Cybersecurity Incident Response

In this episode of the DarkBox Archive, Andrew, Thai, and Josh explore incident response in cybersecurity. They define it as a structured approach to managing security breaches, aiming to limit damage and reduce recovery time. Key steps include Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. They emphasize the importance of having a plan, effective detection, damage control, threat removal, careful recovery, and post-incident analysis. Best practices include updating plans, fostering cybersecurity awareness, using automated tools, and clear communication protocols. Visit darkboxsecurity.com for more resources and join their community on Discord.

The Dangers of Phishing

We discuss the dangers of phishing and give ways to protect yourself. Phishing has evolved overtime and has become more difficult to detect. It is considered the number one way companies get breached.

Why cybersecurity is

important

Join our Discord channel here.

Our first episode of our cybersecurity podcast. We discuss why cybersecurity is so important and give some advice on how to improve your cybersecurity if you are a business or for personal life.

Top 5 reasons to do a penetration test

Penetration testing, also known as pen tests, are authorized attacks against your computer systems to look for any security vulnerabilities. Here are the top 5 reasons on why you should perform a pen test:

1. Identify vulnerabilities: A penetration test can reveal weaknesses in an organization's security infrastructure that could be exploited by attackers.

2. Compliance: Many industries have regulations that require regular penetration testing to demonstrate compliance with security standards.

3. Improve incident response: Understanding how an attacker might penetrate a network can help an organization develop better incident response plans.

4. Prioritize security investments: By

identifying vulnerabilities, a penetration test can help an organization prioritize which security measures to implement first.

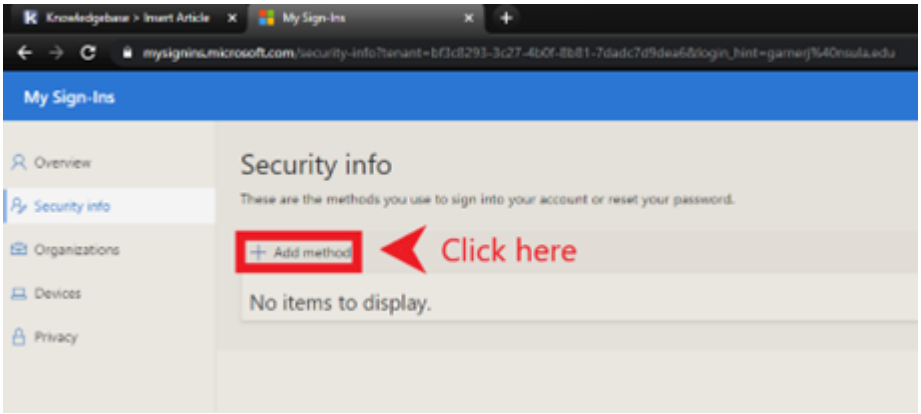
5. Improve employee awareness: A penetration test can help raise awareness among employees about the importance of security and the potential consequences of security breaches.

How To Set Up Microsoft Authenicator on iPhone

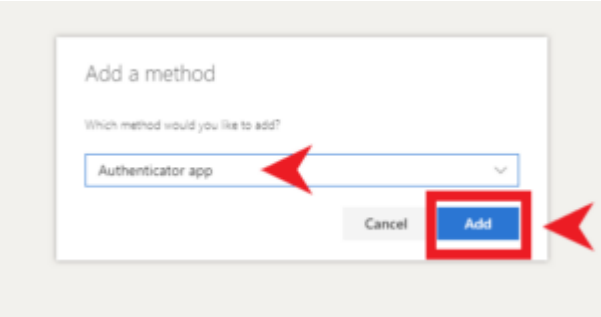
This guide will provide instructions on applying multi-factor authentication (MFA) to your company Microsoft account using the Microsoft Authenticator mobile app on your Apple device (e.g. smartphone or tablet). MFA ensures your account stays secure by prompting you to approve new sign-ins, making it more difficult for other people to sign into your account.

Note: In this article, I will refer to a mobile device as "device", but this will likely be your smartphone. This authentication method will be of much more use to you by using a device you will have with you most often.

1. Navigate to the https://mysignins.microsoft.com/security-info web address. Log into your company Microsoft account. Click "Add method".

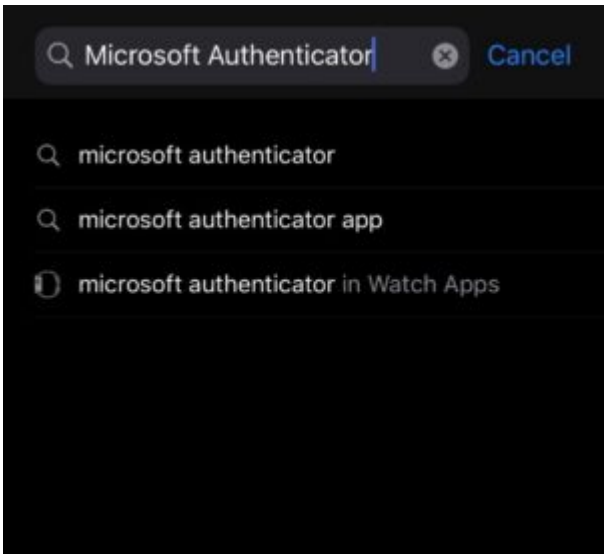


2. Ensure "Authenticator app" is shown in the drop-down field. If it isn't, click the down arrow towards the right and select "Authenticator app" from the choices given. Click "Add".

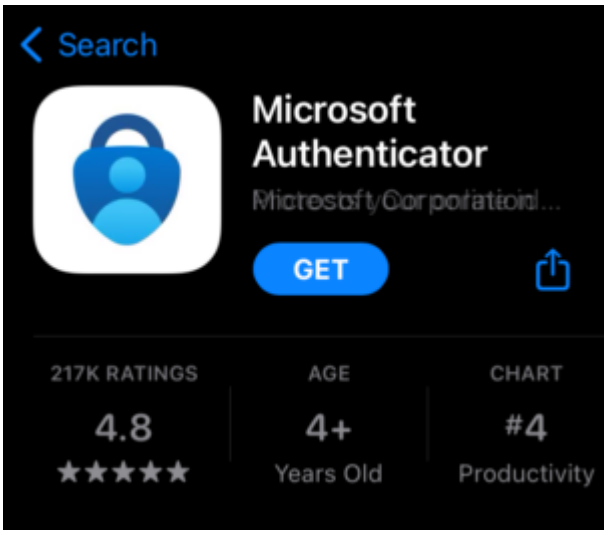


3. Open your Apple device and open the App Store. The icon is a white shaped “A” with a blue background as shown in the image below.

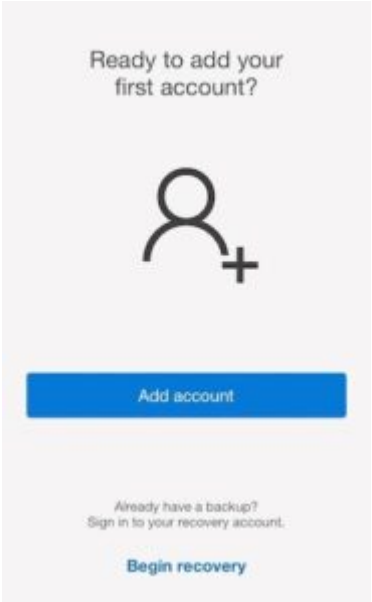
4. Search for “microsoft authenticator” in the store (search icon is at the bottom of the screen when you open the App Store). In the suggestions below the search bar, tap on the suggestion that says “Microsoft Authenticator” (the icon has a blue lock on top of a white background, as shown in the image below). If this suggestion does not show, you can search for it manually on the store and it should be the first app on the page.



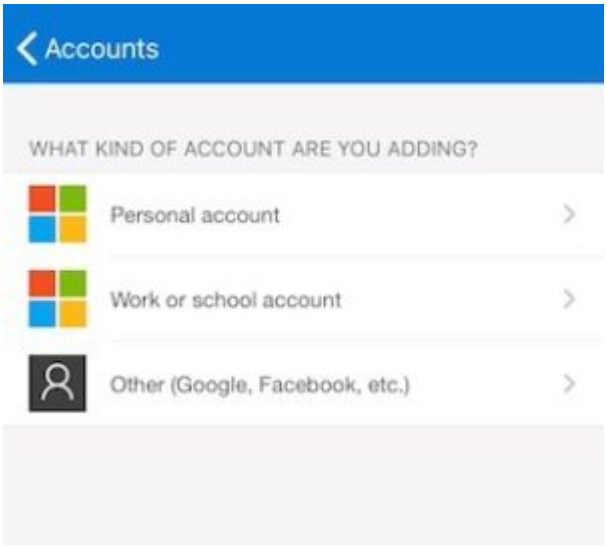
5. Tap on the “Get” button. Once downloaded, “Get” is replaced with “Open”. When you see “Open”, tap on Open to launch the App.



6. After opening the app, tap “Add account” as shown in the below image.

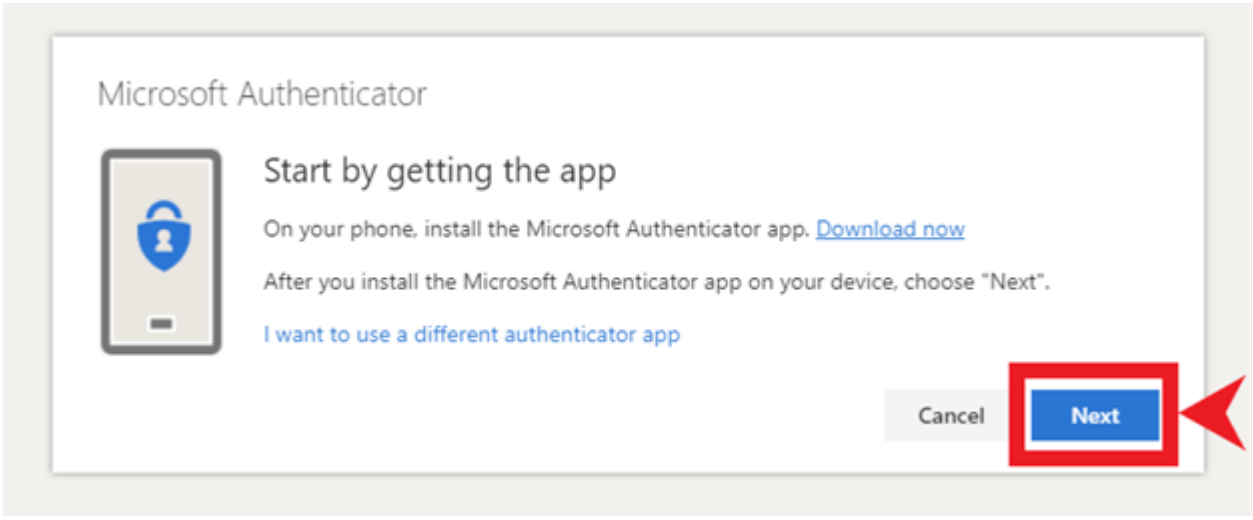


7. Select, “Work or school account”.

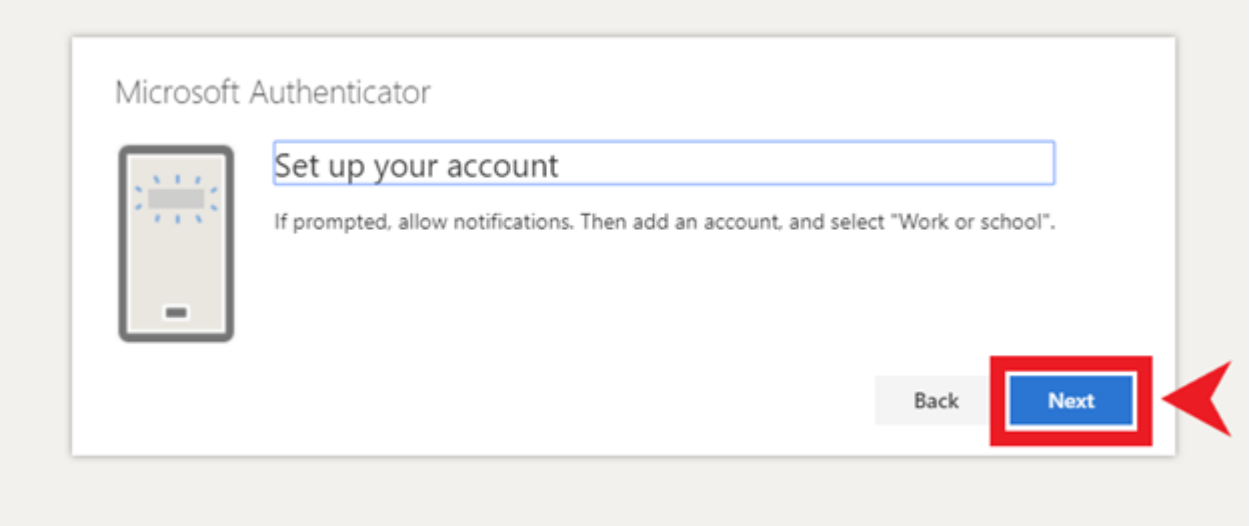


8. The app will open your device's QR code scanner. You will need this for the next step. Go back to your computer and click "Next".

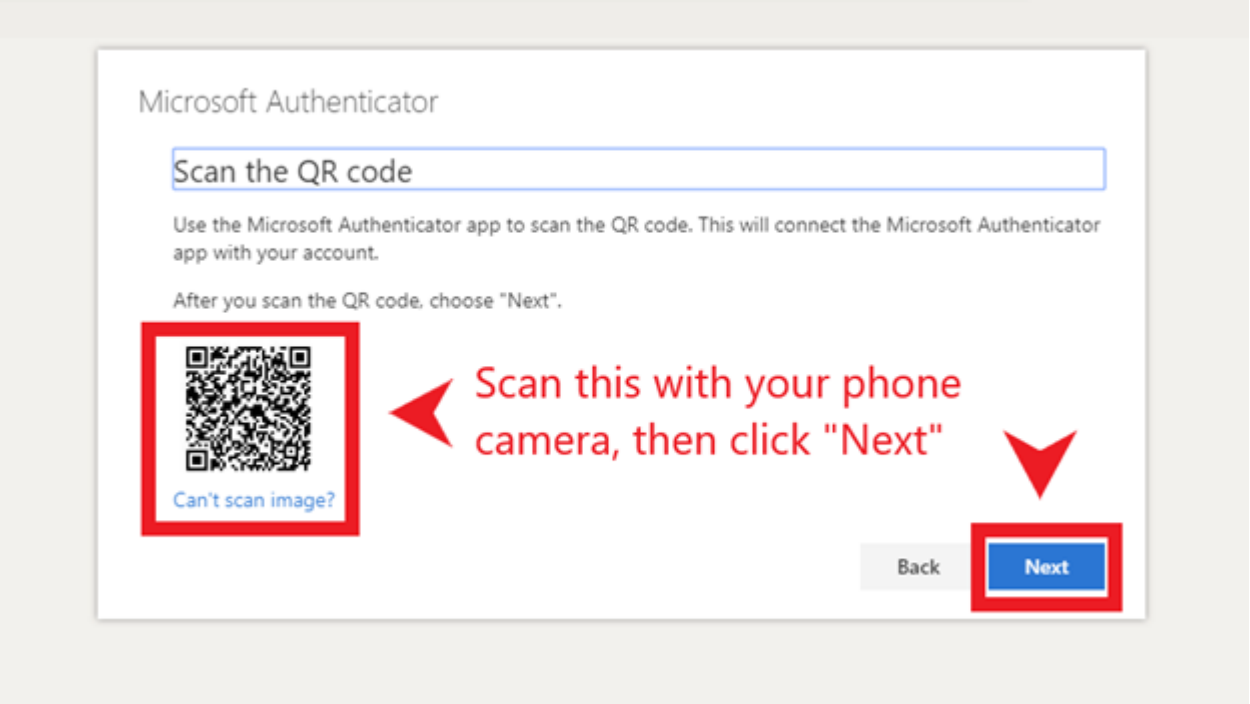
Note: Some of the following instructions will not include visual aids because the app disallows screenshots during the following process.



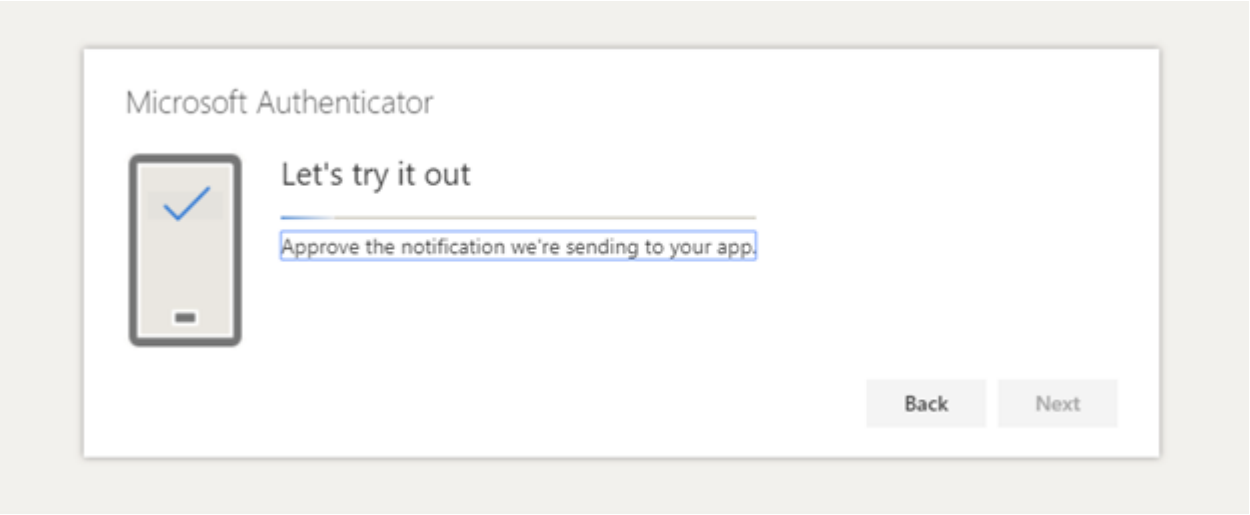
9. Click "Next".



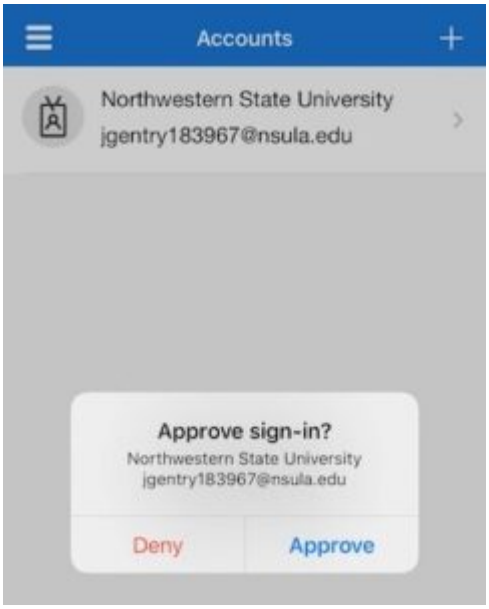
10. Using the QR scanner on your device, scan the QR code shown and click “Next”.



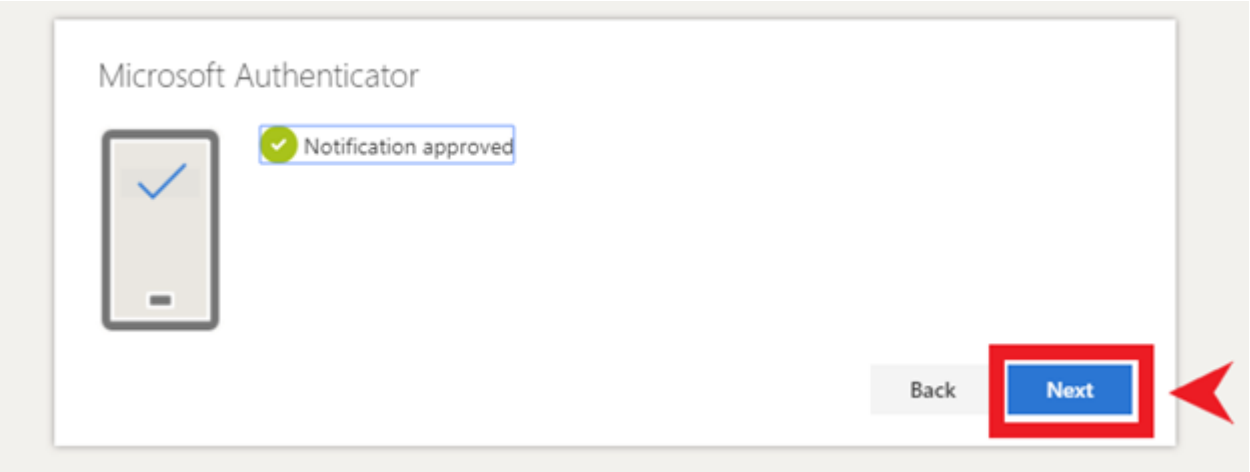
11. There should now be a notification sent to your device.



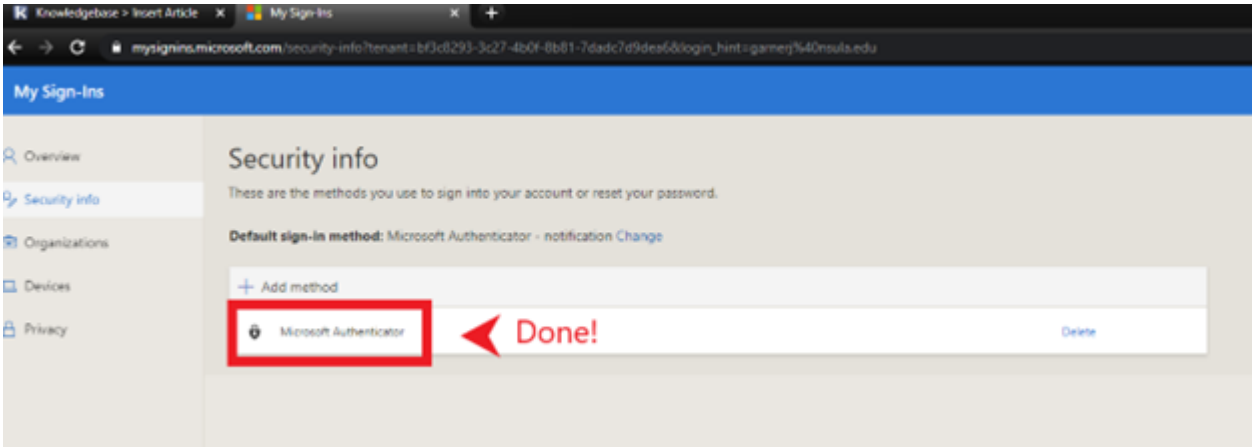
12. Tap on “Approve” when the notification (as shown in the example below) appears. This will be the actual process of authenticating sign-ins from now on.



13. After tapping “Approve” on your device, this next screen should appear on your computer. Click “Next” as shown in the example below.



14. Make sure “Microsoft Authenticator” is shown as a sign-in method. The process is now complete!



Please make sure you set up other alternate MFA methods. With only the Microsoft Authenticator method in place, you must have access to the device you installed it on and remain logged into the app to sign in. It is very important to have these authentication methods in place, but the only way to reasonably prevent most issues with MFA is to also have a phone number and email address set up as well. Feel free to view our other support articles to set up these other methods quickly and easily.

Tips to Protect Yourself Online

Quick tips to stay safe online.