Memo

Attention: All employees

From: Max Santomauro, CISO

Date: October 22, 2024

Subject: Retro on the use of the Microsoft Authenticator App

The organization provided Choose your own device (CYOB) phones to employees are a necessity in the in the continuous function of the organization. However, risks associated with these devices are at an all-time high. There are perpetual external threats that seek to damage and/or steal our network infrastructure and sensitive data. Therefore, this guide provides the phone user a means by which to set up and use the Microsoft Authenticator App as a Multi-factor protection against these external threats. If you want to experience this guide in interactive mode, please click on this link: https://www.canva.com/design/DAGSbyzLlvs/obzAkq9sQOkCoRHDDupSKw/view?utm_content=DAGSbyzLlvs&utm_campaign=designshare&utm_medium=link&utm_source=editor

Work assessment

I created this project with the organization's employee phone usage as my primary focus. The key obstacles to the security of these devices involves the weakest link in security, which is the employee, and how they use their phones. My efforts on this project satisfy the assignment criteria and can be regarded as complete.

- The first page of the book introduces the reader with a title and a short description that informs specifically what type of guide they are about to read.

- The second page lays out for the reader the content of the book.

- The third page informs the reader the purpose of the guide and the set-up requirements before setting up the Microsoft authenticator on their CYOB phones.

- Pages 4 through 9 instructs the reader step-by-step on how to install and set-up the Microsoft authenticator on their CYOB phones.

- The last page informs the reader about certain aspects of the Microsoft authenticator and offers a link for more in-depth details and help.

- The book is design with tabs at the top that the reader that click to skip into the section they want to read, has click tabs on the bottom left and bottom right to skip to the next or previous page, and a search bar for easy skimming.

Creative process, steps, and applications of the Microsoft Authenticator

The Microsoft Authenticator app is a vital tool for enhancing digital security through two-factor authentication (2FA). Setting it up involves a series of well-defined steps, guided by a creative process aimed at ensuring user accessibility and security. This paper outlines the steps taken to set up the Microsoft Authenticator app and explores its applications.

The Creative Process in Setting Up Microsoft Authenticator

1. **Understanding User Needs**: The initial stage involves recognizing the challenges users face with traditional passwords. Microsoft aimed to create a solution that was not only secure but also straightforward to implement, ensuring that users could easily adopt the app.

2. **Defining the Setup Process**: The design team of Microsoft defined a clear and concise setup process. This involved breaking down the steps into manageable parts, ensuring that users, regardless of their technical proficiency, could follow along without confusion.

3. **Designing an Intuitive User Experience**: The app's interface was designed with user experience in mind. Prompts, visual cues, and straightforward language guide users through the setup process, minimizing frustration and errors.

4. **Prototyping the Setup Flow**: Early versions of the setup process were tested with users to gather feedback. This iterative approach allowed for the identification of potential pain points, leading to refinements in the instructions and interface.

5. **Testing and Refinement**: The final setup process underwent rigorous testing. Usability tests ensured that users could successfully set up the app without assistance. Feedback led to enhancements, such as clearer instructions and improved error messages.

3. **Designing an Intuitive User Experience**: The app's interface was designed with user experience in mind. Prompts, visual cues, and straightforward language guide users through the setup process, minimizing frustration and errors.

4. **Prototyping the Setup Flow**: Early versions of the setup process were tested with users to gather feedback. This iterative approach allowed for the identification of potential pain points, leading to refinements in the instructions and interface.

5. **Testing and Refinement**: The final setup process underwent rigorous testing. Usability tests ensured that users could successfully set up the app without assistance. Feedback led to enhancements, such as clearer instructions and improved error messages.

Steps to Set Up Microsoft Authenticator

1. **Download the App**: Users begin by downloading the Microsoft Authenticator app from their device's app store, available for both Android and iOS.

2. **Launch the App**: Upon opening the app, users are greeted with a simple interface and an option to begin the setup process.

3. **Choose Account Type**: Users select the type of account they wish to add (Microsoft account or other accounts) based on their needs.

4. **Linking the Account**: For Microsoft accounts, users can choose to sign in using their credentials. For other accounts, they often need to scan a QR code provided by the service they wish to secure. This QR code is typically found in the security settings of that service.

5. **Confirming Authentication**: After entering a setup key, the app generates a unique time-based one-time password (TOTP). Users are prompted to enter this code back into the service they are securing, confirming the link between the Authenticator app and the account.

6. **Enabling Notifications**: Users can enable push notifications for easier sign-in. This feature sends a prompt to the app whenever verification is needed, allowing for quick and secure access.

Applications of Microsoft Authenticator

1. **Enhanced Security**: The primary application is the addition of a second layer of security for various online accounts, significantly reducing the risk of unauthorized access.

2. **Convenience**: With push notifications and easy account management, the app simplifies the authentication process, making it faster for users to access their accounts.

3. **Multi-Account Management**: Users can manage multiple accounts within the app, allowing for streamlined access to both personal and professional services.

4. **Integration with Services**: The app integrates seamlessly with a variety of services, including Microsoft 365, Google, and many others, enhancing security across platforms.

The setup process of Microsoft Authenticator is a product of a thoughtful creative process aimed at ensuring user-friendly security. By focusing on clear instructions and intuitive design, Microsoft has made it easier for users to enhance their digital security. The applications of the app extend beyond mere authentication, contributing to a more secure and convenient online experience.

Microsoft Authenticator

MICROSOFT AUTHENTICATOR APP USER GUIDE

A GUIDE FOR USING MICROSOFT'S TWO-FACTOR AUTHENTICATOR

🔍 ✕

CLICK ➤

CONTENT

CLICK

CLICK

Microsoft Authenticator

PURPOSE

USING THIS GUIDE FOR MICROSOFT'S TWO-FACTOR AUTHENTICATION (2FA) APP IS ESSENTIAL FOR SEVERAL REASONS. FIRST AND FOREMOST, A STRUCTURED GUIDE SIMPLIFIES THE LEARNING PROCESS, PROVIDING CLEAR, STEP-BY-STEP INSTRUCTIONS THAT ENSURE USERS CAN EFFECTIVELY SET UP AND UTILIZE THE APP. THIS IS PARTICULARLY IMPORTANT FOR THOSE WHO MAY NOT BE TECH-SAVVY, AS IT REDUCES CONFUSION AND INCREASES CONFIDENCE IN MANAGING THEIR ACCOUNT SECURITY.

SET-UP REQUIREMENTS

TO SET UP MICROSOFT AUTHENTICATOR ON YOUR PHONE, YOU'LL NEED TO FOLLOW THESE REQUIREMENTS:

1. COMPATIBLE DEVICE: ENSURE YOUR PHONE IS RUNNING A COMPATIBLE OPERATING SYSTEM (IOS 12 OR LATER FOR IPHONE, ANDROID 6.0 OR LATER FOR ANDROID DEVICES).

2. MICROSOFT ACCOUNT: HAVE A MICROSOFT ACCOUNT OR ANY ACCOUNT THAT SUPPORTS TWO-FACTOR AUTHENTICATION.

3. INTERNET CONNECTION: ENSURE YOUR DEVICE IS CONNECTED TO THE INTERNET.

4. DOWNLOAD THE APP: INSTALL THE MICROSOFT AUTHENTICATOR APP FROM THE APP STORE (IOS) OR GOOGLE PLAY STORE (ANDROID).

5. BACKUP METHOD: CONSIDER SETTING UP A BACKUP METHOD FOR ACCOUNT RECOVERY (LIKE A PHONE NUMBER OR ALTERNATE EMAIL).

ONCE YOU HAVE THESE REQUIREMENTS IN PLACE, YOU CAN START THE SETUP PROCESS IN THE APP

CLICK

🔍 ✕

CLICK

DOWNLOAD THE MICROSOFT AUTHENTICATOR APP

1. STEP 1: OPEN YOUR DEVICE'S APP STORE

OPTION 1

- FOR IOS DEVICES: OPEN THE APP STORE.
- FOR ANDROID DEVICES: OPEN THE GOOGLE PLAY STORE.
- LOOK FOR THE APP WITH THE MICROSOFT LOGO AND THE NAME "MICROSOFT AUTHENTICATOR".
- ENSURE IT'S DEVELOPED BY MICROSOFT CORPORATION.

OPTION 2

- SCAN THE BARCODE FOR THE DEVICE OWNED BELOW

2. STEP 2: DOWNLOAD THE APP

OPTION 1

FOR IOS: TAP THE "GET" BUTTON TO DOWNLOAD AND INSTALL THE APP.

OPTION 2

FOR ANDROID: TAP THE "INSTALL" BUTTON TO DOWNLOAD THE APP.
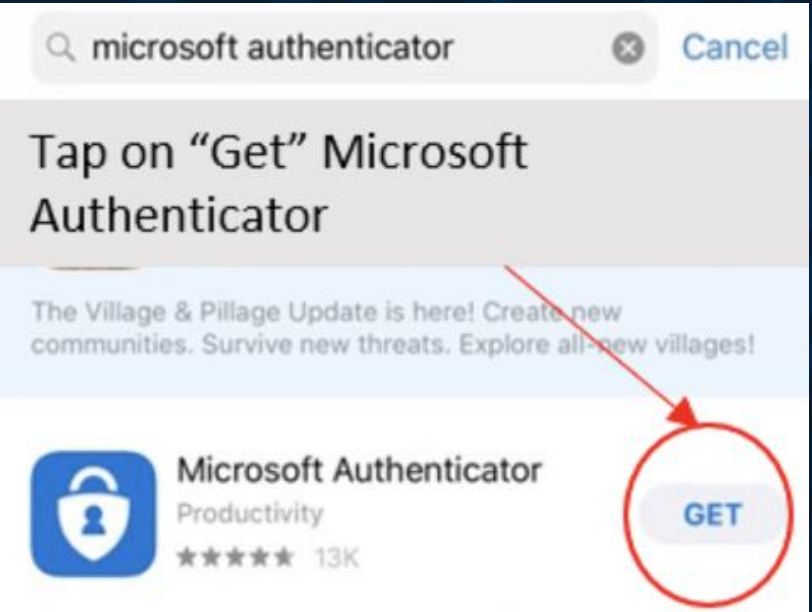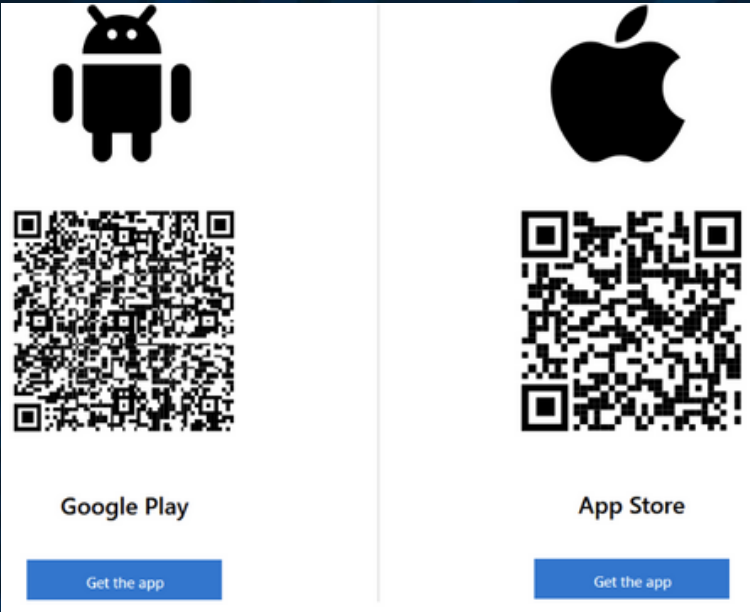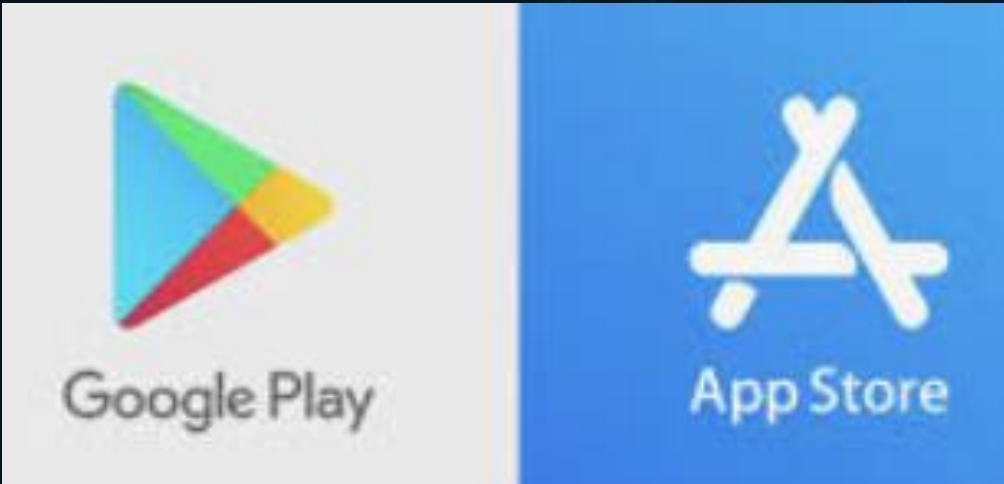
CLICK

CLICK

DOWNLOAD THE MICROSOFT AUTHENTICATOR APP

3. STEP 3: OPEN THE APP

ONCE INSTALLED, TAP THE "OPEN" BUTTON DIRECTLY FROM THE APP STORE, OR FIND THE MICROSOFT AUTHENTICATOR APP ICON ON YOUR HOME SCREEN AND TAP IT TO OPEN. OPEN THE AUTHENTICATOR. AND YOU WILL SEE THE "READY TO ADD YOUR FIRST ACCOUNT" IMAGE SHOWN ON THE RIGHT.
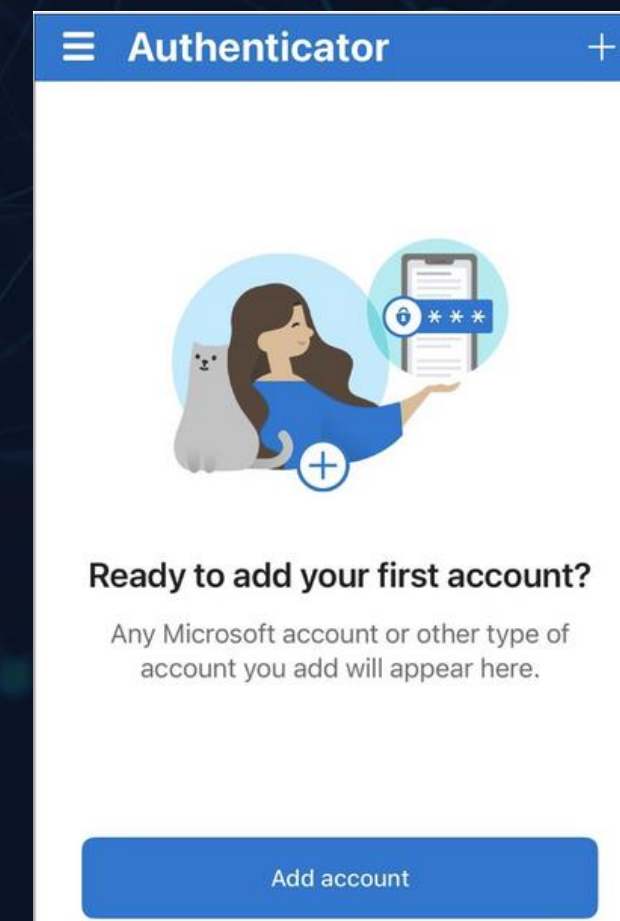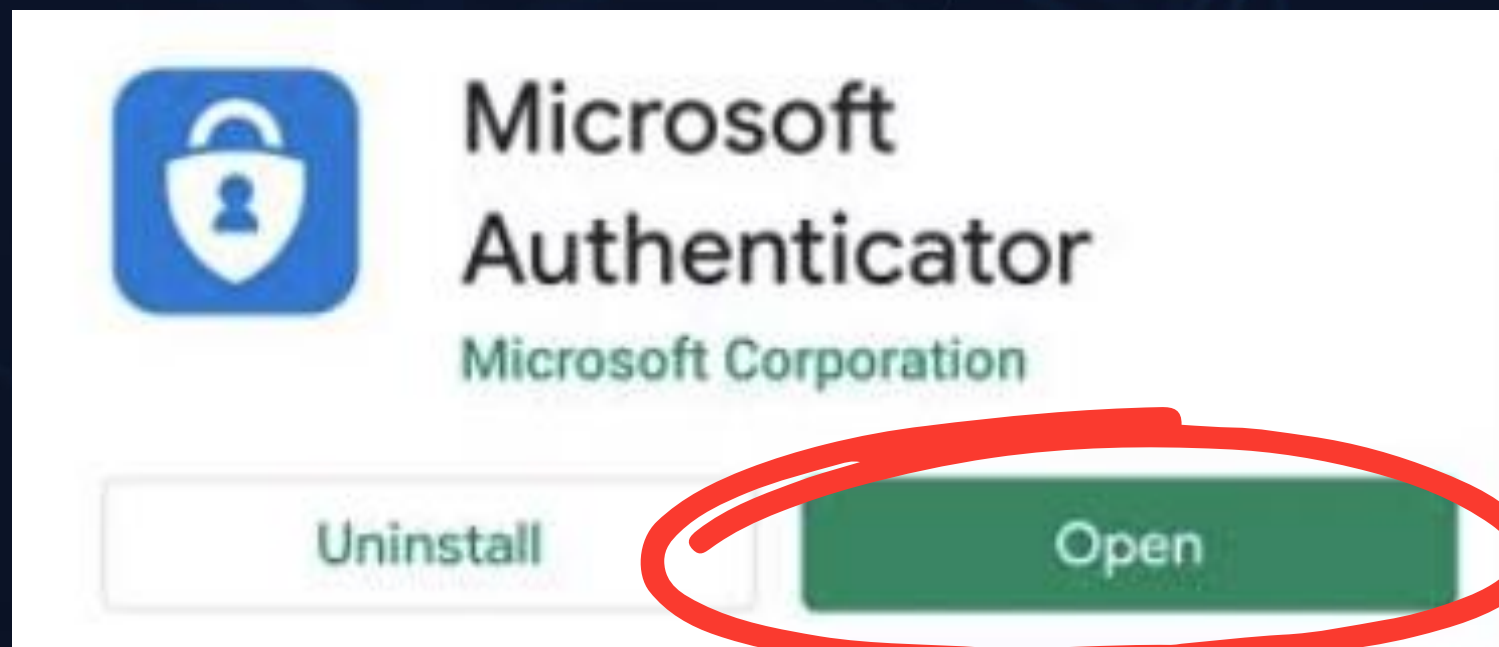
CLICK   CLICK

SETTING UP THE ACCOUNT

Microsoft Authenticator

1. STEP 1: ADD ACCOUNT IN APP

AFTER OPENING THE MICROSOFT AUTHENTICATOR APP ON YOUR PHONE, SELECT "ADD ACCOUNT". "CHOOSE PERSONAL ACCOUNT," "WORK OR SCHOOL ACCOUNT," OR "OTHER" FOR ACCOUNTS THAT ARE NOT MICROSOFT RELATED. ENTER EMAIL AND PASSWORD ONCE ONE OF THE CHOICES ARE PICKED. CHOOSE "OPEN BROWSER" TO CONTINUE SET UP

2. STEP 2: PAIR ACCOUNT

CONTINUE CLICKING NEXT THROUGH THE AUTHENTICATOR PROMPTS UNTIL YOU REACH THE LEFT IMAGE BELOW. CLICK "PAIR YOUR ACCOUNT IN THE APP BY CLICKING THIS" LINK. YOU WILL THEN BE SENT BACK TO THE APP AND PAIRED AS SHOWN IN THE RIGHT IMAGE

SETTING UP THE ACCOUNT

**Microsoft Authenticator**

3. STEP 3: CONFIRM

CLICK ON THE ACCOUNT TO CONFIRM IT IS GENERATING A CODE. THEN SWITCH BACK TO THE BROWSER AND CONTINUE THE PROCESS CLICKING NEXT. A CODE IS GENERATED AND IN THIS CASE THE CODE IS 24. SWITCH TO AUTHENTICATOR APP, ENTER CODE, AND CLICK YES. ENTER PHONE NUMBER AND YOU WILL RECEIVE A TEXT MESSAGE WITH A CODE. ENTER TEXT CODE AND COMPLETE THIS TASK.
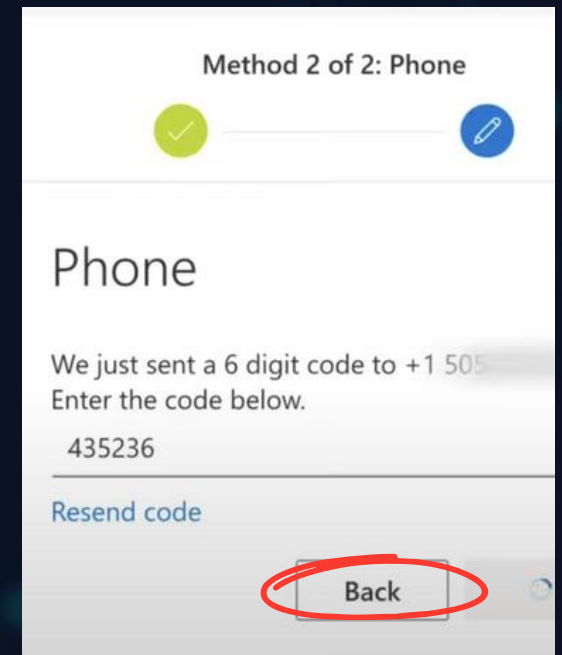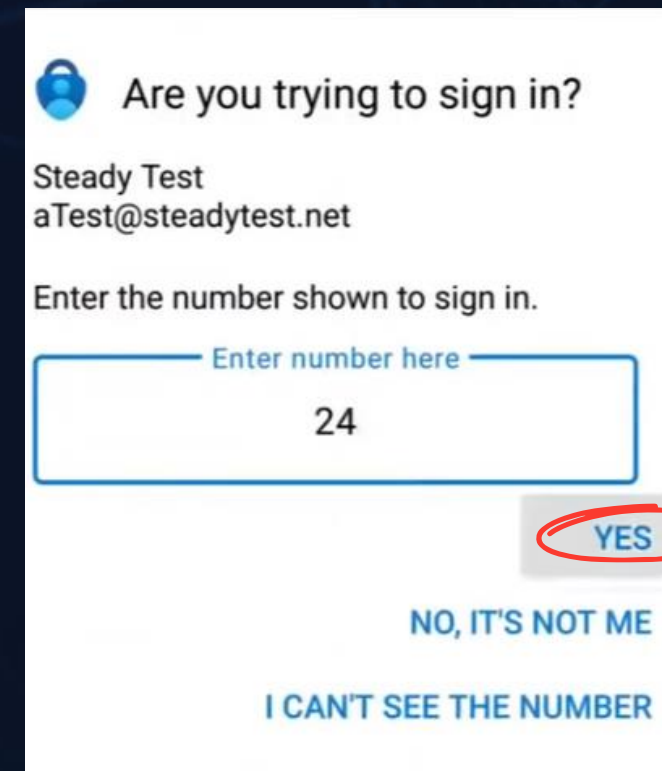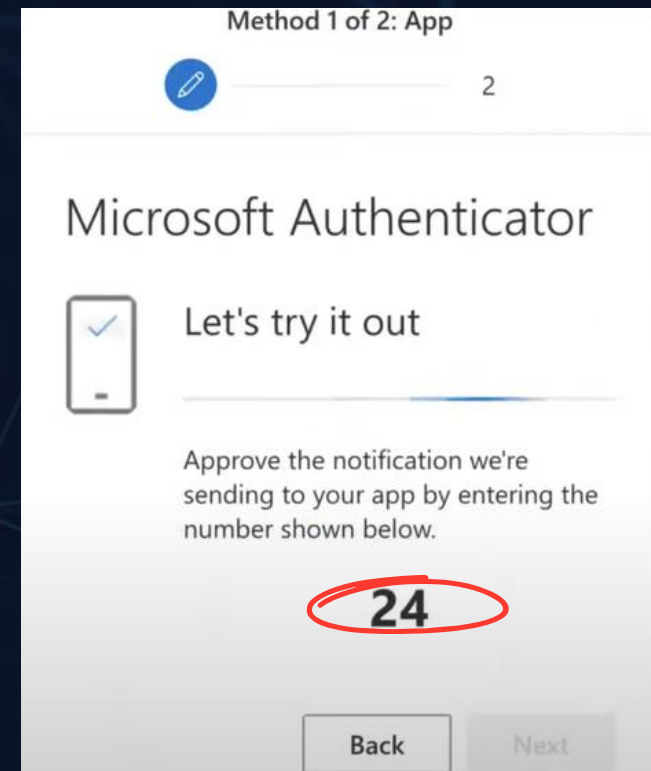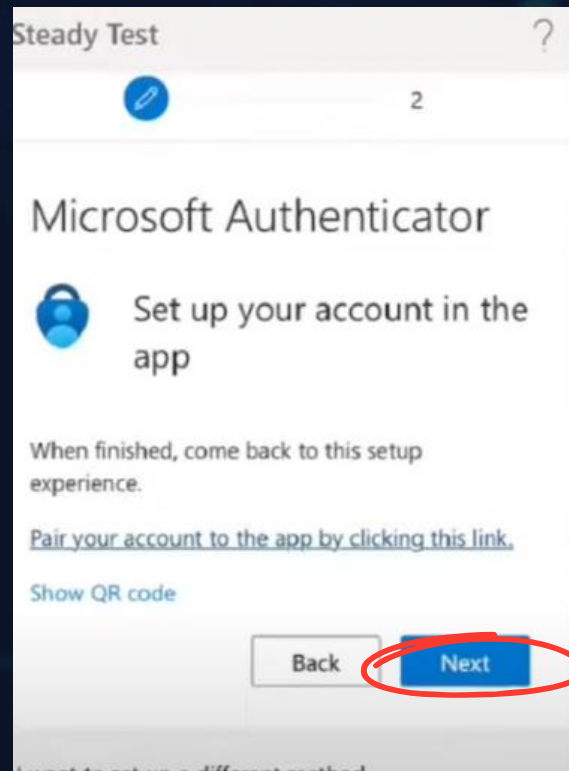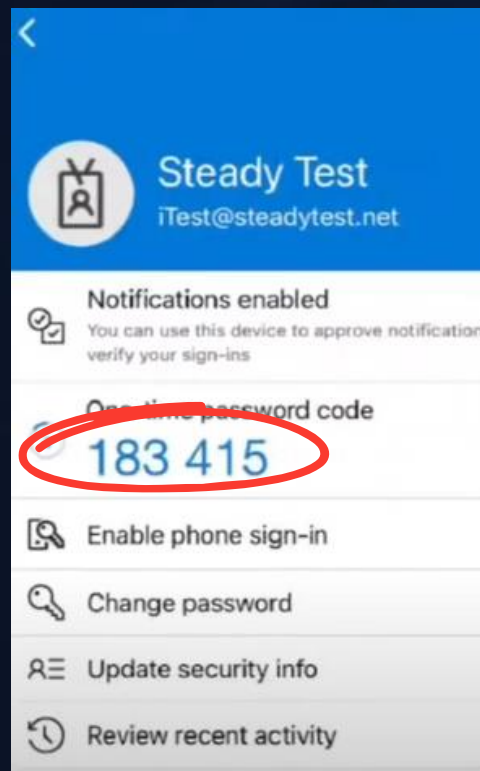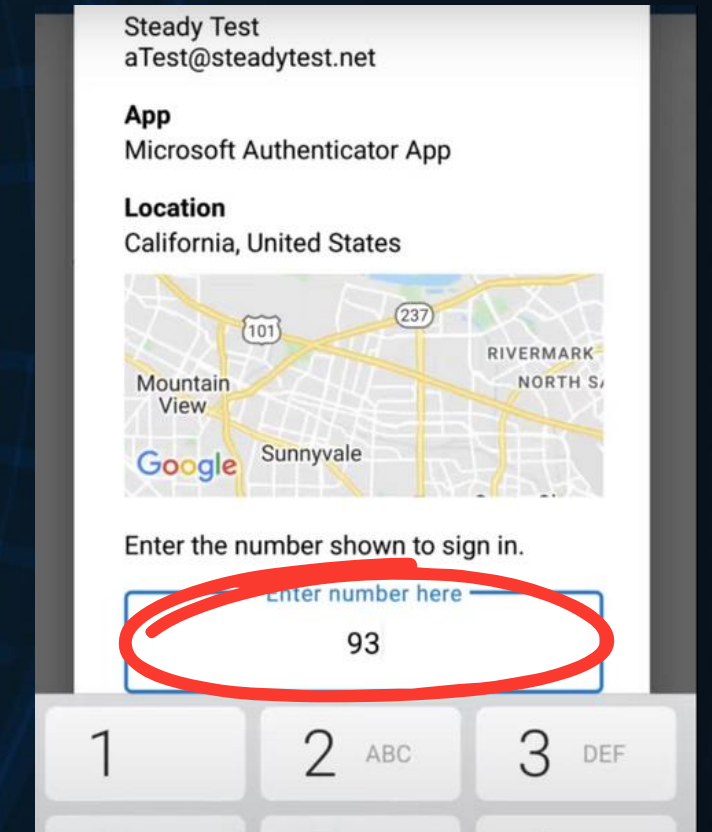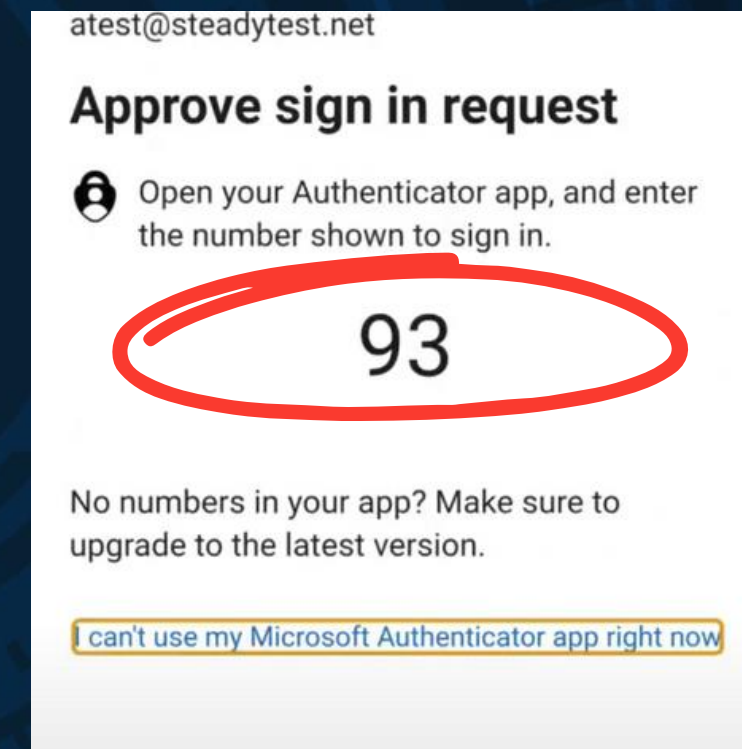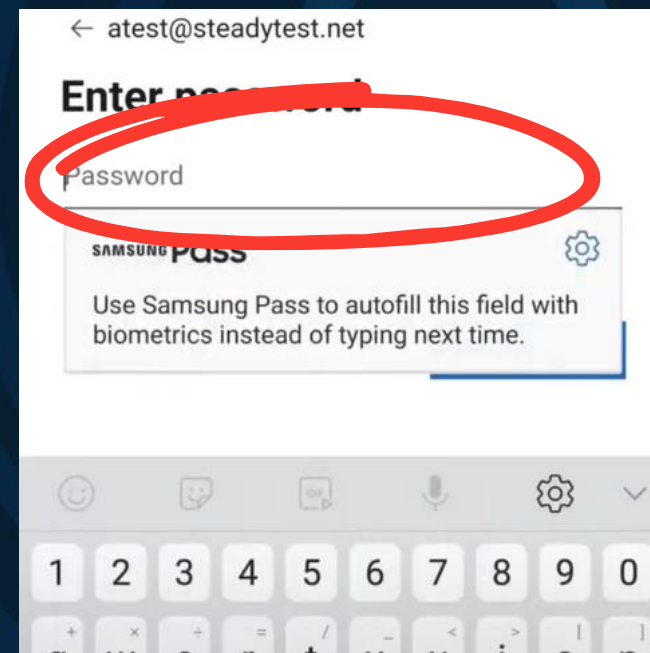

CLICK

CLICK

ENABLE PHONE SIGN-IN

4. STEP 4: ENABLE PHONE SIGN-IN

GO BACK TO THE AUTHENTICATOR APP , OPEN UP THE INDIVIDUAL ACOUNT (IN THIS CASE STEADY TEST), AND CLICK ON "ENABLE PHONE SIGN-IN." CLICK CONTINUE (IF YOU DON'T SEE A GREEN CHECK MARK FOR DEVICE REGISTRATION AND SET PASSCODE AND DOESN'T GIVE OPTION TO CONTINUE, CREATE A SUPPORT TICKET). LOGIN IN AGAIN WHEN AUTHINTICATION SCREEN POPS UP. A CODE (IN THIS CASE 93) APPEARS AND REMEMBER THE CODE. ENTER THE APP AND ENTER THE CODE..
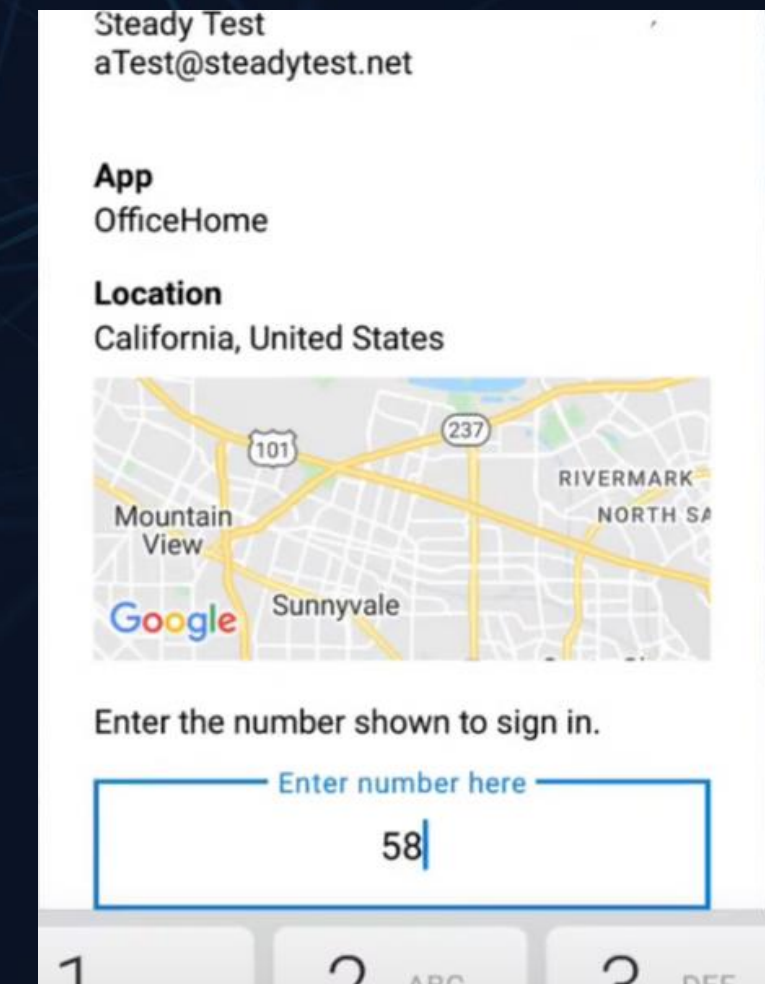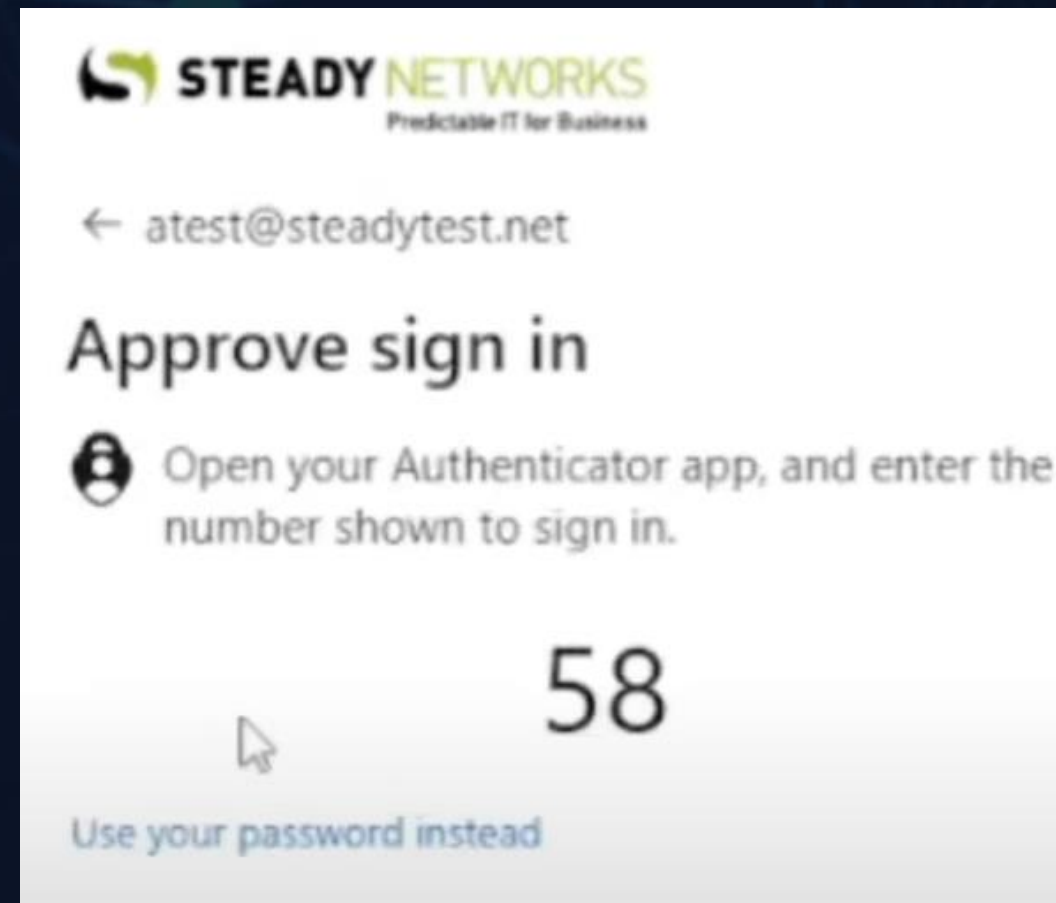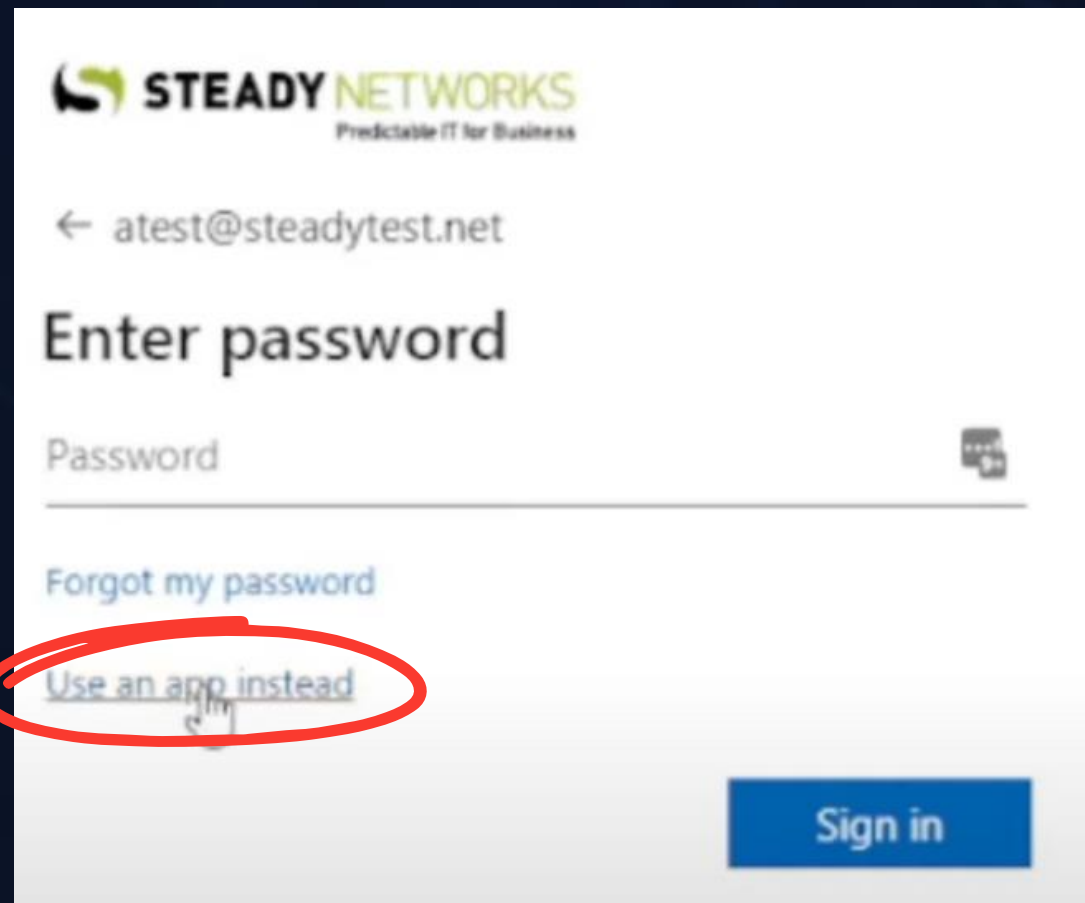

CLICK   🔍 ✕   CLICK

ENABLE PHONE SIGN-IN

Microsoft Authenticator

4. STEP 4: ENABLE PHONE SIGN-IN (CONTINUE)

THIS PROCESS ALLOWS YOU WHEN SIGNING IN TO CLICK ON "USE AN APP INSTEAD" RATHER THAN TYPING IN A PASSWORD AND A MAP OF LOCATION WILL BE DISPLAYED. WHEN TYPING IN CODE.
  - NOTE: MAP MAY NOT BE ACCURATE TO A STATE LEVEL, BUT THAT IS OKAY)

CLICK

CLICK

ABOUT THE MICROSOFT AUTHENTICATOR

MICROSOFT AUTHENTICATOR IS A FREE APP THAT HELPS YOU SIGN IN TO ALL YOUR ACCOUNTS WITHOUT USING A PASSWORD - JUST USE A FINGERPRINT, FACE RECOGNITION, OR A PIN.

YOU CAN USE AUTHENTICATOR TO SIGN IN TO YOUR MICROSOFT PERSONAL, WORK, SCHOOL OR OTHER ACCOUNTS.

AUTHENTICATOR CAN BE USED THREE WAYS:

- AS A WAY TO VERIFY SIGN-IN IF YOU FORGET YOUR PASSWORD.
- AS A WAY TO SIGN IN EVERY TIME, BY USING A ONE-TIME PASSWORD CODE TO INCREASE ACCOUNT SECURITY. THIS IS CALLED TWO-STEP VERIFICATION OR MULTI-FACTOR AUTHENTICATION.
- AS THE ONLY WAY TO SIGN IN - JUST TAP AN APPROVAL ON YOUR PHONE TO SIGN IN. THIS IS CALLED GOING PASSWORDLESS.

JUST FOLLOW THE THREE STEPS TO START USING AUTHENTICATOR TO SIGN IN.

1. GET THE APP.
2. ADD YOUR ACCOUNT.
3. LEARN HOW TO SIGN IN.

FOR MORE IN-DEPTH DETAILS AND HELP WITH THE MICROSOFT AUTHENTICATOR, CLICK THE LINK BELOW.

HTTPS://SUPPORT.MICROSOFT.COM/EN-US/ACCOUNT-BILLING/ABOUT-MICROSOFT-AUTHENTICATOR-9783C865-0308-42FB-A519-8CF666FE0ACC

CLICK