa.edu and click **MAVzone**.



Where

Campus Computers

MAVzone

Username

Assigned during your Check In , based on your last name and preferred first name.

This is also the first part of your email address; *username@coloradomesa.edu*

Password

Minimum; 8 characters, 1 capital letter, 1 lower case letter, 1 numeral or symbol For example:

- **M8zsUH20@0**
- **Sk00LrahkZ!**

Expires every 180 days

Cannot reuse previous passwords, cannot include any part of your name or username

Alert: When changing your MAVzone password, be sure to change it on your mobile devices for CMU WiFi connectivity and for syncing your CMU Outlook email.

Alert: Avoid saving passwords in web browsers, as this can cause issues when you are required to change a login password and it becomes out of sync with what your browser has stored.

Logging Out

- Always log out of shared campus computers, such as instructor PCs or Library PCs, or other common use workstations to protect your information and to allow the next person to log in.
- CMU computers will lock after 10 minutes of inactivity. Always log out or lock your computer if you must leave it unattended.
- You may leave your office computer logged in while unattended, provided you lock the computer.
- You cannot log out of MAVzone. Either close all instances of your web browser or log out of your computer to close MAVzone and other services.

MFA: Multi-Factor Authentication

- Multi-factor Authentication (MFA) is required for access to web services provided by CMU
- MFA is pre-configured to use text messages, sending 6-digit codes to your cell phone number listed with CMU. We highly recommend installing Microsoft Authenticator as soon as possible, because it is more secure and easier to use (only 2 digits); go to https://www.coloradomesa.edu/information-technology/how-to.html, for instructions *Multi MFA: Alternate Verification Method – Microsoft Authenticator*.
- Microsoft Authenticator works from anywhere with internet access, while text messages may not work outside of the U.S. depending on your service provider. It also works even if you change your phone number.
- If you get a new phone and you transfer Microsoft Authenticator to your new phone, it won't be connected to your account. You must go into MAVzone, My Account, Personal, Multi-Factor Authentication, Settings. Remove the Authenticator app, then re-add the Authenticator app. By scanning the QR code, it connects the Authenticator app to your new phone.
- MFA is not required from CMU-owned computers when using Microsoft Edge, allowing you to work from on-campus if you forget your cell phone.

Resetting a Forgotten Password

1. From any Internet connected device, go to www.coloradomesa.edu. Click the **Login to MAVzone** button.
2. At the login screen, click the **I forgot my password** button.
3. At the next dialog, enter your *MAVzone Username*, *Student ID (700#)*, and the *last 4 digits* of your cell phone on record with CMU. Click the **Send Code** button.
4. In the next dialog box, enter the *MAVzone Reset Code* you were just texted and click the **Check Code** button.
5. Now, enter your new password into each box, following the password policy described in this dialog. Click the **Change Password** button.
6. Once the password has been changed, you will see the following dialog box.

Faculty/Staff password resets **ARE NOT** done via phone call. If you need assistance with resetting your password, you must come to the Technology Help desk, located on the 1st floor of Tomlinson Library. Make sure to bring your MAVcard ID and have your 700# memorized.

Memorize your 700# for faster support!

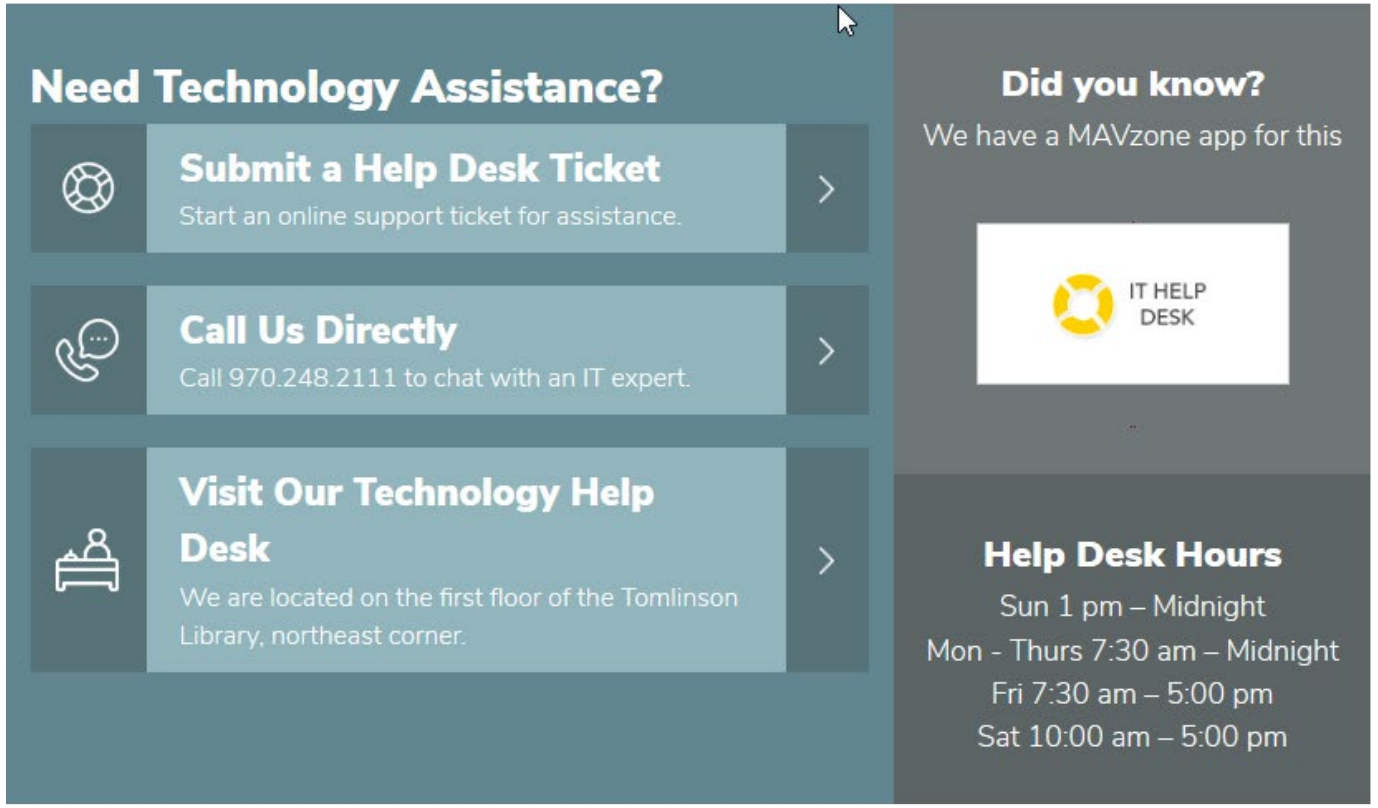
“How To” Documents

Visit https://www.coloradomesa.edu/it, and click **“How To” Documents** for the full repository of tech related documentation. Some of the more popular topics include:

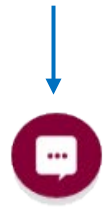
- Change MAVzone Login Password
- Classroom/Computer Lab Software
- Connect to CMU WiFi (Faculty, Staff, Students)
- Multi-Factor Authentication (MFA)
- MFA: Alternate Verification Method – Microsoft Authenticator
- Microsoft 365
- Microsoft Outlook
- Microsoft Teams – Basic
- Microsoft Teams – Guide to Softphone Features
- Panopto
- Reset Forgotten Password
- Synchronizing CMU Mail
- Windows Quick Guides

Technology Help Desk Support

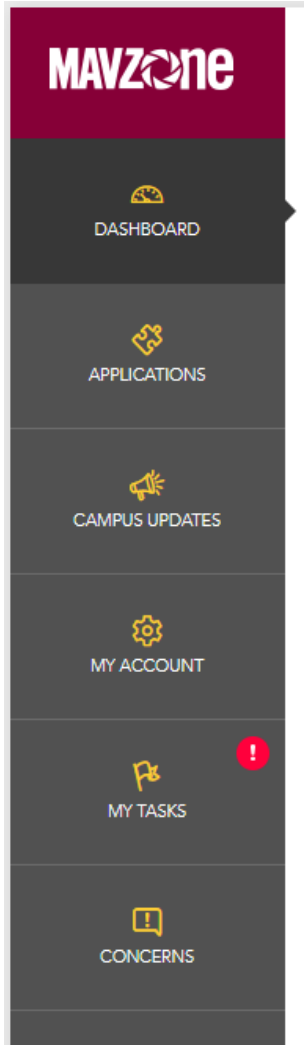
- Navigate to www.coloradomesa.edu.
- Click the **Getting Help** link at the top of the page and then choose **IT HELP DESK**.
- Choose any of the methods shown to reach out to the Help Desk for technology support, including our newest method, LIVE CHAT, which offers immediate response from our Help Desk staff during normal library hours.



Live Chat



MAVzone

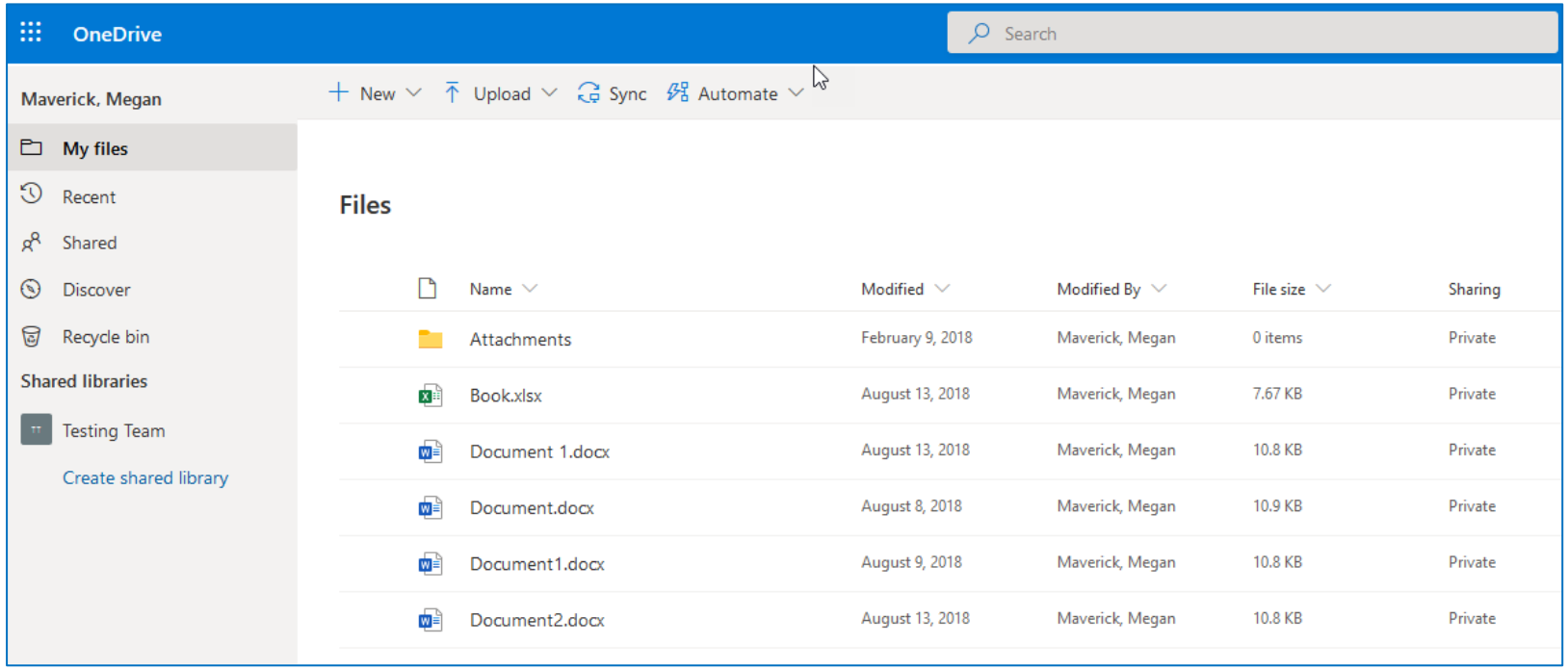


- **MAVzone** is CMU's campus portal for easy access to the applications you will need throughout your career at CMU: campus updates, personal information, current tasks you need to perform, and Applications.
- Check out the **DASHBOARD** for *Campus Updates*, and *Trending Apps* made popular by your peers. Customize your DASHBOARD by adding the Apps you use the most to *My Favorites*.
- **APPLICATIONS** is a directory of just about every online service or application you will ever need. Favorite an App by clicking the **Gold Star** on the *App Tile*. Unfamiliar with an App? Hover over the **Question Mark** bubble on the *App Tile* for a brief explanation.
- **MY ACCOUNT** is where you view and update information about your account, find your 700# (Student ID) access your W2 at tax time, change your password, configure MFA, and update your office location. Your office location populates the 911 database, so you want to make sure that it's accurate. Also, be sure to memorize your 700#.
- Keep an eye on **MY TASKS**! You have something to complete when you see a *Red Exclamation Point*.
- **MAVzone** is easy to use and mobile friendly. The best way to learn how to use it is to dive in and experience it! Just click the button shown below at www.coloradomesa.edu and begin exploring all that MAVzone has to offer.

OneDrive

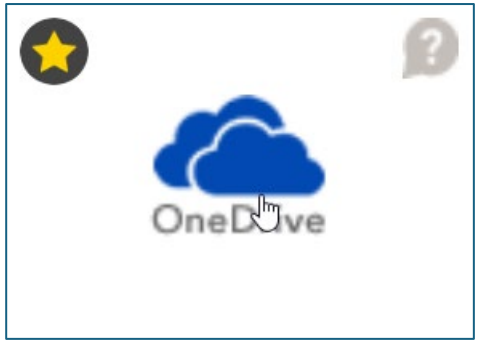
Access from MAVzone

1. OneDrive provides you with cloud storage from any Internet connected device. This is where you will store most of your files while working at CMU.
2. Click MAVZONE to log in. Click **Applications** in the Navigation Bar, and click the **OneDrive** app.



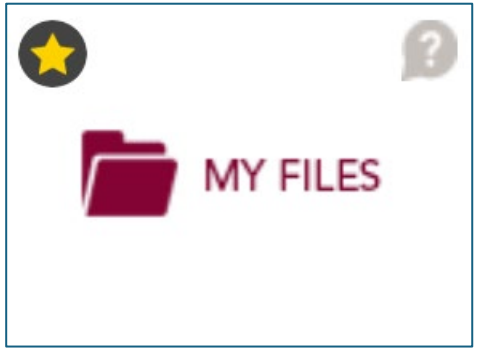
File Storage

- On campus computers, don't save files to the local hard drive. If these computers have issues, the drives are wiped, and data will be lost.
- Always use Teams as your primary file storage location for file sharing, and OneDrive for your personal files. All OneDrive files owned by you will be deleted when you leave CMU.
- Access your Teams and OneDrive folder from anywhere using with MAVzone.



- Other traditional storage locations available are available:

  R: drive (Share); each department has their own R: drive for shared files.
- Access your R: drive files off campus via the MAVzone app, MY FILES. This app permits downloads and uploads only. You can download a file, update it locally, and then upload the file back to R: when finished.



Requesting Software

- Begin first with the CMU Software Lookup tool located on the *How To* page to find out what software is currently installed on campus computers.
- If you want to purchase a new product, there's a formal vetting process that you must go through. Plan to submit your request at least a semester prior to when you want the product.
- Submit a Help Desk ticket, selecting Software, Software Install, and fill out the form and submit the ticket.
- Next, you'll receive a detailed PDF form that you'll need to fill out and return to begin the review process.

IT Policies and Procedures

Information Technology

Get Started

Get Connected

"How To"

Information Security Awareness

Policies and Procedures

Department Info

Contact information

Tomlinson Library (L) first floor

970.248.2111 (p)

Computer Use Policy

CMU Privacy Policy

CMU Data Protection Policy

Electronic Communications Policy

End User Agreement

Network Use Agreement

Project Scoping Document (PSD)

- After you click 'Project Scoping Document', it will open in your browser. Use the DOWNLOAD button to download this file to your computer. Once it's downloaded, open in Acrobat Reader and fill out. Follow the directions at the end of the form to send to IT for review.

Technology Master Plan

Information Security

- Protect Personal Information
- Strong Passwords
- Security Awareness

Annual Information Security Training

95% of all successful attacks on enterprise networks are the result of targeted phishing attacks [1]

www. coloradomesa.edu/information-technology/security.html

[1] https://www.networkworld.com/article/2164139/network-security/**how-to-blunt-spear-phishing-attacks**

Phishing Scams

Computer users are under a constant threat of malware and security attacks, focused on stealing something from you, and/or causing harm to your device. A 'phishing' email or text message is designed to fool you into taking some action; clicking on a malicious link, opening up an infected email attachment, or filling out an online form with **Personally Identifiable Information** (PII).

Ways to Spot a 'Phishing' Attempt

- The message has a strong sense of urgency, meant to rush you into taking action.
- Generic greetings are used, rather than using your name or title.
- The ***From*** or ***Reply-To*** address is a personal email address; @gmail.com, @hotmail.com, etc.
- An offer that plays on your curiosity, or seems to good to be true, such as notification of a package delivery even though you have nothing on order, or notification of winning a contest for which you have not entered.

Ways to Spot a 'Spear Phishing' Attempt

- A kind of phishing attempt where the message targets specific.
- May appear to come from a friend or co-worker, but the tone of the message does not sound like that person.
- Strong sense of urgency, pressuring you to ignore or bypass company policies.
- Email is work related but comes from a personal email address.

Handling Phishing Attempts

- Always assume that a suspicious email is a phishing attempt. Hackers are getting better at this all the time, and some look very real, especially with the use of AI.
- If you do business with a company that is represented in any email, DO NOT use the email to get to the company's web site. Open a browser and use an existing favorite/bookmark, or type in the company's website address manually. Once you are on the site, look for the same notification found in the email and respond directly on the site.
- Use the "Report Phishing" option in Outlook to report phishing emails to both CMU IT and Microsoft
- If an email looks suspicious, but you aren't certain, email the IT Help Desk or itsecurity@coloradomesa.edu.
- Contact the CMU IT Security Officer, Mike Meens, mmeens@coloradomesa.edu for more information and guidance.

Welcome to CMU!
Go MAVS!
Have a great semester!