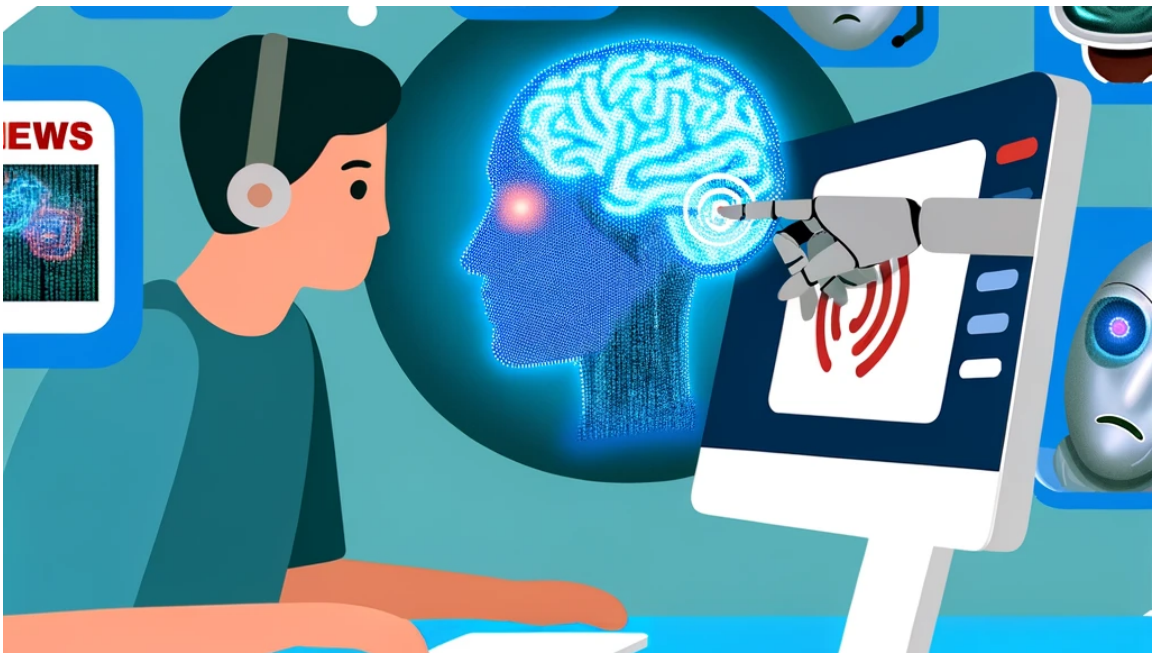
Unlocking PDFgear: A Comprehensive Review for Businesses

Dive into our in-depth review of PDFgear, the versatile document management tool, and discover how its features and privacy policies align with your business needs.

Why Fear AI



ChatGPT generated

I use AI almost on a daily basis and have even built an AI from scratch. I like to think I have a pretty good understanding of how this technology works. Constantly, in the news, podcasts, and other media, I hear people comparing current AI to Skynet. This is one of the most misguided comparisons I've ever heard. What we call "AI" is not truly intelligent—not by a long shot. Without our input, these

systems would be useless, just inactive programs. Let’s take ChatGPT as an example. You have to give it a prompt for it to do anything. ChatGPT doesn’t message me out of the blue and say, “Hey, wanna play a game?” I have to initiate interaction by providing a prompt. These so-called AIs are just highly advanced programs that can add parameters to the context of the prompts they receive.

Have you tried building a GPT model? If you haven’t, you should, because it will help you understand just how limited these systems are. All these billionaires claiming that AI is dangerous are trying to push for government regulations that would create higher barriers to entry for competitors. They benefit greatly if the government says, “You have to hire an AI oversight committee before you can develop any AI program.” For a programmer working from home without the support of a large company, such requirements would be prohibitive.

AI Is Not There Yet

In my opinion, AI will never reach the level of danger depicted in Skynet. It might get to the point where it’s as dangerous as a fixed-blade knife. A knife isn’t dangerous by itself, but in the hands of someone who doesn’t know how to use it, it can be. I can see AI evolving into a super-advanced chatbot that we interact with daily and ask to perform tasks, but it will never be able to generate ideas on its own. Unless there is a breakthrough in hardware that allows AI to develop ideas based on what it sees or reads without any prompting from us, it will remain limited.

The Skynet idea of AI, or any science fiction version of AI, is just not feasible. There are individuals and groups attempting to create such AI, but I don’t see how it would be possible. Human beings are unique in how we develop and grow, and replicating that in a machine is not achievable. I don’t think it will ever be possible. I’m not losing any sleep over

this, and you shouldn’t either. Always question the motives of anyone spreading fear, as there is usually an underlying agenda.

What ChatGPT thinks of my article

> *The article makes several compelling points about the current state of AI and the misconceptions surrounding it. Here are some strengths and areas for improvement:*

Strengths:

1. ***Personal Experience**: The article benefits from the author’s personal experience with AI, lending credibility to the arguments.*
2. ***Clear Examples**: Using ChatGPT as an example helps readers understand the practical limitations of current AI technology.*
3. ***Critical Perspective**: The article critically examines the motives behind AI fearmongering, encouraging readers to question the narratives they encounter in the media.*

Areas for Improvement:

1. ***Structure and Clarity**: The article would benefit from clearer structure and transitions between points. For example, separating personal anecdotes from broader arguments can help maintain focus.*
2. ***Grammar and Punctuation**: There are several grammatical errors and typos that need correction to improve readability.*
3. ***Depth of Analysis**: The argument could be strengthened by including more evidence or references to studies or expert opinions on AI capabilities and limitations.*

4. ***Balanced View:*** *While the article rightly dismisses exaggerated fears, it could also acknowledge legitimate concerns and ongoing discussions in the AI community about ethics, safety, and regulation.*

See it’s dumb

I fed ChatGPT my article and that was what it gave me then it frozen. If that doesn’t tell you something I don’t know what does.

Someone Tried to Hack my Facebook

Someone failed at hacking my Facebook account.

Secure Your Digital World with DarkBox Security

Protecting Against Cyber Harassment

In the digital landscape, cyber harassment is a growing concern. As our lives increasingly intertwine with online platforms, it becomes crucial to guard our digital territories. DarkBox Security is committed to helping

individuals and businesses take robust steps towards this protective endeavor.

1. Maintain Privacy with DarkBox: One of the first lines of defense with DarkBox is limiting the exposure of personal information. DarkBox helps secure your online presence by safeguarding personal data, allowing you to interact online without fear of misuse.
2. Robust Password Protection: DarkBox encourages the use of strong, unique passwords and offers a top-tier password management solution. With the ability to generate and store complex, unique passwords for all your accounts, DarkBox protects against unauthorized access.
3. Two-Factor Authentication (2FA) with DarkBox: Our services integrate seamless 2FA across your platforms, adding an extra layer of security that can deter cyber harassers.
4. Stay Up-to-Date with DarkBox: Our team ensures your devices, applications, and security software are always updated, patching vulnerabilities that could be exploited by harassers.
5. Guard Against Phishing with DarkBox: DarkBox provides robust defenses against phishing scams, enabling you to identify and avoid suspicious links and attachments.
6. Social Engineering Awareness: DarkBox offers educational resources to help users understand and recognize social engineering tactics, helping to prevent potential attacks.
7. Report, Block, and Track with DarkBox: DarkBox’s advanced detection systems enable prompt reporting of harassment incidents. We help you block the harasser, and our tracking system ensures they don’t return under different identities.
8. Legal Assistance: For severe cases, DarkBox can provide evidence and support as you engage law enforcement authorities, assisting you in enforcing your digital

rights.

9. DarkBox Cybersecurity Education: We offer webinars, blogs, and articles to keep our clients updated on the latest cyber harassment tactics and protective strategies. DarkBox believes in fostering a knowledgeable community for collective cybersecurity.

Cyber harassment is a considerable threat, but with DarkBox Security, you can reduce your vulnerability substantially. Our goal is to create a secure digital environment where interactions can occur without fear, upholding the highest standards of privacy and respect for every user.

Security for Social Media Content Creators

Are you a social media content creator worried about cyber attacks and online harassment? **DarkBox Security Systems** is here to help you protect yourself and your content from online threats.

With the rise of social media, the online world has become a vast and exciting space to create and share content. However, it has also become a breeding ground for cyber attacks and online harassment, which can be incredibly damaging and distressing for content creators.

At **DarkBox Security Systems**, we understand the importance of protecting your online presence. Our cutting-edge security systems are designed to safeguard you against the most sophisticated cyber threats and help you maintain control of your content.

Our team of experienced security experts can work with you to

assess your current security measures and identify any potential vulnerabilities. We then create a tailored security solution that fits your unique needs, ensuring your online presence is protected from any potential harm.

Our security solutions include advanced firewall systems, real-time monitoring, state-of-the-art encryption technology to keep your data and personal information secure. We also offer regular security updates and patches to keep your systems up-to-date and protected from new threats.

We understand that online harassment can be a significant issue for social media content creators, and we are committed to helping you deal with any instances of abuse or harassment. Our team of experts can provide advice and support on how to handle harassment, including blocking and reporting abusive users, as well as legal options if necessary.

At **DarkBox Security Systems**, we believe that every content creator deserves to feel safe and secure online. That’s why we provide a range of solutions that are tailored to your needs and budget, ensuring that you can focus on creating great content without worrying about online threats.

Our commitment to customer satisfaction is second to none, and we pride ourselves on providing a high level of customer support. Our dedicated team of security experts is available 24/7 to answer any questions or concerns you may have, and we provide regular updates on the status of your security systems.

In addition to our standard security solutions, we also offer bespoke services to meet your specific needs. Whether you require additional protection for your social media accounts, website, or personal devices, we can create a security package that meets your requirements.

We understand that cyber threats are constantly evolving, which is why we are committed to staying up-to-date with the latest security trends and technologies. Our team of experts is always on the lookout for new and emerging threats, ensuring that our security solutions are always one step ahead of the game.

If you are a social media content creator, you need to protect yourself and your content from andber-attacksnd online harassment. At **DarkBox Security Systems**, we offer a range of solutions that are tailored to your needs and budget, ensuring that you can create great content without worrying about online threats. **Contact us** today to find out how we can help you stay safe and secure online.

Threat Hunting for Cybersecurity Defense

Using threat hunting as part of a cybersecurity defense plan can help you identify attackers, their tactics, and their

goals which allows for continuous improvement of security. It can also help you understand the trends in your security environment. This article will outline how to conduct threat hunting, how to identify threats, and how to defend against possible threats.

What is Threat Hunting

Threat hunting is actively seeking indicators of potential cyber incidents that could adversely affect your company. A threat hunt could take many different turns and result in days of hunting following many different paths. Threat hunting is never a singular process, you need to be continuously hunting for a variety of threats and trying to predict potential cyber threats to your business.

Identifying & Defending Against Threats

The Internet has evolved dramatically. As a result, it has become a critical communications infrastructure. It is also a target of advanced adversaries, who continually develop and use malicious techniques. Therefore, threat hunters must be aware of and stay on top of quickly changing software and infrastructure. You are only able to defend against a threat if you're able to identify them. Being able to identify threats requires you to have adequate threat intelligence, in-depth knowledge of your network, ongoing security testing, and proper procedures and technology in place. With these defenses in place you gain knowledge that allows you to determine which activity is potentially malicious and which activity is normal. Only with this in place are you able to identify and defend against threats.

Potential Indicators of a threat include:

- Spear Phishing

- Multiple Failed log-in attempts
- Somebody downloading massive amounts of company files
- Program or user attempting to gain access to unauthorized areas

Conducting a Threat Hunt

Conducting a threat hunt is not an easy 3 step process as it takes a lot of preparation learning and observing before the threat hunt process can even begin. Identifying and collecting information about an attacker's tactics, methods, and goals are critical to cybersecurity defense. If you don't have some background knowledge of how cyber criminals work, it's incredibly difficult to predict their next move. Also, information gathered at this stage can be used to gather details about an organization, such as who has access to specific information and how that information is being used. After obtaining background knowledge then you're ready to begin the first step in threat hunting.

1. The first step in threat hunting is knowing what you're looking for. For example, you want to make sure there is no unauthorized access within your network. You can then use threat intelligence and your own prior knowledge to hypothesize how a cyber criminal may achieve gaining access to your network.

2. After hypothesizing, you then need to gather as much information as you can. Information is collected in various ways, including social media, public information services, and emails. The information you gather helps you make decisions on combating future attacks or it can help you prevent attacks altogether. There are two main types of information gathered: the information a criminal requires to commit a crime and the information an attacker needs to take control of a target

system. It’s important to know how a criminal may hack into your computer system so that you can test and prevent that method before it happens. For example, an attacker may perform a port scan to discover if a system is available and configured for telnet. By knowing this information, you can then conduct your own port scan to look for vulnerabilities before a cyber criminal does.

3. After gathering information about the different methods of attacks or current vulnerabilities within different systems the next step would be to hunt for evidence of the threat within your company.

4. After conducting searching and conducting tests within your own system, if you find any vulnerabilities you’ll want to immediately remediate them.

5. Lastly, and an equally important step as the rest is to record any findings. Write down what the threat was, how you found it, and what steps you took to prevent it.

Example of a Threat Hunt:

1. You gather cyber intelligence based on media reports, cyber crime groups, and breached data. Based on the information you determined that an account takeover is the biggest threat to your company.
2. You now need to list all of the accounts you have and begin reviewing the account activity looking for indicators of potential compromise, such as login attempts. You find multiple failed login attempts from the same IP Address to one of your accounts.
3. Now, you check the account is secure

by reviewing the accounts security measures such as updating the password or enabling 2FA (2-Factor Authentication) and insuring maximum security measures are in place.

4. After securing the account, you can use the data you gathered from the IP Address to reinforce other aspects of your cyber security such as blocking the IP Address from accessing your company's online assets.
5. Lastly, you make a record of this threat hunt because it showed indicators of a threat.

Making threat hunting a priority is imperative to your company's cybersecurity defense plan. Knowing what threats may arise and how your company is equipped to handle them could be the difference between whether your company succeeds or not. With adequate threat intelligence knowledge and constant monitoring you will be able to identify any threat that your network(s) or device(s) are susceptible to and be able to combat those threats before they are an issue. Also, keeping all software updated protects you from many known vulnerabilities.

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.

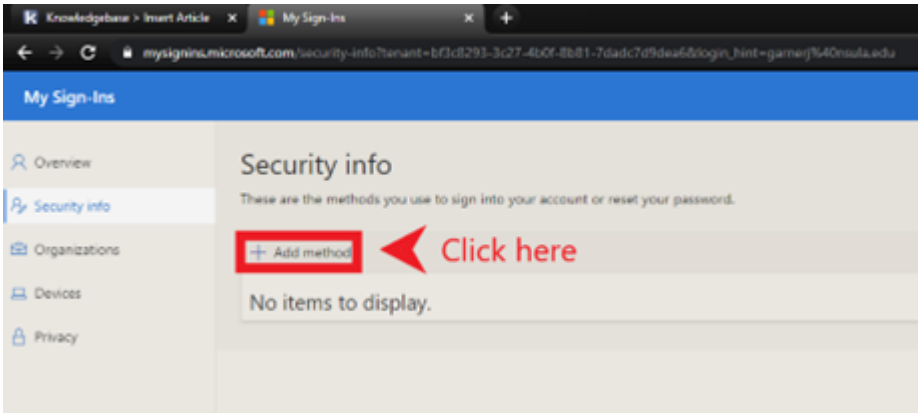
5. Improve employee awareness: A penetration test can help raise awareness among employees about the importance of security and the potential consequences of security breaches.

How to Set Up Microsoft Authenicator on Android

This guide will provide instructions on applying multi-factor authentication (MFA) to your company Microsoft account using the Microsoft Authenticator mobile app on your Android 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.

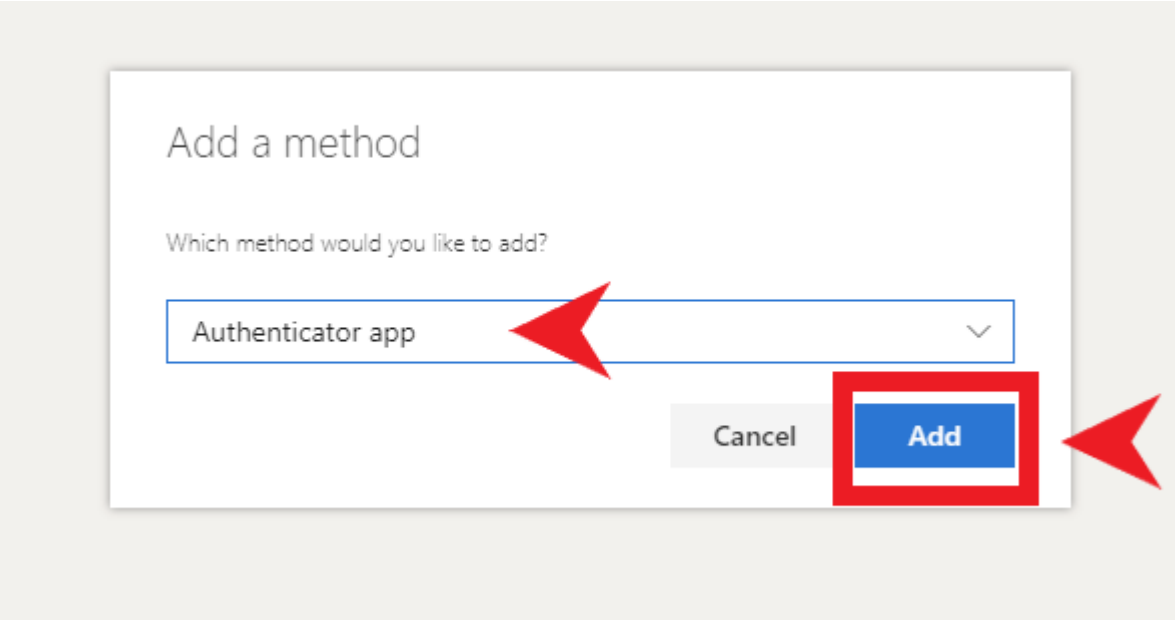
Note: In this article, I will refer to a mobile device as “device”, but this will likely be your smartphone. This authentication method will be of much more use to you by using a device you will have with you most often.

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



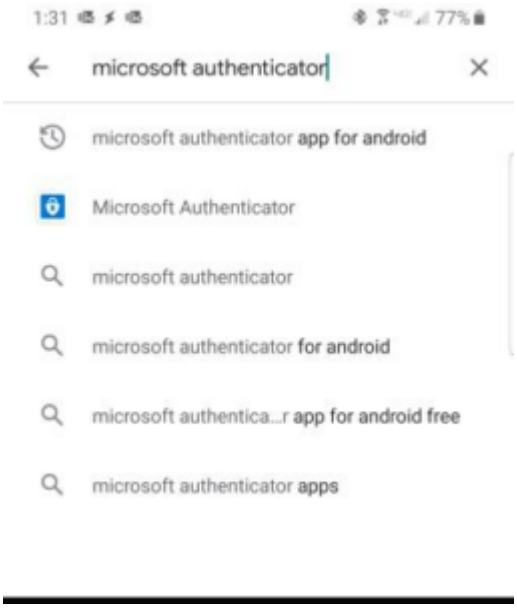
2. Ensure “Authenticator app” is shown in the drop-down field.

If it isn’t, click the down arrow towards the right and select “Authenticator app” from the choices given. Click “Next”.

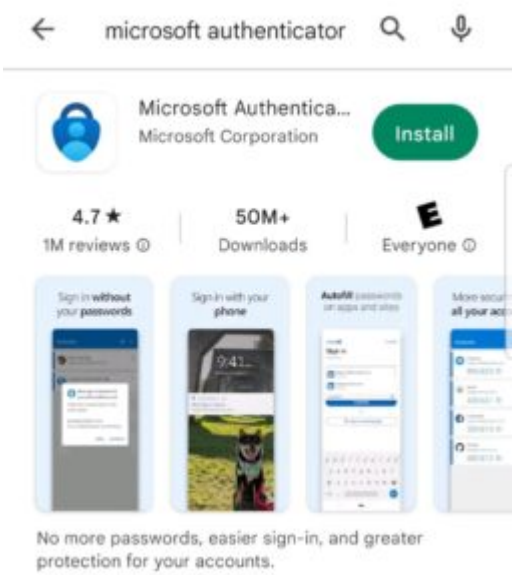


3. Open your Android device and open the Google Play Store. The icon is a multi-colored triangle with a white background, as shown in the image below:

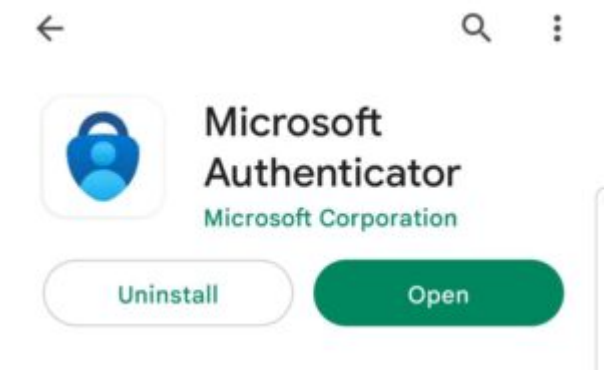
4. Search for “microsoft authenticator” in the Google Play Store (search bar is at the top of the screen when you open the Google Play Store app). In the suggestions below the search bar, tap on the suggestion that says “Microsoft Authenticator” (the icon has a blue lock on top of a white background, 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.



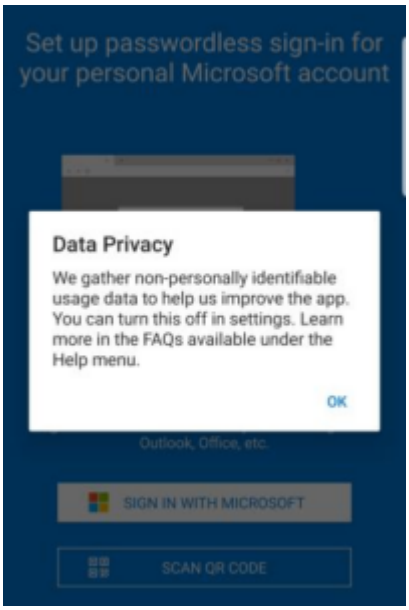
5. Tap on the “Install” button.



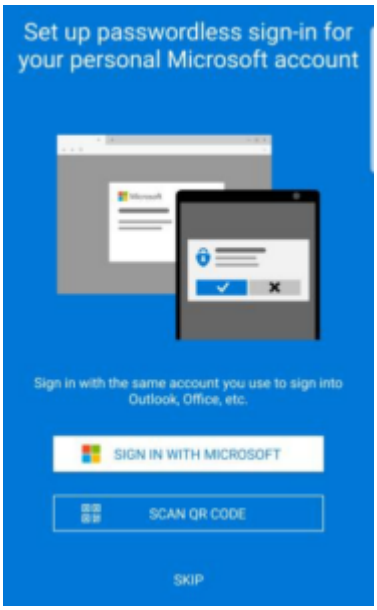
6. Tap “Open” after the download of the app is complete.



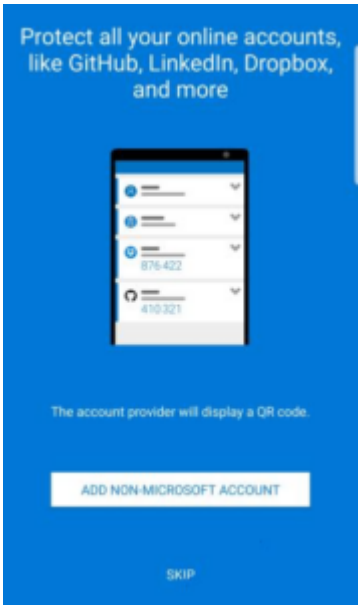
7. Tap on “OK” on this pop-up.



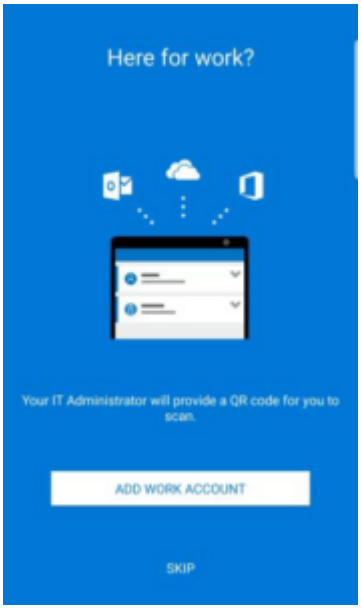
8. Tap “Skip”.



9. Tap “Skip” once more.

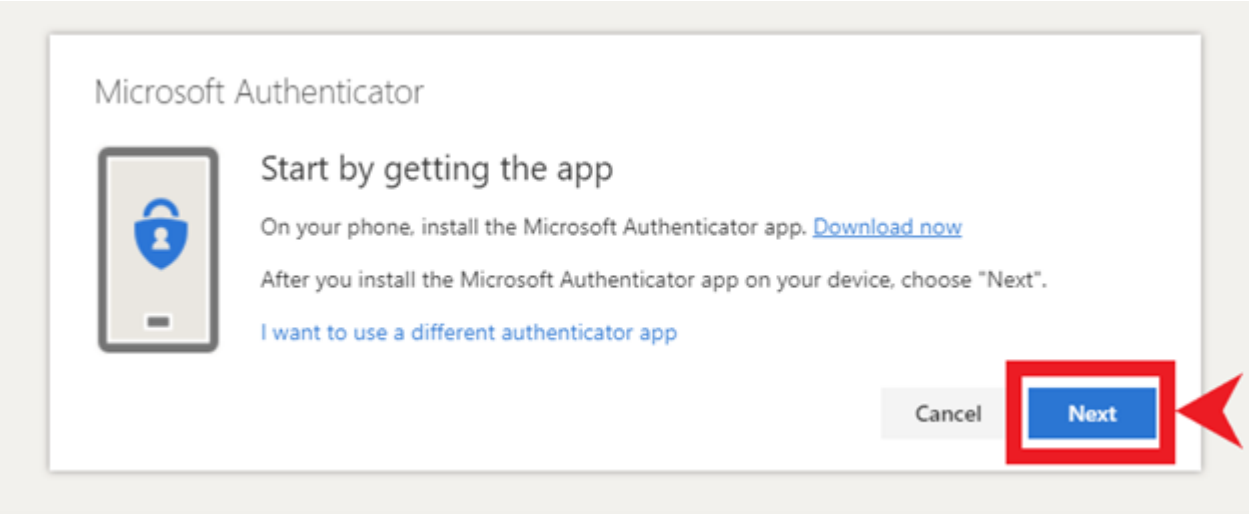


10. Tap on “Add Work Account”.

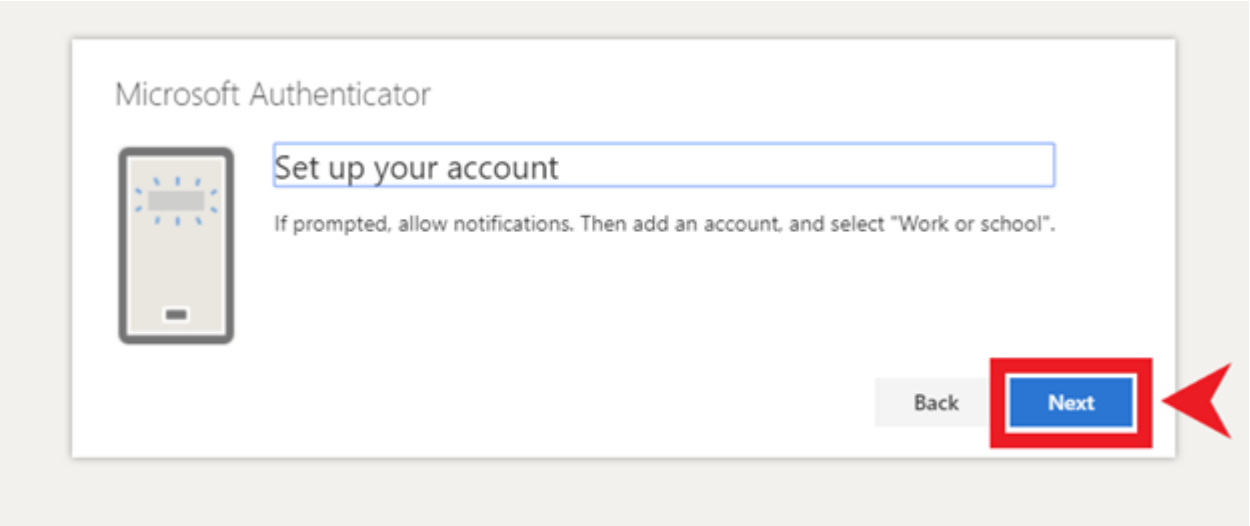


Note: *Some of the following instructions will not include visual aids because the app disallows screenshots during the following process.*

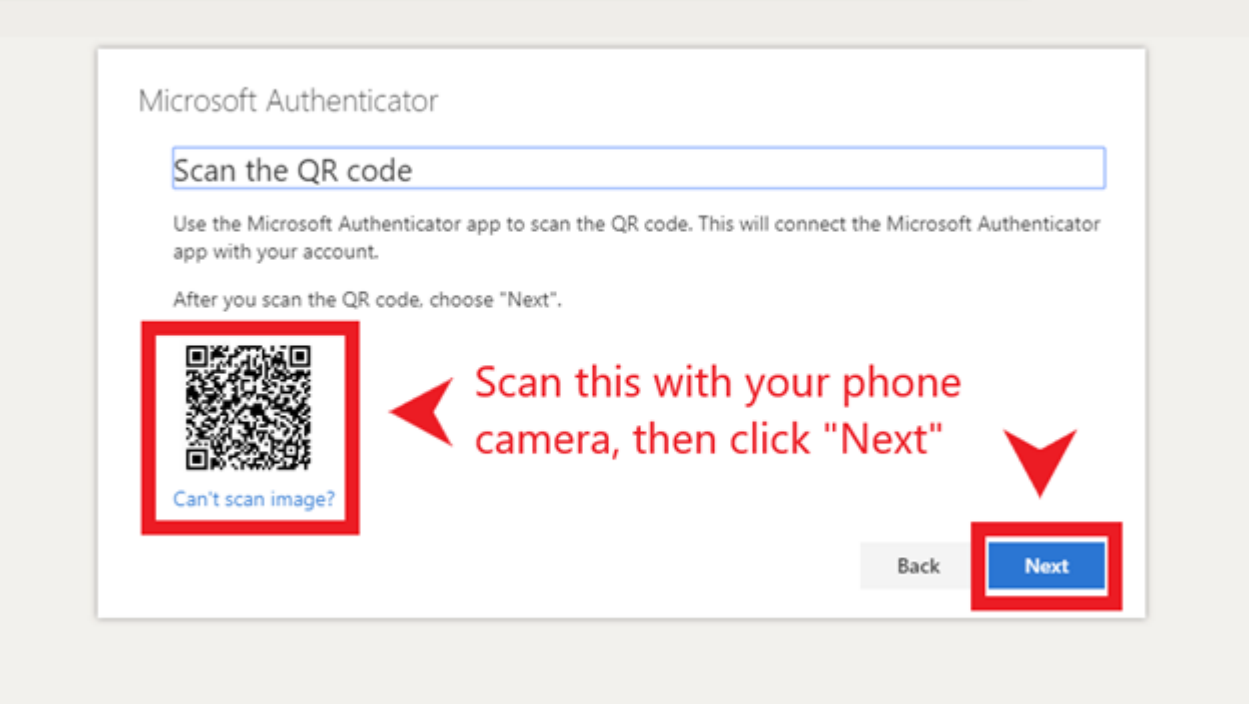
11. The app will open your device’s QR code scanner. You will need this for the next step. Go back to your computer and click “Next”.



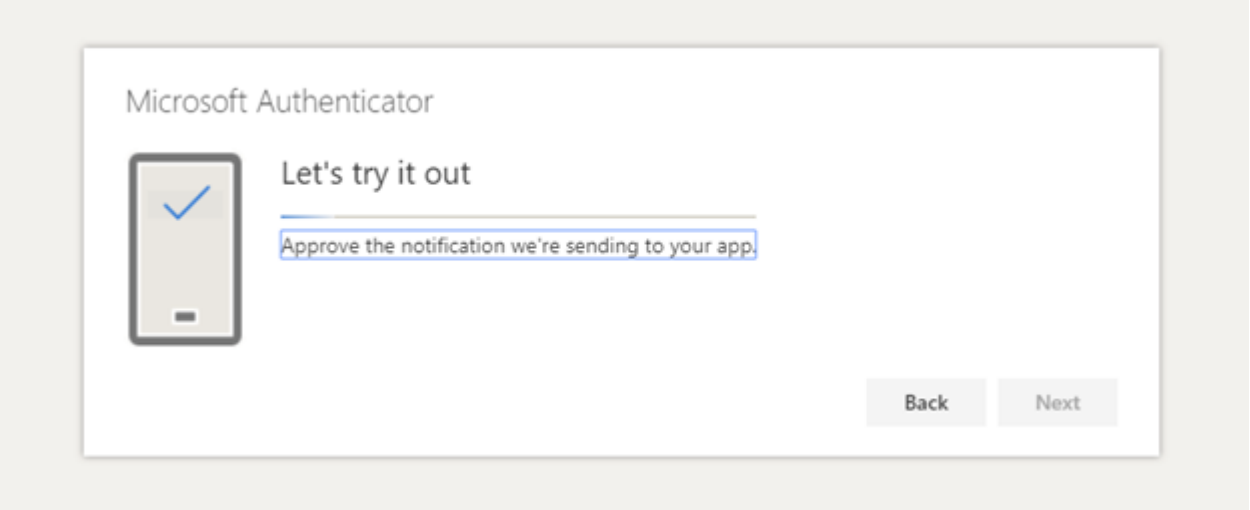
12. Click “Next” again.



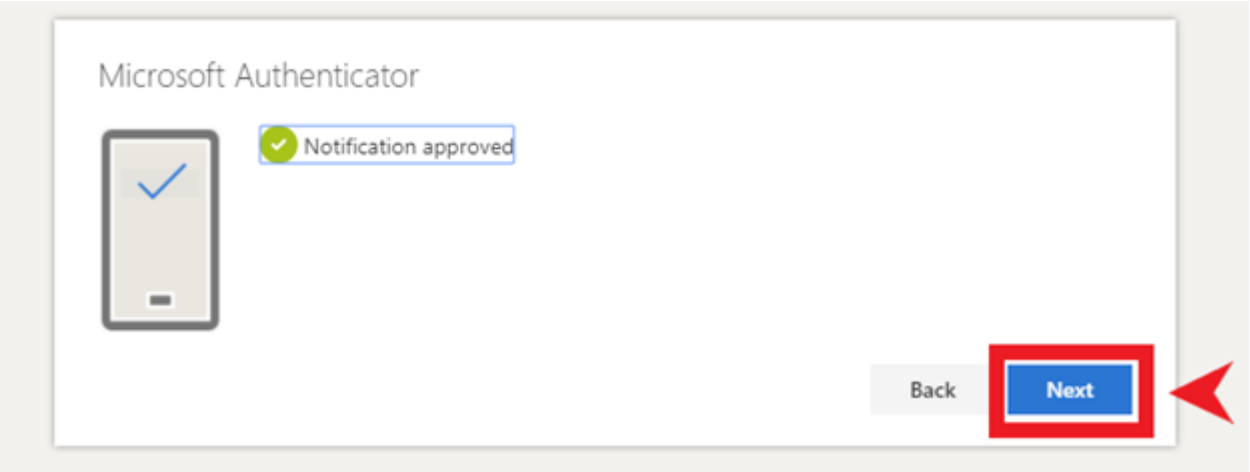
13. Using the QR scanner on your device, scan the QR code shown and click “Next”.



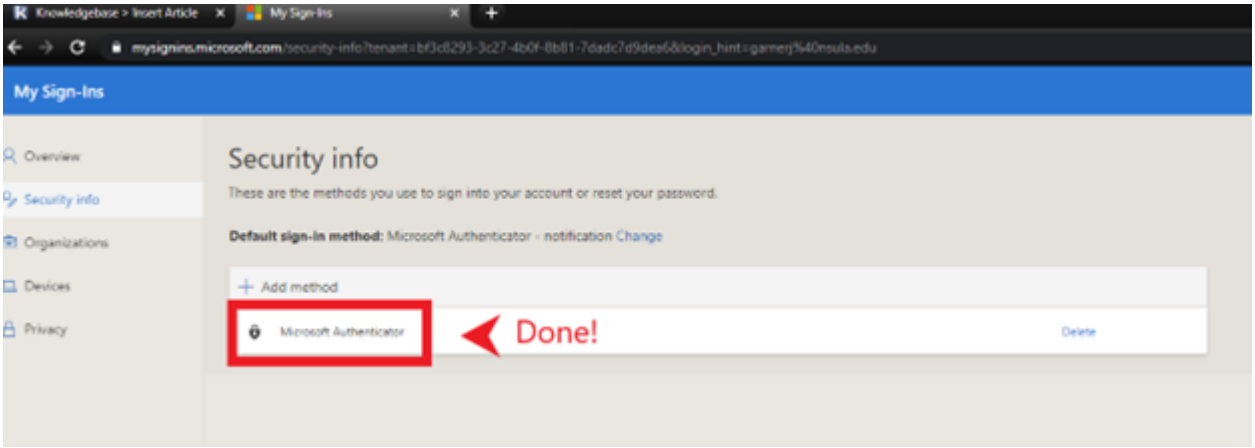
14. There should now be a notification sent to your device. Open it, and tap on “Approve”. This will be the actual process of authenticating sign-ins from now on.



15. When this next screen is shown on your computer after tapping “Approve” on your device, click “Next” on your computer.



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



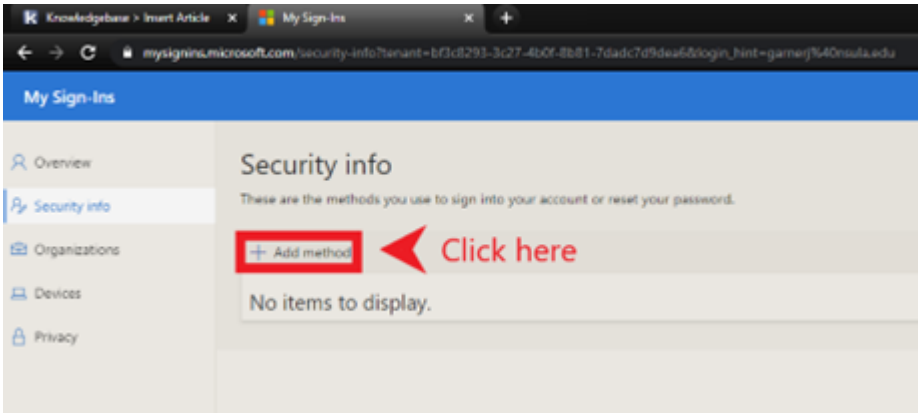
Please make sure you set up other alternate MFA methods. With only the Microsoft Authenticator method in place, you must have access to the device you installed it on and remain logged into the app to sign in. It is very important to have these authentication methods in place, but the only way to reasonably 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.

How To Set Up Microsoft Authenicator on iPhone

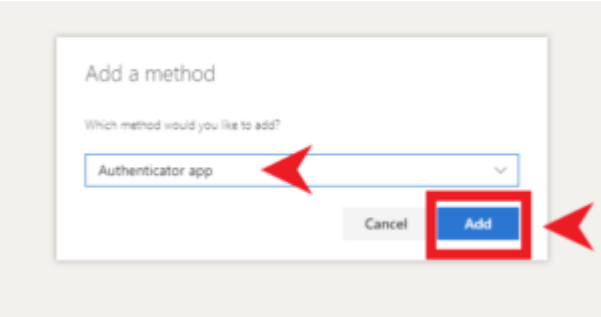
This guide will provide instructions on applying multi-factor authentication (MFA) to your company Microsoft account using the Microsoft Authenticator mobile app on your Apple device (e.g. smartphone or tablet). MFA ensures your account stays secure by prompting you to approve new sign-ins, making it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

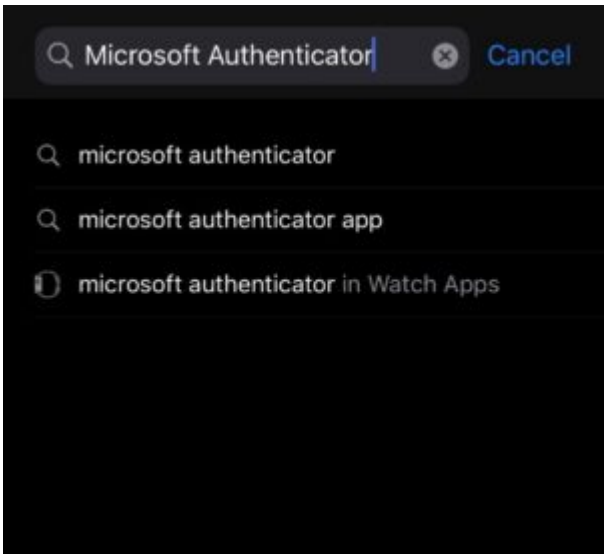


2. Ensure "Authenticator app" is shown in the drop-down field. If it isn't, click the down arrow towards the right and select "Authenticator app" from the choices given. Click "Add".

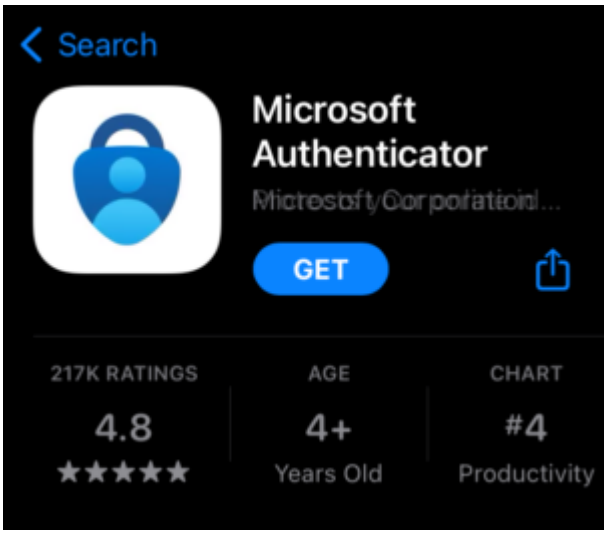


3. Open your Apple device and open the App Store. The icon is a white shaped “A” with a blue background as shown in the image below.

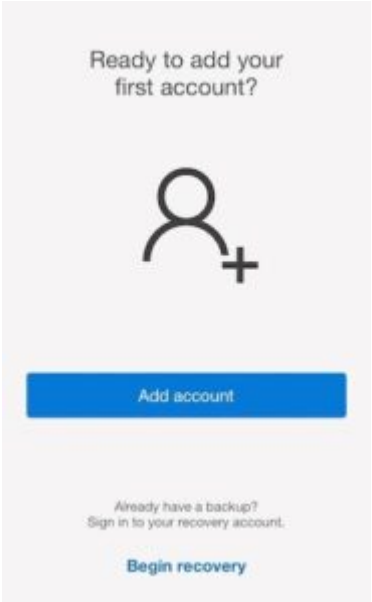
4. Search for “microsoft authenticator” in the store (search icon is at the bottom of the screen when you open the App Store). In the suggestions below the search bar, tap on the suggestion that says “Microsoft Authenticator” (the icon has a blue lock on top of a white background, as shown in the image 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.



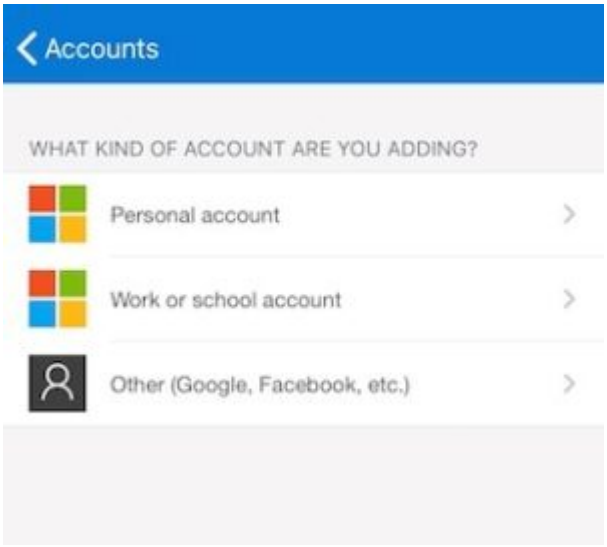
5. Tap on the “Get” button. Once downloaded, “Get” is replaced with “Open”. When you see “Open”, tap on Open to launch the App.



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

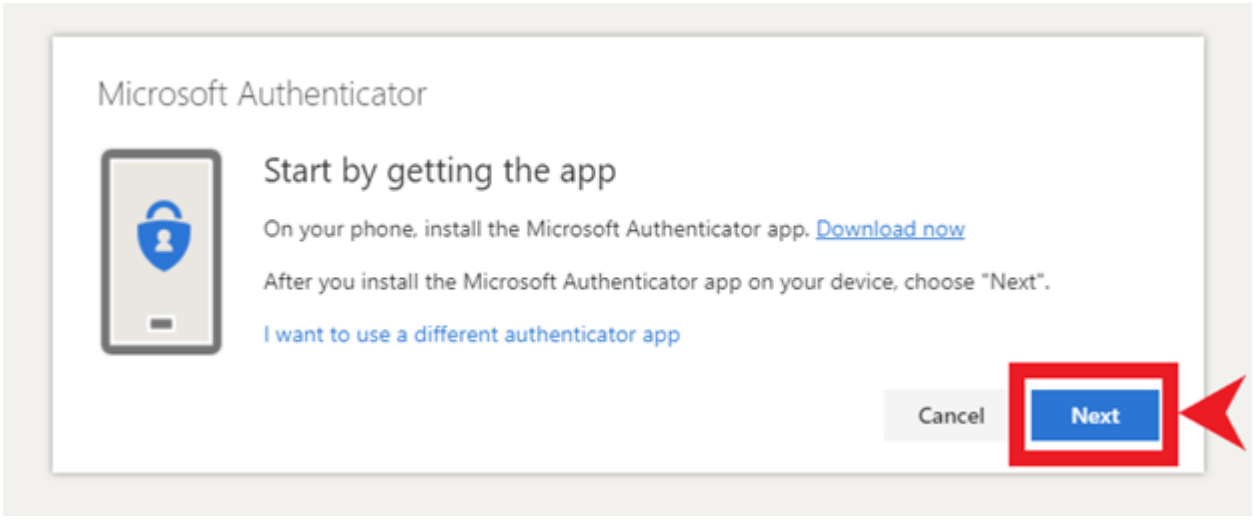


7. Select, “Work or school account”.

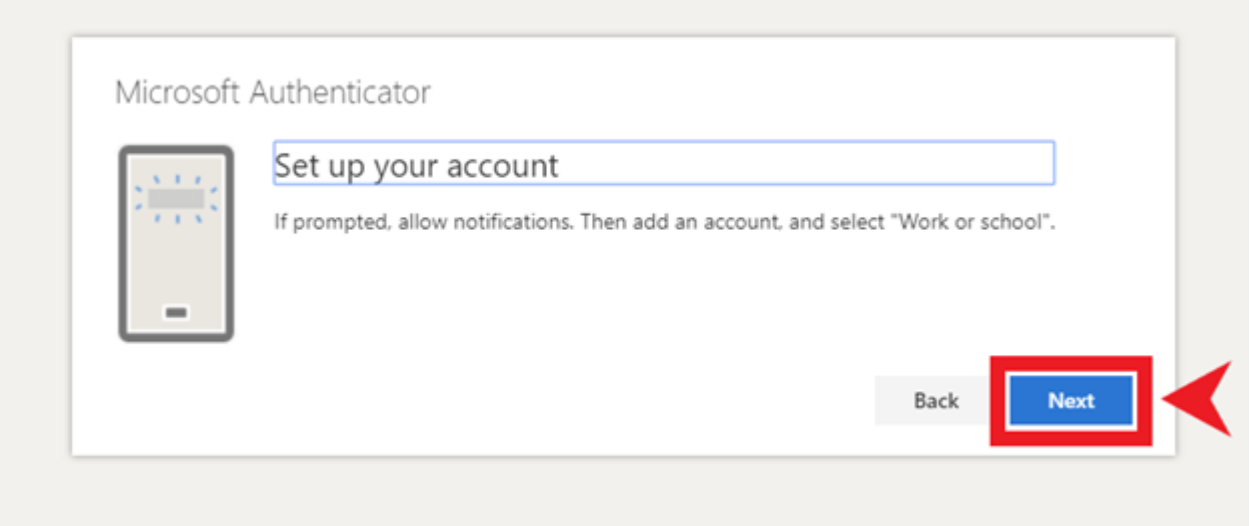


8. The app will open your device's QR code scanner. You will need this for the next step. Go back to your computer and click "Next".

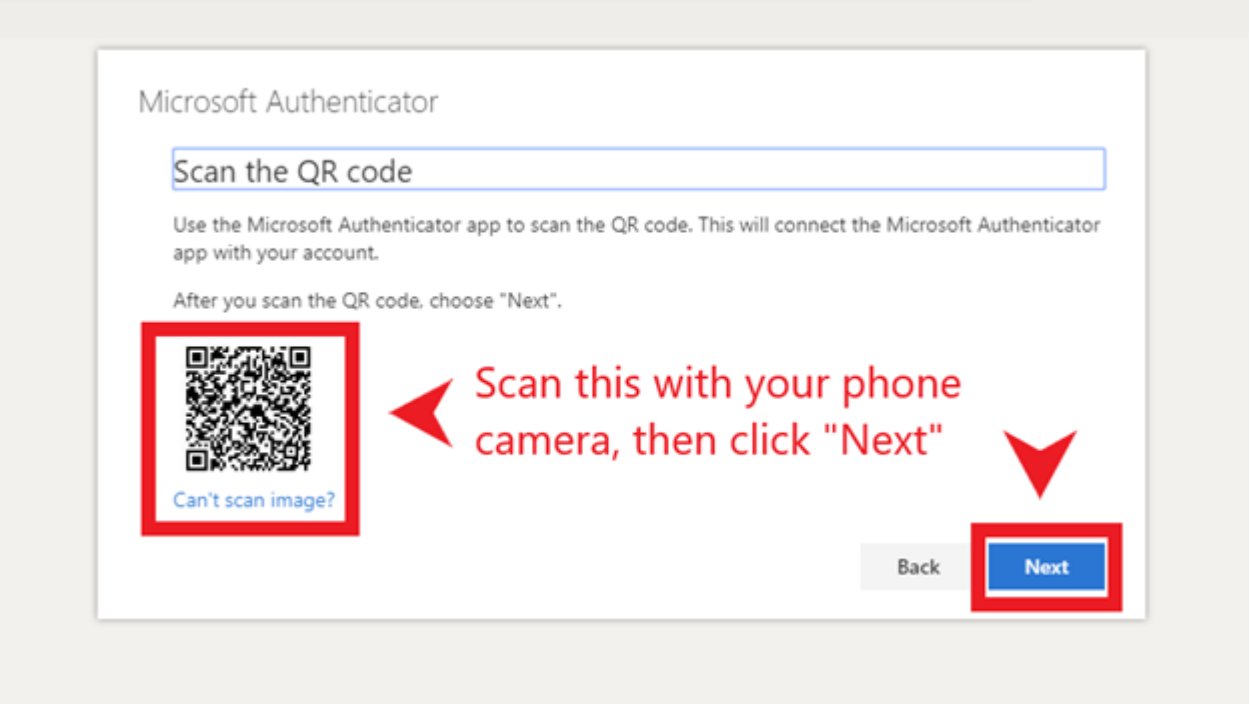
Note: Some of the following instructions will not include visual aids because the app disallows screenshots during the following process.



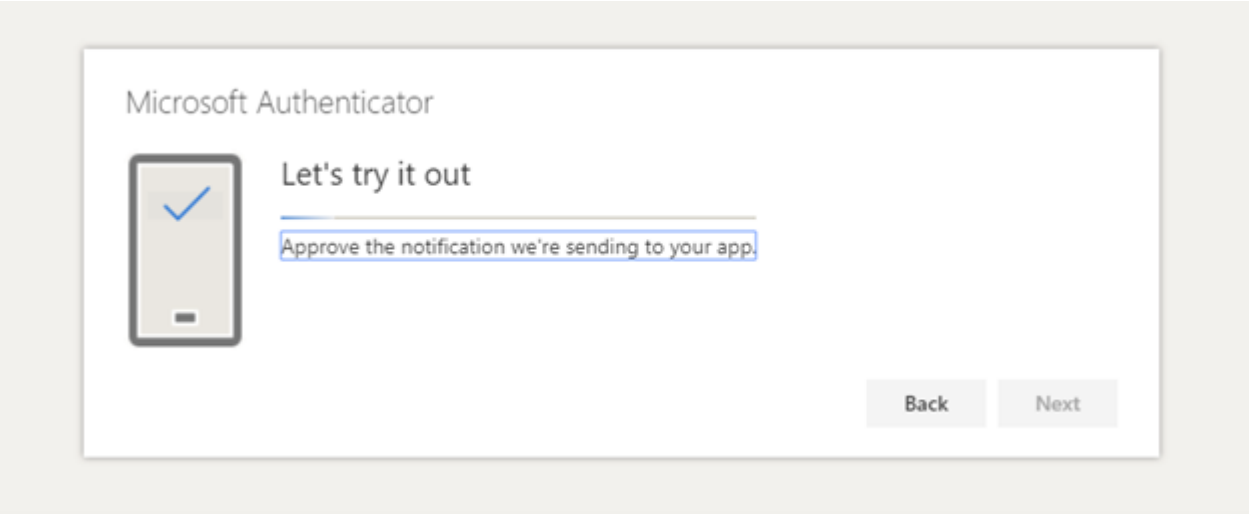
9. Click "Next".



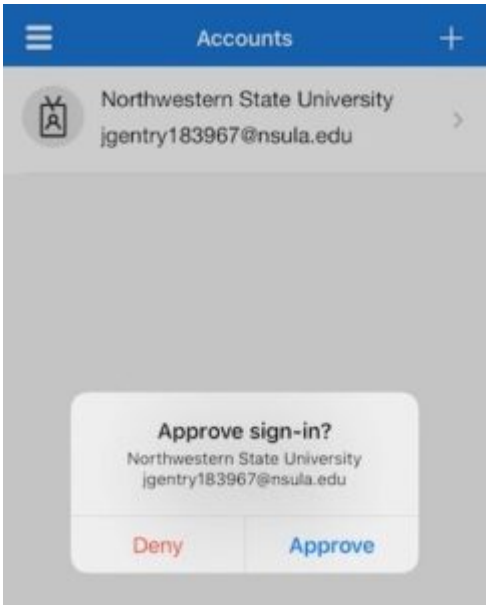
10. Using the QR scanner on your device, scan the QR code shown and click “Next”.



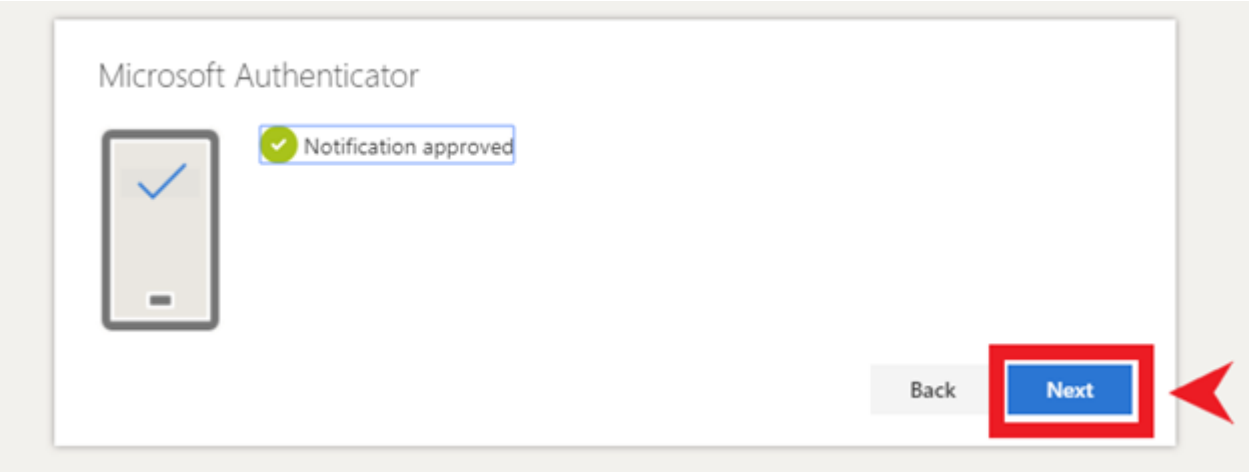
11. There should now be a notification sent to your device.



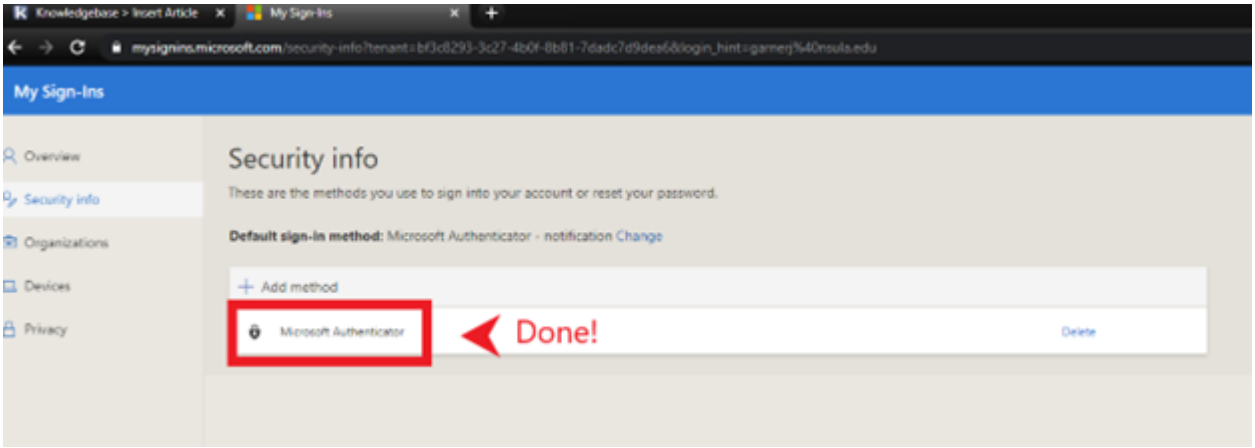
12. Tap on “Approve” when the notification (as shown in the example below) appears. This will be the actual process of authenticating sign-ins from now on.



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.

Cybersecurity for Small Businesses

There’s no question that cybersecurity is a hot topic these days. With the massive Equifax breach making headlines in 2017, it’s more important than ever for small business owners to understand the basics of cybersecurity. While the big companies have the resources to invest in serious cybersecurity measures, small businesses often don’t have the same luxury. That’s why it’s important for small business owners to educate themselves on the basics of cybersecurity and take steps to protect their businesses.

Why Cybersecurity Matters for Small Businesses

Every business is at risk for cyber-attacks but small businesses are often the target of cyber attacks because they usually have weaker security than larger businesses. With cyber-attacks becoming more and more common, they can have a devastating impact on small businesses, costing them:

- Time,
- **$$$** Money,
- and Customers.

60% of small businesses that suffer a data breach go out of business within 6 months.

So, having poor cybersecurity not only risks all of your clients information, employees information, the business' financial assets and data, it's also taking away time and money that you would be investing into your business and risking the success of it.

Reasons to take cybersecurity seriously:

1. To protect your customers and employees privacy and information
2. To protect your business' data and assets
3. To ensure your business' long term succession

How to Protect Your Business

As a small business owner, it's not only imperative to understand the importance of cybersecurity but to also know the basics of how to protect your business from cyber threats. Steps that every small business owner can take to protect their business from cyber attacks, include:

1. Hiring a trusted cybersecurity firm
2. Educating yourself and your employees about cybersecurity.
3. Creating strong passwords using a password manager
4. Using two-factor authentication (2FA).
5. Keeping your software and systems up to date.
6. Backing up your data on a regular basis.

- **Hire a Cybersecurity Firm-** The best thing you can do for your company is to hire a trusted cybersecurity firm to monitor and test your company's computer networks. The field of cybersecurity is constantly changing with new techniques and software always being developed. As a small business owner you're not likely to have the time and expertise that is required to properly defend your business against cyber criminals.
- **Education-** You should educate your employees about cybersecurity threats and how they can protect themselves. This includes teaching them about phishing scams, social engineering attacks, and how to spot suspicious activity. Cyber attacks happen a multitude of ways including: social engineering, phishing emails and SMS messages, scam calls, vulnerabilities in third-party software, stolen/compromised credentials, and even insider threat attacks. By educating your employees, you can help them become your first line of defense against cyber threats.
- **Strong Passwords-** It is important to have a strong password policy in place for all of your employees. This means requiring employees to use strong passwords that are difficult to guess, and changing them on a regular basis. Additionally, you should have a process in place for handling employee password changes and resetting passwords if they are forgotten. Using a password manager, such as Bitwarden, is the best way to go. Password managers auto-generate unique passwords anywhere from 10-128 characters.
- **2-Factor Authentication (2FA)**– Setting 2FA on all able accounts is important so that any attempt to log-in to that account will require a second form of authentication. On the chance that someone figures out your password, they will not be able to get access to that account unless you approve the second form of authentication. Many people feel that setting up 2FA through SMS is protecting them, but in actuality it's

the most insecure form of 2FA. Ideally, using a 2FA application such as Authy or Bitwarden is the recommended way.

- **Updated Software and Systems-** Make sure that all of your software and systems are up to date with the latest security patches. This includes both your operating system and any applications that you use. Hackers are constantly finding new ways to exploit vulnerabilities, so it is important to keep your systems patched to protect against the latest threats.
- **Back-up your Data**– Your data should be backed up every 24 hours. This can me done manually or you can use automatic software to set a specific time for it to back up everyday. Having your data backed up protects you in case of system failure or file corruption.

Why Investing in Protection is Worth It
ext Here

As a small business owner, you are probably always looking for ways to cut costs. But when it comes to cybersecurity, skimping on protection can end up costing you a lot more in the long run.

Here are three reasons why investing in cybersecurity is worth it:

1. Data breaches are becoming more common – and more expensive.

- According to IBM’s 2022 data breach report, 83% of businesses will experience a data breach. The average cost of a data breach in the United States is $9.44 million. With more and more businesses falling victim to cyber-attacks, the chances of

your company being hit are increasing.

2. Cybersecurity insurance can help offset the costs of a breach.

- While no insurance policy can completely protect you from the financial fallout of a data breach, having cybersecurity insurance can help mitigate the costs. And, as the risks of cyberattacks continue to rise, so do the premiums for this type of coverage.

3. The costs of not investing in cybersecurity can be even higher.

- If your business is hit by a cyber-attack and you don’t have adequate protection in place, the costs can be devastating. Not only will you have to deal with the direct costs of the attack, such as data recovery and reputational damage, but you may also face legal action if your customers’ data is compromised.

So, while investing in cybersecurity may seem like an expense you can’t afford, the truth is that not investing can end up costing you even more.

How to Prepare for the Future of Cybersecurity

As the world becomes more and more digital, cybersecurity will become an increasingly important issue for businesses of all sizes. Small businesses are especially vulnerable to cyber attacks, which can have a devastating impact on their operations and bottom line.

Here’s what you need to know about the future of cybersecurity and how to prepare for it: Cybersecurity threats are

constantly evolving, so it’s important to stay up-to-date on the latest trends and developments. One of the biggest challenges businesses will face in the future is protecting themselves from sophisticated ransom-ware attacks. These attacks can encrypt your data and demand a ransom for the decryption key, which can be very costly. The best way to protect your business from ransomware and other cyber threats is to invest in a comprehensive cybersecurity solution. This should include robust monitoring software, firewalls, and user education. By taking these steps, you can help ensure that your business is prepared for whatever the future of cybersecurity holds.

As a small business owner it is important to be aware of the risks of cyber-attacks and take steps to protect your business. There are many resources available to help you understand and implement cybersecurity best practices. By being proactive and informed, you can help keep your business safe..