

From: Gilinson, Randi D <rgilinson@uabmc.edu>
Sent: Friday, March 13, 2020 4:10 PM
To: DOPM All Users <DOPMAllUsers@uabmc.edu>
Subject: FW: Computer Tip of the Week -- Special Edition re Working from Home

Special Edition re Working from Home

Brought to you by
Lisa Schwaiger
 - DOPM HelpDesk Triage and
 Computer Tech in MT-403



SITUATION/QUESTION:

I am thinking I should probably start working from home when I can.
 What is the contingency plan, to let me do that?

SOLUTION/ANSWER:

In general, we have a HelpPages part of our website: <https://www.uab.edu/medicine/dopm/help>

If you want to work from home then you must have VPN. See more about VPN and its installation steps, click the link in **green** below.

So we suggest you do that over the weekend, and then get back with us if you have concerns on Monday.

To check your **email from home**, you will need to do one of these:

	Just use webmail on your browser from your home computer.
	This is easiest because it doesn't require VPN HOWEVER , first (while still at <u>Medical Towers</u>) you will need to set up the 2FA (2 Factor Authentication) that the email provider (HSIS) requires. See BELOW for how to do that.
	Connect the VPN and then use webmail
	Connect the VPN and then remote into TS4 (which is our Terminal Server) and set up Outlook
	Connect the VPN and then remote into your actual work computer

To check your **files from home**, you will need to do one of these:

For all Network drives (i.e., H:drive to Z:drive)	Connect the VPN and then remote into TS4 (which is our Terminal Server) Important: You must first be granted permission to do this, if you don't have it already. (To request it, email to dopmHelp@uabmc.edu)
For all Network drives <u>plus</u> what's on your actual computer (aka C:drive or desktop)	Connect the VPN and then remote into your work computer Important: You must first be granted permission to do this, if you don't have it already

(To request it, email to dopmHelp@uabmc.edu and include your IP Address, which is the large number starting with 138.26 at <https://whatismyipaddress.com/>)

Links you'll need (or helpful) re the above

re	
How to get and use VPN: NOTE: VPN = Cisco Connect	https://www.uab.edu/medicine/dopm/help/remote/vpn
webmail	Directly at https://webmail.uabmc.edu/ More background at https://www.uab.edu/medicine/dopm/help/set-up-email-outlook/web-based-email
How to access TS4 (aka the Terminal Server) NOTE: You need to request access to this first, by emailing to us at dopmHelp@uabmc.edu	<ul style="list-style-type: none"> • Simple version: TOP OF https://www.uab.edu/medicine/dopm/help or • More detailed version: https://www.uab.edu/medicine/dopm/help/remote/gateway
How to access your work computer NOTE: You need to request access to this first, by emailing to us at dopmHelp@uabmc.edu <u>IMPORTANT/REQUIRED:</u> In your request, include the IP address of your work computer, which is the large number starting with 138.26 at https://whatismyipaddress.com/ and note that number down for your use when at home.	Same instructions as just above except you will use your work computer's IP address instead of "TS4.dopm.uab.edu"
How to set up Outlook	https://www.uab.edu/medicine/dopm/help/set-up-email-outlook

Was this helpful? Do you have suggestions for a future Tip of the Week? Do you have any other comments?

Let us know at dopmHelp@uabmc.edu

To see an archive of past Tips of the Week: <http://www.uab.edu/medicine/dopm/help/totw>

From: dopmannouncement <dopmannouncement@uabmc.edu>
Sent: Monday, August 12, 2019 5:20 PM
To: DOPM All Users <DOPMAllUsers@uabmc.edu>
Subject: Additional Information - Multi-Factor Authentication (MFA) for Using Outlook Web Access (OWA) from Offsite

Everyone,

Thank you to everyone who was skeptical of two specific emails that appeared in your inboxes over the weekend. Though they appear suspicious, they are actually legitimate:



AND



HSIS implemented Multi-Factor Authentication (MFA) for webmail over the weekend. The emails describing this implementation are lacking additional details and contain minimal instruction. You can defer multi-factor authentication actions until a later date if:

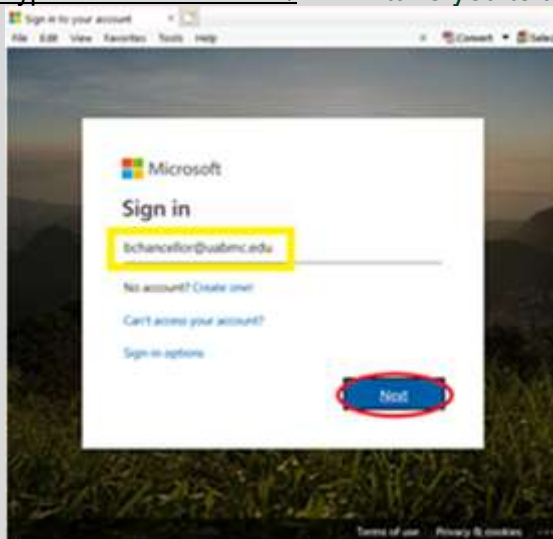
- you do not access your UABMC webmail, OR
- you use UABMC email on your phone by way of MaaS360 or Intune Mobile Device Management

Because of MFA, when you are not connected to a UAB or UABMC network, then opening UAB Webmail, <http://webmail.uabmc.edu/OWA>, will result in a multi-factor screen similar to the following (my iPhone uses Safari):

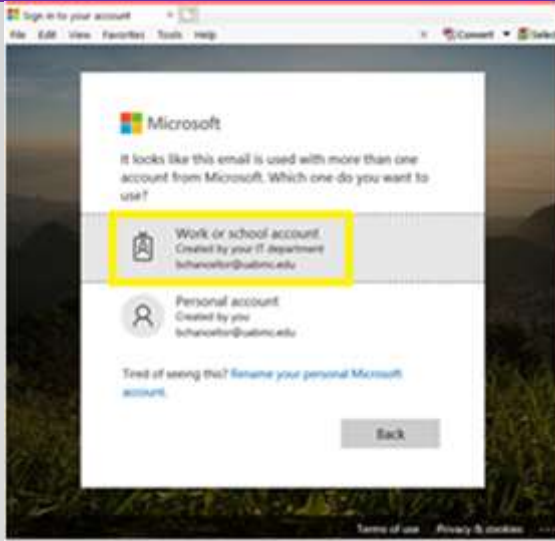


To setup your UAB Health System profile and your security verification methods, then read and follow the following instructions while you are connected to a UAB or UABMC network.

Within each email is a link (circled red above). HOWEVER, the <https://myprofile.microsoft.com/> link from the second email is the only valid one you should access. While you are connected to a UAB or UABMC network, click on the <https://myprofile.microsoft.com/> link to take you to a Microsoft website:



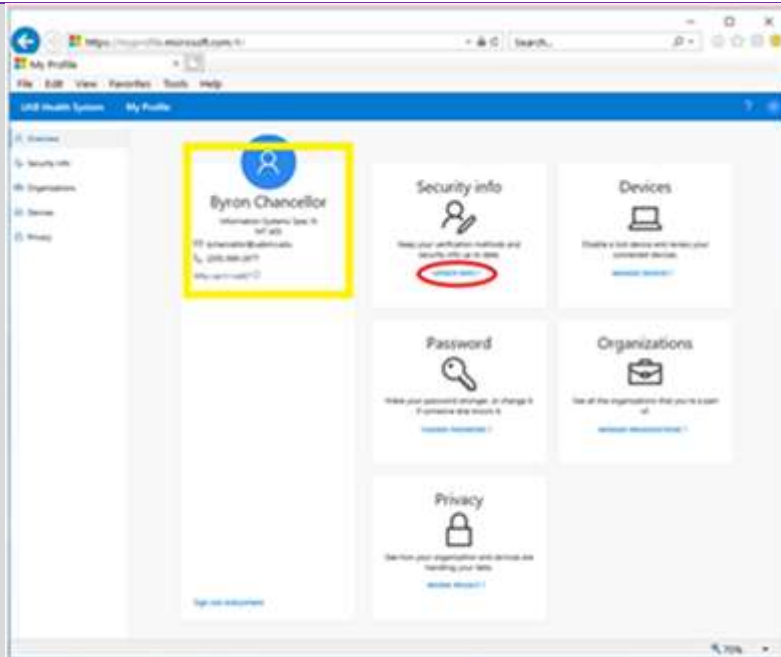
Enter your full UABMC email address
Click Next
Choose "Work or school account":



Enter your email password (One Password) if you are prompted to enter a password
Click "Sign in":



If you are connected to a UAB or UABMC network, then you will see something similar to the following:

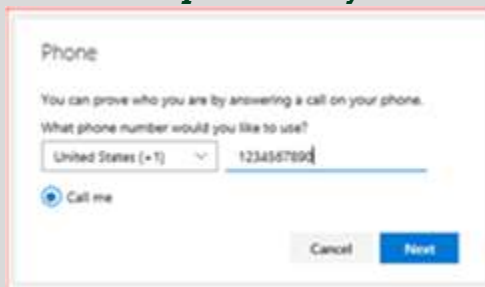


Click/Locate “Update Info” OR “Security Info”
Begin adding security methods to your UABMC email (One Password) Account by clicking
“Add method”:



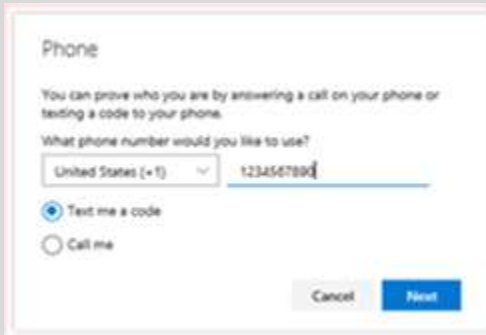
Choose from any and all of the four methods – Alternate phone, Phone, Security questions, and Microsoft Authenticator – which are described below.

Alternate Phone – prove who you are by answering a call on your phone:



You will hear an automated voice prompting you to press the pound (#) key to continue/verify. This message will occur one time and does not repeat.

Phone – prove who you are by receiving a text containing a code on your cell phone:



The screenshot shows a 'Phone' verification screen. It includes a title 'Phone', an explanatory sentence, and a question: 'What phone number would you like to use?'. Below this is a dropdown menu for the country (set to 'United States (+1)') and a text input field containing '1234567890'. There are two radio buttons: 'Text me a code' (which is selected) and 'Call me'. At the bottom, there are 'Cancel' and 'Next' buttons.

and then enter the received code:



The screenshot shows the second step of the 'Phone' verification process. It says 'We just sent a 6 digit code to +1 [REDACTED]. Enter the code below.' There is a text input field labeled 'Enter code' and a 'Resend code' link below it. At the bottom, there are 'Back' and 'Next' buttons.

Security questions – prove who you are by answering questions that only you know:



The screenshot shows a 'Security questions' screen. It contains five questions, each with a dropdown menu and a text input field. The questions are: 'What city were you in on New Year's 2000?' (input: 'Somewhere'), 'What were the last four digits of your childhood teleph...' (input: '9999'), 'What was the make and model of your first car or moto...' (input: 'Make Model'), 'What was your childhood nickname?' (input: 'Nickname'), and 'What was the name of the first school you attended?' (input: 'School Name'). At the bottom, there are 'Cancel' and 'Save' buttons.

Authenticator app – use the Microsoft Authenticator app on your device (similar to using Duo Mobile 2-Factor Authentication):

!! ATTENTION !! RECOMMENDED !! NOTICE !! CONSIDER !!

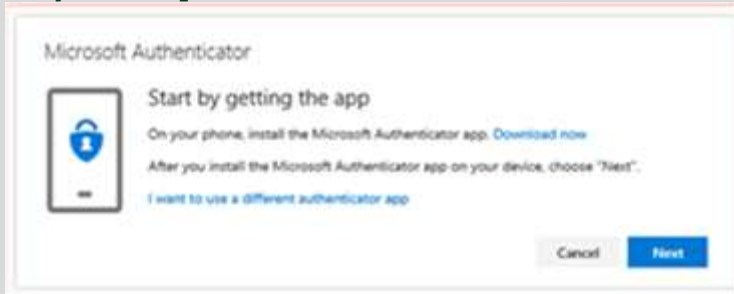
- The Microsoft Authenticator app **REQUIRES** a Passcode/PIN Code to secure your mobile device. Do NOT continue with Microsoft Authenticator app method if your mobile device is not secured with a Passcode/PIN Code.
- Do NOT use the “Download Now” link on your computer (shown in the screenshot below). **USE YOUR “APP STORE”** to install the Microsoft Authenticator app.

- **BEFORE** adding this method, **INSTALL** the Microsoft Authenticator app on your device via your “app store”. The website may time-out during this process depending on your ability to install in a timely manner.

!! ATTENTION !! RECOMMENDED !! NOTICE !! CONSIDER !!

On your device, open Microsoft Authenticator app.
Allow Notifications for Microsoft Authenticator app.

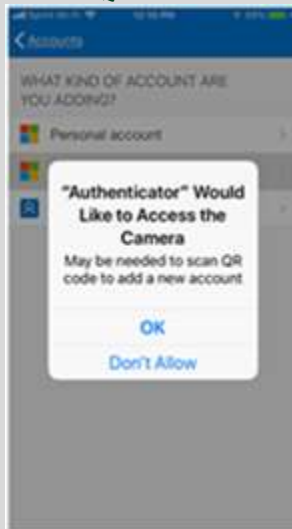
On your computer, Click “Next”:



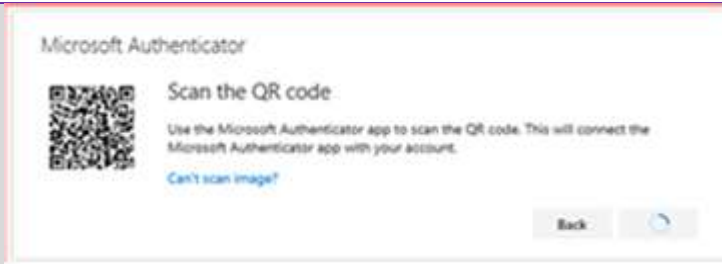
On your device, Add an account and choose Work or school:



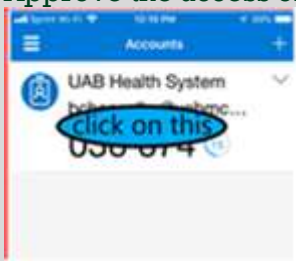
Microsoft Authenticator will need to access the camera of your device in order to scan a QR Code:



Scan the QR Code that appear on the website (NOT the one shown below):



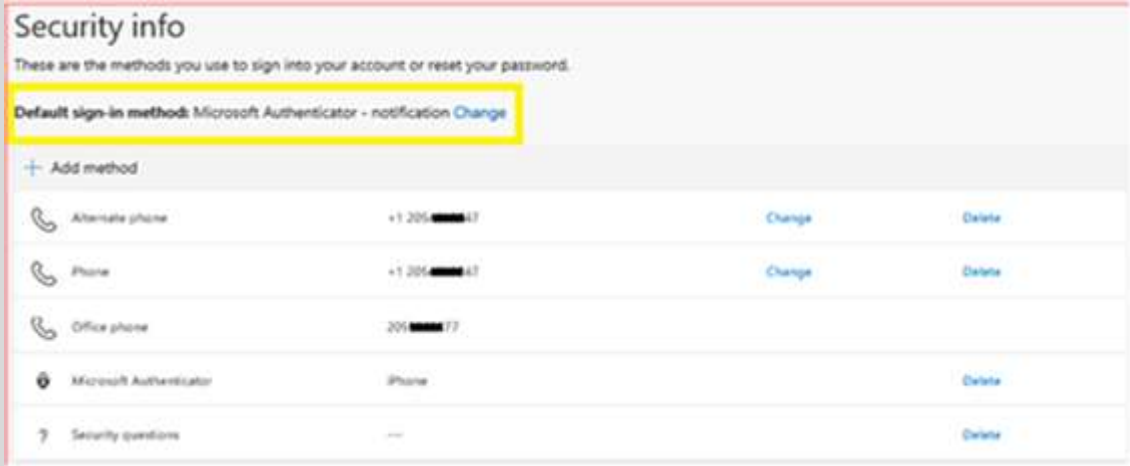
Approve the access on your mobile device within the Microsoft Authenticator app



The website should then indicate the approval:



Once you complete adding security methods to your UABMC email, then you will have the opportunity to set a default sign-in method as well as manage the security methods:



Thank you for your patience. If you have any concerns or questions, then please contact the DOPM Helpdesk, 205-934-7662 OR DOPMHelp@UABMC.Edu. Alternatively, you can

also contact the HSIS Help Desk at 205-934-8888. Regardless of which method you use to enroll, you will need to have a cell phone to setup Multi-Factor Authentication (MFA).

Thank you,

Byron Chancellor

Information Systems Specialist III

Division of Preventive Medicine, School of Medicine

University of Alabama at Birmingham

BChancellor@UABMC.Edu