



# Your Password Needs a Partner: Turn On Two-Factor for Weblogin

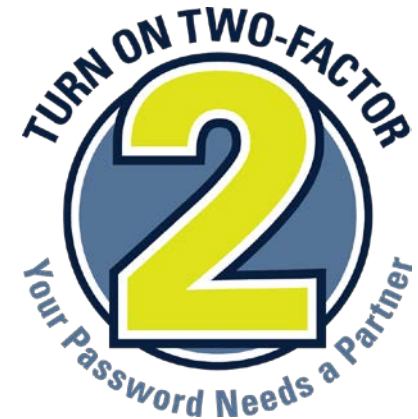


Jessica Rohr, ITS  
Two-Factor Authentication Expansion Project



## Agenda

- U-M & Two-Factor (Duo) Today
- What's Next?
- Turn on Two-Factor for Weblogin Campaign & Pilot
- Two-Factor Authentication
- Why Now?
- How to Turn on Two-Factor For Weblogin
- How You Can Help





# Duo at U-M Today

25,700 Duo users on U-M Campuses



All Platforms

Android Breakdown

iOS Breakdown

**5144** [Android](#)

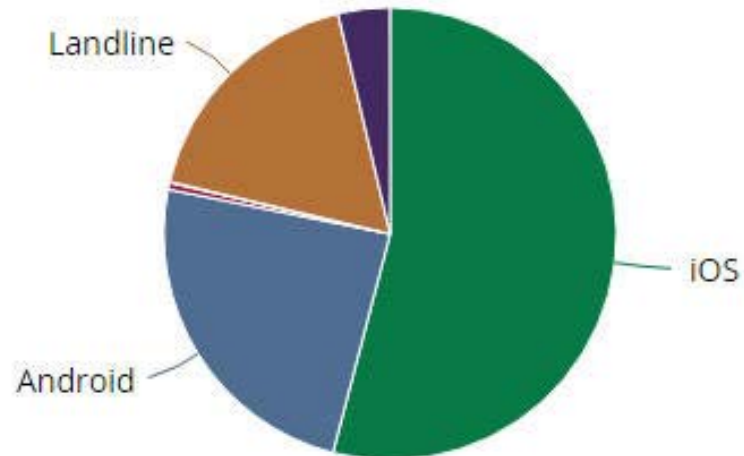
**11557** [iOS](#)

**13** BlackBerry

**104** Windows Phone

**3762** Landline

**790** Other

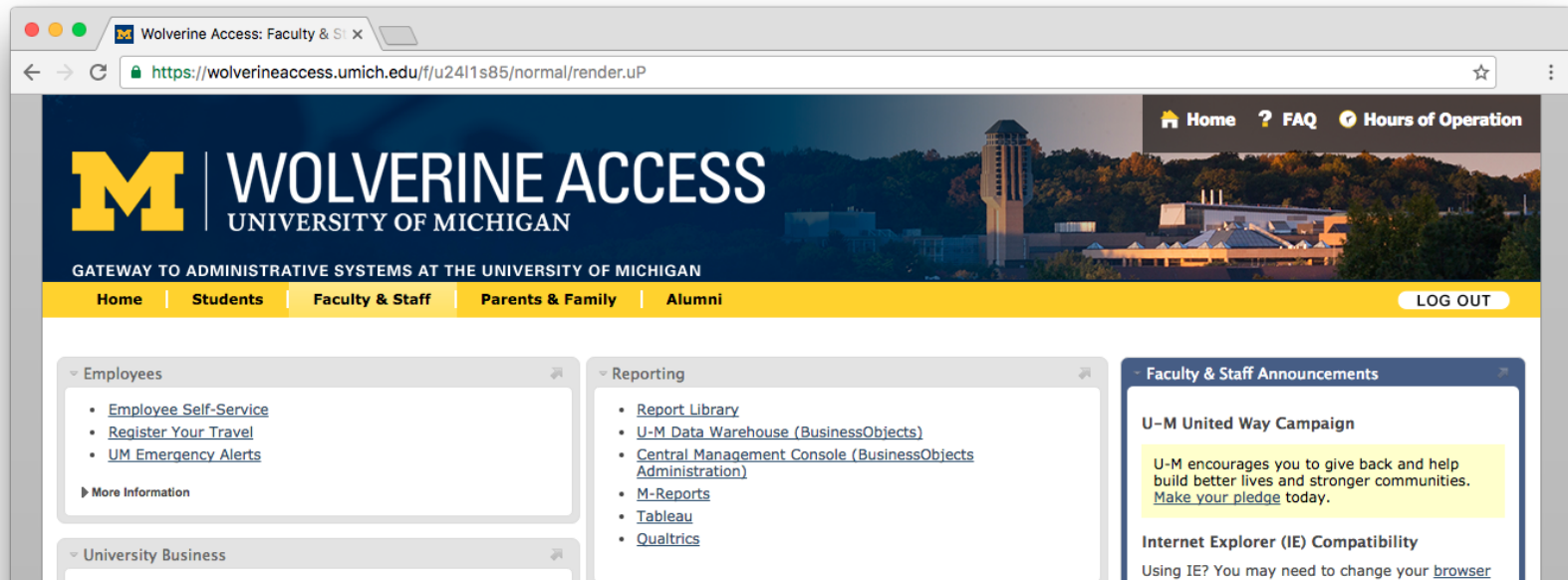


*As of Nov 7, 2016*



# Where is Two-Factor Currently Used at U-M?

**Required** for some U-M Systems: Payroll,  
Human Resources, Timekeeping, etc.





## What's Next?

Protect personal, research, and university data by expanding two-factor (Duo) to other services and individuals; some voluntary, some required.

1. Expansion to other services, including ITS-managed Windows servers; MiServer/MiDatabase; UMHS VPN; others as determined.
2. Expansion to cover services accessed via Weblogin, includes Wolverine Access & U-M Google/Box (optional).






# Where is Two-Factor Currently Used at U-M?

Now also **available** for:





# What Does It Look Like?

 **WEBLOGIN**  
UNIVERSITY OF MICHIGAN

Enter your Login ID and Password

Log In

[Need help?](#)



 **WEBLOGIN**  
UNIVERSITY OF MICHIGAN

Two-Factor Authentication Required



[What is this?](#) 


[Add a new device](#)

[My Settings & Devices](#)

[Need help?](#)

Powered by Duo Security

Choose an authentication method

 Duo Push

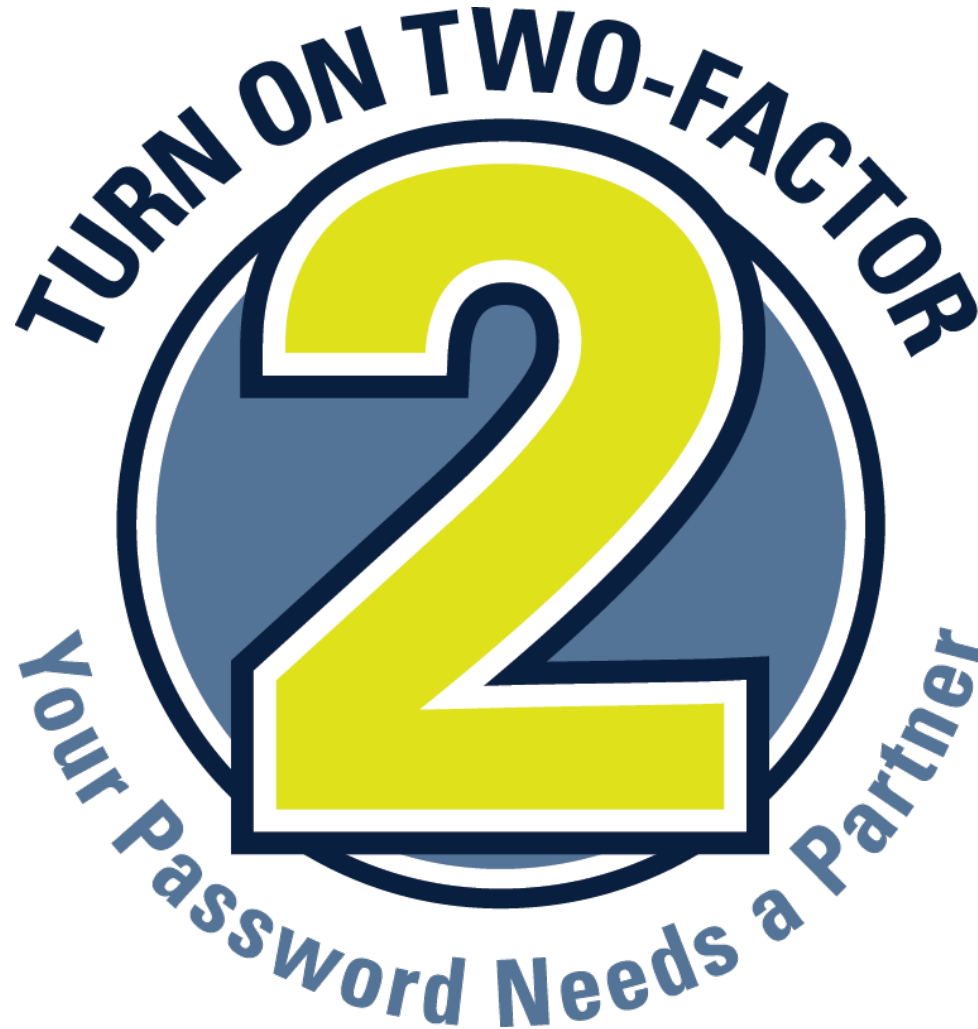
Send Me a Push

 Call Me

Call Me

 Passcode

Enter a Passcode







## How Two-Factor Protects You

Anyone who knows your password can impersonate you. So, two-factor:

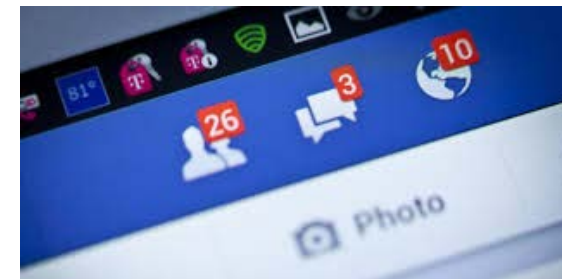
- Provides an additional layer of security.
  - Phishing attacks
- Denies hackers access to your accounts without your second factor device.
- Helps to protect your account even your password has been stolen.





## What's at Stake?

- **Your Money:** W-2s, direct deposit info, credit score
- **Your Personal Life:** Reputation, relationships, identity
- **Your Work Life:** Research, university data, U-M reputation





# In the News: Cybersecurity Threats



**PennState**

**Penn State closes down College of Engineering computer network in response to hack attack**

**Berkeley**  
UNIVERSITY OF CALIFORNIA

**Data breach affects 80,000 UC Berkeley faculty, students and alumni**

**UCLA**

**Health**

**UCLA Health System data breach affects 4.5 million patients**



**Cyberattack hits UVa**

**University of Maryland computer security breach exposes 300,000 records**





# At U-M: Sophisticated Phishing Attacks

From: **Payroll Services** <[payroll@umich.edu](mailto:payroll@umich.edu)>  
Date: Wed, Oct 19, 2016 at 2:36 PM  
Subject: Your Record Updated -- IMPORTANT  
To:

This email is to confirm that you have successfully updated  
your email address in [Wolverine Access](#).

This update occurred on 09/05/2016 at 7:13 p.m.

If you did not update this information online, please  
to <http://www.umich.edu/eid/help/stolen.html>  
or call the Information Technology Services (ITS) Help  
Desk at 734-475-9400 for assistance.

Please note that if you have multiple email accounts  
the university, you may receive this message at each  
address. If you performed multiple updates, you may  
receive separate email confirmations.

Thank you,  
Payroll Services

The screenshot shows a web browser window with a single tab titled 'U-M Weblogin'. The address bar contains the URL 'skyherbsindia.com/fckeditor/editor/plugins/symlink/umich.edu'. The website header features the University of Michigan logo and the text 'WEBLOGIN UNIVERSITY OF MICHIGAN'. Below the header, the instruction 'Enter your Login ID and Password' is displayed. The login form consists of two input fields: the first is labeled 'Uniqname or Friend ID' and the second is labeled 'Password'. Both fields have a small icon to their left (a person icon for the first field and a lock icon for the second field).



## What Are the Benefits?

Turn On Two-Factor for Weblogin to:

- Better protect your U-M account
- Protect information in multiple U-M services and applications
- Be alerted if a hacker tries to log in as you
- Increase peace of mind

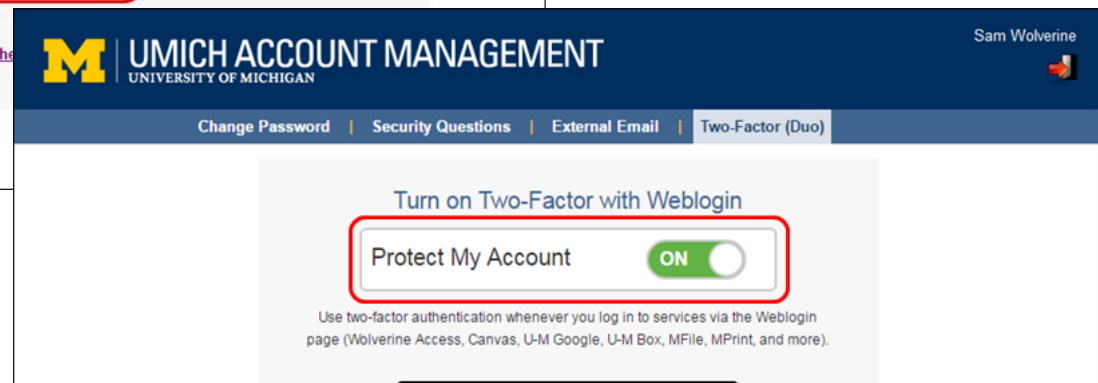
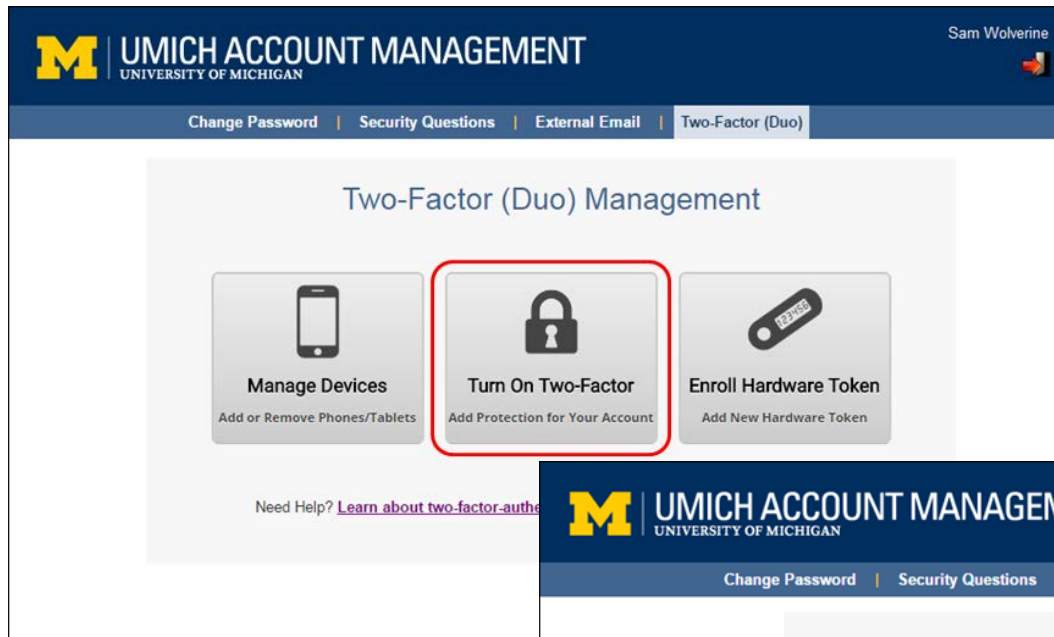
The screenshot shows the Weblogin login page for the University of Michigan. At the top is a dark blue header with the yellow 'M' logo and the text 'WEBLOGIN UNIVERSITY OF MICHIGAN'. Below the header, the text 'Enter your Login ID and Password' is centered. There are two input fields: the first is labeled 'Username or Friend ID' and the second is labeled 'Password'. Below these fields is a blue 'Log In' button. At the bottom right, there is a link that says 'Need help?'.



# Turn On Two-Factor

## Step 1: Enroll      Step 2: Flip the Switch

[password.it.umich.edu](https://password.it.umich.edu)



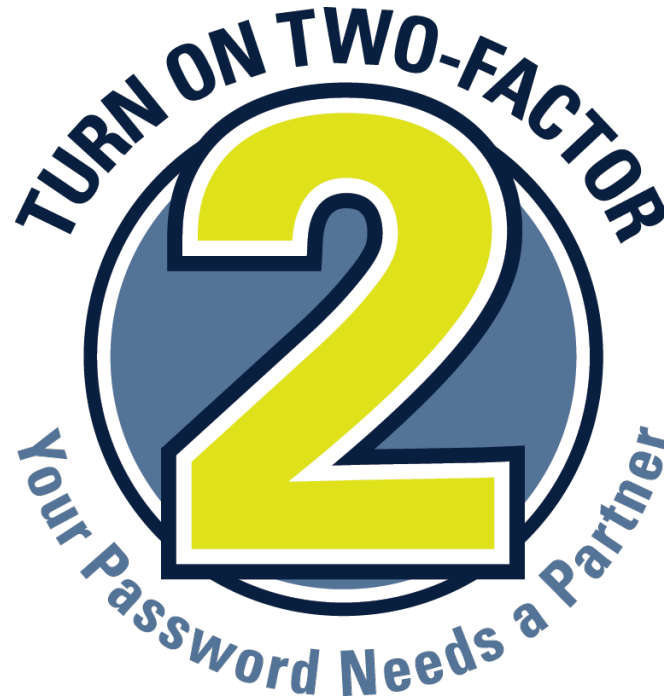


## How You Can Help

- **Be a two-factor champion** in your area!
  - Turn on Two-Factor for Weblogin
- **Encourage your colleagues** to turn it on
- **Help people enroll in Duo** for the first time
  - Show people the smartphone app!
  - Remind them of all options
- **Share your personal stories** of identity theft or phishing attempts or those you know about at U-M



## For More Information



<http://its.umich.edu/two-factor-authentication>

[2FA.Project.Contact@umich.edu](mailto:2FA.Project.Contact@umich.edu)





## Turn on Two-Factor for Weblogin Tips

- Enroll a primary and backup method (app + office phone is popular option)
- Keep your phone/device handy
- Lock your screen instead of logging-off
- Keep in mind you won't be prompted to log-in more frequently; just adding a second step