FAQs: ***Off Campus access to Office 365 is now secure with Two-Factor Authentication***

What is Office 365?

Office 365 is a line of Microsoft applications that reside outside of your computer or on a cloud but accessible to you from anywhere. These applications include SharePoint Online, OneDrive for Business, Microsoft Teams and more. See the complete Office 365 App List or log in to the My UT Health Intranet to access these applications.

What are the upcoming changes to protect University data in Office 365?

Starting on **Wednesday, March 6, 2019,** faculty, staff and student employees who log in to Office 365 from a **non-University network** through a web browser will be prompted for two-factor authentication (**2FA**) with DUO Security. This change will add a dynamic component to Office 365 browser log ins by requiring two components of authentication: something you know (password) and something you have (a registered device with DUO).

Why is this change happening?

About 80% of confirmed data breaches involved weak or stolen passwords, according to Verizon's Data Breach Investigations Report. If your password is compromised, you will be alerted right away with 2FA on your registered device if someone is trying to log in as you. These additional security checks will protect University data in My UT Health Intranet, SharePoint Online, OneDrive for Business and other Office 365 applications.

Will I be affected by this change?

You will not be affected by this change when you are connected to the University's network by: joining HSCwave or HSCguest, having a wired Ethernet network on campus or using the University's Virtual Private Network (VPN) from off campus. Office 365 desktop applications installed on a work or personal computer will not require 2FA, neither will Office 365 mobile applications.

What action am I required to take?

Employees who work off campus and have not enrolled in DUO Security will need to set up 2FA by visiting https://infosec.uthscsa.edu/two-factor-faqs.

How is "on campus" or "University network" defined?

You are connected to the University's network when you join the HSCwave or HSCguest wireless network, have a wired Ethernet network on campus or use the University's Virtual Private Network (**VPN)** from off campus. Some examples of on campus locations include satellite facilities, clinics, observatories and other teaching, research or patient care facilities that are owned/operated by the Institution. 2FA with DUO is *not required* to access Office 365 in these scenarios.

How is "off campus" or "non-University network" defined?

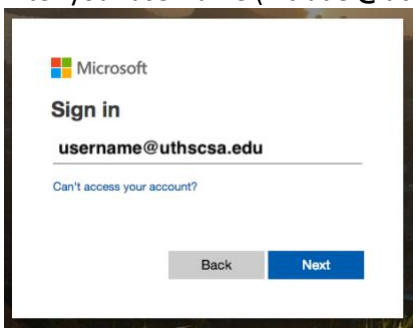
Some examples of off campus or remote locations include an employee's home, hotels, airports, conference centers or coffee shops. The wireless internet provided by a mobile carrier on a phone/tablet is considered a non-University network. 2FA with DUO is required to access Office 365 through a web browser if the VPN is not utilized in these scenarios.

FAQs: ***Off Campus access to Office 365 is now secure with Two-Factor Authentication***

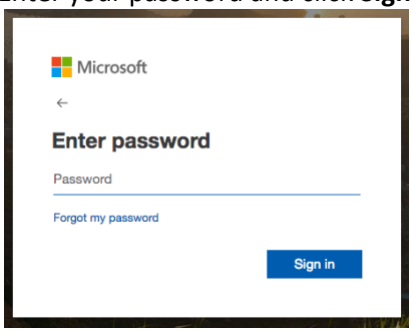
How can I log in to Office 365 using 2FA starting on 3-6-19?

- Step 1: Open a web browser and log in to https://uthealthsa.sharepoint.com/

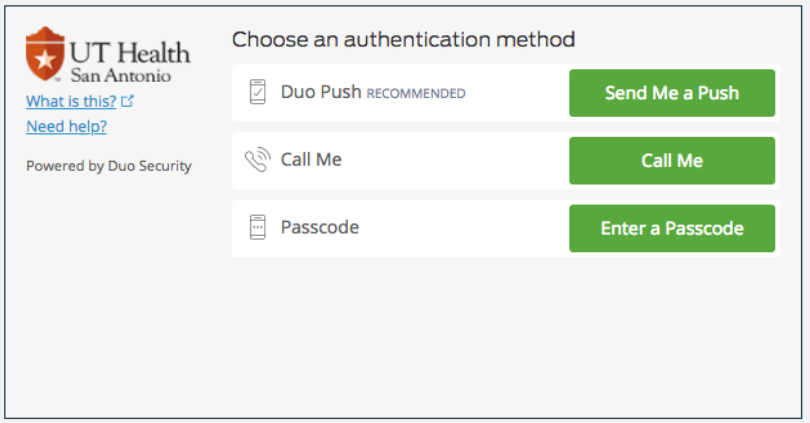
- Step 2: Enter your username (include **@uthscsa.edu**) and click **Next**.



- Step 3: Enter your password and click **Sign in**.



- Step 4: Choose an authentication method via Push (DUO app notification on your mobile device), Phone call or Passcode (from DUO mobile or an SMS text message)



- Step 5: Complete the authentication process by-
  - Acknowledging the DUO app notification on your mobile device; or
  - Following the instructions over the phone; or
  - Entering the passcode from DUO mobile or SMS text message

For more information, visit Infosec.uthscsa.edu or contact the IMS Service Desk at 210-567-7777.