Cyber Foundations Workbook

Copyright Notice

Requests to the author and publisher for permission should be addressed to the following email: support@cybershieldsecurity.co.

Limitation of liability/disclaimer of warranty: While the publisher and author have used their best efforts in preparing this planner, they make no representations or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for particular purpose.

No warranty may be created or extended by sales representatives, promoters, or written sales materials.The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Disclaimer

No part of this publication may be reproduced, stored, or transmitted in any form or by any means, electronic, mechanical, photo copying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the author.

How To Use This Workbook

Cybersecurity is the practice of protecting networks and systems from digital attacks aimed at sensitive information, getting money from users, or interrupting normal business. Cybersecurity threats are real and they are riskier for all businesses and organizations. Your business could be just a click away from absolute ruin.

This is why it is important to improve your cybersecurity posture and understand the nature of threats to your business so you can deploy systems to mitigate risks as much as possible. Investing in proper software applications, employee training and professional help are all necessary steps to protecting your user data, information systems.

We believe the software applications and systems this workbook helps you deploy and install are the foundational components of a complete security program.

This workbook will help you do two things. Assess your current cybersecurity posture and assist you with deploying basic cybersecurity systems and software you need for your laptop, desktop, table or cell phone. This workbook has instructions on how to deploy the following software.

1. Multi-Factor Authentication (MFA)
2. Antivirus
3. Password Manager
4. Virtual Private Network (VPN)
5. Web Application Firewall

Let’s Get Started

You will need the items listed below to complete the steps in this workbook.

1. A desire to want to be more secure
2. A desktop or laptop
3. An internet connection
4. An existing email address

Your IT Security

The way you and your business use IT security will be very similar in your personal life and business life. We're going to give you a rating based on the current IT security you have in place. This rating helps you determine if you need to implement more IT security, if you have just the right amount or if you need more.

Your Organization

1. Read each of the questions below about your organization's IT security.
2. Enter your score in the Score column based on your answer below.
    a. **No** - circle a **1** in the box
    b. **I Don't Know** - circle a **3** in the box
    c. **Yes** - circle a **5** in the box
3. Add up the total and put the number in the total box at the bottom of the table.

Are you?		
	No / IDK / Yes	**Score**
Accessing websites over the Internet without any Antivirus software on their computers and mobile devices?		1 or 3 or 5
Not educating yourself or your team about Phishing attacks and how threat actors pretend to be trusted contacts to get users to click malicious links, download malicious files, or give them access to sensitive information, account details or credentials?		1 or 3 or 5
Using easily guessed passwords, or continuing to use the same passwords for multiple accounts? Sharing the password in plain text and not using a vault?		1 or 3 or 5
Not making backup copies of important business data and information?		1 or 3 or 5

Relying only on username and passwords with no form of two factor authentication deployed?		1 or 3 or 5
TOTAL		____ / 25

Personal

1. Read each of the questions below about your personal security.
2. Enter your score in the Score column based on your answer below.
    a. **No** - circle a **1** in the box
    b. **I Don't Know** - circle a **3** in the box
    c. **Yes** - circle a **5** in the box
3. Add up the total and put the number in the total box at the bottom of the table.

Do you?		
	No / IDK / Yes	**Score**
Reuse passwords for different types of systems? An example of this would be using your Facebook password as the password to log into your bank account.		1 or 3 or 5
Answer online security questions with truthful answers		1 or 3 or 5
Have 2-Factor Authentication enabled on your important accounts (mortgage, email, bank, etc.)		1 or 3 or 5
Have more than one email address?		1 or 3 or 5
Share sensitive data via email?		1 or 3 or 5
Use ephemeral (disappearing) message systems when sending private data?		1 or 3 or 5
Use Anti-Virus software on your personal computer, tablet and cell phone		1 or 3 or 5

TOTAL		_____ / 35

Add your organization's IT security score and your personal IT security score together to get your total. This will provide you with your **SHIELDSCORE**. Enter your score in the space below.

SHIELDSCORE: _____ / 60

Score	Security	Criteria Description
54 - 60	Excellent	Your thought process about IT security exceeds "Industry Best Practice" standards. Your overall posture was found to be excellent.
41 - 53	Good	Your thought process about IT security meets accepted standards for "Industry Best Practice." The overall posture was found to be strong with only a handful of medium- and low- risk shortcomings identified.
27 - 40	Fair	Your thought process about IT security and your current solutions protect some areas of the enterprise from security issues. Moderate changes are required to elevate the discussed areas to "Industry Best Practice" standards
15 - 26	Poor	Your thought process about IT security means its possible significant security deficiencies exist. Immediate attention should be given to the discussed issues to address exposures identified. Major changes are required to elevate to "Industry Best Practice" standards.
0 - 14	Inadequate	Your thought process about security means serious shortcomings potentially exist throughout most or even all of your IT security. Improving security will require a major allocation of resources.

Scoring Rubric

Multi-Factor Authentication

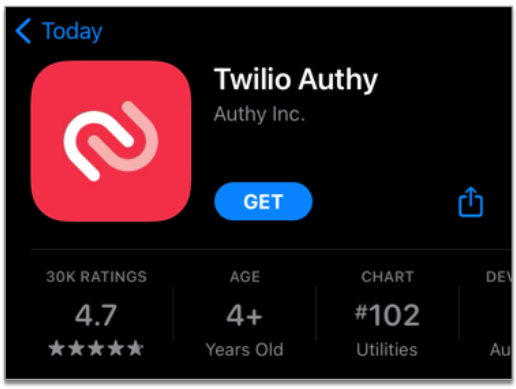
Multi-Factor Authentication is a layered approach to securing your online accounts and the data they contain. When you enable MFA in your systems, you have to provide a combination of two or more pieces of information before you can login. Using MFA protects your account by requiring more than just a username and password.

Instructions
The instructions below will walk you through downloading MFA application **Authy**.

On iPhone

1. Open the App Store. Tap the App Store icon to open it on your iPhone.

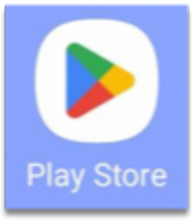
2. Search for the Authy app in the App Store, where it appears under the name “Twilio Authy.”



3. Tap the “Get” button to install the Authy app. Follow the prompts on your screen to confirm and complete the purchase. The Authy app is free of charge.

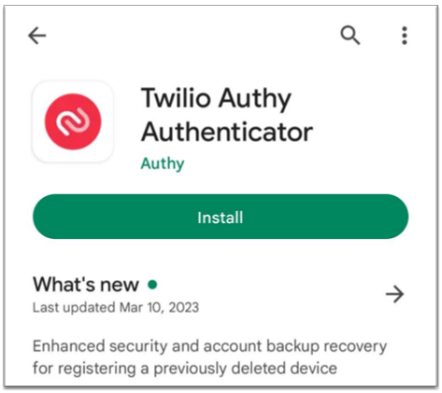
On Android

1. Open the Google Play Store. Tap the Google Play Store icon to open it on your phone.



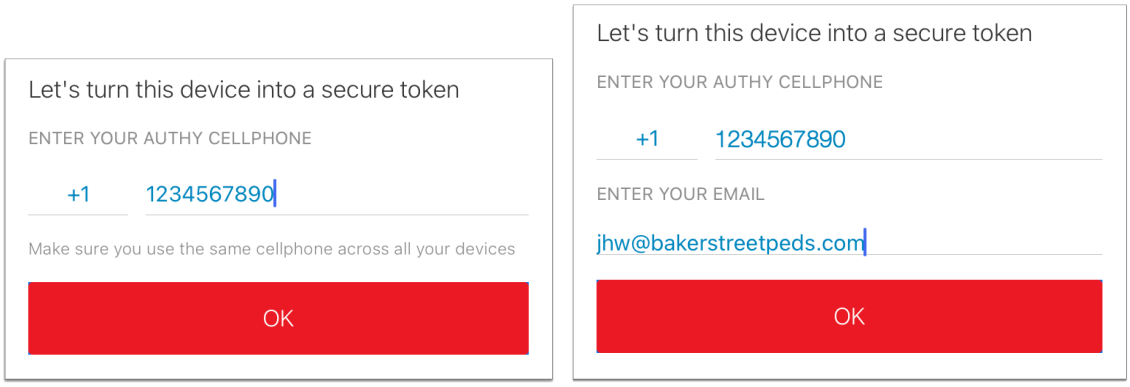
2. Search for Authy

   Search for the Authy app in the Google Play Store, where it appears under the name “Twilio Authy Authenticator”.

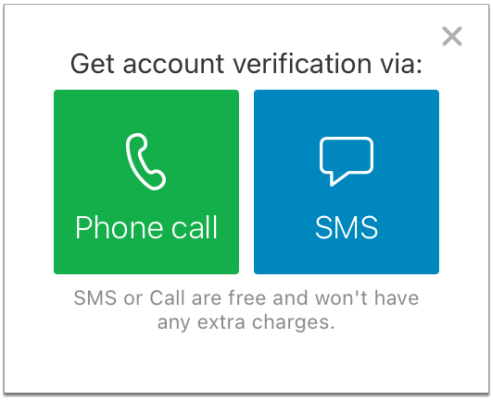


3. Tap the “Install” button to install the Authy app. Follow the prompts on your screen to confirm and complete the purchase. The Authy app is free of charge.
4. After downloading the Authy app, register your device and create an account. Open the Authy app on your smartphone.

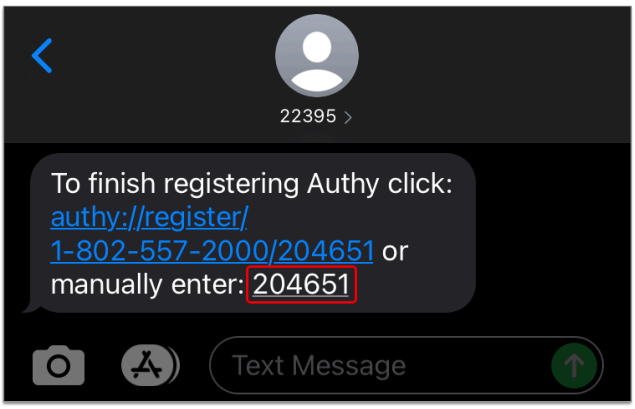
5. Type in your phone number to begin the registration process. After you type in your phone number, an email field appears.



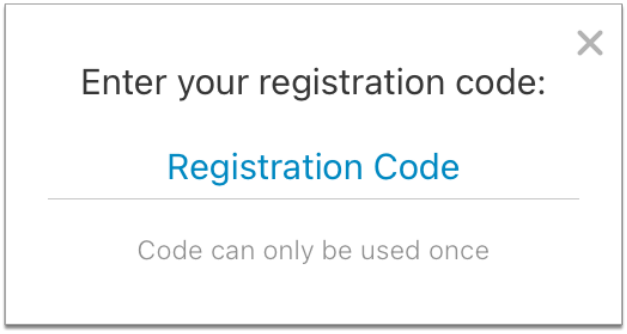
6. Type in your email address then tap the “OK” button.
7. Choose a method to verify your phone number. You can verify by text (SMS) or phone call.



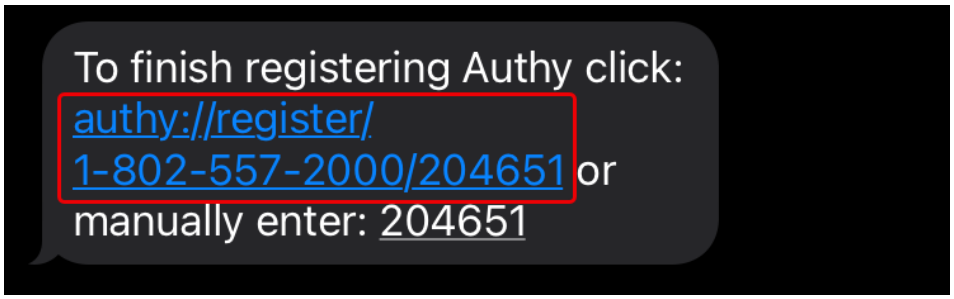
8. Answer the call from Authy or open your text messages to retrieve your registration code.



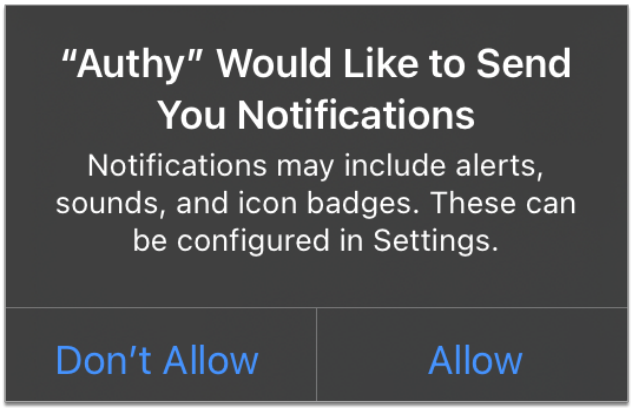
9. Type your registration code into the Authy app.



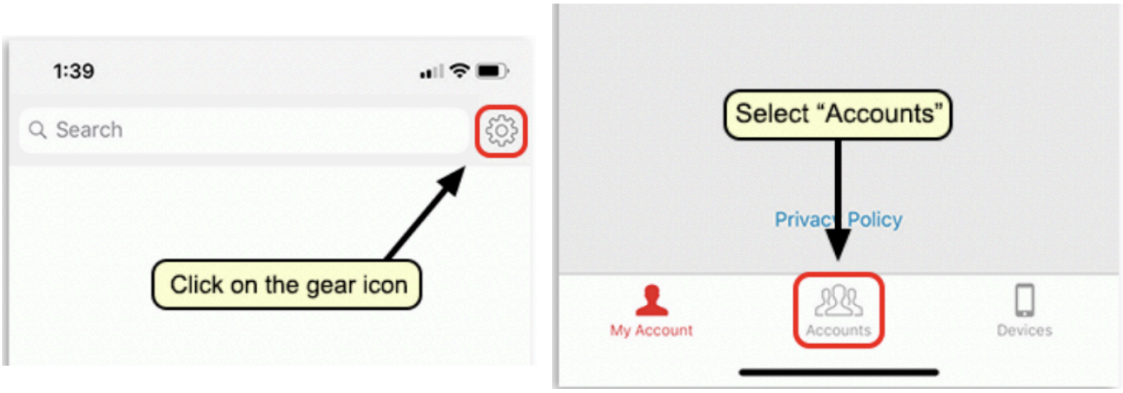
10. Alternatively, if you received your code by text, you can tap the registration link in the text message instead of typing your code into the app.



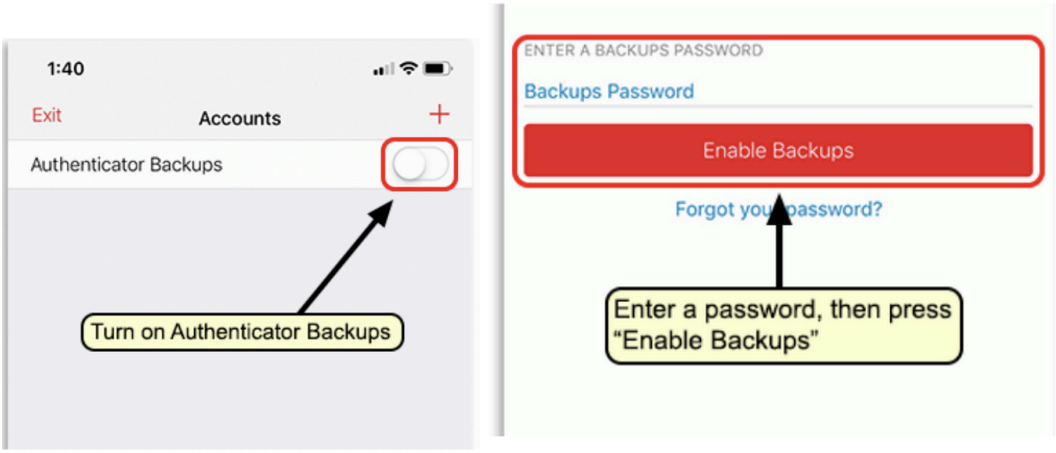
11. If prompted, allow the Authy app to send you notifications.



12. Enable backups in Authy in case you need to be able to access your account from a different device. Backups are most commonly used to regain account access after switching phones. Click on the gear icon, then click "Accounts" to go to your settings.

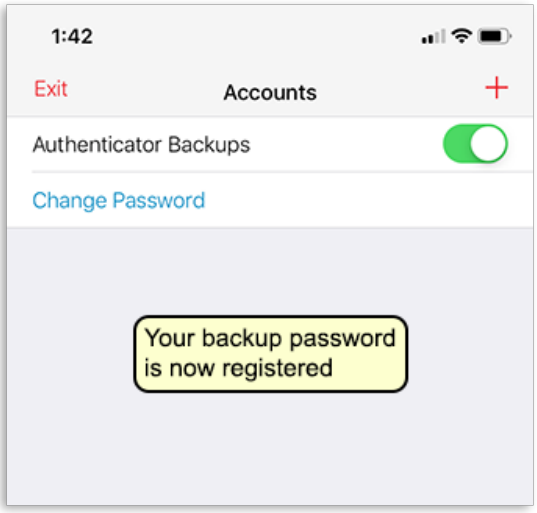


13. Turn on “Authenticator Backups”.



14. Create a password, click “Enable Backups”, then confirm your new backup password by typing it again.

15. Notate your backup password in case you need to use it to access your Authy account on a new device. You can return to this screen to change your backup password at any time.



Next Steps

Install Antivirus

Antivirus

Antivirus software safeguards businesses by detecting and neutralizing various cyber threats like Viruses, Worms, Trojans, Ransomware, and Spyware. Through real-time scanning, it constantly monitors for malicious activity, preventing malware from executing and causing damage. Additionally, it offers web protection features, blocking access to known malicious websites and phishing scams. This proactive defense helps maintain the security and integrity of business systems and data.

The instructions below will walk you through creating an uptime monitor on the website for **Norton™ 360**.

1. Go to https://www.norton.com
2. Click on **Products & Services**
3. Select **Norton 360 Premium** to protect up to 10 devices. Select **Norton 360 Deluxe** to protect up to 5 devices.
4. Enter your email address and password, then select **Sign In**.
5. In the My Norton portal, select **Download**.
6. In the **Get Started** page, select **Agree & Download**.

7. When the download is complete, locate the file and run the installer from the browser.

8. If the User Account Control dialog box appears, select **Continue**.
9. Follow the on-screen instructions to complete the installation.

   By selecting **Install**, you agree to the Norton License Agreement. This agreement can be viewed beforehand by clicking its accompanying link.

How to Install Norton Antivirus on macOS

If you're installing Norton Security on your Mac for the first time or are a returning customer reinstalling the software after previously removing it, follow the steps below.

1. Go to MyNorton.com and select **Sign In**.
2. Enter your email address and password, then select **Sign In**.
3. In the My Norton portal, select **Download**.
4. In the **Get Started** page, select **Agree & Download**.
5. In macOS Catalina, select **Install**.

   In macOS High Sierra, Mojave, Yosemite, or Sierra, select **Agree and Install**.

6. Norton may ask you to join the Norton Community Watch. Select **Join Now** or **Maybe Later**.
7. When prompted, enter your administrator account password, then select **Install Helper**.

   In macOS Yosemite to Sierra, let the installation finish and then restart the Mac. The installation process is complete.

8. If you see an alert that says **System Extension Blocked**, select **OK**.
9. In the Norton installation page, select **Open Now** or **Click Here**.
10. In the **Security & Privacy** dialog box, select the lock icon at the bottom of the dialog box, then enter your administrator account password.
11. If you see **System software from developer Symantec was blocked from loading**, select **Allow**. If you see **some system software was blocked from loading**, select **Allow** > **Symantec**, then select **OK**.

In macOS High Sierra to Mojave, in the Norton Security installation page, select **Continue** and then restart your Mac. The installation is complete. Read on if you use macOS Catalina.

12. Restart the Mac.
13. After you restart the Mac, in the Norton installation page, select **Open Preferences**.
14. In the **Security & Privacy** dialog box, select the lock icon at the bottom.
15. When prompted, enter your administrator account password, then select **Unlock**.
16. If you see **System Software from Norton 360 was blocked from loading**, select **Allow**.
17. In the Norton installation page, select **Open preferences** to allow Norton to access your computer for better protection.
18. In the **Security & Privacy** dialog box, select **Norton System Extension** to enable it.
19. Go back to the Norton installation page and select **Complete**. The Norton security product installation process is finished, and your computer is protected.
10. Login to the console and send emails and/or text messages to all users who are logged in on the devices you want to install antivirus software on.

Next Steps

Install Password Manager

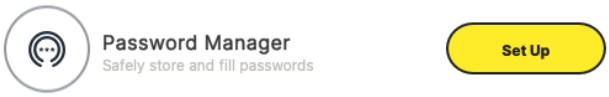
Password Manager

A password manager is online software that can store all your passwords securely, so you don't have to worry about remembering them. This allows you to use unique, strong passwords for all your important accounts (rather than using the same password for all of them, which you should never do).

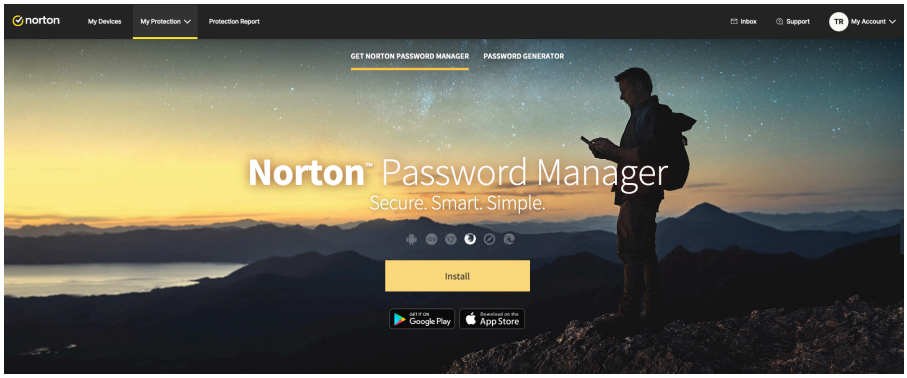
Instructions

The instructions below will walk you through creating an account with **Norton™ 360**. Decide the two email addresses you will use before creating your account and write them down in the box.

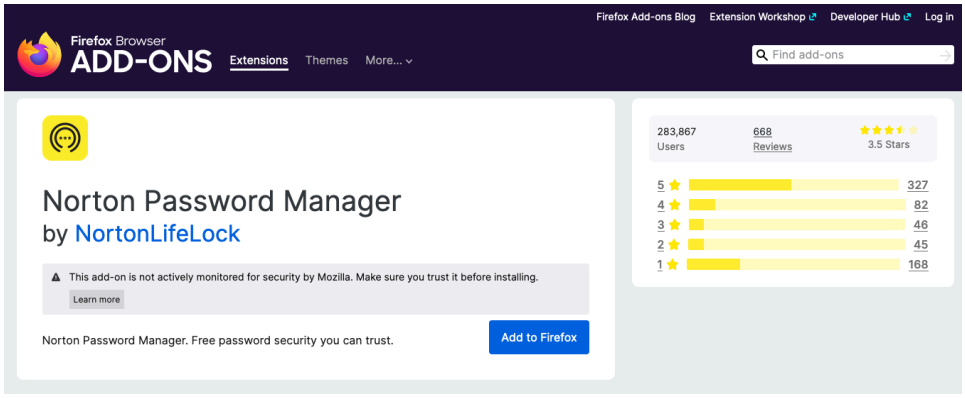
1. Open Norton™ 360 application on your computer or tablet.
2. Beside Password Manager, click **Set Up.**



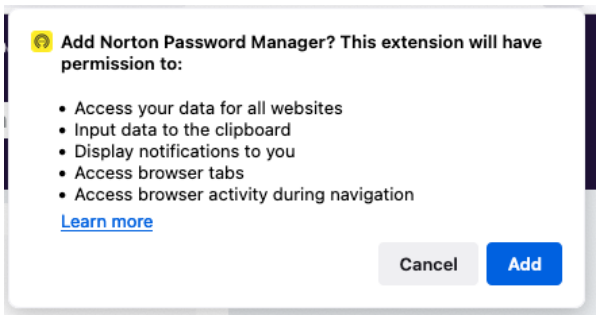
3. A browser window will open. Click the yellow **Install** button.



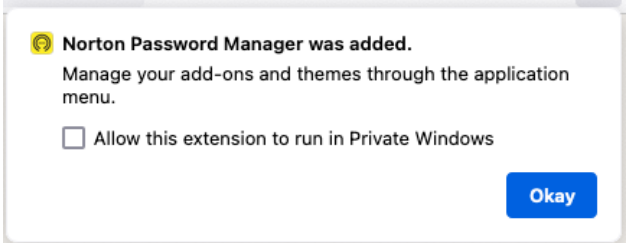
5. The Add-on / Extension Manager for your browser will launch. Find the "**Add**" button and click it.



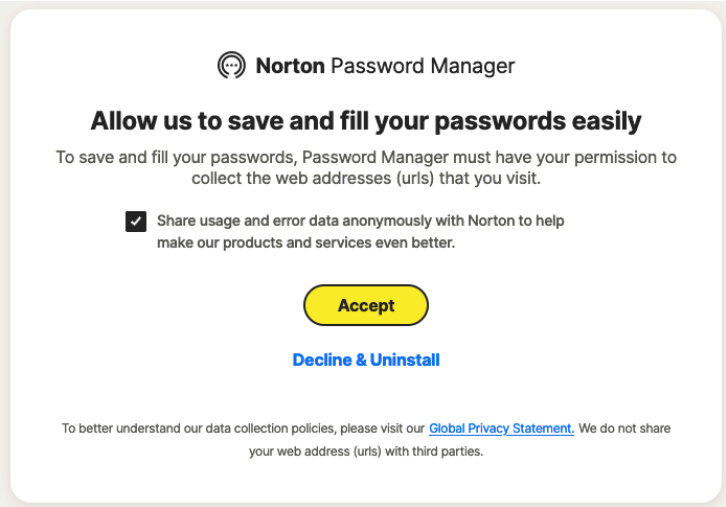
6. When prompted by your browser to add or allow the add-on/extension click "**Add**" or "**Yes**"



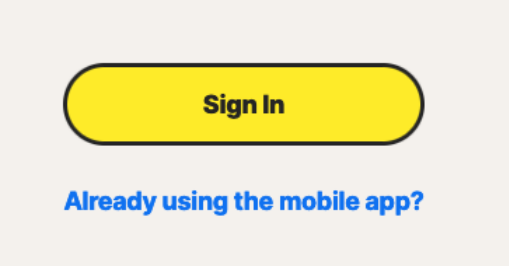
7. Click **Okay** on the popup notification stating that Norton Password Manager was added.



8. If you would like your password manager to automatically enter usernames and passwords into forms for you, click **Accept** on the fill passwords screen.



9. When the Sign In screen appears, Click **Already using the mobile app?**



11. Create vaults and add your important passwords, credentials, certificates and keys to your password manager.

Next Steps
Install VPN.

Virtual Private Network

A web application firewall protects your website from a variety of attacks by filtering, monitoring and blocking bad traffic routed to your website.

Instructions
The instructions below will walk you through creating an account with **Norton™ 360 VPN**.

1. Go to my.Norton.com and click **Sign In**.
2. In the My Norton page, under **Secure VPN**, click **Download**.
3. Open the downloaded file and do one of the following:

    - Windows: Follow the on-screen instructions to complete the installation
    - Mac: Drag the Norton Secure VPN icon into the Applications folder

4. Launch the Norton Secure VPN app.

    For Mac, you need to provide the administrator password when you launch Norton Secure VPN.

5. Sign in to Norton Secure VPN with your Norton account.
6. In the **My Norton** window, next to Secure VPN, click **Turn On.**
7. In the **Secure VPN** window, slide the VPN switch to **ON**.

Next Steps
Deploy Web Application Firewall

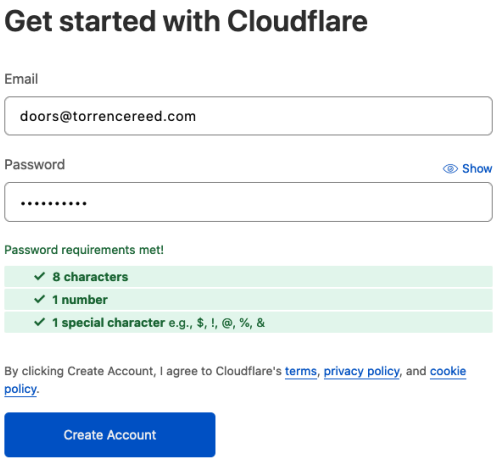
Web Application Firewall

A web application firewall protects your website from a variety of attacks by filtering, monitoring and blocking bad traffic routed to your website.

Instructions
The instructions below will walk you through creating an account with **Cloudflare**.

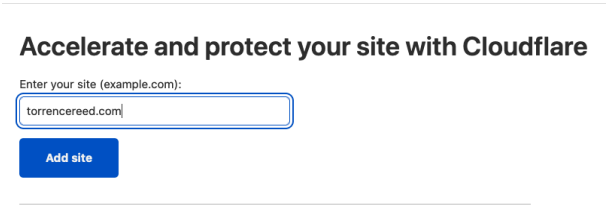
1. Go to https://www.cloudflare.com
2. Click on **Get Started Free**

3. Enter your name and email and click **Create Account.**

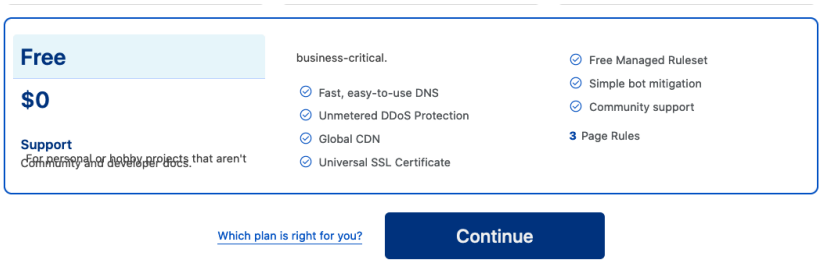


4. Select Cloudflare for Infrastructure and click **Get Started**.

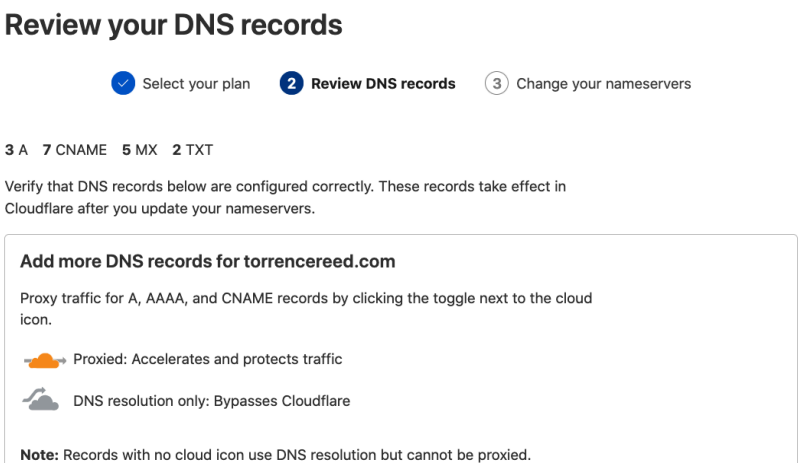
5. Enter your website name and click **Add Site**.



6. Select the Free plan and click **Continue**.



7. On the next screen, you will see results of the records that were found for your domain name and recommendation on what to do next.



Next Steps

Create email security records in your DNS Management system.

Email Security

Click on the links below to view instructions on how to enable the email security records below for Google Workspace or Microsoft 365.

DKIM records [Google Workspace | Microsoft 365]
DMARC record [Google Workspace | Microsoft 365]
SPF record [Google Workspace | Microsoft 365]

What Next?

As you continue to secure and fine tune the systems you have deployed above you will begin to see how more and more interconnected they are. Deploying an endpoint management solution such as and getting security awareness training should be next up on your todo list for IT security.

Now that you have completed this workbook, we can help you assess your next steps regarding IT security when you are ready to scale and grow. We can help you with the solutions below.

1. Complete web and network vulnerability scan
2. Review security setup of User Directory configuration
3. Review database backup setup
4. Deploy data loss prevention policies and Security Documentation
5. Complete Security Awareness Training

Let us know if you need any help and we'll be glad to continue helping you get and remain secure.

Thanks,
Cybershield Support
support@cybershieldsecurity.co