Trend Micro Security 2022 for Windows

Product Guide

Trend Micro™ Antivirus+ Security

Trend Micro™ Internet Security

Trend Micro™ Maximum Security

V0.1

Trend Micro Incorporated
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900
Toll-free: (888) 762-8763
www.trendmicro.com

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before implementing the product, please review the readme file and the latest version of the applicable user documentation.

Trend Micro, the Trend Micro t-ball logo, Titanium, and Trend Micro Security are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2022 Trend Micro Inc., Consumer Technical Product Marketing. All rights reserved.

Trend Micro™ Security 2022 Product Guide provides help for analysts, reviewers, potential customers, and users who are evaluating, reviewing, or using the 2022 (v17) version of Trend Micro™ Antivirus+ Security, Trend Micro™ Internet Security, or Trend Micro™ Maximum Security. The products are understood to be the most recent editions (2022), even when "v17" or "2022" are not designated. Trend Micro Antivirus for Mac is also considered part of the current 2022 Trend Micro Security Family release.

This Product Guide can be read in conjunction with the following companion Product Guides, which can be accessed from the Home and Home Office Support Page

- Trend Micro™ Antivirus for Mac Product Guide
- Trend Micro™ Mobile Security for Android Product Guide
- Trend Micro™ Mobile Security for iOS Product Guide
- Trend Micro™ Password Manager for PC and Android Product Guide
- Trend Micro™ Password Manager for Mac and iOS Product Guide

DOCUMENT PROFILE:

Product: Trend Micro™ Security 2022 for Windows

Document Title: Trend Micro™ Security 2022 for Windows Product Guide

Document Filename: PG - TM Security Windows 2022 - Product Guide GL v0.1

Document Release Date: November 19, 2022

Team: Consumer Technical Product Marketing

Table of Contents

Chapter 1: Introduction to Trend Micro™ Security 5
The Trend Micro™ Security Family 5
Trend Micro Security: Comprehensive Protection 6
Key Features of Trend Micro Security 10
System Requirements 11
Internet Connection, USB Installation 13
Target Audience 13
Global Availability 13
Contacting Trend Micro 14
Consumer Support Line 14
Free Phone, Email and Chat support 14
Premium Support Services 14
Chapter 2: Installing and Activating Trend Micro Security 15
Install Trend Micro Security 15
Set Up Folder Shield 30
Enable Trend Micro Security Toolbar 34
Enable Trend Micro Security for Microsoft Edge 34
Enable Trend Micro Security Toolbar for Google Chrome, Mozilla Firefox, Internet Security, or Pay Guard 41
Enable Email Defender for Gmail and Outlook Webmail 50
Protect Another Device: PCs, Macs, Android and iOS Mobile Devices 53
Chapter 3: Trend Micro Security Overview 60
Quick Start: The Trend Micro Security Console 60
Quick Start: Conducting On-Demand Scans 60
Scan Your Computer's Disk 61
Quick Scan and Full Scan 62
Custom Scan 63
Intensive Scan 64
Quick Start: Viewing Security Reports 65
Chapter 4: Trend Micro Antivirus+ Security 68
Protection Overview 68
Device: Security Settings: Security & Tuneup Controls: Scan Preferences 70
Device: Security Settings: Security & Tuneup Controls > Scheduled Scans 73
Device: Security Settings: Internet & Email Controls > Web Threats 74
Device: Security Settings: Internet & Email Controls > Spam & Emailed Files 75
Device: Security Settings: Internet & Email Controls: Network > Firewall Booster | Wi-Fi Protection 83
Exception Lists: Programs/Folders 84
Exception Lists: Websites 85
Exception Lists: Wireless Connection 86
Other Settings: System Startup 87
Other Settings: Network Settings 88
Other Settings: Smart Protection Network 89
Other Settings: Password 90

Other Settings: Background and Animation 90
Device: Mute Mode 94
Device: Protect Another Device 98
Privacy: Social Networking Protection 98
Privacy: Pay Guard 103
Data: Folder Shield 108
How Folder Shield Works 115
Family: Upgrade Now 118
Chapter 5: Trend Micro Internet Security 120
Protection Overview 120
Device: Security Settings: Security & Tuneup Controls > Scheduled Scans > Smart Scheduled Scan 124
Device: PC Health Checkup | Security Settings 126
Perform a PC Health Checkup 126
Configure PC Health Checkup 128
Security Report: PC Health Checkup 129
Device: Protect Another Device 131
Privacy: Privacy Scanner: Social Network Privacy & Web Browser Privacy 131
Facebook Privacy Settings 133
Facebook App Privacy Settings 137
Twitter Privacy Settings 139
LinkedIn Privacy Settings 141
Web Browser Privacy Settings 144
Privacy: Data Theft Prevention 147
Data: Secure Erase 151
Data: Password Manager - Free Trial 154
Family: Parental Controls 166
Security Report: Parental Controls 178
Chapter 6: Trend Micro Maximum Security 181
Protection Overview 181
Device: Protect Another Device 183
Data: Password Manager - Full Version 183
Install Password Manager in Pay Guard 192
Using Password Manager 195
Data: Vault 198
Chapter 7: Trend Micro Security Feedback, Get Help, Identity, and Tools 203
Feedback 203
Help > Product Support 204
Help > Premium Services 206
Help > Ransomware Help 207
ID > Account 208
ID > Subscription Information 209
ID > About the Software 210
The Trend Micro Tools 212
About Trend Micro 218

Chapter 1: Introduction to Trend Micro™ Security

Trend Micro™ Security secures your connected world, providing protection against malware, ransomware, and online banking threats. Using advanced artificial intelligence, it also helps protect you from identity theft, coin-mining and file-less malware, viruses, online tech support and phishing scams, and other emerging threats.

Trend Micro Security offers multi-device protection and includes robust Parent Controls to help keep your kids safe online, a Password Manager to protect and manage passwords, and a Privacy Scanner to secure your privacy on social media. Its enhanced Folder Shield feature keeps your valuable files safe from ransomware by allowing only authorized applications to have access to protected folders, whether stored locally or synced online. It also provides Pay Guard, a protected web browser, that adds an extra layer of protection when banking or shopping online. And its Advanced Artificial Intelligence capability, which can stop unknown threats in their tracks, works with other key, layered technologies to provide the best and deepest security in the industry.

With 30+ years of internet security leadership, Trend Micro keeps millions of users safe from harm. As attested by AV-TEST, one of the world's premium security software testing labs, the product is one of the best on the market. At the beginning of 2019, Trend Micro Internet Security Received a **Best Protection Award** *for the whole of 2018*. (See *AV-TEST Awards 2018 Go To Trend Micro*.) Indeed, working hard to protect its users from harm, Trend Micro's Smart Protection technology blocks more than *250 million threats every day.*

The Trend Micro™ Security Family

The family of **Trend Micro™ Security** products includes the following:

- **Trend Micro™ Antivirus+ Security.** Our entry-level product keeps you safe online while you work and play. Antivirus+ Security alerts you to dangerous ransomware threats in web searches and emails. Also, it gives you simple screens and clear, easy-to-understand security status reports. You can protect 1 Windows® PC.
- **Trend Micro™ Internet Security**. Our mid-range product provides advanced online protection for up to 3 Windows® PCs. It keeps you safe online while you socialize, browse, work, and play. It also helps safeguard your privacy on social networks. Internet Security alerts you to dangerous ransomware and other threats in web searches and emails. Parental controls are included to help keep children safe online.
- **Trend Micro™ Maximum Security**. Our high-end product provides comprehensive, multiple device protection so you can enjoy your digital life safely. It keeps you safe while you socialize, browse, work, and play online. It safeguards against viruses and ransomware, dangerous websites, and identity theft. It also helps you secure your privacy on social networks. You can use Maximum Security to keep kids safe online and

protect your passwords. Additionally, you have the flexibility to protect 5 to 10 devices, depending on your subscription – for any combination of PC, Mac, or mobile.

- **Trend Micro™ Antivirus for Mac.** Industry experts know that Macs are no longer immune to viruses and other Internet threats. As a Mac user, you need privacy protection when shopping, banking and socializing online. **Antivirus for Mac®** provides online privacy and protection so you can enjoy your digital life safely. It shields you from Internet threats, dangerous websites, and phishing that can lead to identity theft. It also helps you guard your privacy on Facebook, Twitter, and LinkedIn.

Trend Micro Security: Comprehensive Protection

Trend Micro Security is equipped with special protection features and is bundled with companion products to address specific needs:

New or Updated Features

- **Email Defender.** Scam webmail that contains no malicious URLs or attachments, but which is nonetheless dangerous, is undetected by traditional email security technology. Trend Micro's Email Defender for Gmail and Outlook Webmail is developed to deal with this type of scam. It utilizes AI to identity the topic and to understand the intention of the scam emails and warns you against it upon discovery. You can then delete it with confidence.
- **Trend Micro Security for Microsoft Edge.** Trend Micro's Toolbar, which provides Web Threat Protection on websites and in search results, is now available for the Microsoft Edge browser. With additional protection against annoying or malicious advertising, as well as password protection with Password Manager, Microsoft Edge is now included in the browser family of protection of Google Chrome, Mozilla Firefox, and Internet Explorer.
- **PC Health Checkup** – Now with enhanced Potentially Incompatible Program (PIP) detection, Trend Micro Security provides additional performance optimization for your PC. Powered by Trend Micro's Platinum technology, you can check for PIPs, security vulnerabilities, and clean up unneeded files to boost your performance.
- **Pay Guard.** Trend Micro Security's protected web browser adds an extra layer of protection when you're banking or shopping online with Chrome, Firefox, or Internet Explorer. You can now launch Pay Guard directly from the Trend Micro Toolbar, so its powerful protection features are more easily applied to your default browser automatically, protecting all the data in your financial transactions, including credit card information and personal data.
- **Gamer-Friendly Mute Mode.** Mute Mote lets you temporarily stop non-critical notifications while you're gaming or doing an important task, so you're not distracted. Game compatibility has been enhanced, as well as auto-enablement, and you can now set a specific time-limited for Mute Mode, which will automatically turn off when the time interval has expired.

Highlights

- **Coin-mining Malware Protection**. Trend Micro Security can protect you against the latest coin-mining malware, which can hijack your computer's resources to secretly mine cryptocurrencies.
- **Fileless Malware Protection**. Trend Micro Security provides improved protection against fileless malware infections from spam campaigns or malicious websites, which can alter the Windows Registry and execute in Windows PowerShell, delivering malicious payloads that execute within memory.
- **Tech Support and Phishing Scams.** Protects against automated online scams that alert you with phony warnings in emails or when browsing to fake infections, or prompt you to call fraudulent tech support hotlines for purposes of hijacking your computer, to steal your identity data or your money.
- **Enhanced Folder Shield.** Enhances Trend Micro Security's ransomware protection by extending it to every user account on your computer. Protects your key documents from modification by malware or encryption by ransomware. You can customize which folders and files are protected and can include folders synced to Microsoft OneDrive, Google Drive, or Dropbox.
- **Network Scan.** You can now scan your network to detect unprotected devices, to alert you where you should install the unused seats in your multi-device license, to protect other members of your family.
- **Artificial Intelligence**. It's all about making the unknown known. With its evolutionary, hybrid blend of the latest threat protection techniques and infused machine learning, Trend Micro's artificial intelligence capability, active in Trend Micro Security, is always adapting to identify and defeat new ransomware and other unknown threats.
- **Trend Micro Troubleshooting Tool.** Our enhanced **Troubleshooting Tool** makes it quick and easy for Trend Micro Support Professionals to make repairs and fix problems.

Privacy Protection and Social Networking Security

- **Privacy Protection for Facebook, Twitter, and LinkedIn.** Trend Micro Security features an easy-to-use Privacy Scanner for social media, which identifies privacy settings that may leave your personal information publicly available and vulnerable to identity theft. Facebook applications are also scanned and the user warned if the app is posting with too wide of an audience.
- **Privacy Protection for Browsers.** Privacy Protection is provided for leading PC browsers. A simple scan of Google Chrome, Internet Explorer, or Mozilla Firefox helps increase your privacy when browsing the web.
- **Facebook Application Privacy Scanner.** Scans Facebook applications used and warns if the app is posting to your wall with too wide of an audience (Public).
- **Social Networking Security (SNS) Protection.** Trend Micro Security provides protection from threats you may encounter from malicious links in Facebook, Twitter, MySpace,

LinkedIn, Pinterest, Mixi, and Sina Weibo—the broadest and most effective SNS protection available on the market for consumers today.

- **Clear Warning.** Our SNS proactively warns you when a link is bad by highlighting it in red. When it's a safe link, it's highlighted in green. You can also mouse over a link to get real-time details about its safety from our Web Threat Protection servers.
- **Warn a Friend.** Trend Micro Security even allows you to easily and quickly inform your Facebook friends when it identifies a malicious link, so they can delete it from their Facebook page.

Family Protection

- **Parental Controls** let you restrict your kids' usage of the Internet and prevent them from visiting inappropriate websites, now including blogs/web communications and protection from illegal drugs. Enhanced functions include program restrictions, which can be set by schedule; safe search filtering, which helps prevent adult content from appearing in search results; and blocking of untested websites, to increase security when browsing.

Data Theft Prevention

- **Data Theft Prevention (DTP).** DTP lets you stop specific data, such as email accounts or credit card numbers, from being shared in Outlook outward-bound email or online forms.
- **Secure Erase** lets you overwrite and delete data from your disk, so it can't be recovered.
- **Vault** lets you encrypt data on your hard drive and remotely lock it up if your laptop is lost or stolen; when the device is found you can then unlock that data.
- **Trend Micro™ Password Manager** helps you securely store all your passwords and sensitive information, so you can access them when needed on PCs, Macs, and Android and iOS mobile phones and tablets. It's automatically installed with Trend Micro Maximum Security, so you can get started easily, or you can purchase it separately.

Other Highlights

- **Smart Scheduled Scan** – Trend Micro Security provides a Smart Scheduled Scan. Based on recent computer usage, the most suitable scan will start automatically at an appropriate time.
- **Screen Reader –** Screen Reader support is now available for visually-impaired users.
- **Intensive Scan Switch** – Automatically increases the protection level only when you need it – for intensive scans when your computer is infected.
- **Search Results Rating –** When you conduct a search on the internet the search results give you a list of URLs, proactively highlighted.
- **Manual URL/Link Scanner –** As with SNS, when you hover your mouse over a link in search results, the manual link scanner rates the safety and reputation of any links on the web page.

- **Mobile Security for Android and iOS** – Trend Micro Maximum Security includes Trend Micro Mobile Security for Android and iOS, for protection of your mobile devices.
- **Windows 11 compatibility –** Trend Micro Security is fully compatible with Microsoft's Windows 11 operating system, with backwards compatibility with Windows 10, 8.1 and 7. See System Requirements for details.

Clean User Interface

- **Easy to Use.** Trend Micro Security provides a clean interface design. Both easy-to-use and powerful, the Trend Micro Security Console provides all the tools you need at the touch of mouse or a tap of a finger to easily configure your solution to meet your security needs. Conduct scans and obtain reports that let you know just how Trend Micro Security is protecting you.

Key Features of Trend Micro Security

Table 1. Trend Micro Security 2022 - Key Features

TREND MICRO SECURITY 2022 – Key Features	Trend Micro Antivirus for Mac	Trend Micro Antivirus+ Security	Trend Micro Internet Security	Trend Micro Maximum Security
Licensing	1 user Mac only	1 user PC only	3 users PC & Mac	5 / 10 users PC, Mac & Mobile
Pricing	$29.95/yr	$29.95/yr	$39.95/yr	5 - $89.95/yr 10 - $99.95/yr
Virus and Spyware Protection	✓	✓	✓	✓
Rootkit Detection and Removal		✓	✓	✓
Web Threat Protection	✓	✓	✓	✓
Anti-Spam	✓	✓	✓	✓
Anti-Phishing	✓	✓	✓	✓
Ransomware Protection	✓	✓	✓	✓
AI / Machine Learning	✓	✓	✓	✓
Auto Intensive-level Protection Scan Switch		✓	✓	✓
Authenticate Wi-Fi Networks and Hotspots		✓	✓	✓
Windows Firewall Booster		✓	✓	✓
Block Malicious Links in Email	✓	✓	✓	✓
Search Results Ratings	✓	✓	✓	✓
Gamer-Friendly Mute Mode		✓	✓	✓
Social Networking Protection	✓	✓	✓	✓
Smart Schedule Scan			✓	✓
Privacy Scanner: Facebook, Twitter, LinkedIn; Facebook Applications Internet Explorer, Google Chrome, Mozilla Firefox	✓		✓	✓
Folder Shield	✓	✓	✓	✓
Email Defender		✓	✓	✓
Pay Guard		✓	✓	✓
Data Theft Prevention			✓	✓

Table 2. Trend Micro Security 2022 – Key Features (Continued)

TREND MICRO SECURITY 2020 – Key Features	Trend Micro Antivirus for Mac	Trend Micro Antivirus+ Security	Trend Micro Internet Security	Trend Micro Maximum Security
Secure Erase			✓	✓
PC Health Checkup			✓	✓
Vault with Remote File Lock				✓
Password Manager with Integrated Installer / Activation				✓
Parental Controls	✓		✓	✓
Android				✓
iOS				✓
MacOS	✓			✓

*Trend Micro Maximum Security provides seats for Windows, MacOS, Android, and iOS

System Requirements

Table 3. Trend Micro Antivirus+, Internet, and Maximum Security 2022

Operating System	CPU	Memory	Disk Space
Windows® 10, (32 or 64-bit)	1 GHz	2 GB (32-bit) 2 GB (64-bit)	1.3 GB 1.5 GB recommended
Windows® 8.1 (32 or 64-bit)	1 GHz	1 GB (32-bit) 2 GB (64-bit)	
Windows® 7 Service Pack 1 (32 or 64-bit)	800MHz (1GHz recommended)	1 GB (32-bit) 2 GB (64-bit)	
Other Requirements			
Web browser	Google Chrome™ - 74/75 Mozilla Firefox® - 67/68 Microsoft® Internet Explorer® 11.0 Microsoft Edge - Latest Version		
Display	High-color display with a resolution of 800x600 pixels or above		

Table 4. Trend Micro Antivirus 2022 (v10) for Mac

Operating System	CPU	Memory	Disk Space
Mac OS® X version 10.14 or higher (Mojave)	Apple Macintosh computer with an Intel® Core™ Processor	2 GB	1.5 GB
Mac OS® X version 10.13 or higher (High Sierra)			
Other Requirements			
Web Browser	Apple® Safari® 11.0 or higher Mozilla® Firefox® latest and most recent previous versions Google Chrome™ latest and most recent previous versions		

Table 5. Password Manager 5.0 (WIN, MAC) / 5.1 (Android, iOS)

Operating System (Windows)	CPU	Memory	Disk Space
Windows 10 (32bit and 64bit)	1 GHz or faster processor	2 GB or more	300+ MB
Windows 8.0, 8.1 (32bit and 64bit)			
Windows 7 Service Pack 1 or above (32bit and 64bit)			
Web Browser	Microsoft Internet Explorer 11.0 Microsoft Edge (via Trend Micro Security for Edge) – the latest 2 versions Mozilla Firefox – the latest 2 versions Google Chrome – the latest 2 versions		
Operating System (Mac OS)	**CPU**	**Memory**	**Disk Space**
Mac OS X 10.14 (Mojave) Mac OS X 10.13 (High Sierra)	Intel Core 2 Duo 2.0 GHz or faster processor	2 GB or more	300+ MB
Web Browser	Safari 12.0 or higher Mozilla Firefox – the latest 2 versions Google Chrome – the latest 2 versions		
Mobile Operating System	**Devices**		
Android 5.1-9.0	Android Smartphones App, Tablets App		
iOS 11-12.3	iOS iPhones, iPads, iPods		

Table 6. Trend Micro Mobile Security 12.0 for Android

Requirements	Description
Operating Systems	Android OS 4.1 or later
Device Space	50MB minimum
Memory	40MB-100MB Android (varies by device)
Other	3G/4G (LTE) | Wi-Fi Internet Connection

Table 7. Mobile Security 8.0 for iOS

Requirements	Description
Operating Systems	iOS 10.0 or later. 64-bit device required for latest version.
Device Space	Global / EMEA / APAC: 50MB minimum
Supported iOS Devices	iPad® Air 1, Air 2, Mini 2, Mini 3, Mini 4, iPad® Pro, iPod® Touch 6
Other	3G/4G (LTE) | Wi-Fi Internet Connection

Internet Connection, USB Installation

Trend Micro Security needs an Internet connection for you to register online, download installs and updates, obtain virus information, send email to support, and browse the Trend Micro web site. While online, Trend Micro Security also takes advantage of the Smart Protection Network's reputation systems in combination with Smart Scan to help obtain the reputation of files. See Section 6: Trend Micro Security and the Smart Protection Network for more details on the SPN and how users are still protected offline.

Note: Tend Micro may be transferred to another computer and installed from a USB thumb drive without any issues.

Target Audience

The target audiences for the Trend Micro Security products are mainstream consumers and home/small offices with 10 users or less who need effective protection against viruses, spyware, and other malware that doesn't impact their system's memory consumption and other resources.

Global Availability

October 14, 2021

Contacting Trend Micro

Trend Micro Incorporated
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900
Toll-free: (888) 762-8763
www.trendmicro.com

Consumer Support Line

(800) 864-6027
Monday - Friday, 5:00AM - 8:00PM Pacific

Free Phone, Email and Chat support

Trend Micro offers free phone, email, and chat support. For more info, contact eSupport at:
http://esupport.trendmicro.com/support/consumer/consumerhome.do?locale=en_US

You can also contact the Trend Community at: http://community.trendmicro.com/

Premium Support Services

Trend Micro provides users with Premium Support Services for a wide variety of technical issues including installation, virus and spyware removal, PC Tune-ups, etc. These services are offered as a bundle with a purchase of Trend Micro Security or as stand-alone and ad-hoc services. For more information, select **Premium Services** in the **Trend Micro Security Console > ID** drop-down menu, or go to:

http://www.trendmicro.com/us/home/products/support-services/index.html

Chapter 2: Installing and Activating Trend Micro Security

Trend Micro™ Security has separate installs for each version of the product:

- Trend Micro™ Antivirus+ Security
- Trend Micro™ Internet Security
- Trend Micro™ Maximum Security
- Trend Micro™ Antivirus for Mac™

(See our separate Product Guide for instructions to install and use Trend Micro™ Antivirus for Mac™.)

In the following example we install Trend Micro Maximum Security on Microsoft Windows 10, but each version of Trend Micro Security has a nearly identical installation and activation process on the various versions of Windows.

Install Trend Micro Security

To install Trend Micro Security on Windows 11 using a Download:

1. Go to https://www.trendmicro.com/en_us/forHome.html to download Trend Micro Security 2022. The main page **For Home** appears.

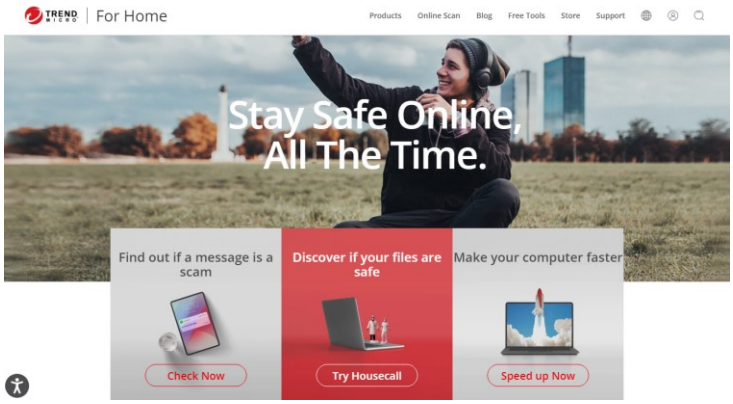

Figure 1. Trend Micro for Home

Paid Version:

1. If you want to buy Trend Micro Security, scroll down to **Top Rated Antivirus Protection For You** and click **Learn More** on the version you want.

Figure 2. Top Rated Antivirus Protection For You

2. Select an edition that works for you and click **Buy Now,** then follow the directions to complete your purchase.

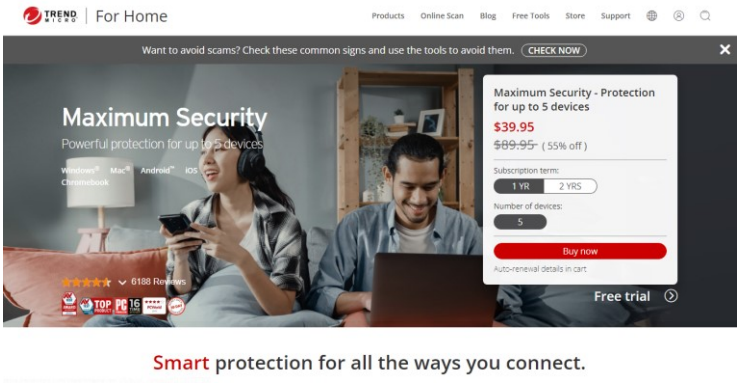

Figure 3. Buy Now

Trial Version:

1. If you want to install a **Trial** version, click **Free Tools** in the upper right-hand corner of the **For Home** webpage. The **Free Tools** page appears.

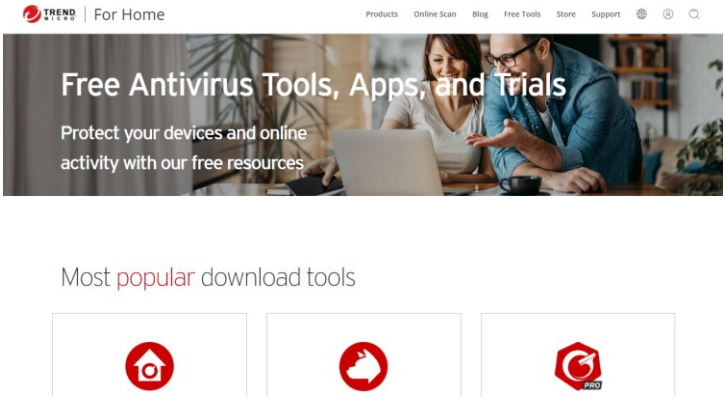

Figure 4. Free Tools

2. Scroll to the edition of Trend Micro Security you wish to download and click **Download Now**.

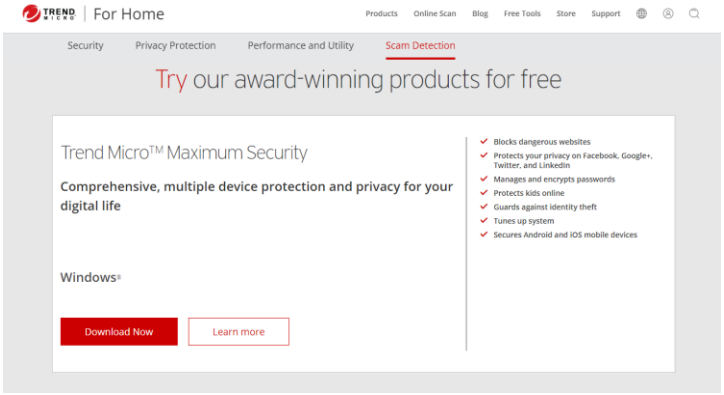

Figure 5. Try our award-winning products for free

3. A **"Why try when you can buy"** window will open. Click **Continue to free trial** to continue.

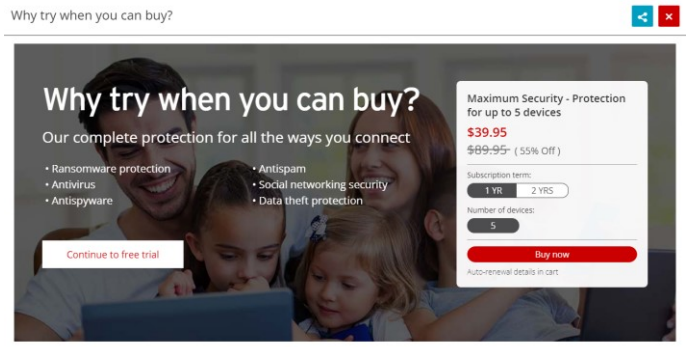

Figure 6. Why try when you can buy

4. You are taken to the eSupport webpage, where you can download the Trial. Click **FREE Download**.

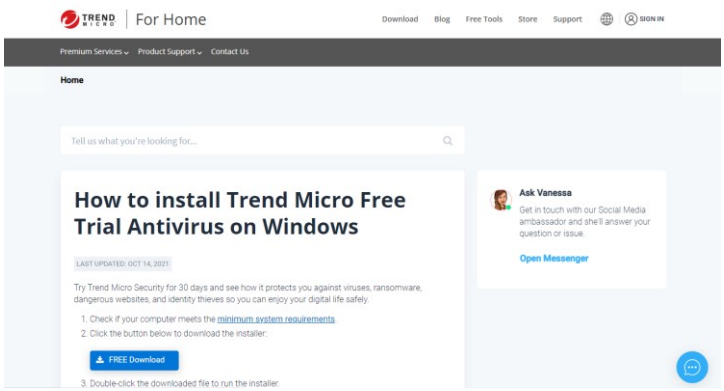

Figure 7. Install Trial Version

5. In this example, click Save As**.** A **Save As** dialog window appears. Navigate to the Downloads folder where you will put the downloader and click **Save**.

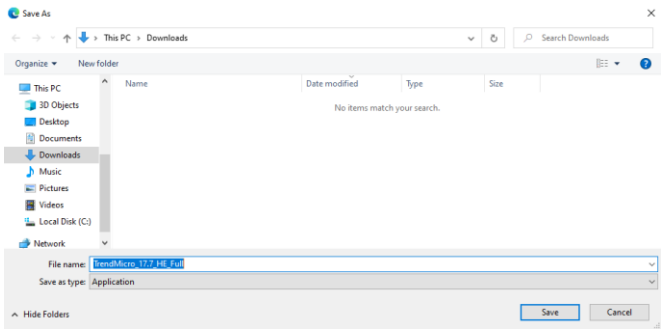

Figure 8. Save As

6. The **Downloader** execution file downloads and displays at the top of your browser (Edge browser sample below).

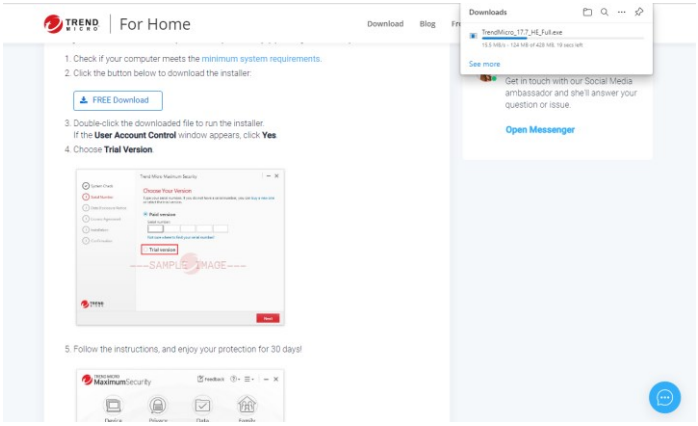

Figure 9. Downloader Exe (Edge)

7. Once the installer finish downloading, double-click the **Installer exe** file. A Windows **User Account Control** pop-up dialog appears, asking if you want to allow the app to make changes to your computer. Click **Yes**.

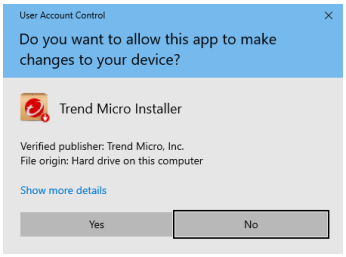

Figure 10. User Account Control

8. The installation begins, extracts the installer files, and gives you a progress screen.

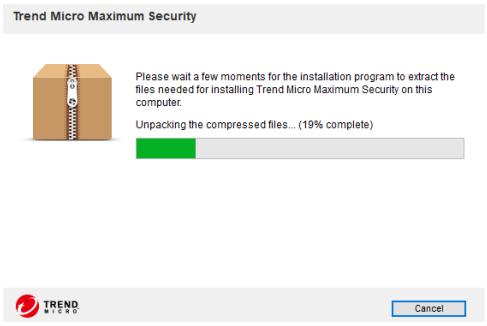

Figure 11. Unpacking Files

9. Trend Micro Security will then do a **System Check**, to see if your computer meets the minimum system requirements and will conduct a quick malware scan.

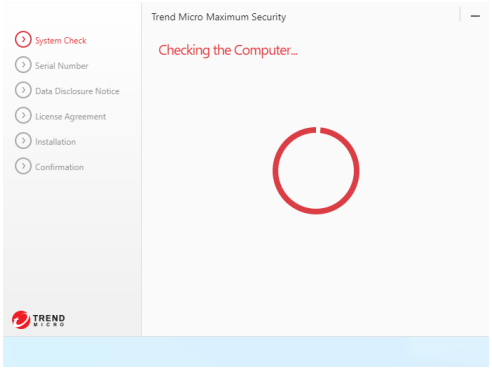

Figure 12. Checking the Computer

10. When the process completes, a **Serial Number** screen appears asking you to **Choose Your Version.**

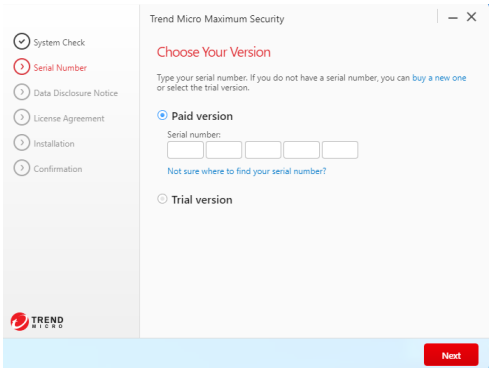

Figure 13. Choose Your Version > Paid

11. If you're installing a **Paid** version, enter the **serial number** provided by Trend Micro in your retail box or confirmation email. If you're installing a Trial version, click the **Trial version** button. Click **Next**.

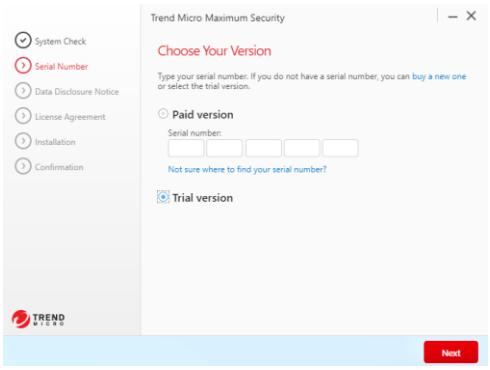

Figure 14. Choose Your Version > Trial

12. In each case, the **Data Disclosure Notice** appears.

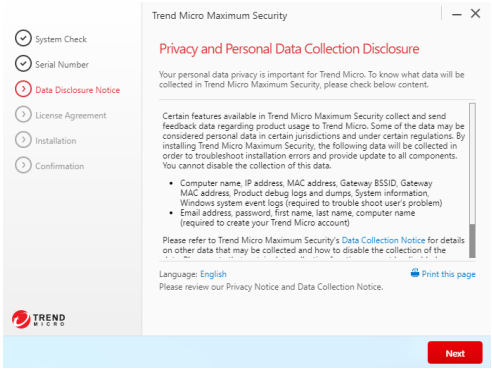

Figure 15. Data Disclosure Notice

13. Read the **Data Disclosure Notice** to know what kind of feedback and detection data will be collected by Trend Micro, then click **Next**. The **License Agreement** appears.

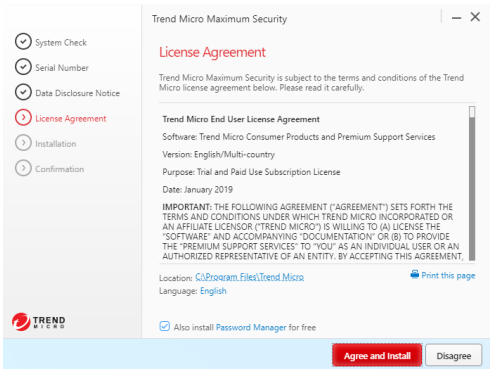

Figure 16. License Agreement

14. Trend Micro Security chooses a default location for the installation. You can change this by clicking the **Location** link and browsing to another location. (Trend Micro recommends you use the default.)
15. If you wish, click the **Language** link to stop the software from automatically adjusting to the language of your operating system, then pick the language you want the software to display.
16. Note too that **Password Manager** is installed automatically with Trend Micro Maximum Security. Uncheck the checkbox if you don't wish to also install **Password Manager.**
17. Read the **License Agreement** using the scrollbar. If you agree with the **License Agreement**, click **Agree and Install**. (Click **Print this page** to print it out.)
18. Trend Micro Security begins the installation. This takes a few minutes. A progress indicator indicates the stages and progress of the install.

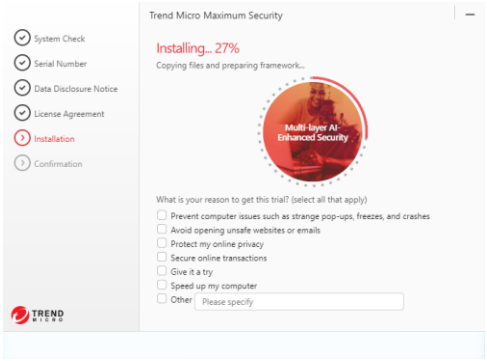

Figure 17. Progress Indicator

Trial Version

1. If you've installed a **Trial** version, when the installation is complete a screen appears, saying **Installation Completed.**

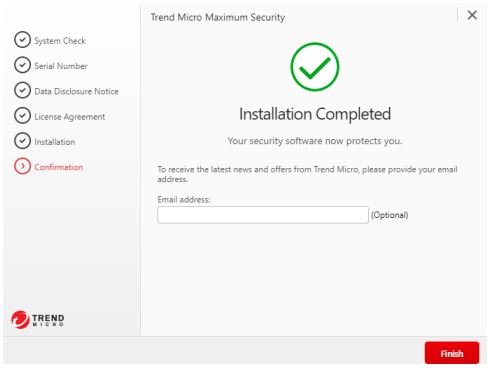

Figure 18. Installation Completed

2. To receive the latest news and offers from Trend Micro, enter your email address and click **Finish**. This completes your installation. Trend Micro Security automatically updates its components.

Figure 19. Welcome to Trend Micro Security

3. The Trend Micro Security **Welcome** screen appears, and your PC is now protected against security threats. Click **OK**.

Figure 20. Protect Your Folders from Ransomware

4. The **Protect Your Folders From Ransomware** appears. Toggle the **checkbox Do not show this agai**n to hide the folder shield setup every time you open the Trend Micro Security. Click **Protect More Folders** to customize the list of folders to protect or click **Use Default Protection** to use the default folder list.

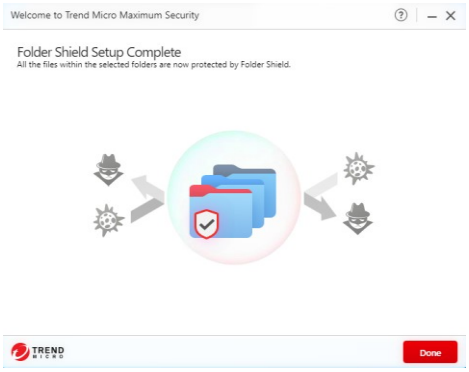

Figure 21. Folder Shield Setup Complete

5. The **Folder Shield Setup Complete** appears. Click **Done**.
6. The installation is complete.

Paid Version

1. If you've installed a **Paid** version, a screen appears, asking if you wish to **Receive Monthly Email Reports.**

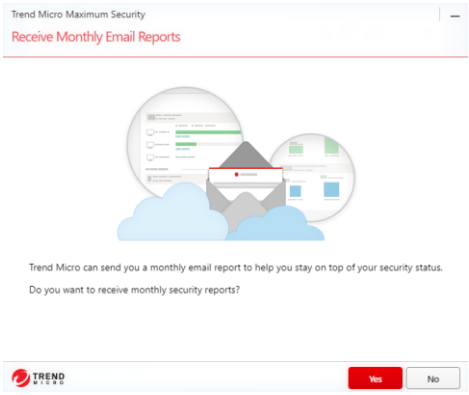

Figure 22. Receive Monthly Email Reports

2. Click **Yes** if you wish. The wizard then asks you to **Activate Your Protection.**

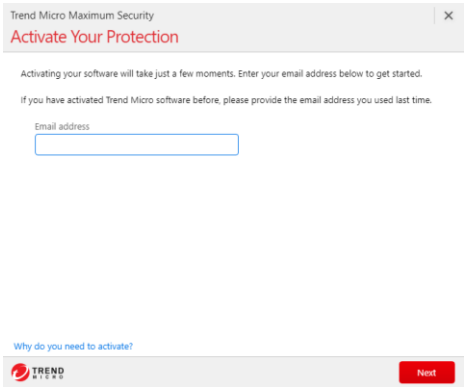

Figure 23. Activate Your Protection

3. You now have two options for the email address:
   - **Use an existing Trend Micro Account.** Provide the email address for this account.
   - **Create a new Trend Micro Account.** Provide a preferred email address.

Use an Existing Trend Micro account:

1. If you have activated Trend Micro software before, open or go to the **Trend Micro Security console**.

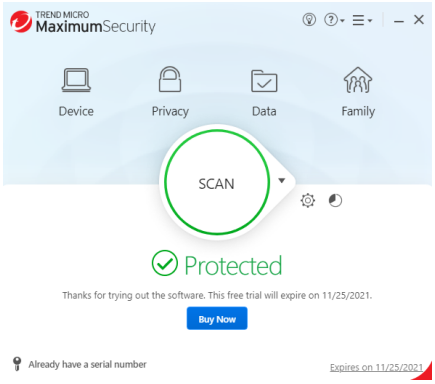

Figure 24. Trend Micro Maximum Security Console

2. Click **Already have a serial** link.

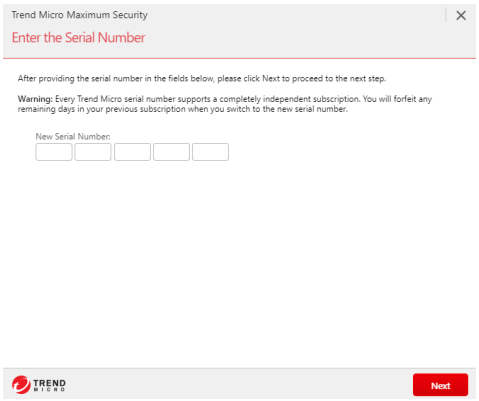

Figure 25. Enter the Serial Number

3. Enter the **Serial Number** of your Trend Micro Product and click **Next**.

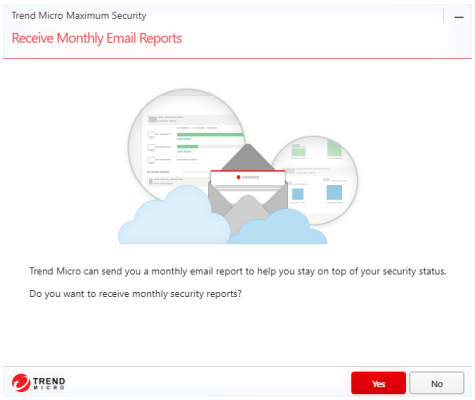

Figure 26. Receive Monthly Email Reports

4. The **Receive Monthly Email Reports** appears, click **Yes** to receive monthly security reports.

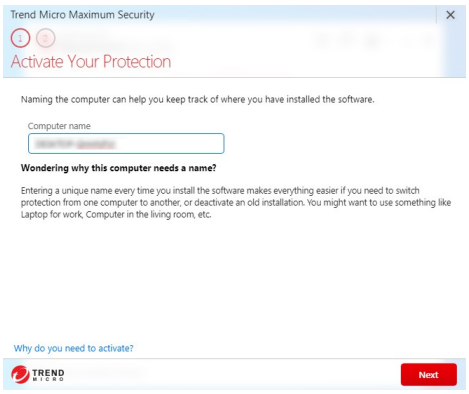

Figure 27. Activate Your Protection

5. The **Activation Protection** appears. Enter a **computer name** and click **Next**.

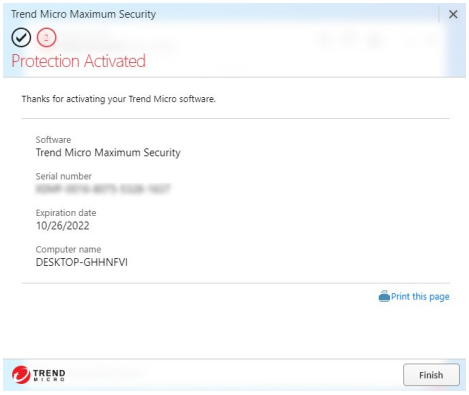

Figure 28. Protection Activated

6. Click **Finish** to complete the activation.

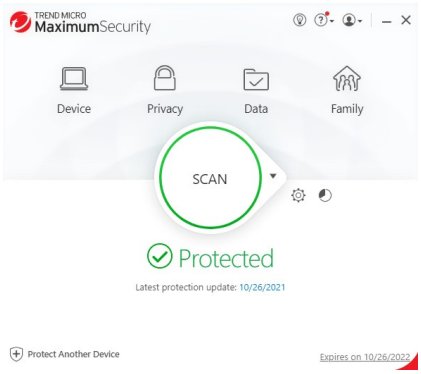

Figure 29. Trend Micro Maximum Security Console

Create a New Trend Micro account:

1. If you have **not** activated Trend Micro software before, enter your preferred email address and click **Next**. A screen appears, asking you to **Enter Account Information.**

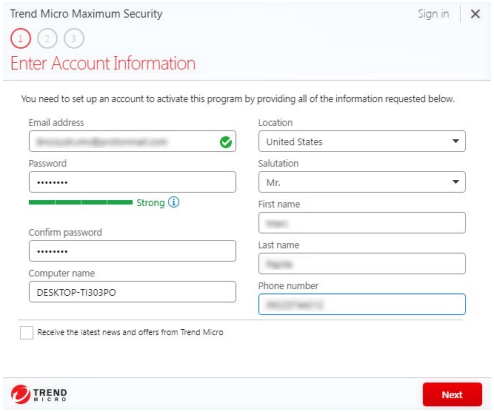

Figure 30. Enter Account Information

2. Enter your account information. For the password, use only simple letters and numbers, but not less than 8 characters. For the computer name, use the name of your computer that's automatically entered, or enter a new name to identify it.

3. Read the **Trend Micro Privacy Statement**. If you agree, check **I have read and agree to the Trend Micro Privacy Statement.**

4. You may retain or remove the check to **Receive the latest news and offers from Trend Micro** and click **Next**. A screen appears for you to **Check What You Entered.**

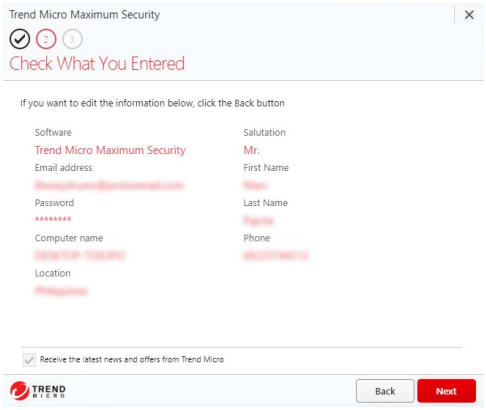

Figure 31. Check What You Entered

5. If your entries are accurate, click **Next**. A dialog indicates **Protection Activated.** You may print this page.

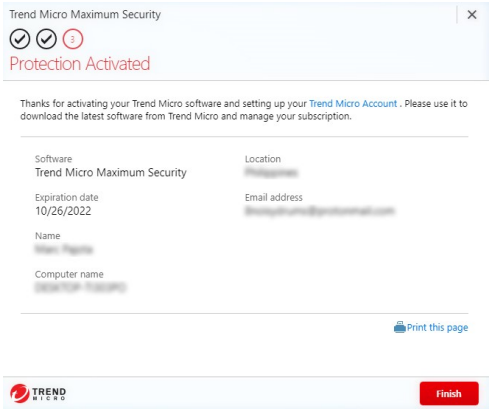

Figure 32. Protection Activated

6. Click **Finish** and the Trend Micro Security Welcome screen appears, and your PC is now protected against security threats. Click **OK**.

Figure 33. Welcome to Trend Micro Security

7. Click **OK** and the **Secure and Enhance Your Mobile Life** window appears. You can scan the QR Code from your mobile device, then follow the instructions to install and activate Trend Micro Mobile Security on the device.

Figure 34. Secure and Enhance Your Mobile Life

8. Click **Close** and the **Trend Micro Security Console** appears.

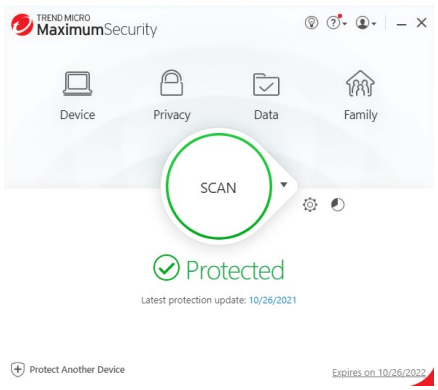

Figure 35. Trend Micro Maximum Security Console

9. Close the **Trend Micro Security Console** by clicking the **X** in the upper-righthand corner of the screen.

Set Up Folder Shield

1. Trend Micro strongly urges you to set up **Folder Shield** right after you've installed Trend Micro Security, to protect yourself from ransomware. The default setting is quick and easy to enable.

Figure 36. Open the Main Console

2. Click **Open the Main Console** in the Trend Micro Security menu in the **System Tray**, or double-click the **Trend Micro Security** shortcut on the desktop. The **Trend Micro Security Console** appears, with the **Welcome** screen in front of it.

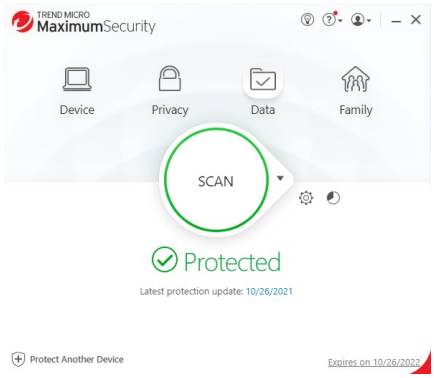

Figure 37. Trend Micro Maximum Security Console

3. The **Trend Micro Security console** appears, click **Data**.

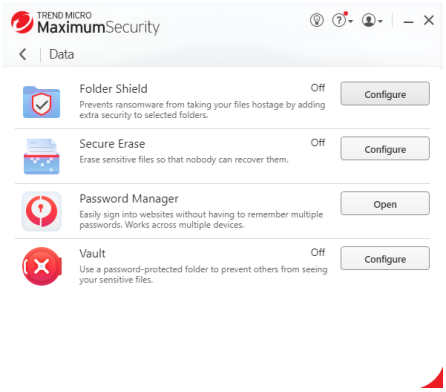

Figure 38. Data

4. Click **Configure** to setup **Folder Shield**.

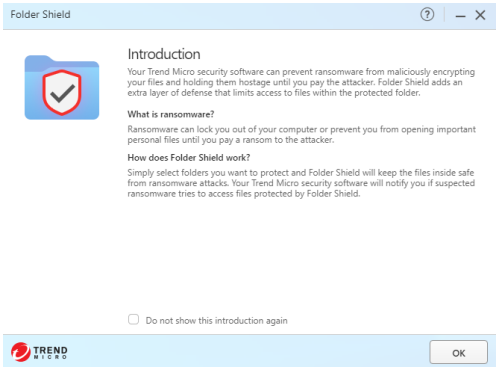

Figure 39. Folder Shield Introduction

5. The **Folder Shield** window appears providing you information about ransomwares and how **Folder Shield** will protect your files. You can toggle the **Do not show this introduction again** to hide the window when you reopen the Folder Shield configuration. Click **OK**.

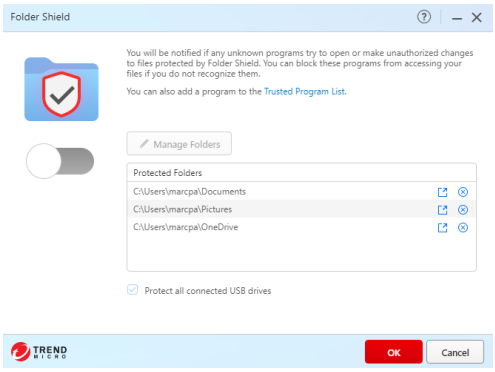

Figure 40. Folder Shield Configuration

6. Toggle the **Folder Shield slider** on the left to enable it. A default folder list is already available.

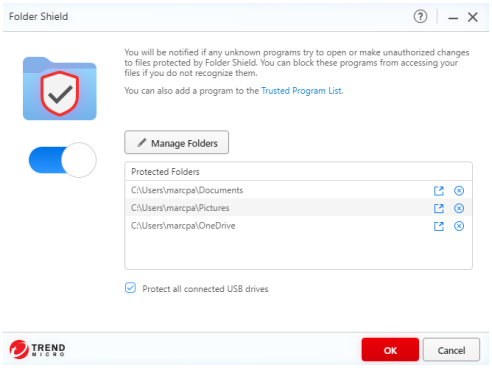

Figure 41. Folder Shield Configuration

7. Toggle **Protect all connected USB drives checkbox** to protect inserted USB hard drives and thumb drives. To customize the folder list, click **Managed Folders**.

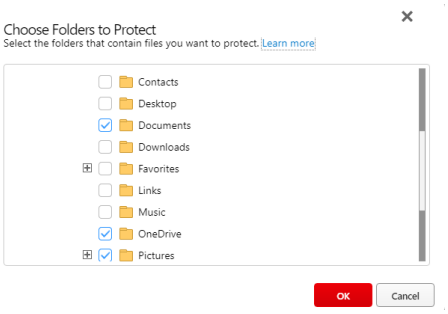

Figure 42. Choose Folders to Protect

8. Select the folders that contains files you want to protect. Click **OK**.

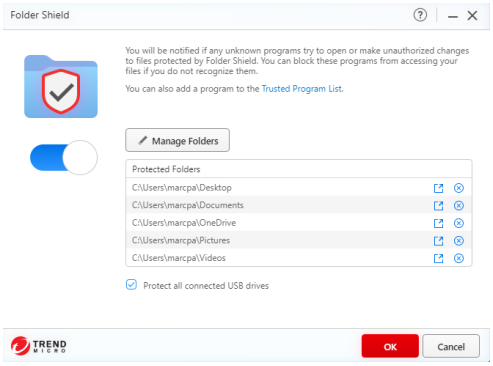

Figure 43. Folder Shield Configuration with Custom List

9. Click **OK** to finish the setup.

Enable Trend Micro Security Toolbar

Once you've installed Trend Micro Security, you should enable the **Trend Micro Security Toolbar** in your browser of choice to protect yourself against web threats.

There are two versions of the Toolbar:

- Trend Micro Security for Microsoft Edge
- Trend Micro Toolbar for Chrome, Firefox, and Internet Explorer

See the sections following to install and enable one or both of the two options.

Enable Trend Micro Security for Microsoft Edge

The default browser in Microsoft Windows 11 and 10 is Microsoft Edge. Once you've installed Trend Micro Security, you should enable **Trend Micro Security for Microsoft Edge** to improve your browsing protection. It provides web threat protection, ad blocking, and in Trend Micro Maximum Security, Password Manager is also included.

1. If Microsoft Edge is active as your default browser, Trend Micro Security will prompt you to install **Trend Micro Security for Microsoft Edge**, to **Safeguard Your Browser**.

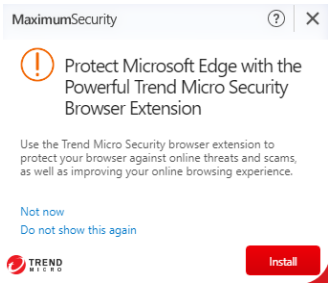

Figure 44. Protect Microsoft Edge

2. Click **Install** in the popup. Trend Micro Security will launch the Microsoft Edge and take you to directly to the extension **Trend Micro Security for Microsoft Edge.**

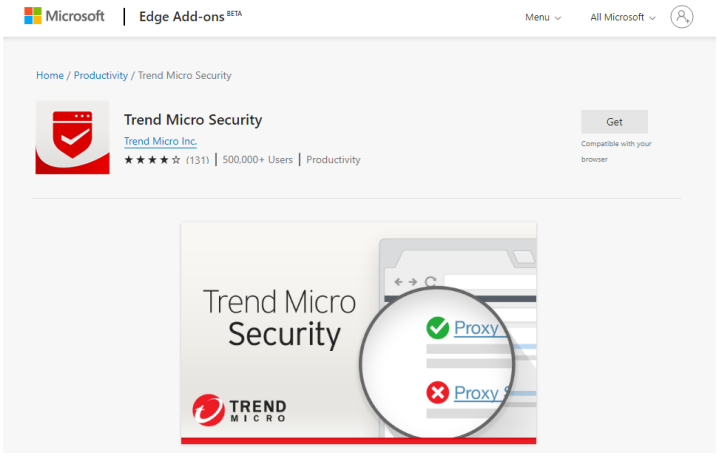

Figure 45. Edge Add-ons

3. Click the **Get** button and the **Add "Trend Micro Security" to Microsoft Edge?** popup appears. Click **Add extension** and wait for the add-on to download and install.

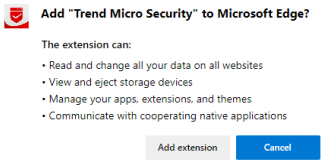

Figure 46. Add "Trend Micro Security" to Microsoft Edge?

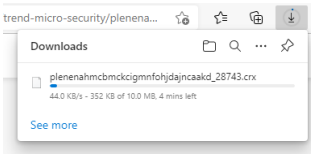

Figure 47. Microsoft Edge Downloads

4. Once installed, the page redirects to a welcome page of **Trend Micro Security Edge Add-on**.

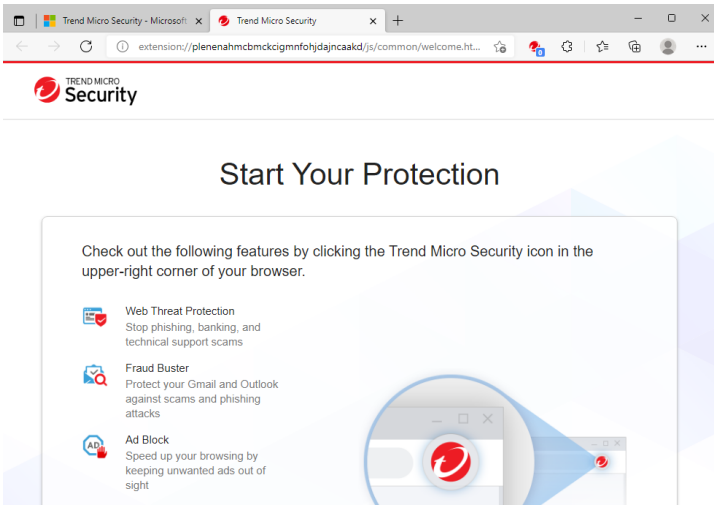

Figure 48. Trend Micro Security Extension Welcome Page

5. Click **Trend Micro Security** in the **Edge Extensions** screen.

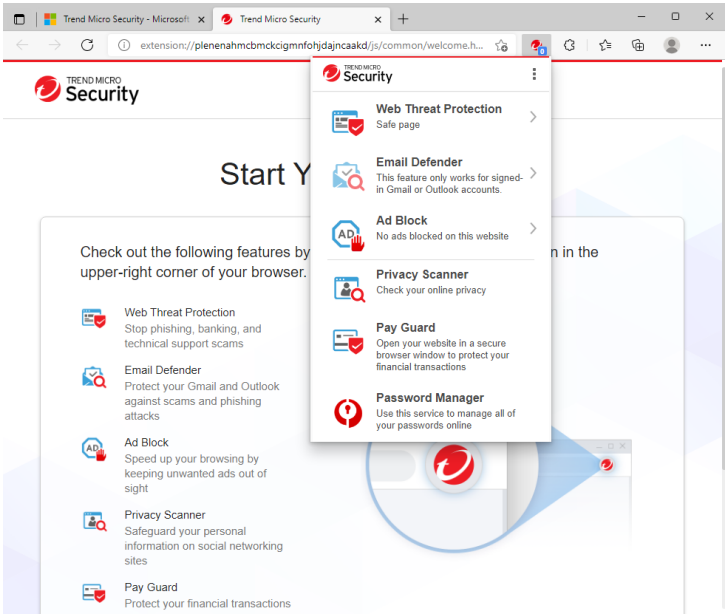

Figure 49. Trend Micro Security Extension for Microsoft Edge

6. Trend Micro Security Extension automatically rate links on web pages and blocks ads. To enable Password Manager, click **Password Manager**. Password Manager is only available in the Premium (Paid) version of Trend Micro Security for Edge, or as part of your Trend Micro Maximum Security subscription.

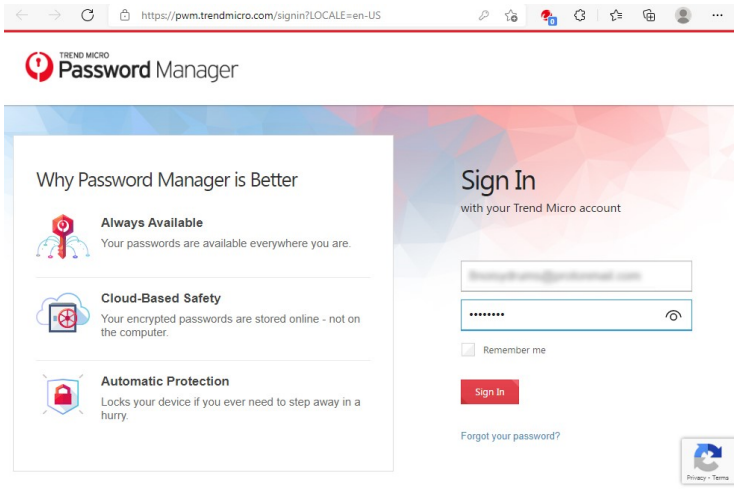

Figure 50. Password Manager

7. Enter your **Trend Micro account and password** and click **Sign In**.

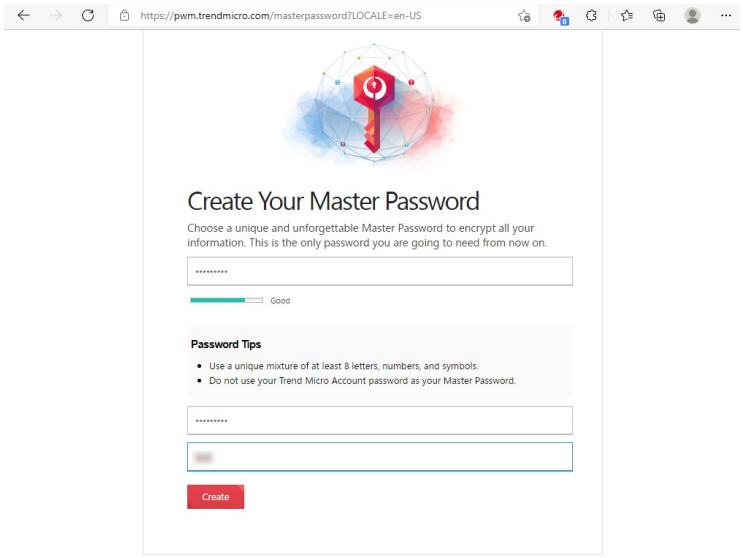

Figure 51. Create Your Master Password

8. The **Create Your Password page** appears. Input a password with at least 8 letters, numbers, and symbols. Enter a password hint and click **Create**.

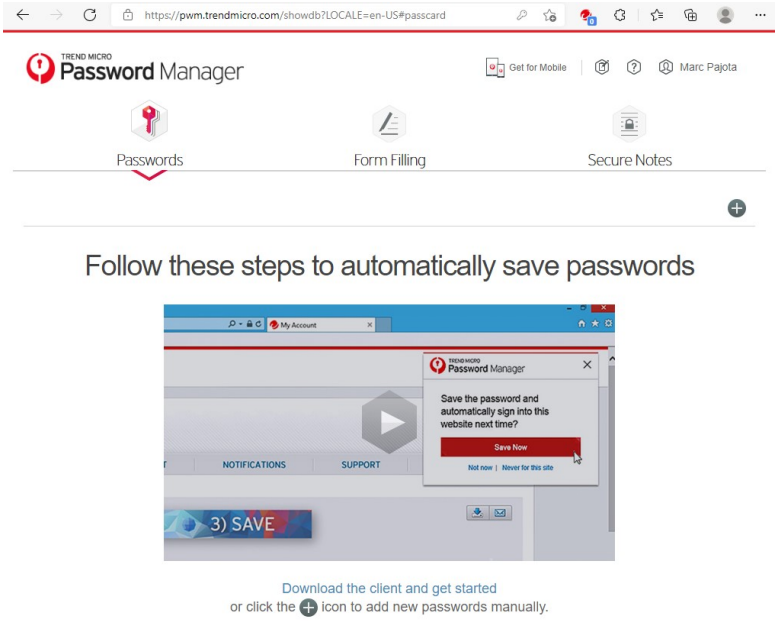

Figure 52. Password Manager Dashboard

9. The **Password Manager dashboard** page appears. You can know **save passwords**, **form information** and **secure notes**.

Note: **Trend Micro Antivirus + and Internet Security users need to purchase the Premium edition of Trend Micro Security for Edge separately to use Password Manager in Edge. However, if you install Trend Micro Maximum Security, Trend Micro Security for Microsoft Edge with Password Manager is automatically included as part of your subscription. Once you've created your Password Manager account via your Trend Micro Maximum Security activation, Password Manager will also be active in Trend Micro Security for Microsoft Edge, once you sign into your account. See the Password Manager section in this guide for instructions on using Password Manager.**

10. Now, if you attempt to go to a dangerous page, with **Web Threat Protection** active you'll be blocked.

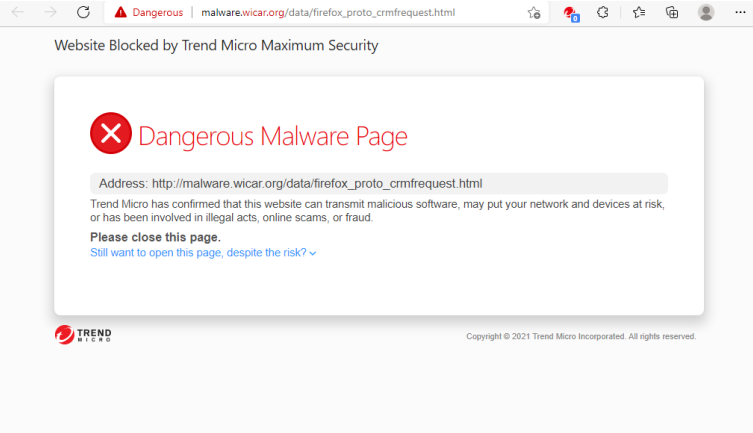

Figure 53. Web Threat Protection Block

11. Additionally, with **Ad Block** active, if you go to a page with advertising, the ads will be blocked.

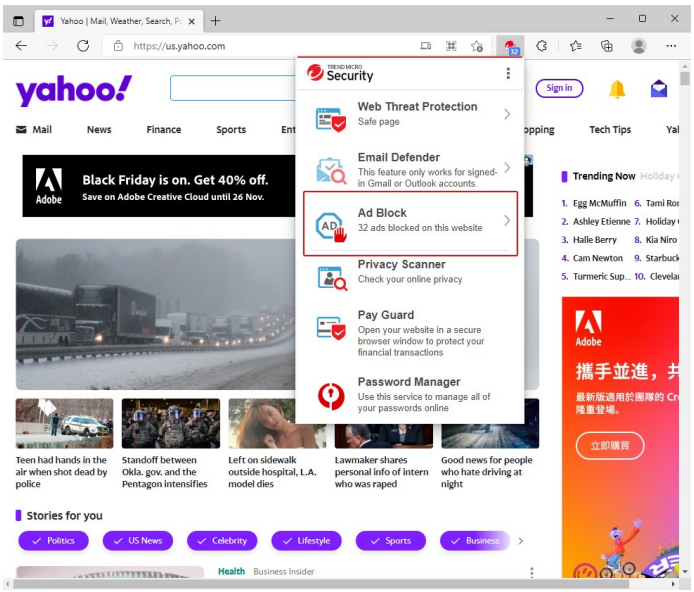

Figure 54. Ads Blocked

12. Click the **Web Threat Protection** banner in the drop-down menu to review the **Trend Micro Security 30-day report** of pages scanned and blocked.

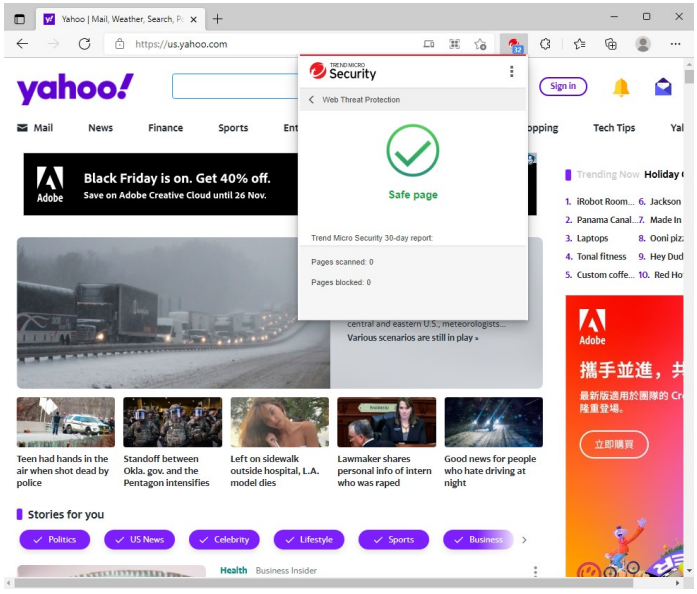

Figure 55. Trend Micro Security 30day Report

13. Click **Ad Block** in the drop-down menu. The drop-down menu pages allow you **Stop** or **Resume Ad Block** by clicking the **Stop/Resume Add Block** button. You can also use the slider to turn off the feature.

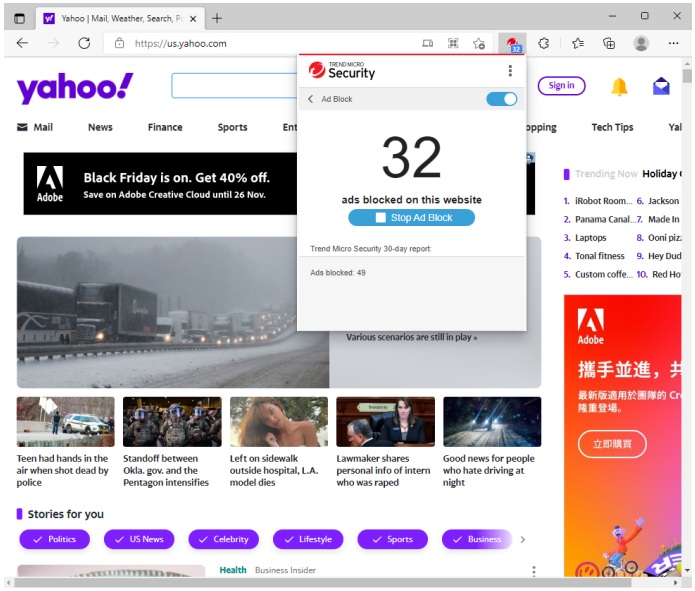

Figure 56. Stop Ad Block | Turn Off Trend Micro Security Slider

14. To turn **Trend Micro Security for Edge** on or off, click the **Menu** icon, then **Extensions** in the Edge drop-down menu to show the extensions installed in Edge.

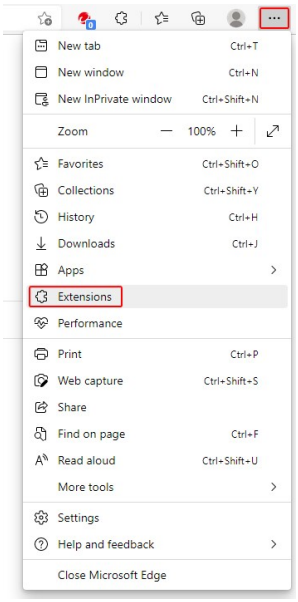

Figure 57. Edge Menu > Extensions

15. Slide the slider to **Off** to turn off **Trend Micro Security for Microsoft Edge**, or to **On** to turn it on.

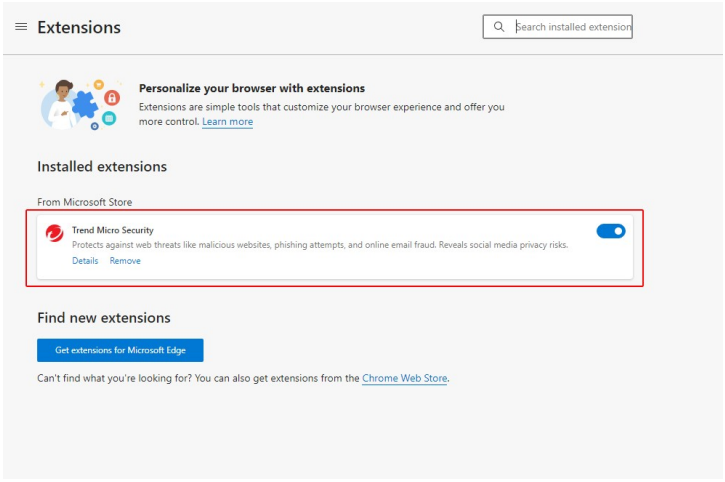

Figure 58. Trend Micro Security Extension

Enable Trend Micro Security Toolbar for Google Chrome, Mozilla Firefox, Internet Explorer, or Pay Guard

Though Microsoft Edge is the default browser in Windows 11 and 10, you can change your default to Google Chrome or Mozilla Firefox (you need to install these browsers first).

Once you've installed Chrome or Firefox, you can then activate or install **Trend Micro Security Toolbar** in the browser to increase your security when browsing.

The example below uses Google Chrome, but a similar activation process occurs for Mozilla Firefox or Microsoft Internet Explorer.

To install Trend Micro Toolbar in Chrome

1. Launch your browser of choice (e.g., Internet Explorer, Google Chrome, or Mozilla Firefox) and go to:

   https://helpcenter.trendmicro.com/en-us/article/tmka-18432

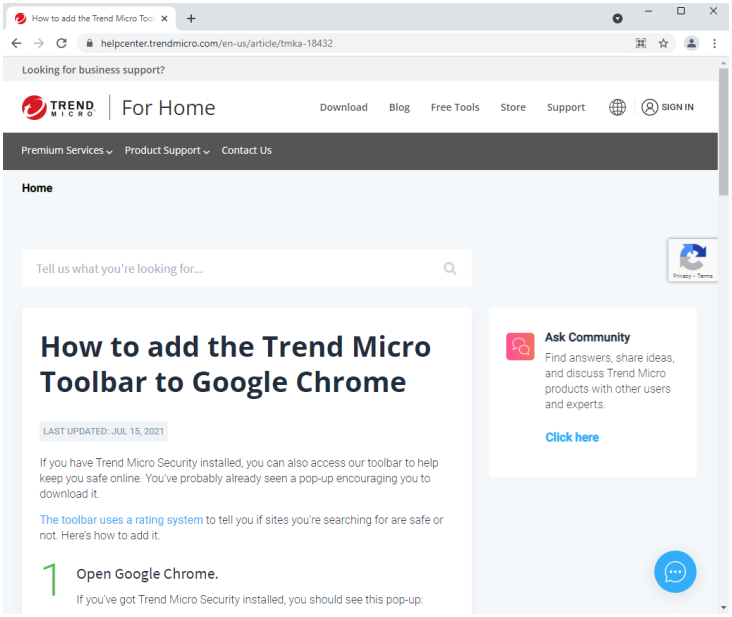

Figure 59. How To Add the Trend Micro Toolbar

2. The **Trend Miro Support page** appears. Scroll down to **Click 'Install Trend Micro Toolbar'** and click **install it here**.

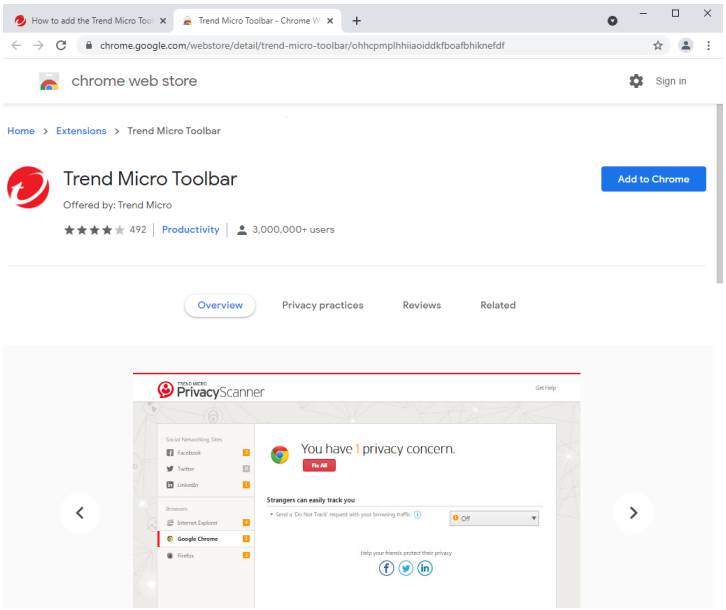

Figure 60. Google Chrome Web Store

3. The **Google Chrome Web Store** appears. Click **Add to Chrome**.

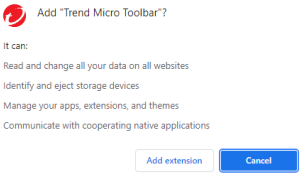

Figure 61. Add Trend Micro Toolbar

4. The **Add "Trend Micro Toolbar"** popup appears. Click **Add extension**.

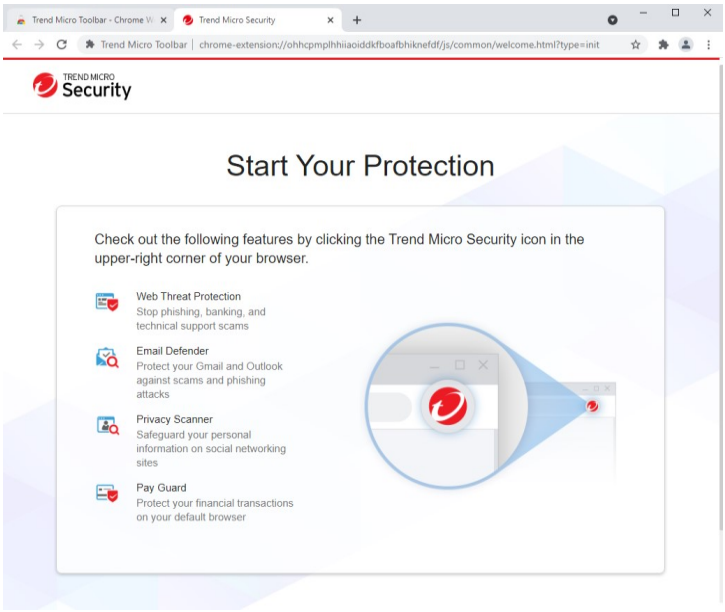

Figure 62. Trend Micro Toolbar Start Your Protection

5. The **Start Your Protection page** appears. To pin the toolbar, click the **Extension** Icon.

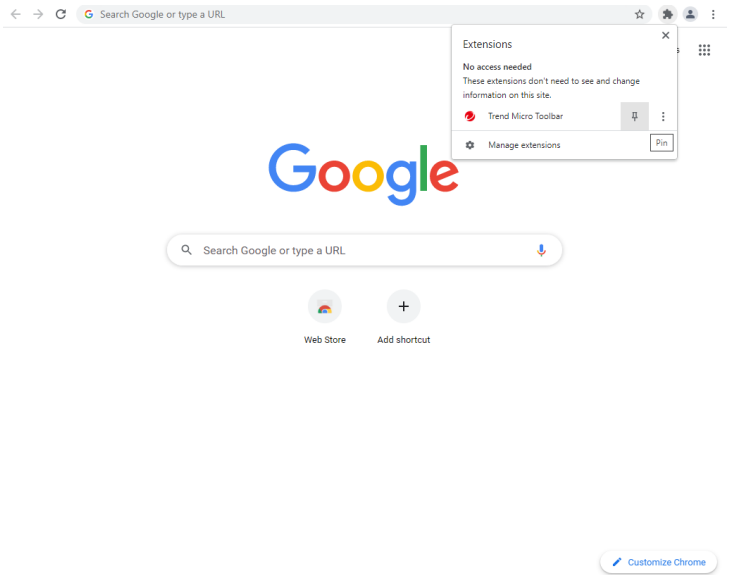

Figure 63. Google Chrome Extension

6. Click the pin icon of the Trend Micro Toolbar.

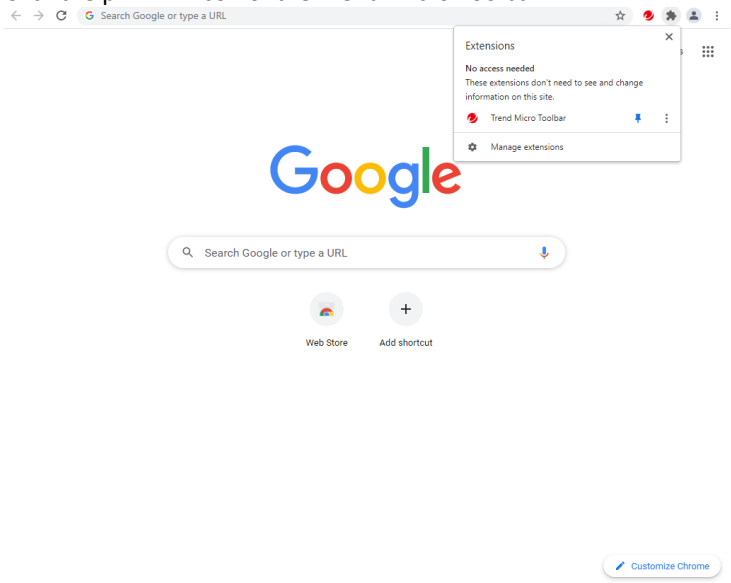

Figure 64. Trend Micro Toolbar

7. The Trend Micro Toolbar is pinned in the extension toolbar. To enable or disable the toolbar go to **Menu > More tools > Extensions**.

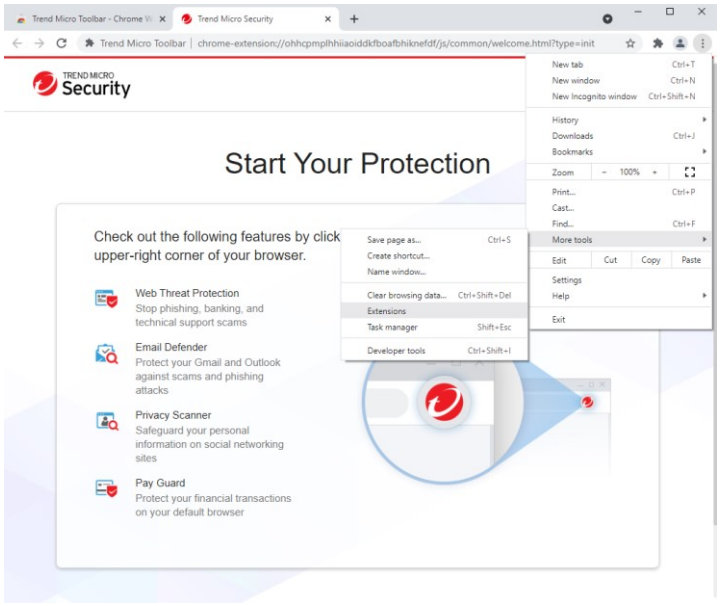

Figure 65. Chrome > Menu > More tools > Extensions

8. The **Google Chrome Extension page** appears. Slide the slider to **Off** to turn off Trend Micro Security for Microsoft Edge, or to **On** to turn it on.

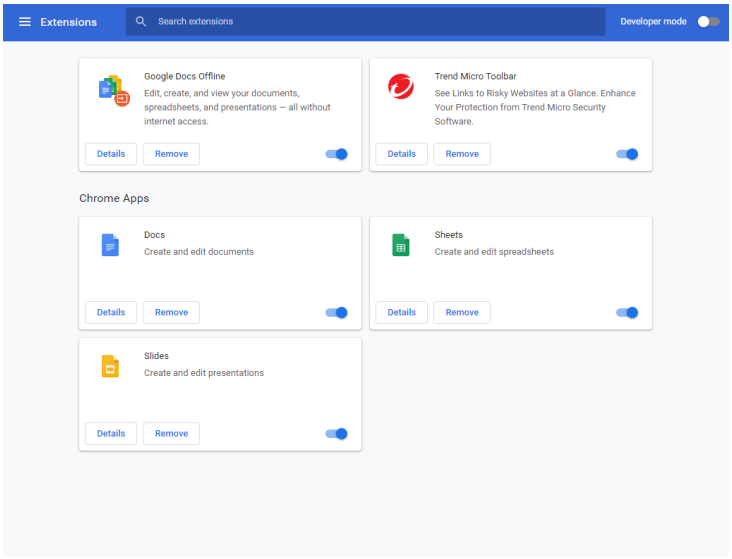

Figure 66. Google Chrome Extensions

To enable Trend Micro Toolbar in Pay Guard:

1. Similarly, you may enable **Trend Micro Toolbar** in the **Trend Micro Pay Guard** browser, which is a hardened version of your default browser, tailored to keep you safer when banking or shopping online. (Our example here again shows Chrome.)
2. Double-click the **Pay Guard** icon on your desktop to launch it.

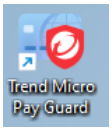

Figure 67. Pay Guard Desktop Icon

3. The **Pay Guard** window and the **Trend Micro Toolbar** popup appears. Click **Install** to install the Trend Micro Toolbar.

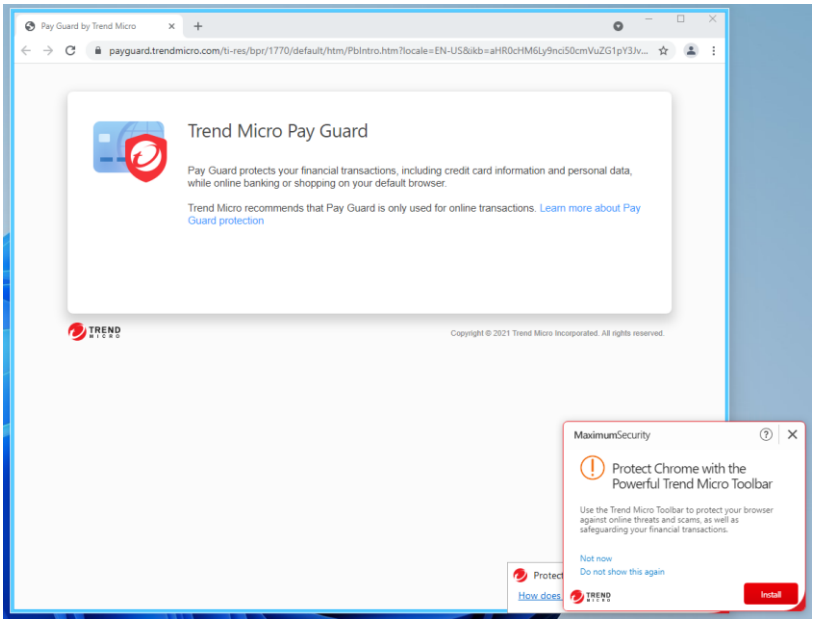

Figure 68. Trend Micro Pay Guard

4. The **Google Chrome Web Store** page appears. Click **Add to Chrome**.

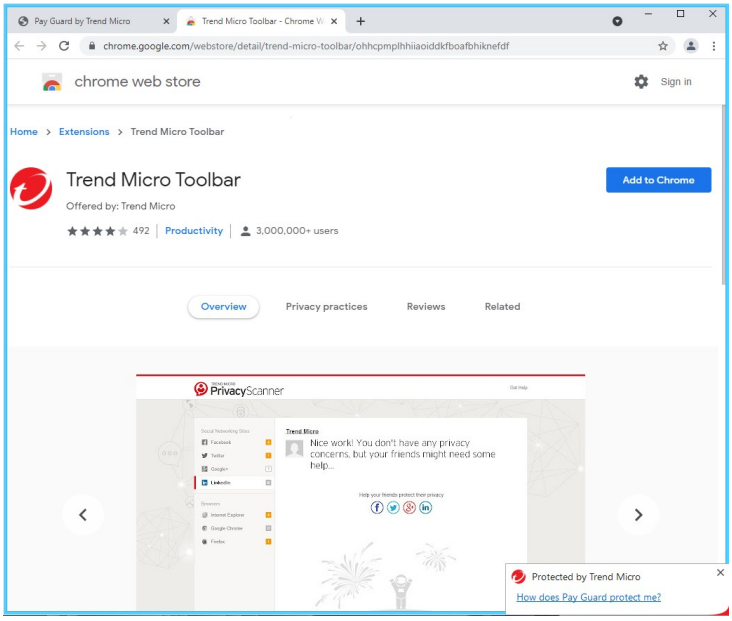

Figure 69. Google Chrome Web Store

5. Select it as shown to activate the **Trend Micro Toolbar**. A popup appears, letting you enable it.

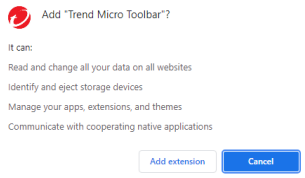

Figure 70. Add Trend Micro Toolbar

6. The **Add "Trend Micro Toolbar"** popup appears. Click **Add extension**.

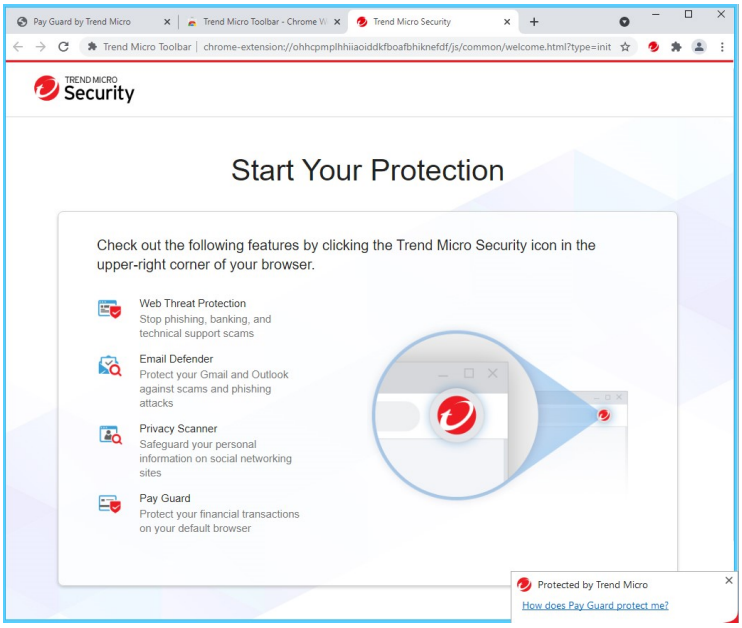

Figure 71. Pay Guard with Trend Micro Toolbar

7. Now, either in the full version of your default browser, or in **Pay Guard**, the **Trend Micro Toolbar** supplements your **Rate links on web pages** protection, adding detailed on-demand ratings to automatic Search results, indicated by green checkmarks (good), question marks (untested), or red Xs (bad).

8. In the example below, we return to Microsoft Edge.

Note: **Pay Guard is best used for online transactions. Trend Micro Maximum Security users may also enable Trend Micro Password Manager in Pay Guard, to use strong passwords for your transactional accounts. See the chapter on Trend Micro Maximum Security for more details.**

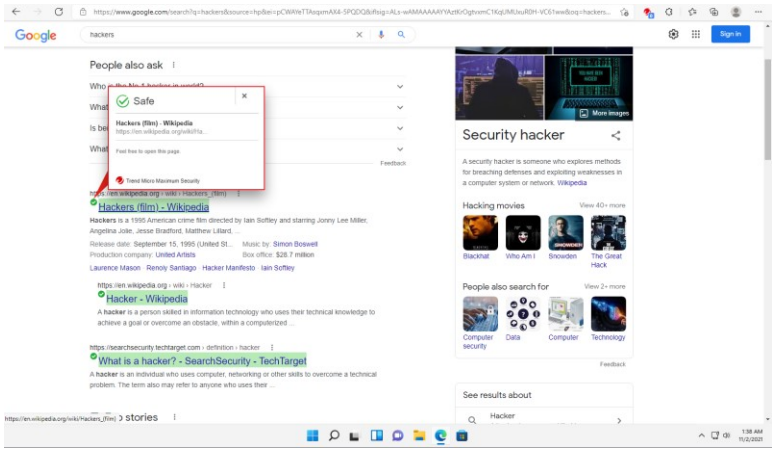

Figure 72. Google Chrome > Search Results Showing Safe Pages

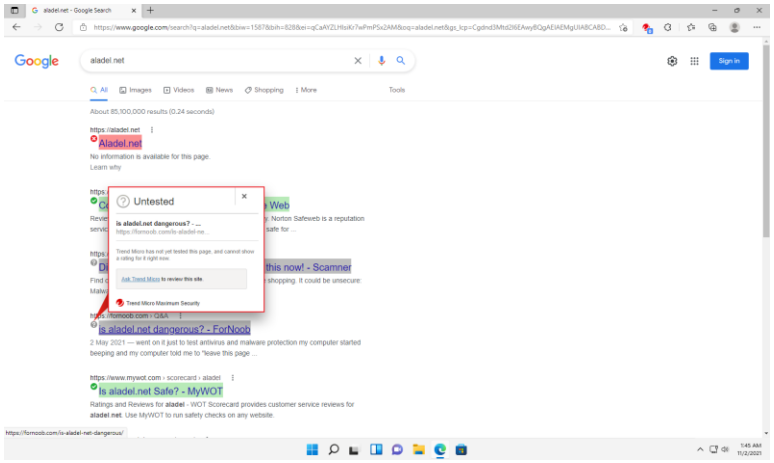

Figure 73. Google Chrome > Search Results Showing Untested Page

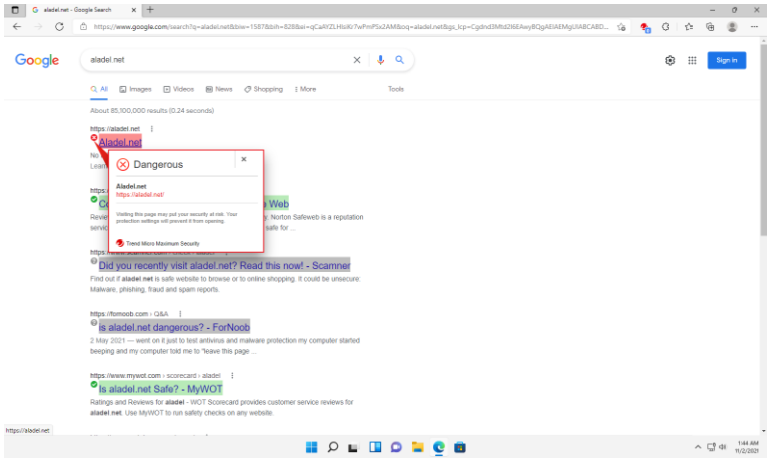

Figure 74. Google Chrome > Search Results Showing Dangerous Pages

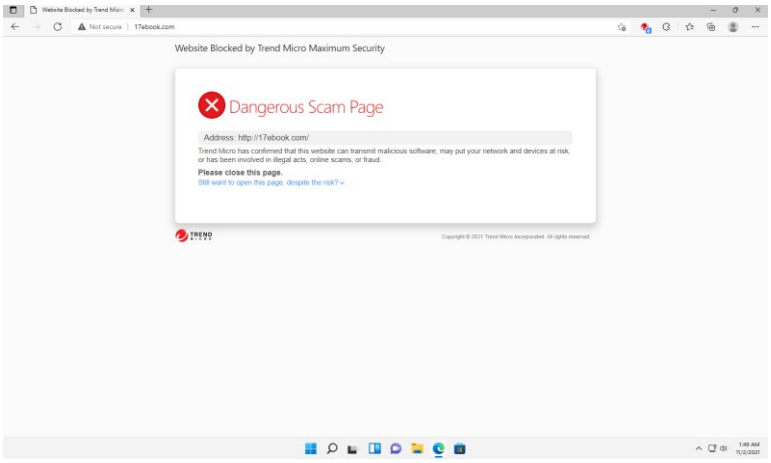

Figure 75. Dangerous Page

Enable Email Defender for Gmail and Outlook Webmail

More and more scam emails these days may contain no obvious malicious URLs or attachments but can nonetheless be a threat, using social engineering to snare the unsuspecting user. However, such emails can't be detected by traditional email security technology. **Email Defender** is designed to deal with this type of scam email, using artificial intelligence (AI) technology to identify the topic and to understand the intention of the scam. As part of **Trend Micro Toolbar**, **Email Defender** protects Gmail and Outlook webmail in Microsoft Edge, Internet Explorer, Chrome, and Firefox. The example below uses Gmail in Microsoft Edge to show the setup.

To enable Email Defender:

1. **Email Defender** requires first that you log into your Gmail or Outlook webmail account.

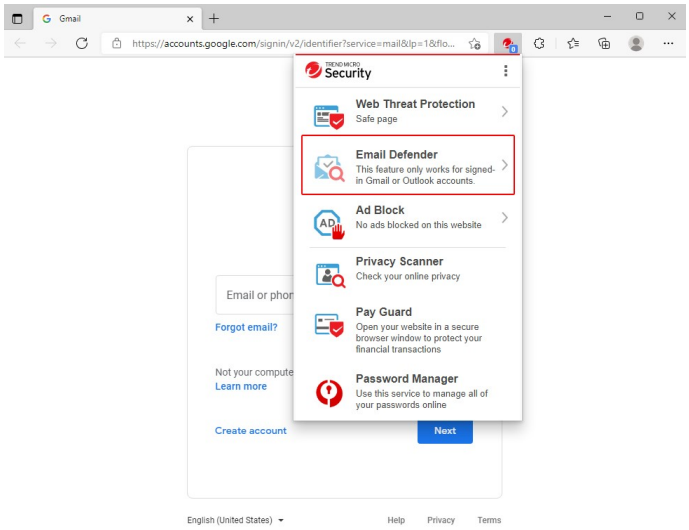

Figure 76. Log Into Gmail or Outlook to Enable Email Defender

2. For example, log into your Gmail account in Edge.

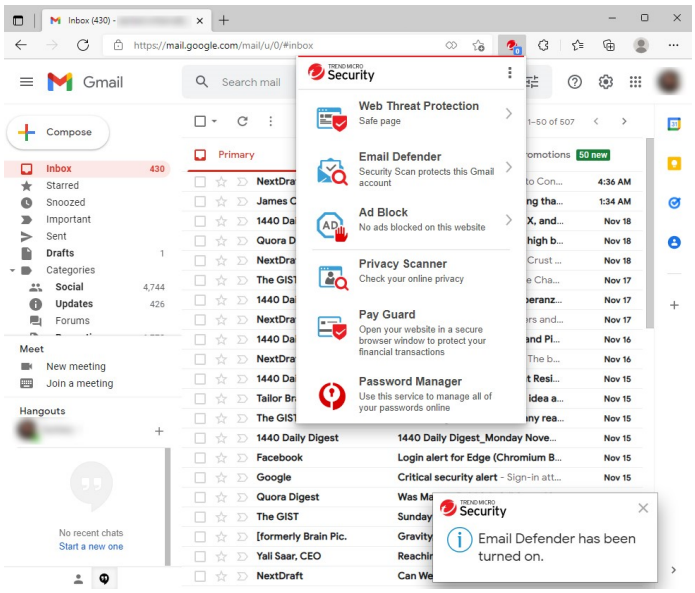

Figure 77. Gmail Account Page

3. Email Defender is now enabled and you can now see it active in the Trend Micro Toolbar.

4. Your Gmail (or Outlook.com) webmail will now be scanned for potential scams and you'll be alerted with a warning popup when you open a scam email, telling you to not follow any instructions contained in the email.

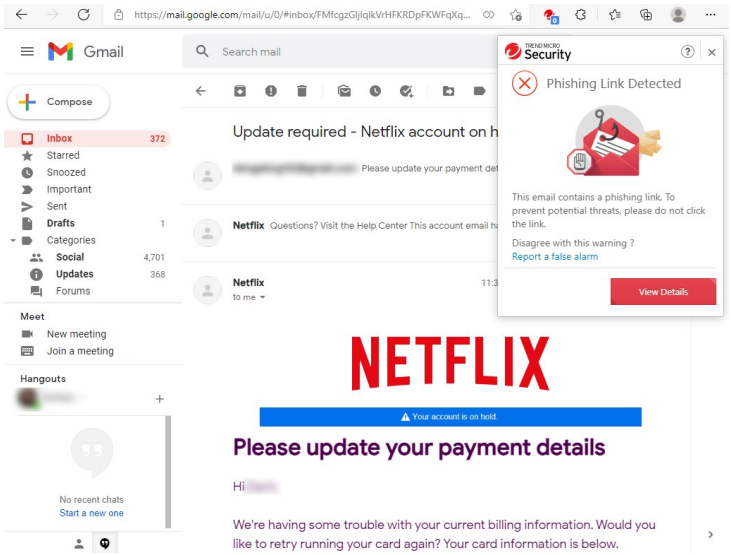

Figure 78. Phishing Link Detected

5. Click **View Details** in the popup warning to get more details about the scam.

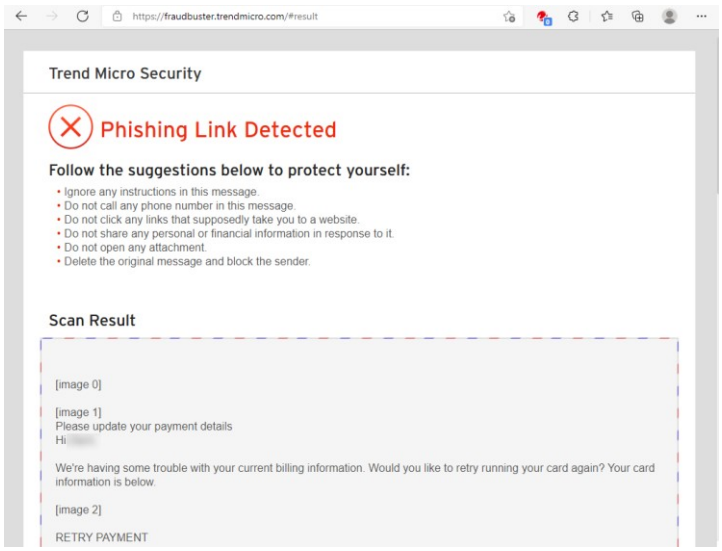

Figure 79. Phishing Link Detected: Details

6. Follow Trend Micro's instructions to better protect yourself from scams; or contact Trend Micro to get more support. When done, you should close the **Details** window as well as the scam email, then delete the scam email from your inbox.

Protect Another Device: PCs, Macs, Android and iOS Mobile Devices

Subscriptions to Trend Micro™ Antivirus+, Internet Security, and Maximum Security variously let you protect other PCs and Macs, as well as Android and iOS mobile devices.

- Trend Micro Antivirus+: 1 PC, though you may switch your protection to another PC
- Trend Micro Security Internet Security: up to 3 PCs and Macs
- Trend Micro Security Maximum Security: from 5 devices, including PC, Mac, Android and iOS Mobile devices
- Trend Micro Security Premium Security: from 10 devices, including PC, Mac, Android and iOS Mobile devices

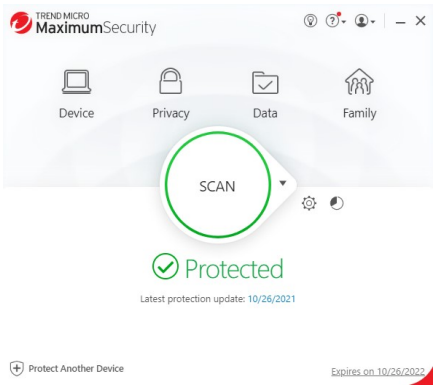

Figure 80. Protect Another Device

1. To get started with your protection for another device, click **Protect Another device.** The **Protect Another Device** screen appears. The range of options depends on the edition of Trend Micro Security you have purchased.

Note: **A subscription to Trend Micro Antivirus+ allows you to protect only one device. To transfer this subscription to another device you need to log into your My Account page, download the installer on the second device, and install it. Once you register the application, you'll be given the option to disable Trend Micro Antivirus+ on the first device so you can activate it on the second.**

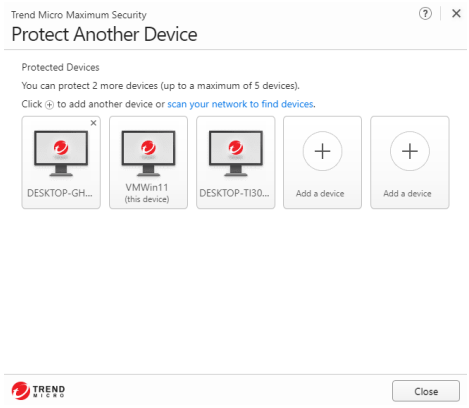

Figure 81. Maximum Security > Protect Another Device

2. With Trend Micro Internet or Maximum Security, you can click the link **scan your network to find** devices on your network. A popup appears asking "Do you want Trend Micro Internet/Maximum Security to scan your home network (LAN) to find connected devices?"

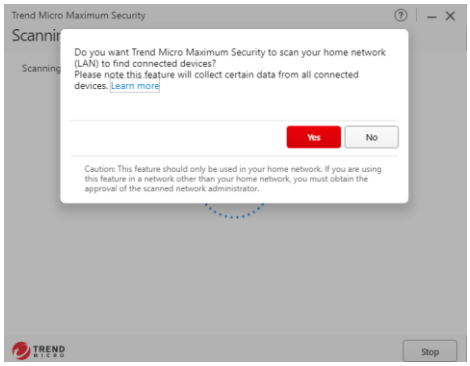

Figure 82. Scan Prompt

3. Click **Yes** to scan your network. The scan begins.

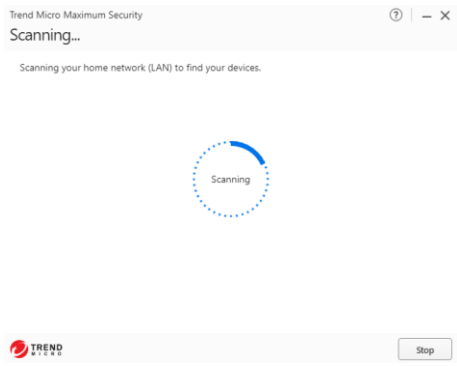

Figure 83. Scanning for Other Devices

4. When the scan is complete, a **Scan Results** screen appears.

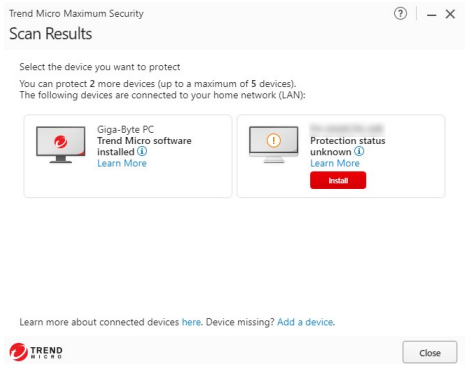

Figure 84. Devices Found > Install

5. If the **Scan Results** finds other devices to protect, it provides an **Install** button to install protection on that device.

6. Tap **Install** to install Trend Micro Security/Mobile Security on that device. A screen appears, with options for downloading and installing it.

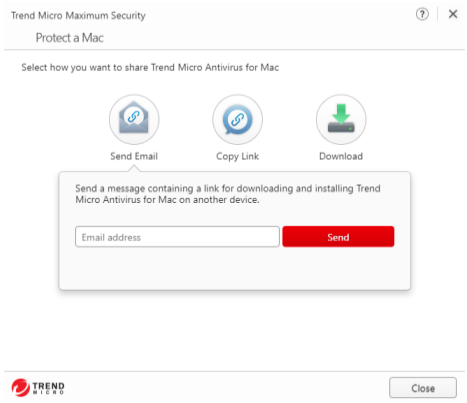

Figure 85. Protect an iOS Device

7. If it finds no devices, the screen says **No Devices Found.**

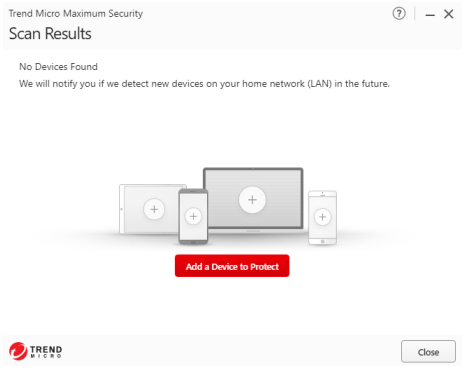

Figure 86. No Devices Found > Add a Device to Protect

8. If you know that your family has other devices currently not on the network, you can still tap **Add a Device to Protect.** The **Protect Another Device screen** appears.

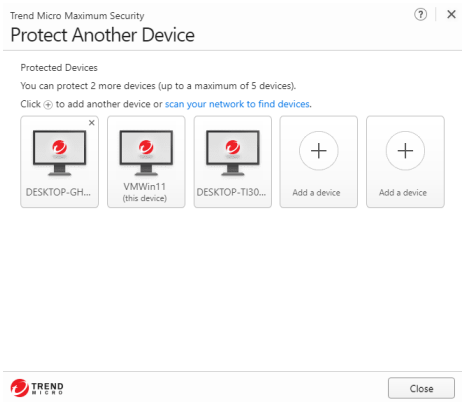

Figure 87. Protect Another Device

9. For Trend Micro Internet and Maximum Security, click an icon to **Add a device.** A popup appears, letting you choose the platform you would like to share protection with.

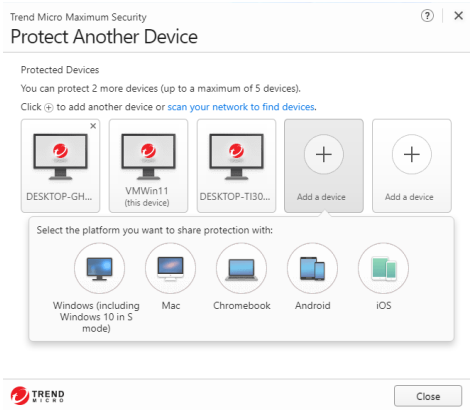

Figure 88. Add a Device Popup

10. Click the icon for your chosen platform. A screen appears, providing email, copy link, and download options for getting the software.

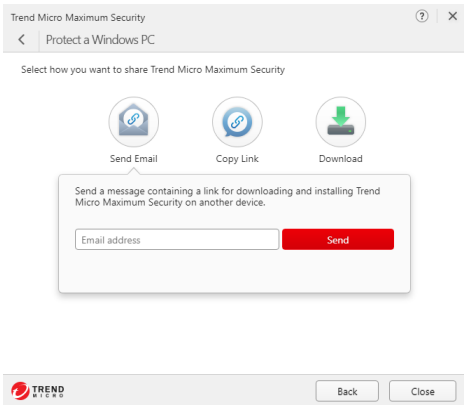

Figure 89. Send Email

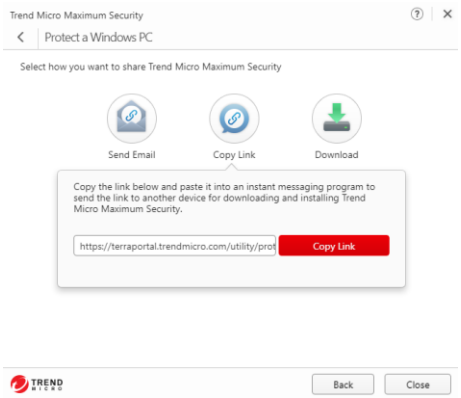

Figure 90. Copy Link

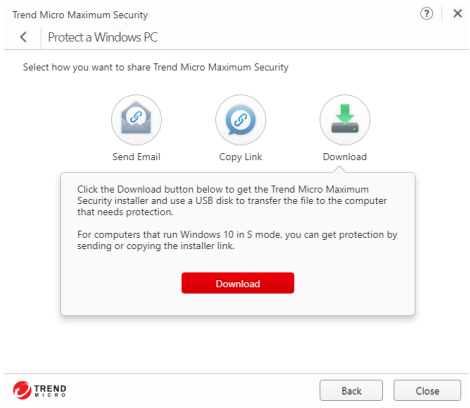

Figure 91. Download

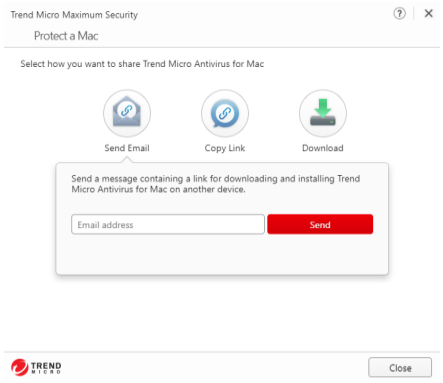

Figure 92. Protect a Mac

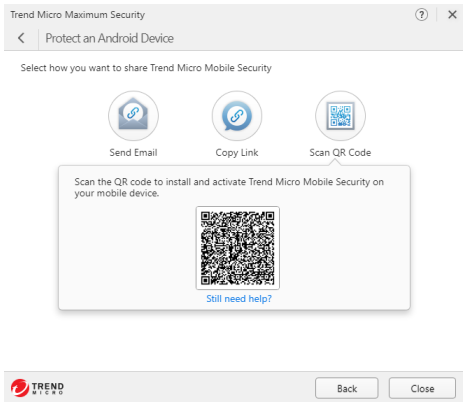

Figure 93. Protect an Android Device

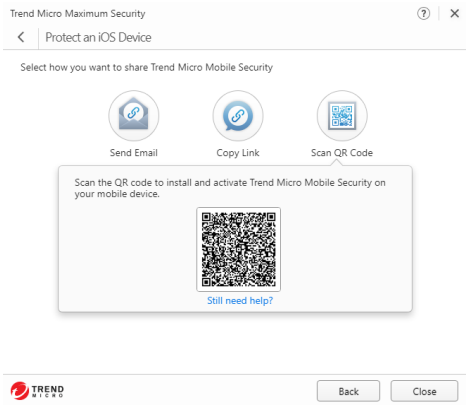

Figure 94. Protect an IOS Device

11. For PC or Mac protection, pick how you want to get the application: Email, Link, or Download. If you download the installer to your active computer, you may use a USB thumb drive to physically take the file to the other computer.
12. For Android or iOS protection, pick how you want to get the app: Email, Link, or QR Code, (for Google Play™, Trend Micro™, Amazon Appstore™, or Apple App Store™).
13. To install, follow the instructions on the page, store, or email.

Chapter 3: Trend Micro Security Overview

In the following chapters, we'll walk through each edition of Trend Micro Security, explaining the key features provided in each. In this chapter, we'll give you a quick overview of some easy-to-use functions.

Note: **Since each more advanced edition of Trend Micro Security includes the features of the simpler edition, but adds more features, you should read all chapters in this guide *front to back* to fully understand how to use the complete set of features in Trend Micro Internet and Maximum Security.**

Quick Start: The Trend Micro Security Console

All editions of Trend Micro Security provide essentially the same **Console**, with additional features as you step up from **Trend Micro Antivirus+** to **Internet Security** and **Maximum Security.**

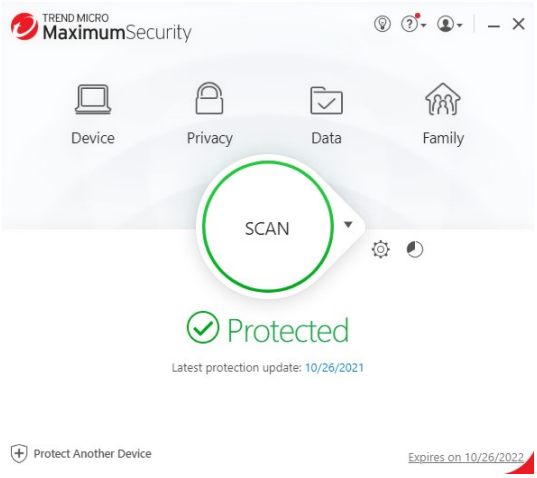

Figure 95. Trend Micro Maximum Security Console

All editions of Trend Micro Security allow you to scan on-demand using **Quick, Full,** or **Custom** scans, and each lets you view security reports. We'll quickly review these features in the following sections.

Quick Start: Conducting On-Demand Scans

By default, Trend Micro Security activates a **real-time scan** when it is installed. This is always present in memory, to proactively protect you from real-time threats. Threats are caught as they try to enter memory or touch the hard drive, preventing infections. This includes protection against ransomware, which may infect you from dangerous websites or emails.

Trend Micro Security also provides a **disk scan**—which you can execute on-demand or by schedule—that utilizes Trend Micro Smart Scan technology on the client when it scans your

hard drive. This references Trend Micro's file reputation services in the cloud—part of the Smart Protection Network—for a shorter "time-to-protect."

Unlike other local-protection-based products that require you to frequently update a large local signature database on your computer, Trend Micro Security updates the signature database mainly on Trend Micro Servers in the cloud, so all consumers of the Smart Protection Network are instantly protected whenever the online database is updated. Other cloud-based and local Trend Micro technologies correlate threat data of different kinds, since modern threats can simultaneously use multiple techniques to infect your computer.

Smart Scan reduces network bandwidth usage (for updating/downloading signatures), while saving disk space and memory.

Scan Your Computer's Disk

Scanning is a simple process to execute, though users are recommended to initiate a manual scan when they are not doing other tasks.

To scan your computer disk:

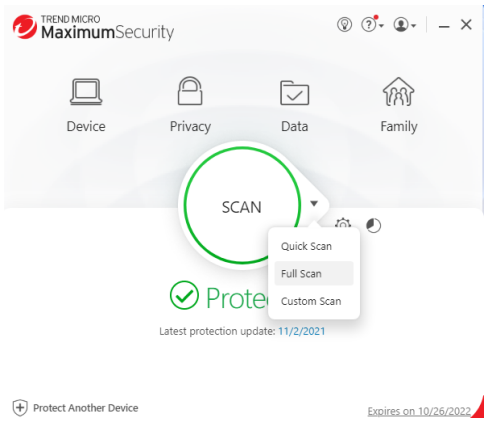

Figure 96. Quick | Full | Custom Scan Menu

Trend Micro Security provides a **Scan** Tool on the console (shown above) which can be used in two ways:

1. Click the center of the circular **Scan** tool to execute a **Quick Scan**.
2. Use the **Scan Options** popup menu on the right side of the **Scan** tool to select among the various options:
   - A **Quick Scan** conducts a scan of those directories on your system that are most likely to be infected.
   - A **Full Scan** conducts a full scan of your system.
   - A **Custom Scan** lets you designate which parts of your system you wish to scan.

Quick Scan and Full Scan

To conduct a Quick Scan or a Full Scan:

1. To conduct a **Quick Scan**, click the **Scan** button on the main console, or optionally select **Quick Scan** or **Full Scan** from the **Scan Options** popup menu. A window appears, showing the **Quick** or **Full Scan in Progress** and the percentage completed. Scans can kick off messages when malware is quarantined or deleted.

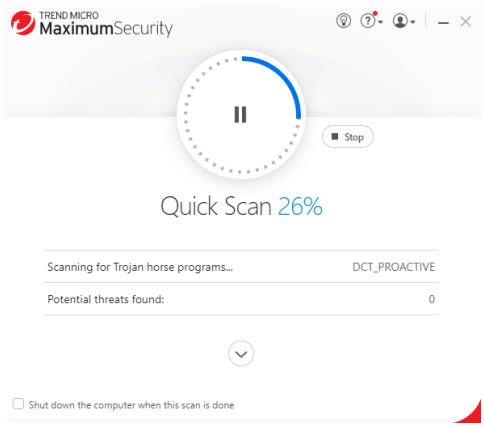

Figure 97. Quick Scan in Progress

2. You may stop the scan by clicking the **Stop** button. You may also select **Shut down the computer when this scan is done.**

3. When the scan has completed, a **Scan Results** screen appears, showing **File Scanned**, as well as **Threats resolved.**

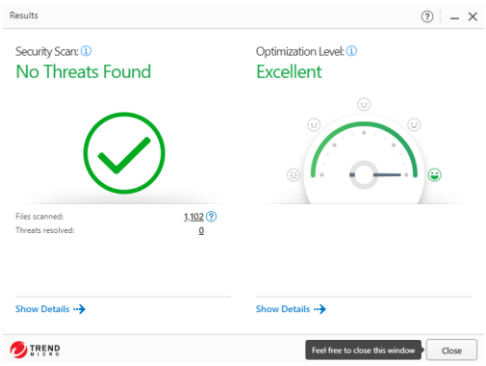

Figure 98. Scan Results

4. Click **?** near the number of **Files scanned** to obtain more details on the files scanned.

5. Click **Show Details** for more details on the threats found and actions taken. The **Details** screen appears.

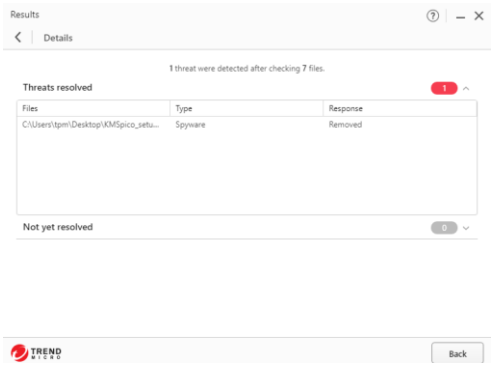

Figure 99. Details

6. Click each of the collapsible panels in turn to show the **Details** tables, which include file names, types, and responses to the threats.

7. Click **Back** to close the **Details** window, then **Close** to close the **Scan Results** window.

Custom Scan

To conduct a Custom Scan:

1. Choose **Custom Scan** from the **Scan Options** popup menu. A dialog appears, letting you **Select Targets** you wish to scan.

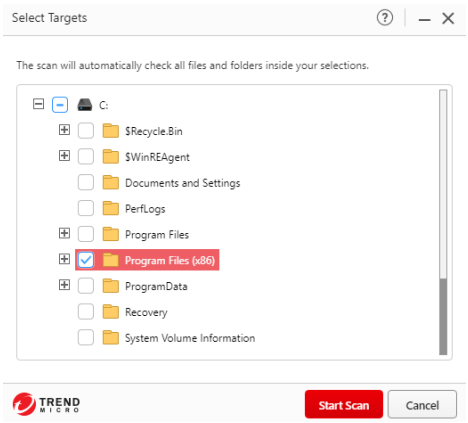

Figure 100. Select Targets

2. Expand any tree by clicking the **+ (Plus)** signs, then check the checkbox for the chosen target(s).

3. Click **Start Scan** to start the scan.

4. When the scan has completed, the **Scan Results** and **Details** screens appear in the same format as **Quick** and **Full Scans.**

Intensive Scan

Trend Micro Security automatically performs an **Intensive Scan** whenever a **Quick, Full, Custom, Scheduled Scan,** or **"Smart Schedule"** scan detects a high amount of malware on your computer.

Note: **In the *real world,* Trend Micro Security does not allow a large virus data set to get onto your computer. To obtain this condition artificially, you have to dump a large collection of malware files onto an unprotected system *before you install Trend Micro Security;* or you would have to turn off all the proactive features, such as the real-time scan, which would prevent such a large infection from occurring in the first place.**

To activate an Intensive Scan on a previously badly infected computer:

1. Click the **Scan > Quick Scan** tool to begin a **Quick Scan**. The **Quick Scan** process begins.

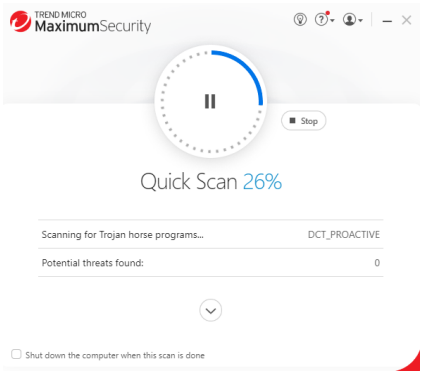

Figure 101. Quick Scan in Progress (TM Maximum Security)

2. When the scan detects a large volume of malware, the **Quick Scan** stops and an **Intensive Scan** starts.

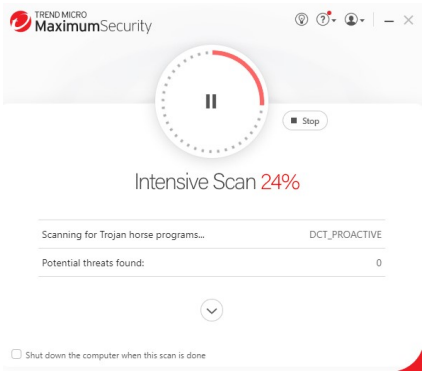

Figure 102. Intensive Scan in Progress

3. Note that the scan wheel color changes to **red** to indicate that an **Intensive Scan** is in progress. You can get more information about what triggered the scan by clicking **What triggered the Intensive Scan?**

Quick Start: Viewing Security Reports

Trend Micro Security allows you to view **Security Reports** at the click of a button. The reports provide a wealth of detail on the dates and types of threats blocked. You can also generate a **Root Cause Analysis Report** to investigate the source of an infection and the effects upon your system.

Note: **All versions of Trend Micro Security produce a security report that tells you how many and what kinds of viruses, spyware, and web threats it detected during real-time and on-demand scans. Higher editions than Antivirus+ provide more information in their Security Reports.**

To View a Security Report:

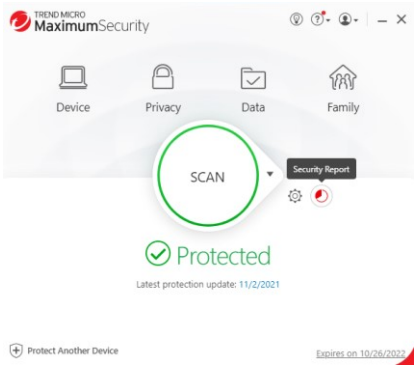

Figure 103. Security Report

1. Click the **Security Report** button on the **Trend Micro Security Console**. The **Security Report** screen appears. (Note that if you've created a password to secure your settings, you'll be asked to enter this password before the **Security Report** is displayed.)

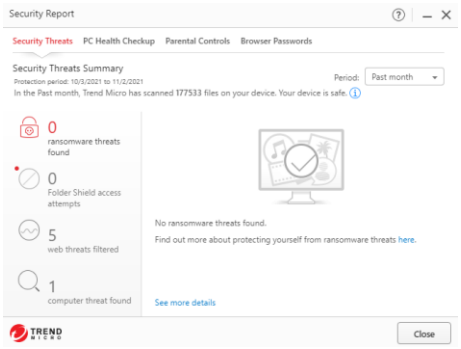

Figure 104. Security Report (Maximum Security)

2. The **Security Report** provides the following data:

   - **Security Threats** – The number of web threats, viruses, spyware, ransomware, and suspicious software found. (All editions)

- **PC Health Checkup** – Shows the space and startup time saved and the privacy data safety confirmed, and includes a check for potentially incompatible programs. (Internet Security and higher)
- **Parental Controls** – Shows a summary of the top websites blocked. (Internet Security and higher)
- **Browser Passwords** – The number of passwords saved in browsers (a privacy risk). (Maximum Security)

3. Use the **Period** popup menu in the upper right-hand corner to designate the period the report will cover.
4. Select **See more details about your protection** from any of the four main screens to obtain logs pertaining to that type of protection.

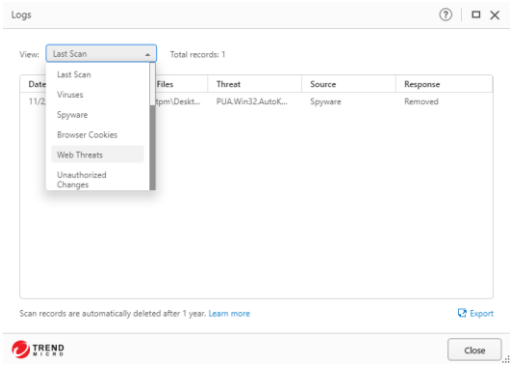

Figure 105. Logs

5. Double-click an item in the table to view details on the specific threat.

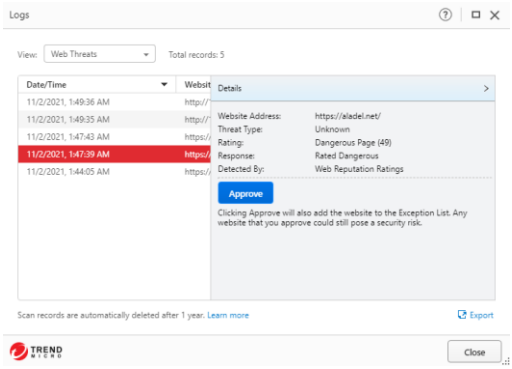

Figure 106. Logs > Item Details

6. Click **Approve** to add items to the **Exception List.**
7. Click **Export** in the lower right-hand corner to export the logs in .CSV or .TXT format.
8. When an item in a log warrants a deeper look, Trend Micro Security will provide a link to show more details on the source of the infection.

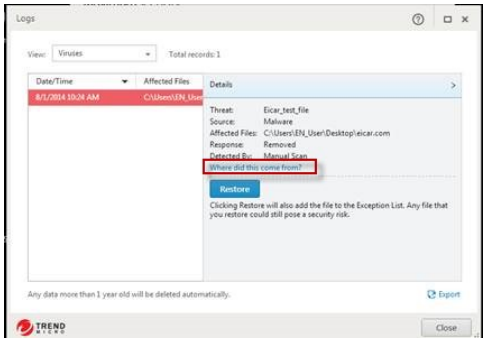

Figure 107. Where did this come from?

9. Click **Where did this come from?** to generate a **Root Cause Analysis Report.** When the report generates, it displays in graphic format.

Figure 108. Root Cause Analysis Report

10. The **Root Cause Analysis Report** maps the root cause and triggering event(s) graphically, using **Process, Website, File, Library,** and **Group** icons to show you items involved in the infection chain. Use the **Root Cause Analysis Report** to analyze the source of infections, so you can help prevent them in the future.

Chapter 4: Trend Micro Antivirus+ Security

This chapter provides detailed instructions for configuring and using Trend Micro Antivirus+ Security.

Protection Overview

Trend Micro™ Antivirus+ Security provides essential protection for customers against viruses, spyware, web threats, and other malware threats, including bad links on social networking sites and ransomware.

Figure 109. Trend Micro Antivirus+ Security Welcome Page

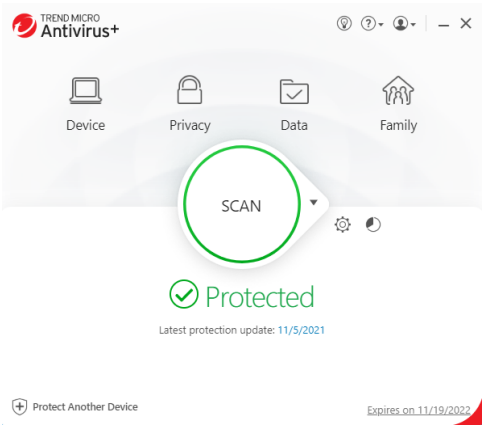

Figure 110. Trend Micro Antivirus+ Security Console

Note: **Trend Micro Antivirus+ Security Console Main Features:**

Device: Security Settings | Mute Mode | Protect Another Device

Privacy: Social Networking Protection | Pay Guard

Data: Folder Shield

Family: Keep Your Family Safe Online - Upgrade Now

KEY MALWARE PROTECTIONS FOR TREND MICRO ANTIVIRUS+ SECURITY

Antivirus and Antispyware

Trend Micro Antivirus+ Security provides essential protection against viruses; that is, any malicious program that can replicate itself and infect your computer. Antivirus+ also protects you from a broad range of other malware, including worms, Trojans, bots, and rootkits. It also provides protection from spyware; that is, any program that installs itself in the background and gathers information about you or your computer without your knowledge. Since browser cookies can act like spyware, Antivirus+ will delete cookies as well.

Windows Firewall Booster and Wi-Fi Protection

The Windows Firewall Booster provides additional network-level protections, including a Network Virus Scan and Anti-Botnet feature. The Firewall Booster is automatically activated for increased network security. Antivirus+ also provides authentication for Wi-Fi networks, displaying a warning when connected to potentially unsafe wireless networks or hotspots.

Anti-Spam

Antivirus+ includes anti-spam in its list of features. Users of POP3 e-mail can be protected from spammers, stopping unsolicited advertisements and other unwanted bulk email. Trend Micro Security's anti-spam function taps into the email reputation services of the Smart Protection Network. Trend Micro Security Antivirus+ also protects you from threats in files attached to email messages.

New! Email Defender also provides anti-spam and WTP protection for Gmail and Outlook webmail.

Unauthorized Change Prevention

Trend Micro Security includes behavior monitoring in its list of security protections. Unauthorized changes to system settings and other suspicious behavior can be blocked, as well as autorun programs on portable drives. Antivirus+ includes the ability to switch your protection level automatically, to aggressively eliminate programs that pose even a small risk of bad behavior. And the increased protection against ransomware that Folder Shield provides helps protect your computer and files from encryption or blocked access and the extortion that comes with ransomware. All editions of Trend Micro Security provide ransomware protection and Folder Shield.

Web Threat Protection

The majority of threats nowadays come from the web, when you're simply browsing the Internet or visiting a site. However, attacks may also begin with a phishing email that uses social engineering techniques to coax you to click a URL link in the email. You then may be

taken to a website that secretly harbors malicious threats, which either steals your personal data or infects you with malware.

Antivirus+ proactively protects you from a variety of these web threats, so that they never touch your computer. To provide thorough protection from and rapid response times to emerging threats, Antivirus+ uses the Trend Micro Smart Protection Network cloud-client security infrastructure along with a combination of cloud-based web, file, and email reputation services. It also employs real-time scans of what's in memory and on disks. Antivirus+ also blocks malicious links and image spam in emails, including Google and Outlook webmail with Email Defender.

Privacy

Social Networking Protection in Trend Micro Antivirus+ Security is also enabled by the Web Threat Protection function. See risk ratings for Facebook, Twitter, LinkedIn, MySpace, Pinterest, Mixi, and Sina Weibo. Mouse over URLs to get further details on the website. In Facebook, warn your friends of bad URLs on their pages, so they can delete them.

Pay Guard protects your financial transactions when you're banking or shopping online using your default browser.

Device: Security Settings: Security & Tuneup Controls: Scan Preferences

Upon install, Trend Micro Antivirus+ Security chooses a group of default settings to immediately protect the user. However, users can modify settings as they wish. Antivirus+ Security keeps its controls simple and suitable for the everyday user.

To modify Security & Tuneup Controls settings:

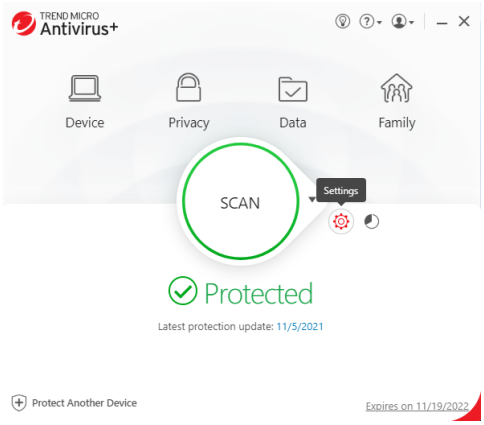

Figure 111. Console > Settings Tool

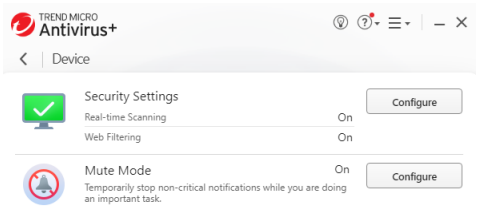

Figure 112. Device > Configure

1. Click the **Settings** tool in the **Console**; or click the **Device** button, then **Configure** in the **Security Settings** panel. The **Protection Settings** screen appears, with **Security & Tuneup Controls > Scan Preferences** selected by default in the **Command Menu**.

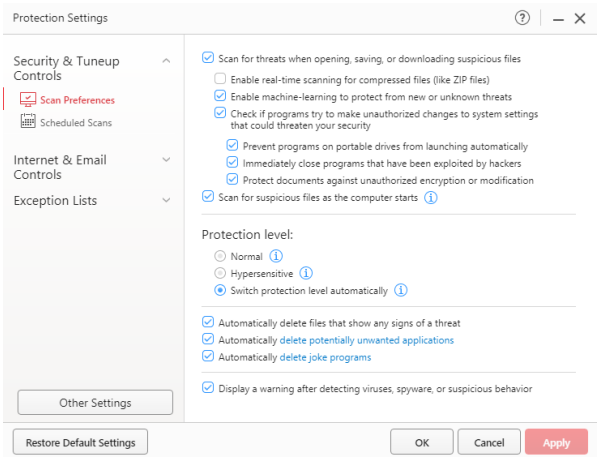

Figure 113. Scan Preferences

2. The following **Scan Preferences** are displayed. Check or uncheck to change a setting.

- **Scan for threats when opening, saving, or downloading suspicious files.** This is the real-time scan that protects you at all times when you're using your computer. This is enabled by default.
    - **Enable real-time scanning check compressed files (like ZIP files).** This is disabled by default. Checking the checkbox enables the item, but the deeper scan uses more CPU cycles.
    - **Enable machine-learning to protect from new or unknown threats.** This is enabled by default. New or unknown threats, such as ransomware, will be removed upon detection; or when suspicious software tries to execute, it will be blocked.

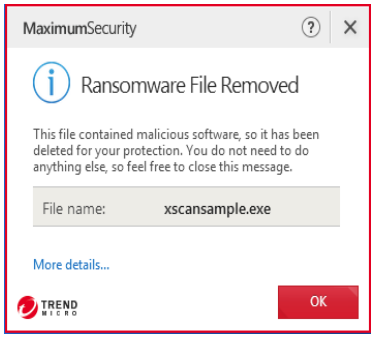

Figure 114. Ransomware File Removed [Maximum example]

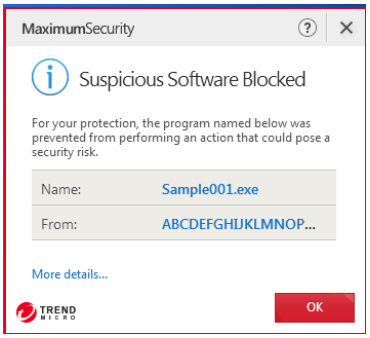

Figure 115. Suspicious Software Blocked from Executing [Maximum example]

- **Check if programs try to make unauthorized changes to system settings that could threaten your security.** This is enabled by default.
  - **Prevent programs on portable drives from launching automatically.** This is enabled by default.
  - **Immediately close programs that have been exploited by hackers.** This is enabled by default.
  - **Protect documents against unauthorized encryption or modification.** This protects against ransomware and is enabled by default.
    - **Back up files encrypted or modified by suspicious programs.** This ransomware protection is enabled by default.

- **Scan for suspicious files as the computer starts.** Key security components begin working even before Microsoft Windows has finished loading—before threats have a chance to attack.
- **Protection Level**. This behavior monitoring function is enabled by default to switch from Normal to Hypersensitive only when needed, but you can change this setting.
  - **Normal -** Detects and stops security threats based on clearly risky behavior.
  - **Hypersensitive -** Aggressively eliminates programs even if they only pose a small risk of bad behavior.
  - **Switch protection level automatically** - Increases the protection level only when you need it. This is the default setting.
- **Automatically delete files that show any signs of a threat**. This is enabled by default, to automatically delete threatening files.
- **Automatically delete potentially unwanted applications.** This is enabled by default.

- **Automatically delete joke programs.** This is enabled by default.
- **Display a warning after detecting viruses, spyware, or suspicious behavior.** This is enabled by default. Trend Micro Security is selective when using pop-ups; it's never overly intrusive.

3. If you wish, click **Restore Default Settings** at any time (in this and any subsequent screens) to restore default settings to their factory condition.
4. Click **Apply** to apply your changes, then **OK** to close the **Protection Settings** window.

Device: Security Settings: Security & Tuneup Controls > Scheduled Scans

To modify Scheduled Scan preferences:

1. Click **Security & Tuneup Controls > Scheduled Scans**. The schedule options panel displays.

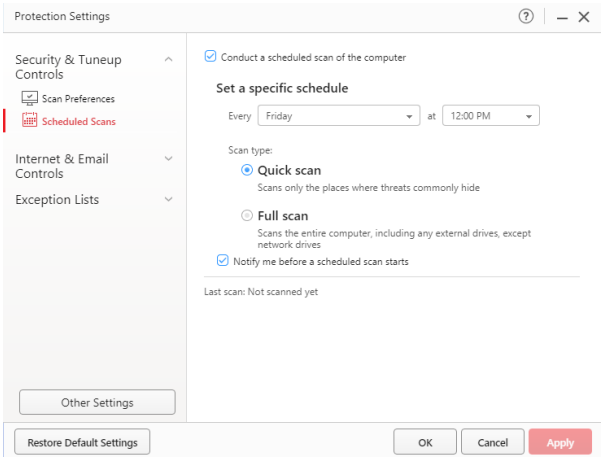

Figure 116. Security & Tuneup Controls > Scheduled Scans

2. Choose among the following options:

- **Conduct a scheduled scan of the computer.** This is enabled by default. "Friday at 12:00 PM" is chosen by default as the day and time to conduct the scheduled scan. Use the popup menus to change the day and time the scheduled scan will be conducted.

TIP: **Scheduled scans are best conducted when the computer is on but not in use, as they take up a portion of Memory, CPU, and Disk processes.**

- **Scan Type. Quick Scan** is selected by default.
  - Select **Quick Scan** to scan only the places where threats commonly hide.
  - Select **Full Scan** to scan the entire computer, including any external drives, except network drives.

- Notify me before a schedule scan starts. Selected by default.

3. Click **Apply** to apply any changes, then **OK** to close the **Protection Settings** window.

Device: Security Settings: Internet & Email Controls > Web Threats

To modify the Internet & Email Controls > Web Threats settings:

1. Click **Internet & Email Controls.** The **Web Threats** panel appears by default.

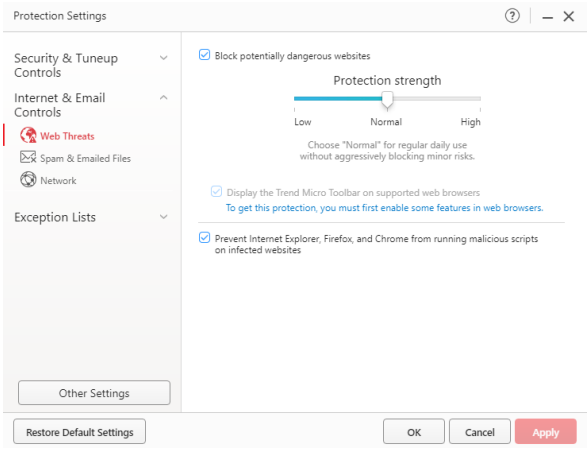

Figure 117. Internet & Email Controls > Web Threats

2. **Block potentially dangerous websites** is checked by default.
3. For **Protection strength**, use the slider to select the strength. More aggressive blocking blocks more websites, some of which you may not wish to be blocked.
   - **Low** - Choose “Low” to block only websites confirmed as fraudulent or dangerous.
   - **Normal** - Choose “Normal for regular daily use without aggressively blocking minor risks. This is the default setting.
   - **High** - Choose “High” to block threats in sites that show *any* signs of fraud or malicious software.
4. **Display the Trend Micro Toolbar on supported web browsers.** This enables Antivirus+ to rate links on webpages or mouseovers for malicious URLs and their accompanying payload for Internet Explorer, Mozilla Firefox, and Google Chrome. This is enabled by default.

Note: **To get this protection you must first enable some features in web browsers. See Enable Trend Micro Toolbar in Chapter 2 for details.**

5. **Prevent Internet Explorer, Firefox, and Chrome from running malicious scripts on infected websites.** This is enabled by default.
6. Click **Apply** to apply your changes, then **OK** to close the **Web Threats** window.

Device: Security Settings: Internet & Email Controls > Spam & Emailed Files

You can block spam from your Microsoft Outlook email client.

Note: **Email Defender also blocks spam and phishing emails with dangerous files and links in Gmail and Outlook webmail. See Antispam: Enable Email Defender for Gmail and Outlook Webmail following for details.**

To modify the Internet & Email Controls > Spam & Emailed Files setting:

1. Click **Internet & Email Controls > Spam & Emailed Files** to open the panel. The panel opens with the settings unchecked by default.

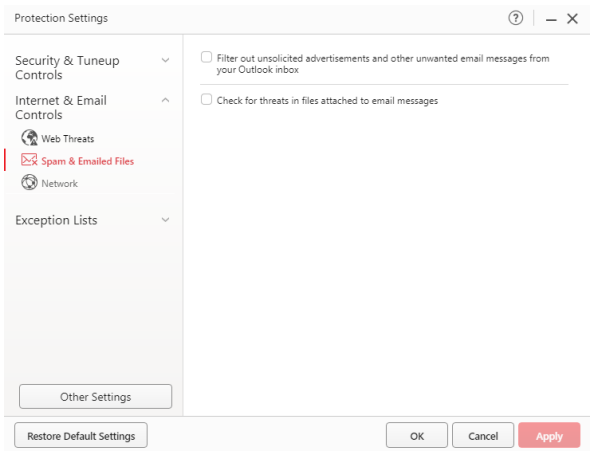

Figure 118. Internet & Email Controls > Spam & Emailed Files

- **Filter out unsolicited advertisements and other unwanted email messages from your Outlook inbox.** Check this if you wish to stop spam and other unsought messages.
- **Check for threats in files attached to email messages**. Check this to scan all email messages for malicious attachments and remove them.

2. Click **Apply** to apply any changes, then **OK** to close the **Protection Settings** window.
3. Trend Micro Anti-Spam (TMAS) support per OS Platform and Outlook version is given in the table below. Apart from Outlook 2003, the Data Theft Prevention feature also applies to these platforms and versions of Outlook.

Table 8. TMAS OS Platform and Mail Client Support

OS Platform	Mail Client
Windows 7, 8.1, 10, 11 (32 and 64 bit)	**Outlook 2003 (32bit), 2007 (32bit), 2010 (32bit, 64bit), 2013 (32bit, 64bit), 2016 (32bit, 64bit)**

To modify the Antispam Settings in the Microsoft Outlook Application:

Once you've enabled the Antispam features for Outlook, you can modify the settings to your liking.

1. In the Microsoft Outlook application, select **Add Ins** in the **Main Outlook Toolbar.** The **Add-ins** panel appears.

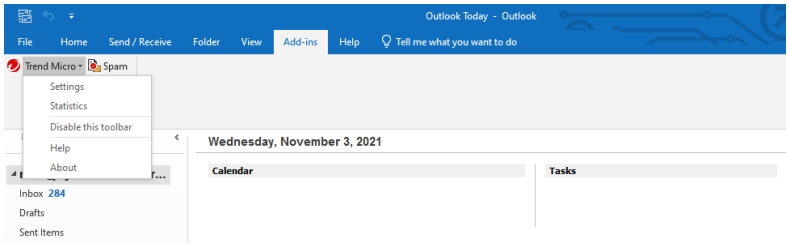

Figure 119. Trend Micro Antispam Toolbar

2. To mark an email as spam and add it to the **Spam** folder in Outlook, select the email in your email list, then click the **Spam** button.
3. See **Settings** below to set your settings.
4. Select **Statistics** to view statistics about the number of messages processed, spam messages deleted, spam messages you reported, and legitimate messages misidentified as spam.
5. You can also **Reset** the **Statistics** window to Zero by clicking **Reset**.

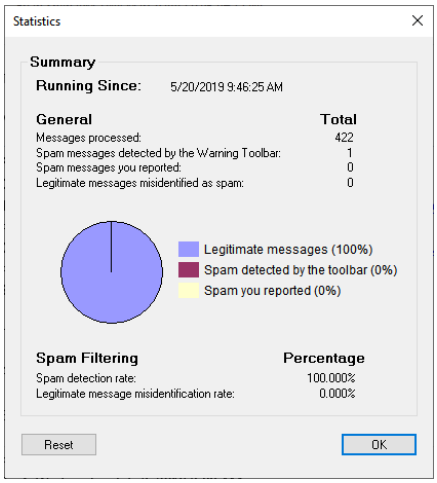

Figure 120. Spam Statistics

6. Select **Disable this toolbar** to disable it.
7. Select **Help** to get help using the **Antispam Toolbar.**
8. Select **About** to view the toolbar version.

9. Select **Settings** to configure the settings for the **Antispam Toolbar**. The **Settings** dialog box appears, with the **Spam Filter** tab selected by default.

Spam Filter

Spam Email Filter Strength is set to **Medium** filtering by default.

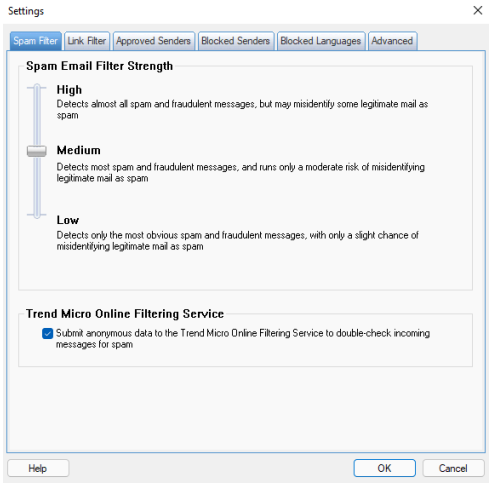

Figure 121. Spam Filter

1. Choose the **Spam Email Filter Strength** you want:
   - **High**. Detects almost all spam and fraudulent messages but may misidentify some legitimate email as spam.
   - **Medium**. Detects most spam and fraudulent messages and runs only a moderate risk of misidentifying legitimate email as spam.
   - **Low**. Detects only the most obvious spam and fraudulent messages, with only a slight chance of identifying legitimate email as spam.
2. **Trend Micro Online Filtering Service.** Submit anonymous data to the Trend Micro Online Filtering Service to double-check incoming messages for spam.
3. Click **OK** to save any changes.

Link Filter

1. Click the **Link Filter** tab to edit the setting. The **Link Filter** screen appears.

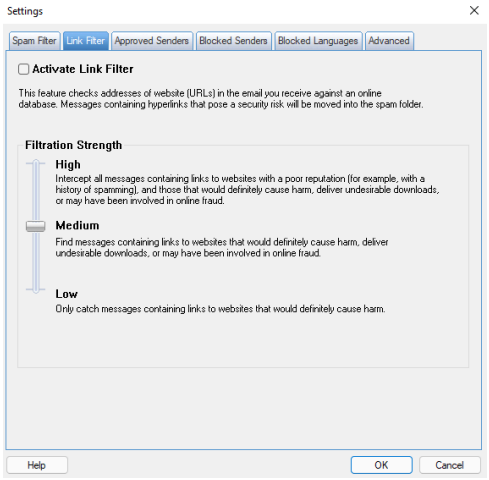

Figure 122. Link Filter

2. **Activate Link Filter.** This is turned off by default. Check this checkbox to activate the link filter. This filter checks addresses of website URLS in the email you receive against an online database. Messages containing hyperlinks that pose a security risk will be moved into the spam folder
3. **Filter Strength.** Choose the Filter Strength you want:
   - **High.** Intercept all messages containing links to any site with a poor reputation (such as a history of spamming, and all those that would definitely cause harm, deliver undesirable downloads, or seem associated with online fraud.
   - **Medium.** Find messages containing links to websites that would definitely cause harm, deliver undesirable downloads, or seem associated with online fraud.
   - **Low.** Only catch messages containing links to websites that would definitely cause harm.
4. Click **OK** to save any changes.

Approved Senders

1. Click the **Approved Senders** tab to add approved senders. The **Approved Senders** screen appears.

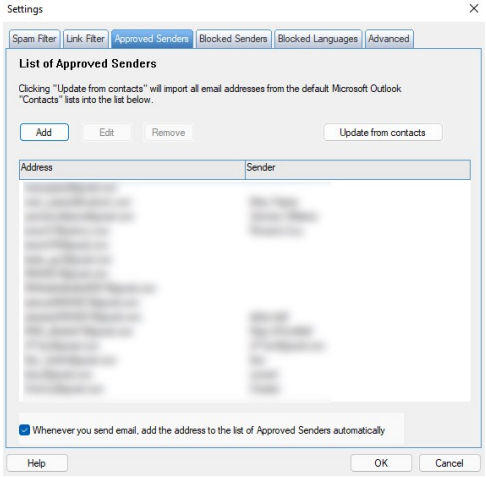

Figure 123. Approved Senders

2. **Update from Contacts**. Clicking “Update from contacts” will import all email addresses from the default Microsoft Outlook “Contacts” list into the list in the window.

3. **Add**. Click **Add** to add individual contacts. The **Add approved senders** dialog box appears.

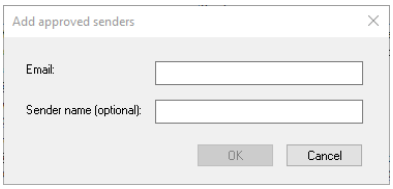

Figure 124. Add Approved Senders

4. Type in the email address of the person you wish to add to the list of **Approved Senders**.

5. Type in the sender’s name (optional).

6. Click **OK** in the dialog box to save the email address/contact in the list of **Approved Senders**.

7. Select an email address and click **Edit** to edit an email entry. A dialog appears to let you edit the entry; click **OK** to save your changes or **Cancel** to cancel the edit.

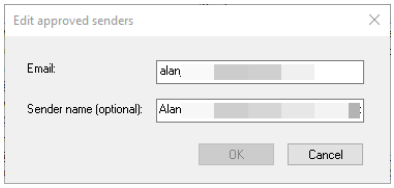

Figure 125. Edit Approved Senders

8. Select an email address and click **Remove** to remove an email entry. A dialog appears to let you remove the entry; click **OK** to remove it or **Cancel** to retain it.

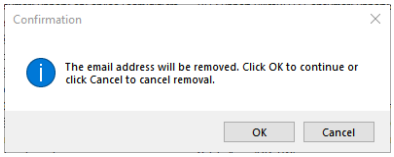

Figure 126. Confirm Removal

9. Check/uncheck the checkbox **Whenever you send email, add the address to the list of Approved Senders automatically.**
10. Click **OK** in the **Approved Senders** window to save your changes.

Blocked Senders

1. Click the **Blocked Senders** tab to add **Blocked Senders** to the list. The **Blocked Senders** screen appears.

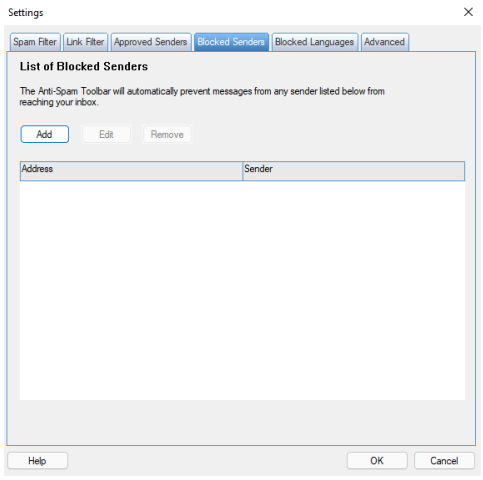

Figure 127. Blocked Senders

2. **Add, Edit,** or **Remove Blocked Senders** to the list in the same way you did for **Approved Senders.**
3. Click **OK** to save your changes.

Blocked Languages

1. Click the **Blocked Languages** tab to edit the settings. The Blocked Languages screen appears.

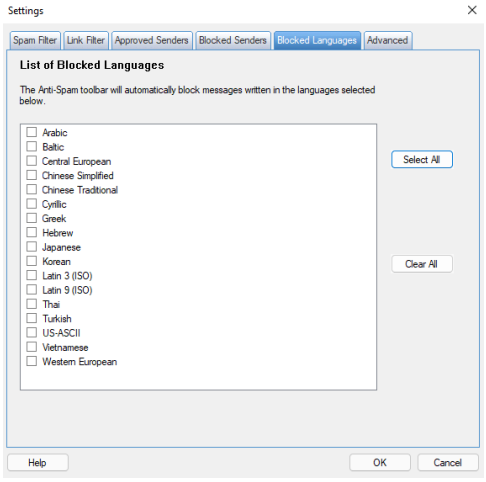

Figure 128. Blocked Languages

2. Individually check the languages you wish to block or **Select All** or **Clear All**.
3. Click **Ok** to save your changes.

Advanced

1. Select the **Advanced** tab to open the **Advanced** screen.

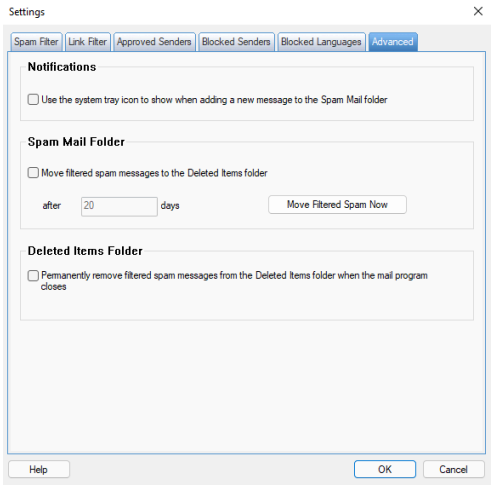

Figure 129. Advanced

- **Notifications**. Check this checkbox to use the system tray icon to show when adding a new message to the **Spam Mail** folder.

- **Spam Mail Folder.** Check this checkbox to move filtered spam messages to the **Deleted Items** folder. Options include:
    a. **Move after XX days.** Add the number of days you wish to hold messages before they're moved to the **Deleted Items** folder.
    b. **Move Filter Spam Now.** Click this button to move all **Filtered Spam Now** to the **Deleted Items** folder now.
- **Deleted Items Folder.** Check this checkbox to permanently remove filtered spam messages from the Deleted Items folder when the mail program closes.

2. Click **OK** to save your changes.

Device: Security Settings: Internet & Email Controls: Network > Firewall Booster | Wi-Fi Protection

To modify the Wi-Fi Protection Settings:

1. Click the **Settings** tool in the **Console**. The **Protection Settings** screen appears, with **Security & Tuneup Controls > Scan Preferences** selected by default.
2. Click **Internet & Email Controls > Network** in the **Command** menu. The **Network** screen appears.

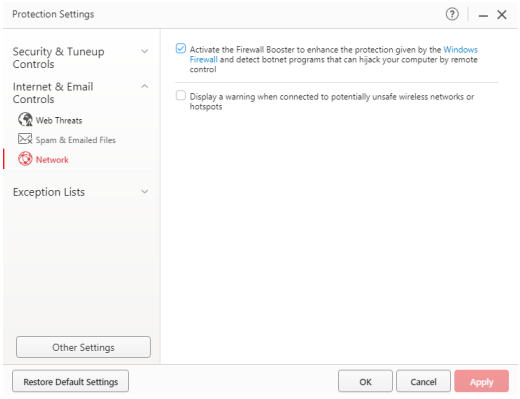

Figure 130. Internet & Email Controls > Network

3. **Activate the Firewall Booster** is checked by default. This enhances the protection given by the Windows Firewall and detects botnet programs that can hijack your computer by remote control.
4. **Display a warning when connected to potentially unsafe wireless networks or hotspots**. This is disabled by default. Check this to enable the feature.
5. Click **OK** to save your changes.

Note: **The Exception List for Wi-Fi Protection allows users to add unprotected home networks to an exception list, so that users are not subject to frequent warnings for networks they know to be safe. See the Exception Lists section below for more details.**

Exception Lists: Programs/Folders

To add items to Exception Lists Programs/Folders:

Trend Micro Security lets you add programs, folders, or websites to exception lists so that scans will ignore them. Adding programs or folders to exception lists can increase performance during scans, while adding frequently-accessed websites can prevent unwanted blockage. Users are advised to use exception lists wisely, as it may open computers up to more threats.

1. To add items to exception lists, click **Exception Lists**. **Programs/folders** appears by default.

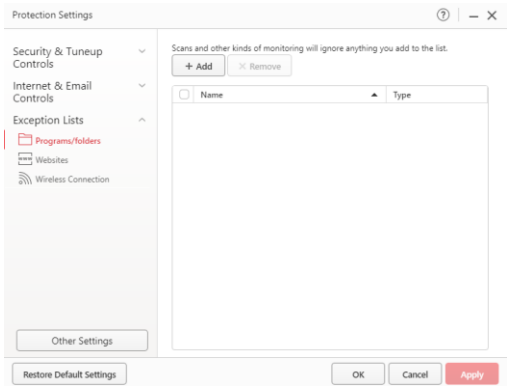

Figure 131. Exception Lists > Programs/folders

2. Click **+Add** to add a program or folder to the exception list. A dialog appears, letting you **Add an Item.**

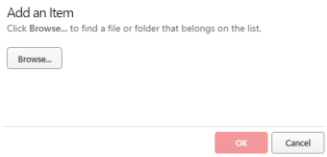

Figure 132. Add an Item

3. To select the file or folder you wish to add, click **Browse**. An **Open** dialog appears.

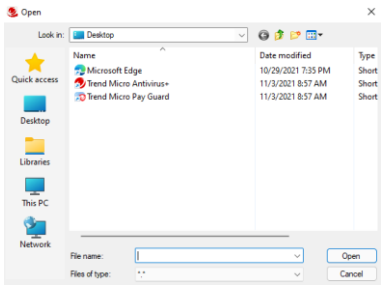

Figure 133. Open Dialog

4. Select the item you wish to add, then click **Open**. This adds the item to the **Add an Item** dialog.

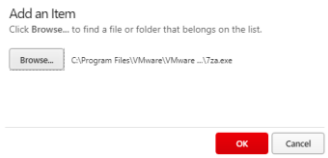

Figure 134. Add an Item (item added)

5. Click **OK** in the **Add an Item** dialog. The item is added to the exception list.

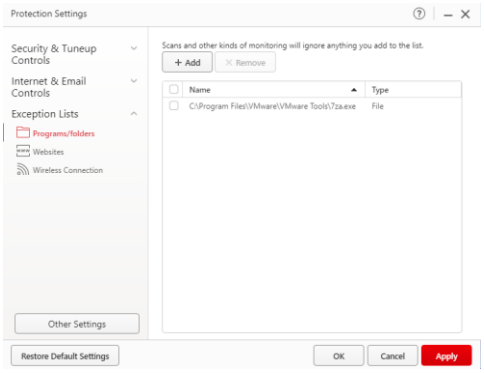

Figure 135. Item Added to Exception List

6. To remove an item, check it, and then click the **X Remove** button.
7. Click **Apply** to save any changes, then **OK** to close the Trend Micro Security Console.

Exception Lists: Websites

To add websites to an exception list:

1. In a similar way, to add or remove a website from its exception list, click **Exception Lists** > **Websites** in the **Command Menu**. The **Websites** exception list appears.

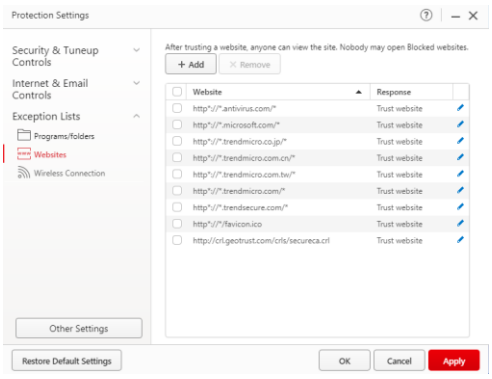

Figure 136. Exception Lists > Websites

2. Click **Add** to add a website. A dialog appears, letting you **Add** or **Edit an Item.**

3. Choose among the following options:

   a. Type in the URL you wish to add in the edit field.

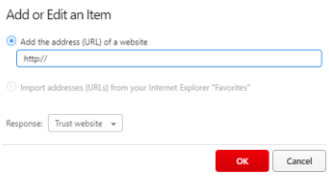

Figure 137. Add or Edit an Item

   b. Choose **Block** or **Trust** from the **Response** pop-up (for either option).

   c. Click **OK** to save the option.

4. Click **Apply** to save your changes, then **OK** again to close the Trend Micro Security Console.

Exception Lists: Wireless Connection

Trend Micro Security allows you to add access points to the **Wireless Connections Exception List** that Trend Micro Security may consider risky or dangerous. Wi-Fi hotspots added to the list are considered trusted access points.

To add and remove a Wireless connection to the Exception List:

1. When you attempt to log onto an access point, Trend Micro Security may give you a pop-up warning that the network connection is risky or dangerous.

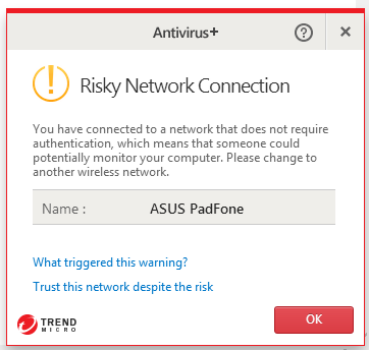

Figure 138. Risky Network Connection

2. If you know this access point probably isn't risky, you may wish to add this network to the Wireless Connections Exception List. To do so, simply click **Trust this network despite the risk** and the site will be added to the list.

3. Later, you may wish to delete this from the Exception List. To do so, click the **Settings** tool to open the **Protection Settings** screen. The **Virus & Spyware Controls** screen opens by default.

4. Click **Exception Lists > Wireless connection** in the Command menu. The **Exception** List for **Wireless Connection** appears.

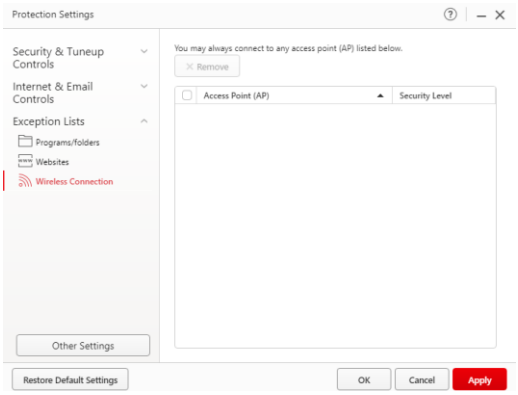

Figure 139. Exception Lists > Wireless Connection

5. Select the access point in the list and click **Remove**. Trend Micro Security deletes it from the list.

6. Click **Apply** to save your changes.

Other Settings: System Startup

By default, Trend Micro Security chooses the optimal settings when starting your computer. You can change these settings.

To modify Other Settings > System Startup:

1. Click **Other Settings** in the Command Menu. The **System Startup** screen appears by default, with **Balanced Protection (Recommended)** chosen by default.

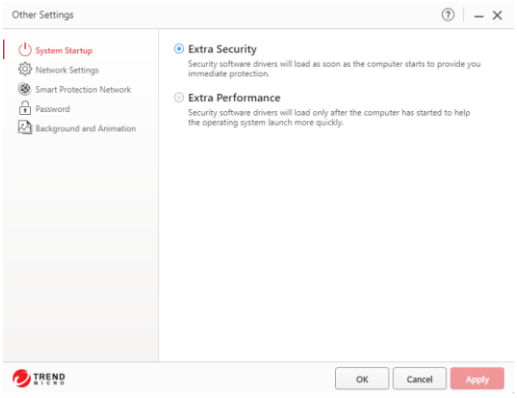

Figure 140. Other Settings > System Startup

2. Select between the following options:

   - **Extra Security** – This is the default option. Security software drivers will load as soon as the computer starts, which makes the operating system launch more slowly.

- **Extra Performance** – Security software drivers will load only after the computer has started to help the operating system launch more quickly.

3. Click **Apply** to save your changes, then **OK** to close the **Protection Settings** window.
4. Restart the computer to apply the changes to your system.

Other Settings: Network Settings

To modify Other Settings > Network Settings:

1. Click **Other Settings > Network Settings** in the Command Menu. **Network Settings** appears, with **Use a proxy server to connect to the Internet** and **Use the proxy settings saved on your computer** chosen by default.

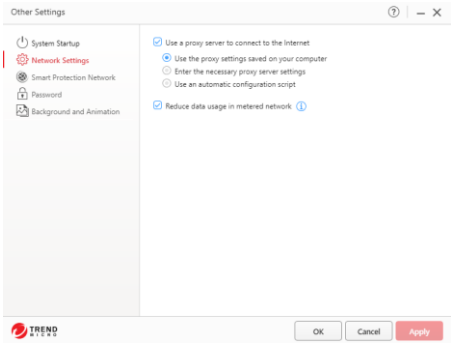

Figure 141. Other Settings > Proxy Settings

2. **Reduce data usage in metered network** is also selected by default. The frequency of maintenance software updates will be less than on a non-metered network.
3. Select **Enter the necessary proxy server settings** to manually enter a proxy server's name, port, and credentials (if required).

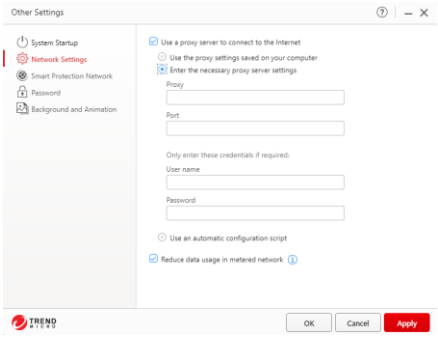

Figure 142. Other Settings > Proxy Settings > Enter Settings

4. Or select **Use an automatic configuration script** and enter the script in the **Address** field provided.

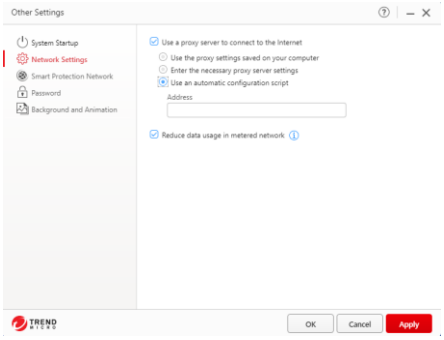

Figure 143. Other Settings > Automatic Configuration Script

5. Click **Apply** to save your changes, then **OK** to close the **Protection Settings** window.

Other Settings: Smart Protection Network

Trend Micro Security can provide feedback to the Smart Protection Network (SPN), to automatically correlate and analyze information about threats found on your computer (and millions of others), for better protection. By opting into the SPN feedback process, you improve yours and others' threat protection, since threats sent from your computer are immediately added to the threat analysis/detection/prevention process, but the choice is yours to opt in or out. You can also opt into sharing computer performance information with Trend Micro, to help yours and others' computers work better.

To share/not share feedback with the Smart Protection Network:

1. Select **Other Settings > Smart Protection Network** from the **Command Menu.** The threat information feedback panel appears.

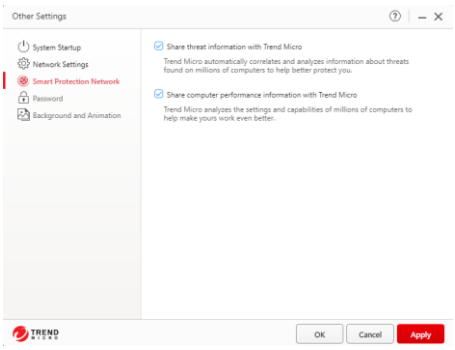

Figure 144. Other Settings > Smart Protection Network

2. Check/Uncheck **Share threat information with Trend Micro** to opt in or out of the feedback process. (This will be checked or unchecked depending upon the choice you made to participate or not participate when you installed Trend Micro Security.)

3. Check/Uncheck **Share computer performance information with Trend Micro.** Trend Micro analyzes the settings and capabilities of millions of computers to help yours work even better. No personal information is gathered or shared.
4. Click **Apply** to save your changes, then **OK** to close the **Protection Settings** window.

Other Settings: Password

To add or change your password:

Trend Micro Security allows you to add a password to protect your overall program settings, so only those who know the password can make changes. For Trend Micro Security Internet Security (TIS) and Maximum Security (MS), the password enables other functions, such as **Parental Controls** in IS and MS and **Trend Micro Vault** in MS. See the two following chapters for details.

1. Select **Other Settings > Password** from the Command Menu. The **Password** screen appears.

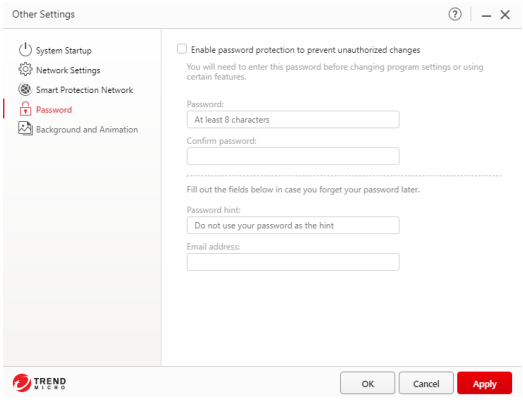

Figure 145. Other Settings > Password

2. Check **Enable password protection to prevent unauthorized changes**.
3. Enter your email address, a password, and the password again to confirm it. Trend Micro Security gives you feedback on your password strength.
4. Fill out the **Password Hint** and **Email Address** fields in case you forget your password later.
5. Click **Apply** to save the password changes, then **OK** to close the **Protection Setting** window.

Other Settings: Background and Animation

Trend Micro Security allows you to change the background picture and animation effects on the **Trend Micro Security Console.** You can use backgrounds provided by Trend Micro or customize the background using your own pictures. You can also show animation effects on the main Console.

To change your Trend Micro Security interface:

1. In **Other Settings**, select the **Background and Animation** menu item. The **Background Editor** appears.

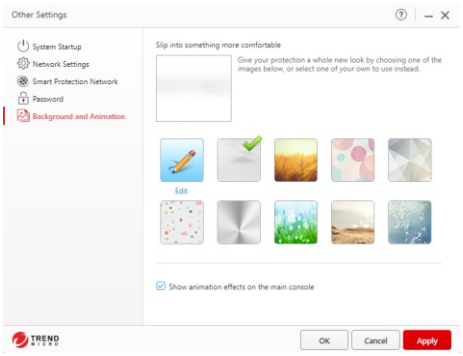

Figure 146. Background Editor

2. Select any background picture provided and click **Apply** to save the new background or add a picture from your computer.

3. For the second option, click the **Edit** button to edit your user interface. The **Select a Picture** dialog displays.

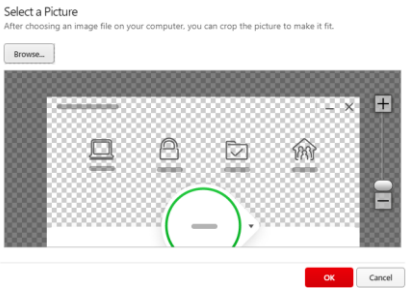

Figure 147. Select a Picture

4. Click **Browse** to select a picture, then navigate to a folder containing your pictures.

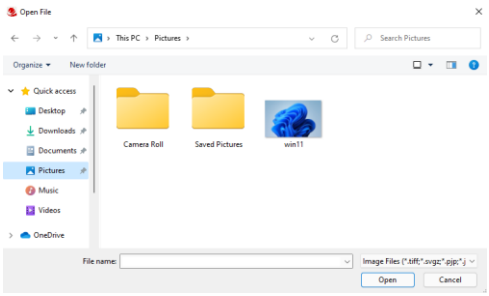

Figure 148. Browse to Picture

5. Select your picture and click **Open**. The picture is loaded into the editor.

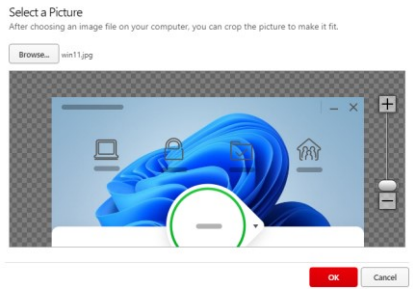

Figure 149. Sizing

6. Use the **Sizing** tool to make your image larger or smaller. Click the (**+**) or (**-**), or drag the slider.
7. When you're done, click **OK** to close the editor.
8. Click **Apply** to save your UI change, then **OK** to close the **Background Picture** tab.
9. Navigate to the main Console screen. Your new picture appears in the background.

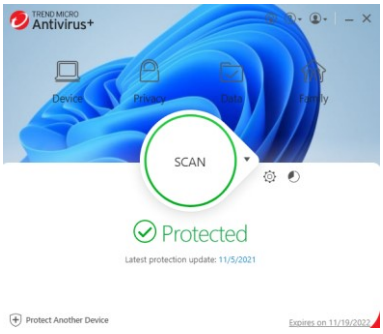

Figure 150. Trend Micro Security Console with New Skin

10. You can return to the classic Trend Micro Security background at any time by clicking its icon in the editor and clicking **Apply,** then **OK**; then return to the main Console screen.

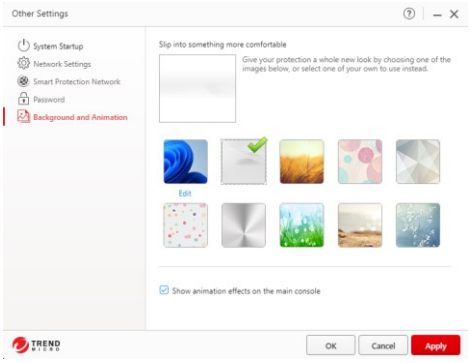

Figure 151. Classic Trend Micro Security Background

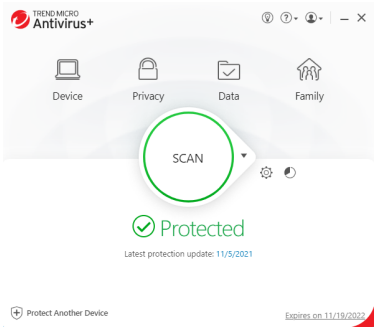

Figure 152. Trend Micro Security Console

11. If you wish, you may also uncheck the checkbox **Show animation effects on the main console**. This reduces the animation effects in the four functional icons of **Device, Privacy, Data,** and **Family.**

Device: Mute Mode

All editions of Trend Micro Security now provide a **Mute Mode** to temporarily stop non-critical notifications while you are doing an important task. This can also be applied while gaming.

To configure Mute Mote:

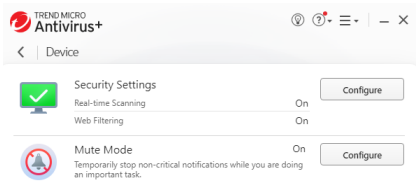

Figure 153. Device > Mute Mode > Configure

1. Click **Device > Mute Mode > Configure**. The **Mute Mode Introduction** screen appears.

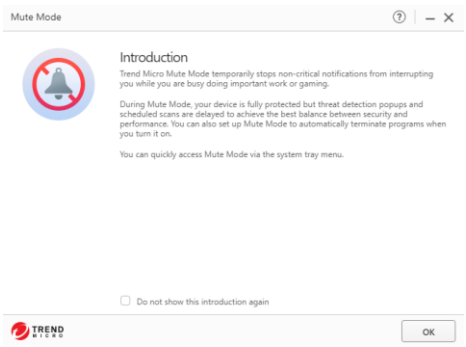

Figure 154. Mute Mode Introduction

2. Click **OK** to close the **Introduction**. The **Mute Mode Configure** screen appears, with the feature toggled off by default.

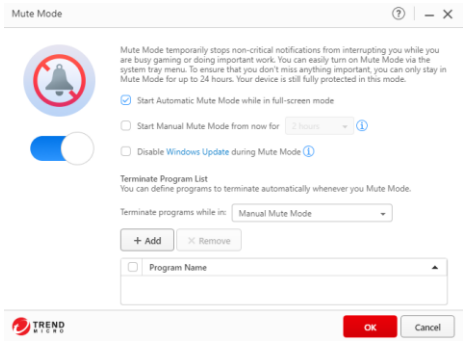

Figure 155. Mute Mode Configure

3. Click the toggle to **On**, then configure the various options:
   - **Start Automatic Mute Mode while in full-screen mode.** Once the toggle is on, this is enabled by default.
   - **Start Manual Mute Mode from now for X hours**. Select your choice in the drop-down menu to turn off Mute Mode after 1 to 24 hours.
   - **Disable Windows Update in Mute Mode**. Check the checkbox to disable Windows Update for as long as **Mute Mode** is active. (Disabling Windows Update for a long time may expose your system to security threats.)
4. **Terminate Program List**. You can define programs to terminate automatically whenever you enable Mute Mode.
5. **Terminate Programs while in** [dropdown menu]:
   - **Automatic Mute Mode**
   - **Manual Mute Mode**
   - **Automatic and Manual Mute Modes**
6. Click the **+ Add** button to add program(s) you would like to terminate in **Mute Mode.** The **Mute Mode** program selection dialog appears.

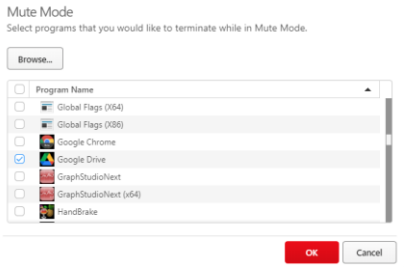

Figure 156. Mute Mode Program Selection List

7. Select the program(s) you wish to terminate in **Mute Mode**, then click **OK**. The program(s) you wish to terminate are added to the list.

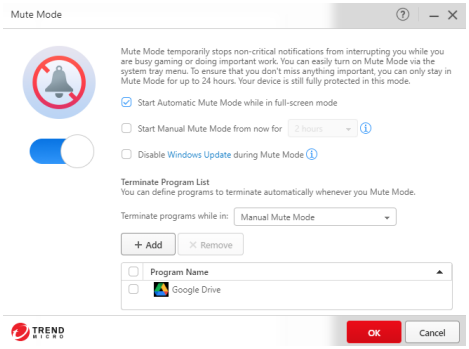

Figure 157. Mute Mode Program Selected List

8. Click **OK** to complete the setup. A popup appears, telling you that **Mute Mode is ON**.

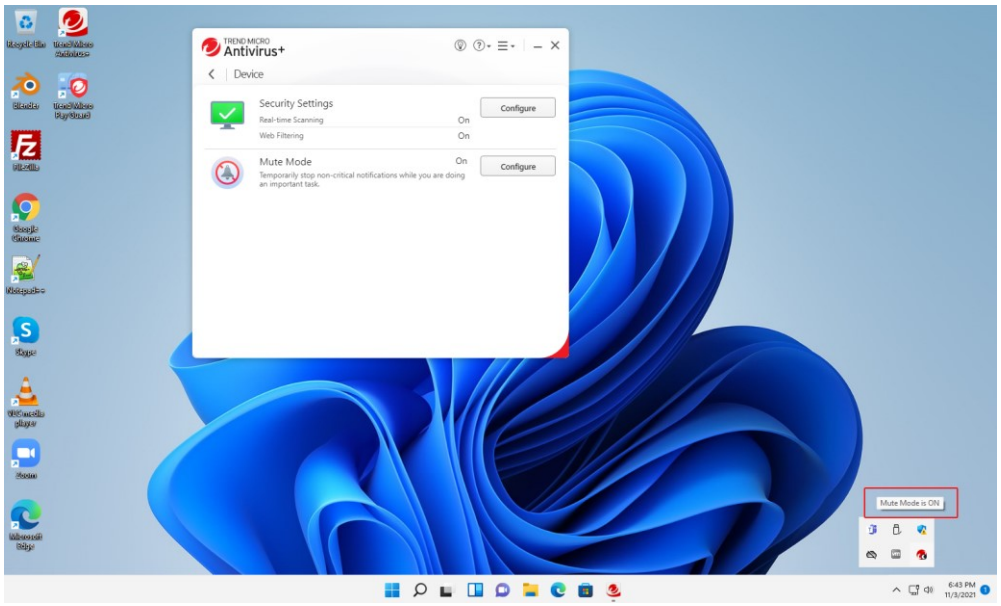

Figure 158. Mute Mode is ON

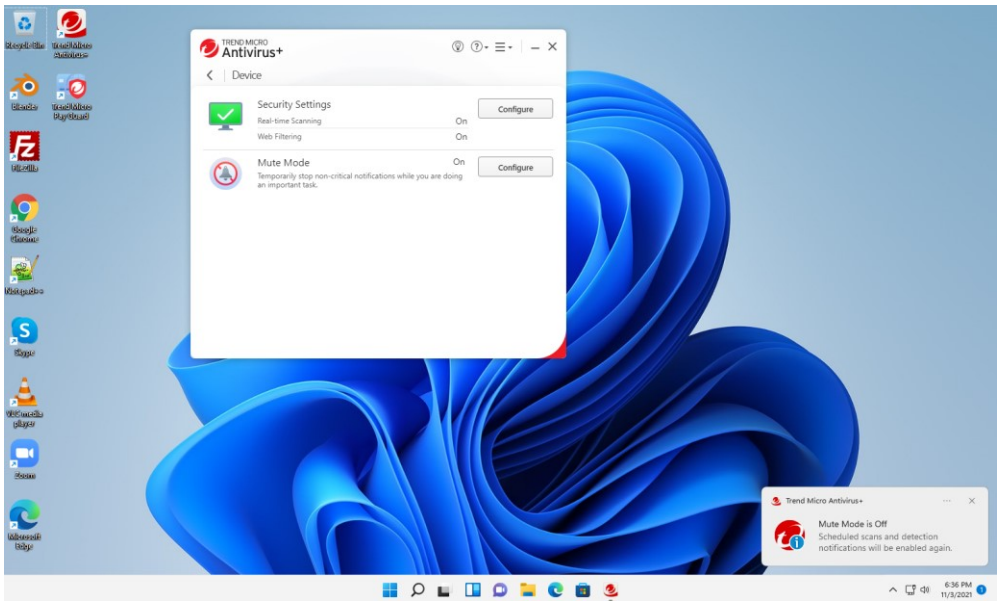

Figure 159. Mute Mode is OFF Popup

9. Click **OK** to complete activation of **Mute Mode. Mute Mode** shows as **On** in the **Device** window.

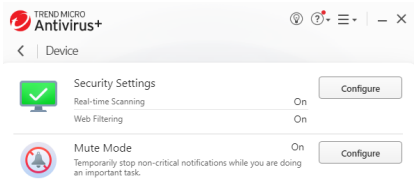

Figure 160. Mute Mode On

10. Click **Configure** again, then toggle **Mute Mode** to **Off** to turn it off before the allotted time has expired.

Device: Protect Another Device

Trend Micro Antivirus+ Security provides a subscription for one Windows device, but also lets you switch your protection to another Windows device. When you do so, you lose protection on the first device.

Go to Protect Another Device: PCs, Macs, Android and iOS Mobile Devices for more details.

Privacy: Social Networking Protection

All editions of Trend Micro Security provide Social Networking Protection to keep you safe from security risks when visiting the most popular social networking sites such as Facebook, Twitter, Google+, LinkedIn, Mixi, MySpace, Pinterest, and Weibo. In Facebook, you can also warn a friend when a link is dangerous. The function is turned on by default in Trend Micro Antivirus+, Internet Security, and Maximum Security, automatically activating the Trend Micro Toolbar.

To use Social Networking Protection:

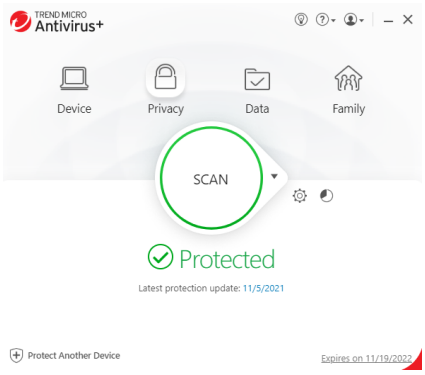

Figure 161. Console > Privacy

1. To configure **Social Networking Protection**, click **Privacy** in the Console. The **Privacy** screen appears, with the **Social Networking Protection** panel at the top.

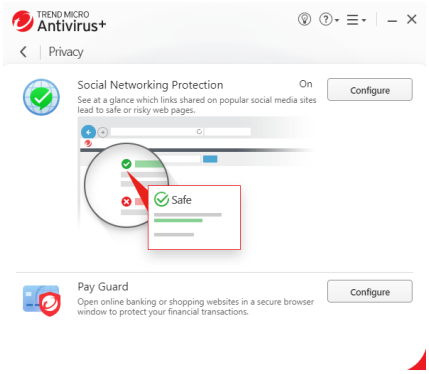

Figure 162. Social Networking Protection

2. Click **Configure**. The **Social Networking Protection** toggle screen appears.

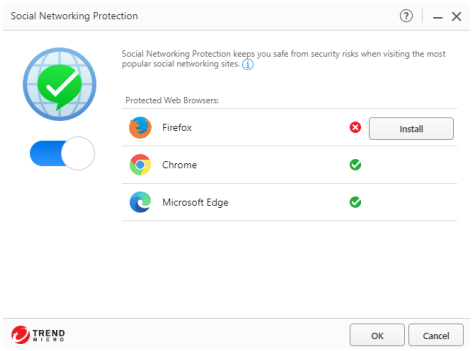

Figure 163. Social Networking Protection On

3. **Social Networking Protection** is turned **On** by default and the browser(s) installed on your system are shown. Trend Micro Security protects Internet Explorer, Firefox, Chrome, and Edge on the PC. If you wish, click the slider from **On** to **Off** to disable the function. Trend Micro does not recommend this.

4. Open your browser, select the **Trend Micro Toolbar > Menu > Settings**, and note that **Rate links on web pages** is turned **On**.

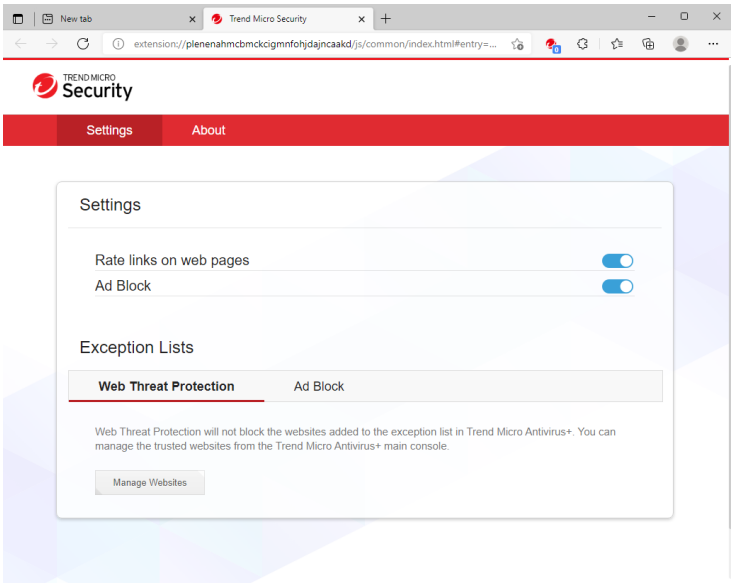

Figure 164. Rate Links on Web Pages

5. Now, when you mouse-over a link in search results, Trend Micro Security will scan it in real-time and provide you with a rating and details about it.

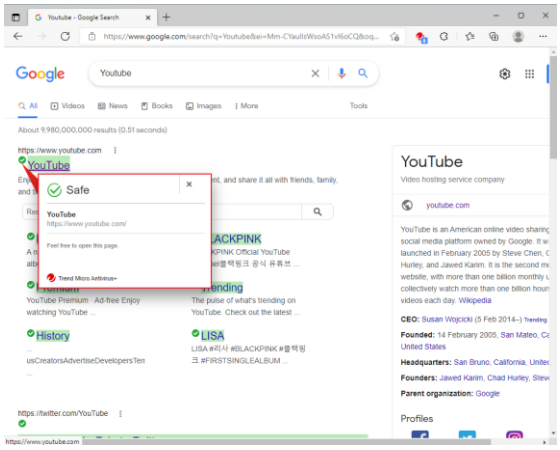

Figure 165. Safe Trend Micro Page Rating

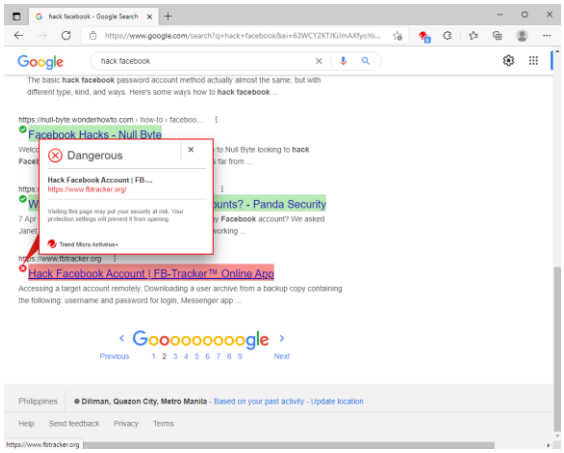

Figure 166. Dangerous Trend Micro Page Rating

6. Simply position your mouse over the checkmark to view details about the rating.
7. If you click on a bad link, you'll be blocked.

Figure 167. Dangerous Page

8. You can still open the page by clicking **Still want to open this page, despite the risk?** Trend Micro doesn't recommend this.

9. The same link ratings and mouse-over functions are available from within supported social networking sites. Note too, that when a URL posted on Facebook is rated as dangerous by Trend Micro Security, you can warn your friend about it.

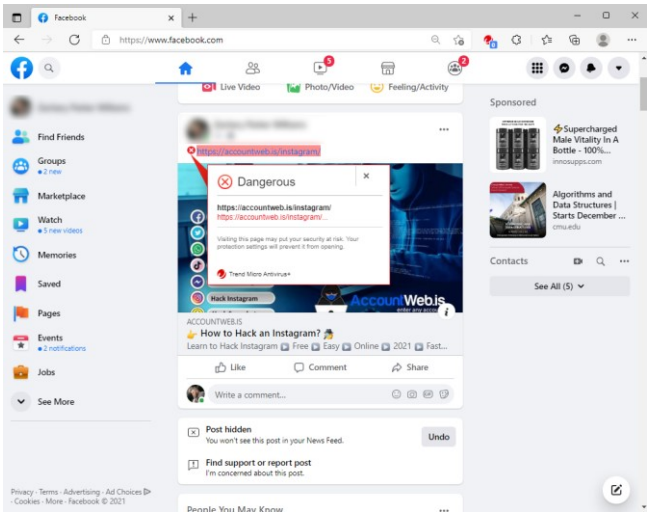

Figure 168. Dangerous URL on Facebook Detected by Trend Micro Security

10. Clicking the link redirects you to a blocking page.

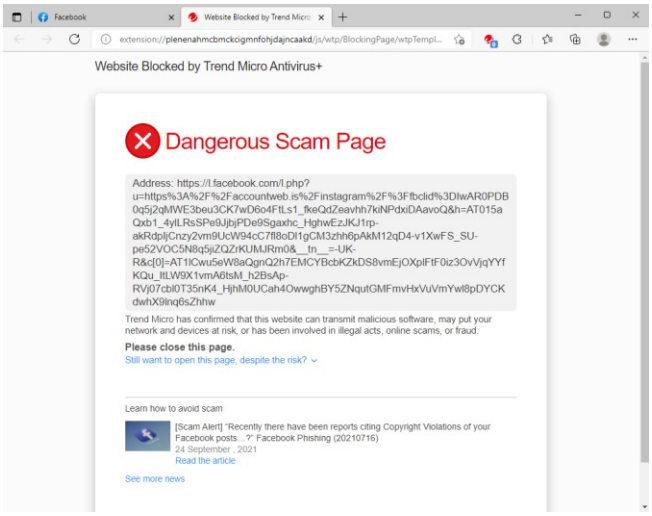

Figure 169. Website Blocked by Trend Micro Antivirus+

Privacy: Pay Guard

All editions of Trend Micro Security provide **Pay Guard**, which helps keep you safe from security risks when banking or shopping online with Microsoft Edge, Chrome, Firefox, or Internet Explorer. When you open Pay Guard, its powerful protection features are applied to your default browser automatically.

Pay Guard protects all the data in your financial transactions, including credit card information and personal data. With Pay Guard, all the extensions in your default browser are turned off. Security-related extensions, such as **Trend Micro Toolbar** or **Password Manager**, can be added later, or others, if you choose. The next time you use Pay Guard, they'll be loaded also.

To open Pay Guard:

1. Double-click the **Pay Guard** shortcut on your Windows desktop.

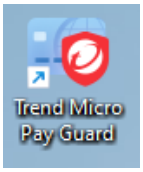

Figure 170. Pay Guard Shortcut

2. **Trend Micro Pay Guard** opens, using the protected version of your default browser.

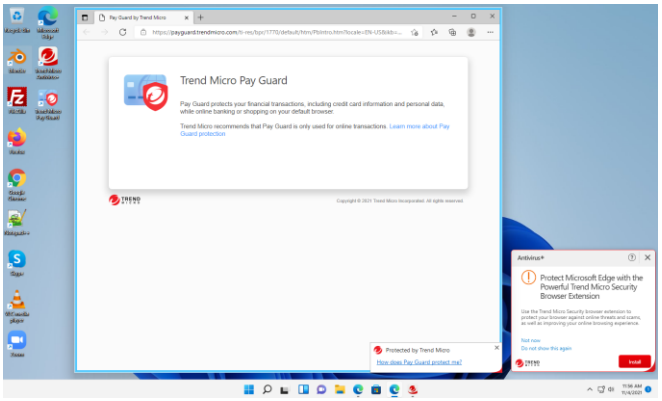

Figure 171. Trend Micro Pay Guard (Edge Example)

3. Note that the **Protect Microsoft Edge with the Powerful Trend Micro Security Browser Extension popup** in the lower right-hand corner of the desktop indicates that the **Trend Micro Toolbar** may be activated within Pay Guard to increase your protection. Click **Install**.

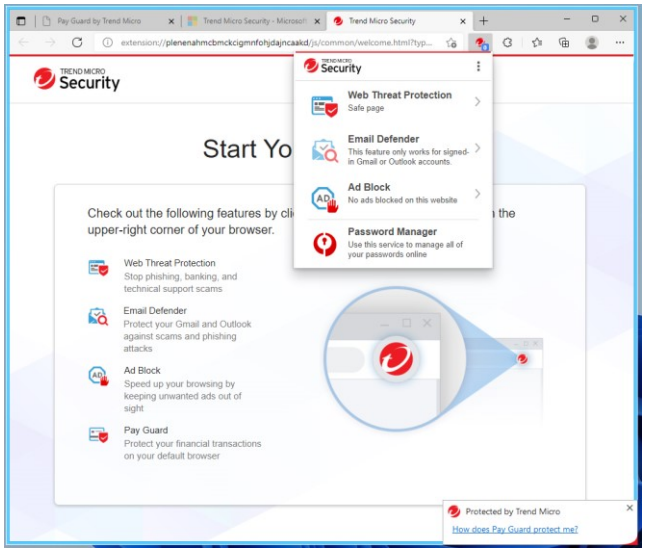

Figure 172. Notice of New Extension Added (Trend Micro Toolbar)

4. To enable or disable the Trend Micro Security Toolbar in Pay Guard. Go **to Trend Micro Extension > Menu > Settings**. Click slider to **Enable** or **Disable** the **Trend Micro Security Toolbar.**

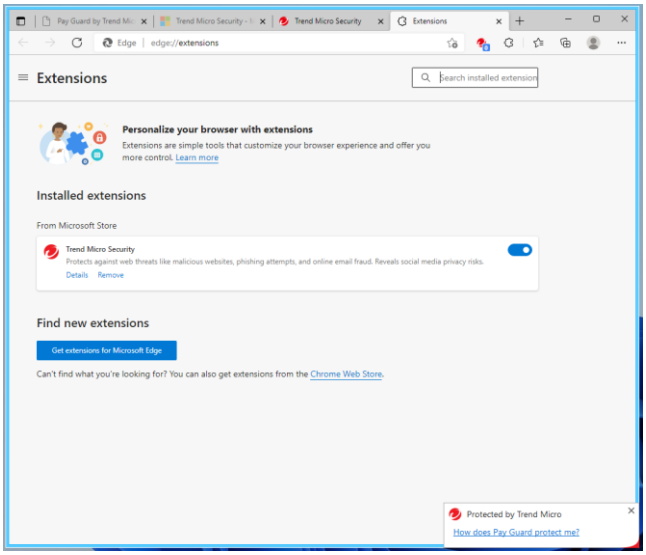

Figure 173. Microsoft Edge > Menu > Extensions > Trend Micro Toolbar

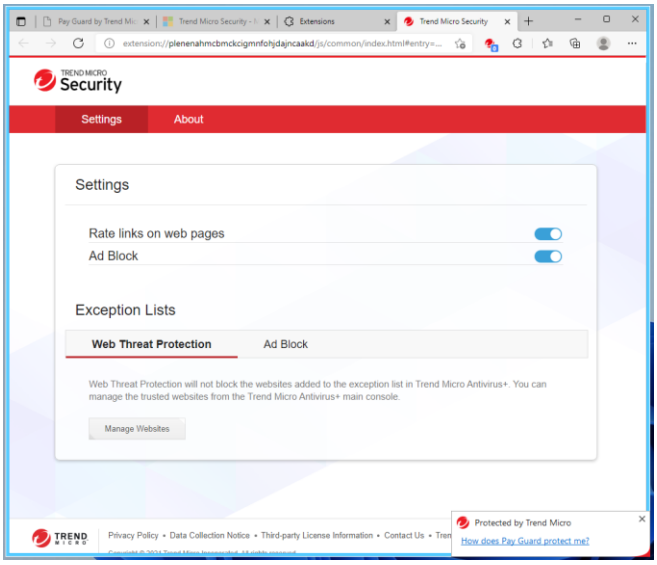

Figure 174. Pay Guard > Trend Micro Toolbar > Menu > Settings

5. **Trend Micro Toolbar** is activated within **Pay Guard** and will be present whenever you launch **Pay Guard**. The **Rate links on mouseover** is automatically enabled as an added protection when using Pay Guard.

6. Browse to your bank or to a commercial site where you may wish to conduct financial transactions and sign in as you normally would. **Pay Guard** protects you against browser injections and other threats to your identity or security.

Note: **Trend Micro Maximum Security also enables Trend Micro Password Manager as a second extension you may install into Pay Guard, to ensure you use strong passwords when conducting online transactions. See the section on Trend Micro Maximum Security > Password Manager > Pay Guard for more details.**

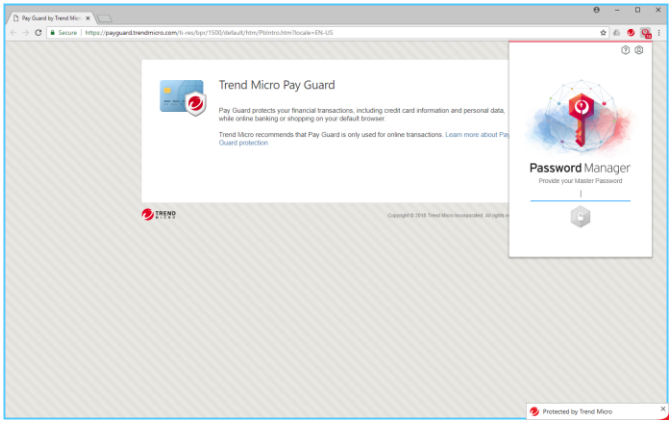

Figure 175. Pay Guard > Password Manager

7. You may also launch **Pay Guard** from the **Trend Micro Security Console.**

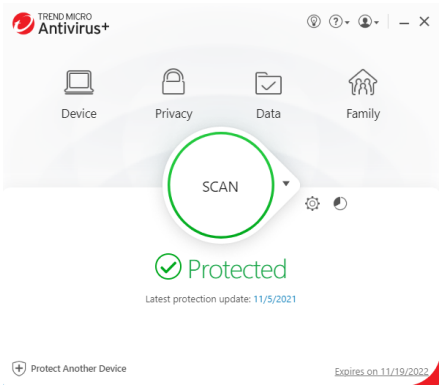

Figure 176. Trend Micro Security Console

8. Once the **Console** is open, simply click the **Privacy** icon. The **Privacy** screen appears, with the **Pay Guard** panel second in the list.

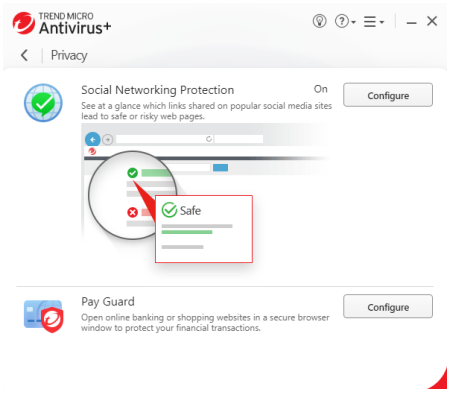

Figure 177. Privacy > Pay Guard

9. Click **Configure** in the **Pay Guard** panel.

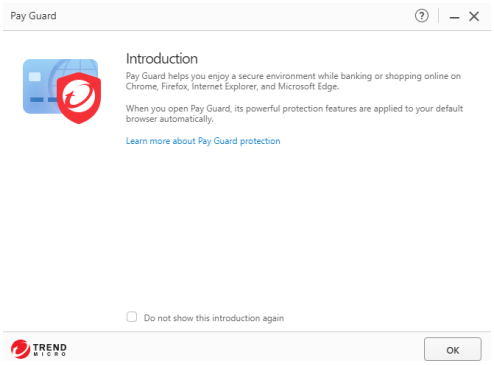

Figure 178. Pay Guard Introduction

10. The **Pay Guard Introduction** window launches explaining how it can protect you while banking or shopping online. Click **OK**.

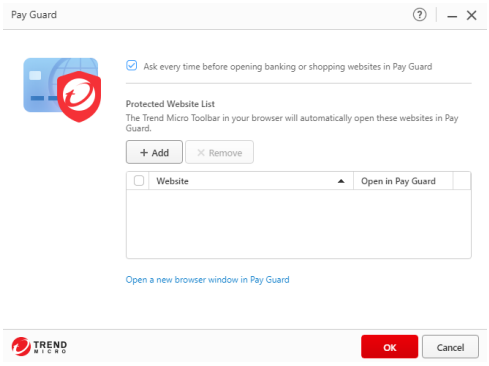

Figure 179. Pay Guard Protected Website List

11. The **Pay Guard Protected Website List** window appears. To open a new Pay Guard browser click **Open a new browser window in Pay Guard**. To add a new website in the list, click **Add**.

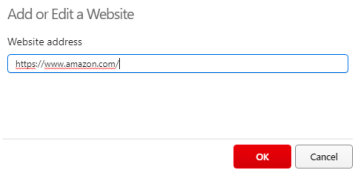

Figure 180. Add or Edit a Website

12. Enter the website and click **OK.** The Trend Micro Toolbar in your browser automatically opens the websites in your list in Pay Guard.

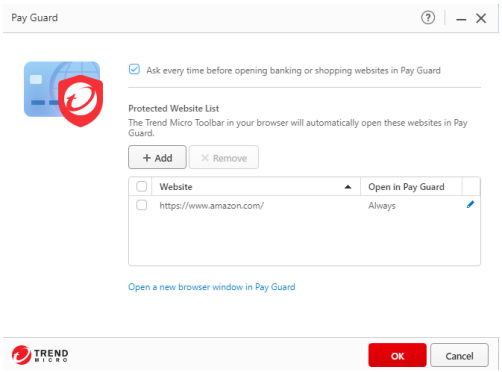

Figure 181. Pay Guard Protected Website List

Data: Folder Shield

In the **Data** window, you can configure **Folder Shield** to your specifications.

To configure Folder Shield:

1. Open the **Trend Micro Security Console.**

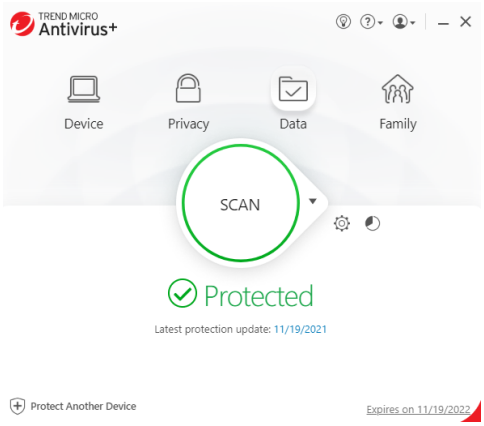

Figure 182. Console > Data

2. Click the **Data** icon. The **Data** screen appears.

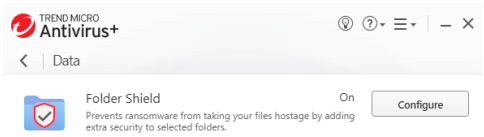

Figure 183. Data | Folder Shield

3. Click **Folder Shield > Configure** to configure the settings. The **Introduction** screen appears.

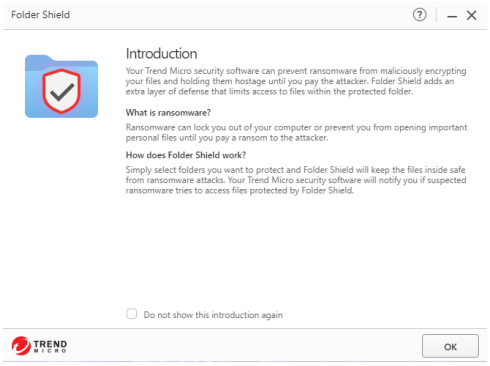

Figure 184. Folder Shield Introduction

4. Click **OK** to close the **Introduction**. The **Choose Folders You Want to Protect** window appears.

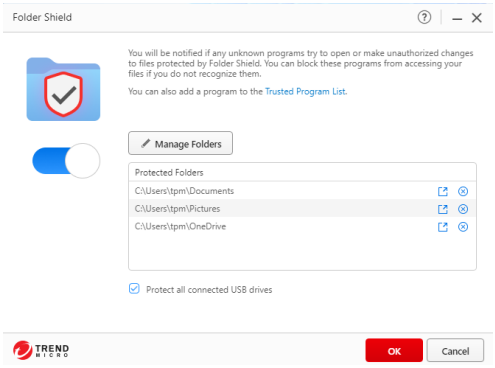

Figure 185. Choose Folders You Want to Protect

5. Click the **X** button for any folders you wish to delete from the **Protect Folders** list.
6. Click the **Managed Folders** to add folders to the **Protected Folders** list. A window appears letting you **Choose Folders to Protect.**

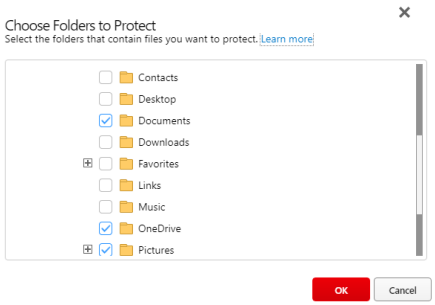

Figure 186. Choose Folders to Protect

7. Scroll up or down to choose the additional folder(s) in the **Folder Tree**. For example, you can select the main User's folder (this should be your name) to protect all folders for that User; or you may select additional individual folders for protection.

8. In this example, we choose **Videos**. Click **OK** to save your selection.

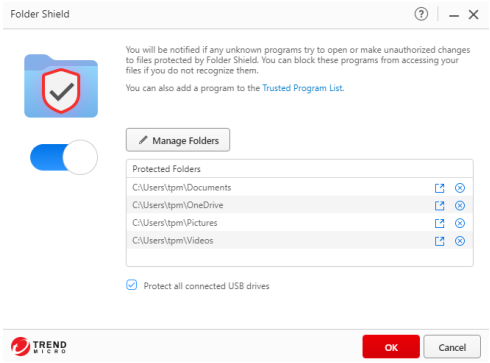

Figure 187. Videos Added

Note: **If you select the main User's folder, you may encounter additional warning popups under certain conditions. Don't worry! If you follow the rules given below for adding programs to the Trusted Program List, you will still keep yourself safe.**

9. **Videos** now appears in the list. You can also click the link **Trusted Program List** to add a trusted program to a list of applications that can access protected folders. The **Trusted Program List** appears.

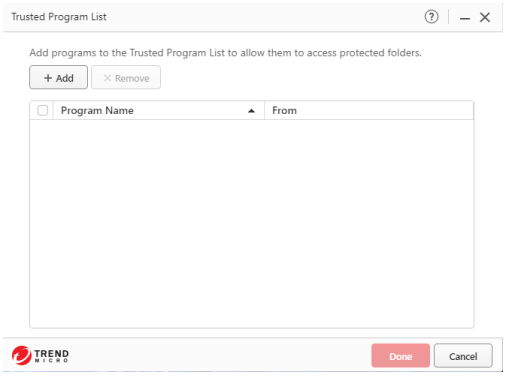

Figure 188. Trusted Program List

10. Click **+ Add** to add a program. A dialog appears, letting you **Add an Item** to the list.

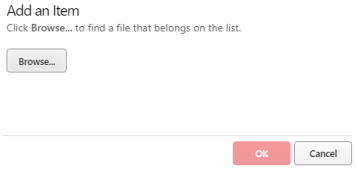

Figure 189. Add an Item

11. Click **Browse**, then navigate to the **Program Files** folder on your computer.

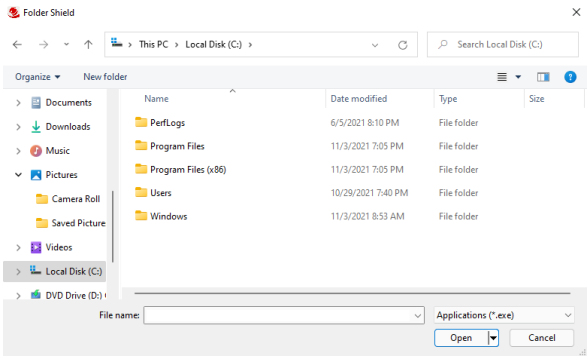

Figure 190. Local Disk (C:) - Program Files

12. In the **Program Files** folder, double-click folders to open them, until you locate the program you wish to add.

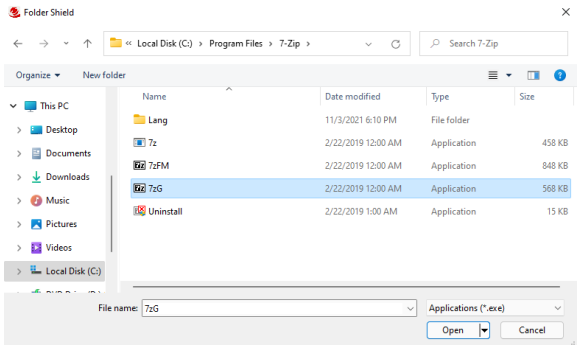

Figure 191. 7-Zip

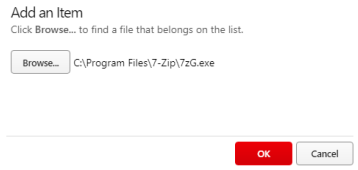

Figure 192. Add an Item

13. Select the **Application**, click **Open** to add it, then **Ok** to complete the process. The program appears in the **Trusted Program List.**

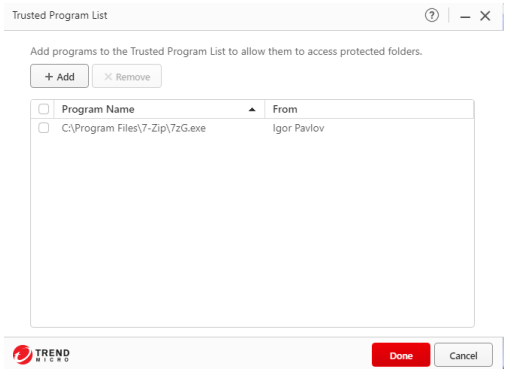

Figure 193. Trusted Program List

14. Click **Done.** Your program is now added to the **Trusted Program List.**

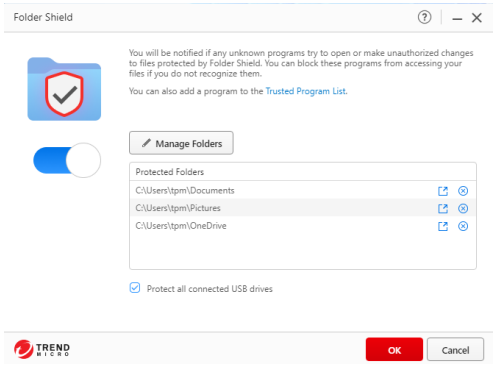

Figure 194. Protected Folders

15. Check the **Protect all connected USB Drives checkbox** to protect all connected USB hard drives and thumb drives. Click **OK** to close the **Folder Shield Configure** window.

How Folder Shield Works

Example 1:

1. Now, what if a program that's not in Trend Micro's list of known good programs, such as encrypting ransomware, unexpectedly tries to change any files in your protected folder?
2. A popup will appear, asking if you want to **Block this program**. Because you also have the option to **Trust this program**, what should you do?

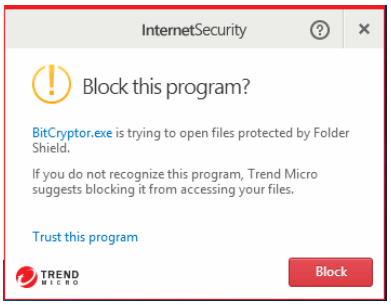

Figure 195. Block this program?

3. In a setting where you're just doing a search, or browsing a website, or watching a video and the pop-up appears, it's quite likely that malware or ransomware is trying to install, to maliciously change or encrypt your files. In this case, **Block** is the recommended action.
4. Note too, that even if the program trying to execute shows up under a familiar name—such as winword.exe (for Microsoft Word), excel.exe (for Microsoft Excel), or photoshop.exe (for Adobe Photoshop), *you should also click **Block**.*
5. Malware or encrypting ransomware can disguise itself under familiar program names and the unexpected nature of the event that triggered the popup is a clue that it's probably dangerous.

Example 2:

1. But what if you're just trying to open a file in your protected folder and the popup appears, asking you if you want to **Block this program**?

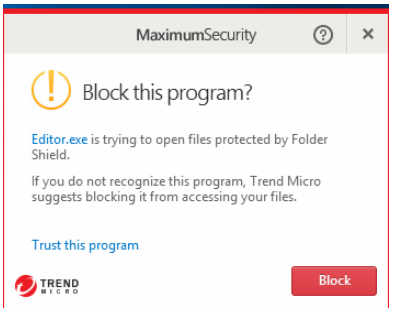

Figure 196. Block this program?

2. *Even in this case,* you should generally accept **Folder Shield's** judgment and click **Block** to stop the action.
3. So, when *should* you click **Trust this program?** Because trusted programs are automatically added to the **Trusted Program List,** potentially exposing you to risk, you should *only* click **Trust this program** under one or more of the following conditions:
   - If you remember downloading, installing, and using the program before.
   - If the program was downloaded from a reputable site, such as CNET's **Download.com**, which tests all software submitted to the site for malware before posting.
   - If you've done your research and have determined that the software has a known good reputation, as given on the official download page, along with frequently asked questions (or F-A-Qs) and/or a Support page, and does not appear in any websites that list malicious software.
   - If it's software that you have developed personally or internally for organizational purposes.
4. In this last instance, you may wish to file a reclassification case to Trend Micro Support, so the program will not be blocked by default by Folder Shield. Go here to find out how to do that: [Reclassification Requests]
5. Or go here for advice if you're worried you may be under attack by ransomware: [Ransomware Support]

6. After a few moments, if you don't click **Block**, **Folder Shield** will block the program anyway. The popup will change to **Programs Blocked**, and the **Trust this program** link will change to **More details…**

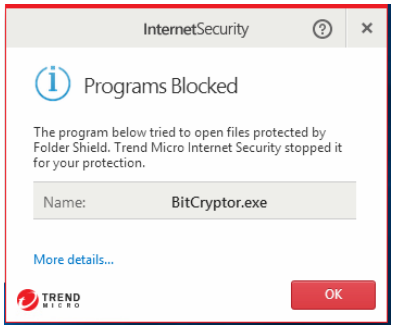

Figure 197. Programs Blocked

7. Click **More details…** to get more details on the programs blocked and the targeted file or files. The **Logs** window appears.

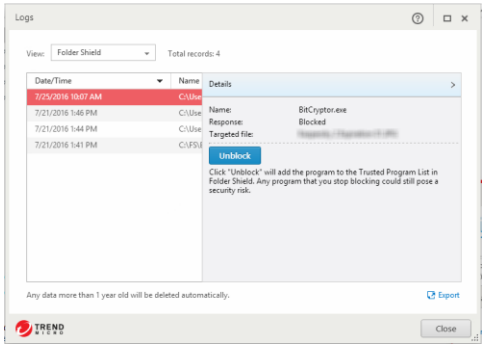

Figure 198. Details

8. The **Details** panel will show the **Name** of the program blocked, the **Response** taken, and the **Targeted file** or **files**.

9. If you click **Unblock**, the program will be added to the **Trusted Program** list. As mentioned, if you do this, you *could* open yourself to a security risk now or in the future.

10. Click the right-arrow to close the **Details** panel and view the **Folder Shield** log table, with the **Date/Time** of all incidents, the **Name** of the offending program, and the **Responses** shown in the table.

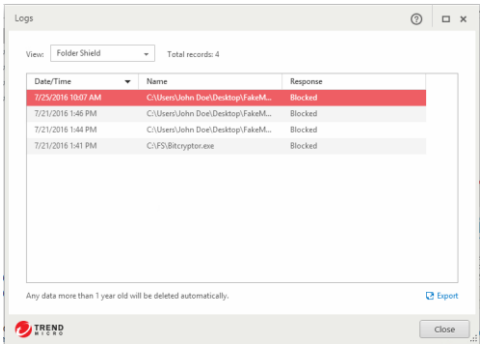

Figure 199. Folder Shield Logs

11. Click **Export** if you wish to export the table for future reference or for troubleshooting with a Trend Micro Support expert.
12. Click **Close** to close the table, then **OK** to close the warning popup.

Family: Upgrade Now

Keep your family safe online by upgrading to **Trend Micro Maximum Security** for **Parental Controls.**

To get Parental Controls:

1. Open the Trend Micro Security Console.

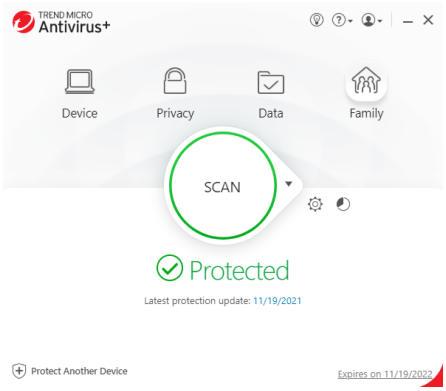

Figure 200. Console > Family

2. Click the **Family** icon. The **Family** screen appears.

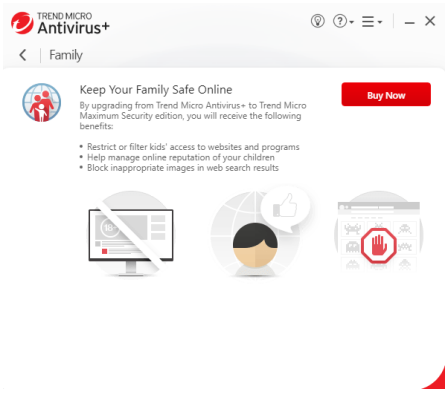

Figure 201. Family

1. Click **Buy Now** and follow the online instructions to upgrade to **Trend Micro Maximum Security** to enable **Parental Controls**.
2. By upgrading to **Maximum Security**, you can
   - Restrict or filter kids' access to websites and programs
   - Help manage online reputation of your children
   - Block inappropriate images in web search results

Chapter 5: Trend Micro Internet Security

This chapter provides detailed instructions for configuring and using Trend Micro Internet Security.

Protection Overview

Trend Micro Internet Security provides everything included in **Trend Antivirus+ Security**, but adds some significant protections and tools, outlined below. To enable all functions, you need a paid version of Internet Security.

Figure 202. Trend Micro Internet Security Welcome Screen

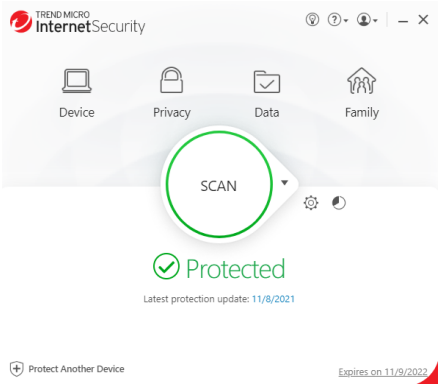

Figure 203. Trend Micro Internet Security Console

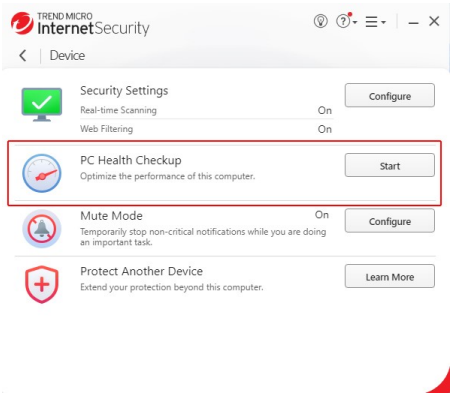

Figure 204. Device > PC Health Checkup

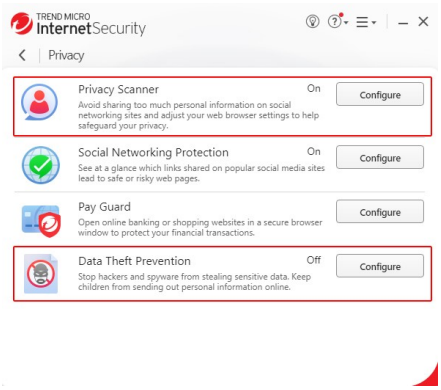

Figure 205. Privacy > Privacy Scanner | Data Theft Prevention

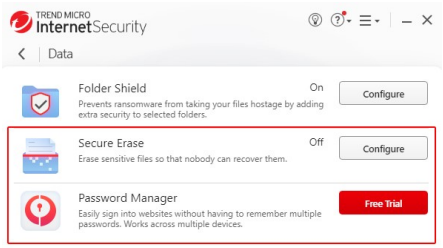

Figure 206. Data > Secure Erase | Password Manager Free Trial

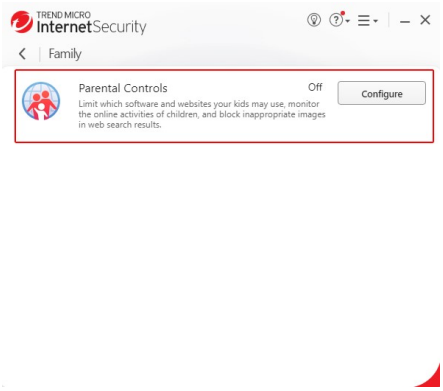

Figure 207. Family > Parental Controls

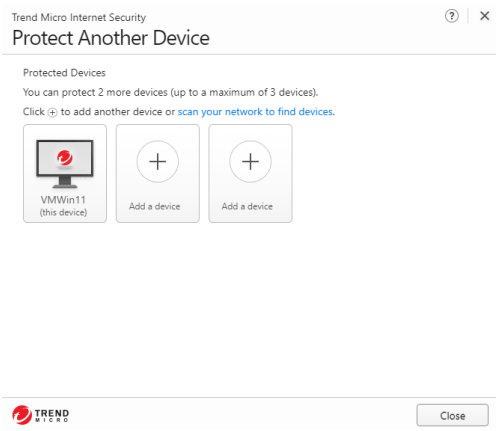

Figure 208. 3-Device Option – Windows and Mac

Note: **Trend Micro Internet Security has additional features beyond Trend Micro Security Antivirus +. These include**

Device: Smart Scheduled Scans, PC Health Checkup

Privacy: Privacy Scanner, Data Theft Prevention

Data: Secure Erase and Free Trial Offer for Password Manager

Family: Parental Controls

Additional Offerings: 3-Device Option – Windows and Mac: Protect 2 more devices or scan your network to find devices.

ADDITIONAL TOOLS FOR TREND MICRO SECURITY INTERNET SECURITY PAID VERSION

Smart Schedule Scans

Trend Micro Internet Security provides a new way to conduct scheduled scans with its Smart Schedule. Based upon recent computer usage, the most suitable scan will start automatically at an appropriate time.

PC Health Checkup

Trend Micro Internet Security adds the **PC Health Checkup**, which can improve PC performance by cleaning up temporary files, registries, and the Start-up Manager. It also checks for potentially incompatible programs (PIPs). Reports provide information on how your computer has been optimized.

Privacy Scanner

Trend Micro Internet Security adds the Privacy Scanner for Facebook, Twitter, and LinkedIn, and your PC browsers (Internet Explorer, Microsoft Edge, Chrome, and Firefox). The Privacy Scanner scans your privacy settings, alerts you to settings that expose you to potential identity theft, and lets you automatically change them.

Data Theft Prevention

With its **Data Theft Prevention** feature, Trend Micro Internet Security allows you to prevent data leakage (from email and instant messaging tools) or data theft (from tools such as keyloggers).

Secure Erase

Trend Micro Internet Security also adds **Secure Erase**, which shreds computer files that have sensitive information, making it impossible for an unauthorized person to recover them.

Parental Controls

Trend Micro Internet Security allows parents to restrict access to websites by users, rule sets, and categories. **Parental Controls** also gives parents the ability to limit the amount of time their child is allowed to use the Internet. Trend Micro Security's Parental Controls tap into Windows User Accounts, assigning each rule set to a specific user.

Password Manager

Trend Micro Internet Security provides easy download access to a Free Trial 5-account version of Trend Micro Password Manager, which helps you to manage all your online credentials. Trend Micro Security users can buy the full version for unlimited password management.

Protect Another Device: Windows and Mac

Trend Micro Internet Security's allows you to protect up to three Windows and Mac devices. For example, when you click the Mac icon in **Protect Another Device**, you can email an install link, copy a link, or directly download Trend Micro Antivirus for Mac. You can also scan your network to find other devices to protect.

Device: Security Settings: Security & Tuneup Controls > Scheduled Scans > Smart Scheduled Scan

Trend Micro Internet Security provides a new way to conduct scheduled scans with its Smart Schedule. Based upon recent computer usage, the most suitable scan will start automatically at an appropriate time.

To view Smart Schedule scan:

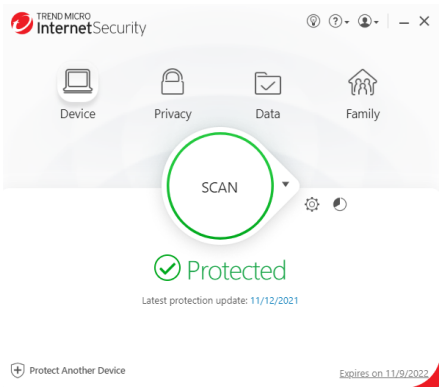

Figure 209. Trend Micro Internet Security Console

1. In the **Trend Micro Internet Security Console**, click **Device.** The **Device** window appears.

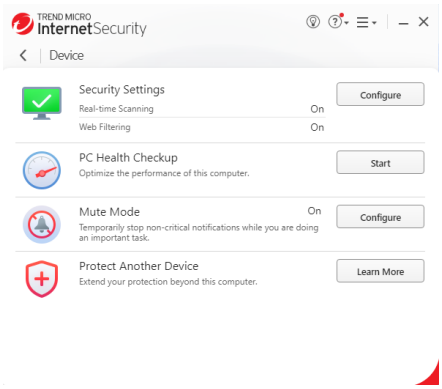

Figure 210. Device

2. Click **Configure** in the **Security Settings** panel. The **Security & Tuneup Controls** window appears, with **Scan Preferences** selected by default.

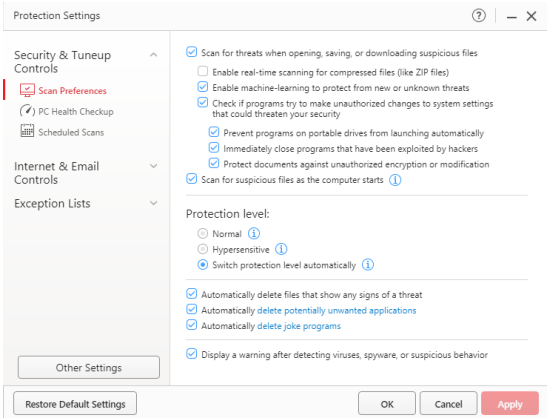

Figure 211. Security & TuneUp Controls > Scan Preferences

3. Click **Scheduled Scans.** The **Scheduled Scans** screen appears.

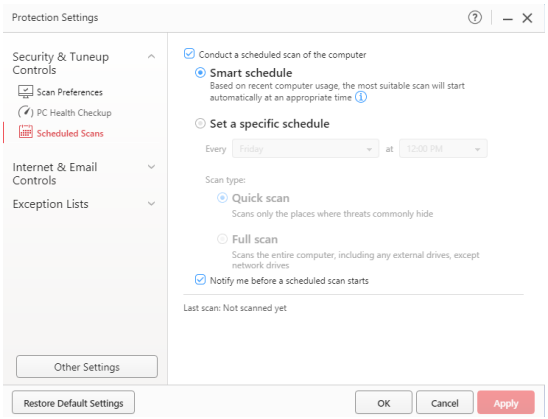

Figure 212. Scheduled Scans > Smart Schedule

4. Observe that **Smart Schedule** is chosen by default. If you leave this setting as is, **Trend Micro Internet Security** will itself decide, based on your recent computer usage, when the most suitable scan (Quick or Full) should be conducted.

5. Alternately, you may **Set a specific schedule**, along with **Scan type** (Quick or Full), as described in the previous chapter.

6. The option **Notify me before a scheduled scan starts** is turned on by default. Uncheck the checkbox if you do not wish to be notified.

Device: PC Health Checkup | Security Settings

Trend Micro Internet, Maximum, and Premium Security provide a **PC Health Checkup** that can help you recover disk space, make Microsoft Windows start faster, clean up your instant messaging history, and optimize your computer's performance. You can also plan scheduled tune-ups that can automatically keep everything running smoothly.

Note: **PC Health Checkups are automatically performed whenever you do a Quick or Full Scan, but you can also conduct a PC Health Checkup on its own.**

Perform a PC Health Checkup

To perform a PC Health Checkup:

1. Click **Device > PC Health Checkup > Start** in the **Console**.

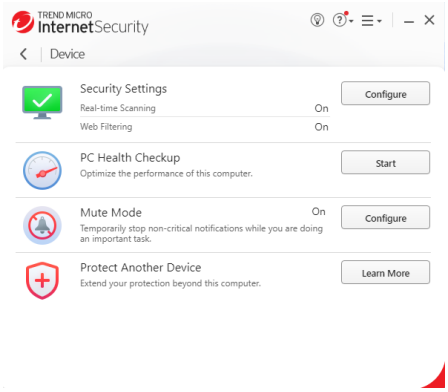

Figure 213. Device > PC Health Checkup

2. A **PC Health Checkup** scan begins immediately, showing the progress of the optimization.

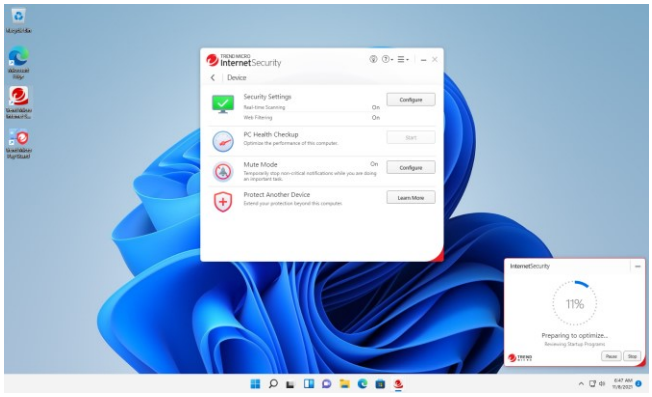

Figure 214. Device > PC Health Checkup > Start

3. When the scan completes, a **Results** screen appears, providing an indicator of your Optimization Level—in this case, **Very Good**, suggesting possible improvements.

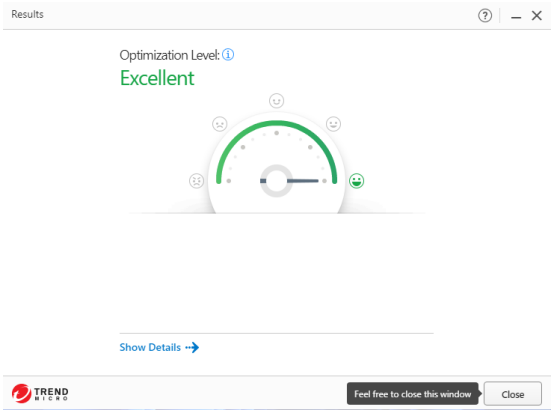

Figure 215. PC Health Checkup Results

4. Click **Make Improvements** to make the improvements. **PC Health Checkup** makes the improvements to your system.

5. You can also click **Show Details** to obtain more details about the suggested improvements. The **Details** screen appears.

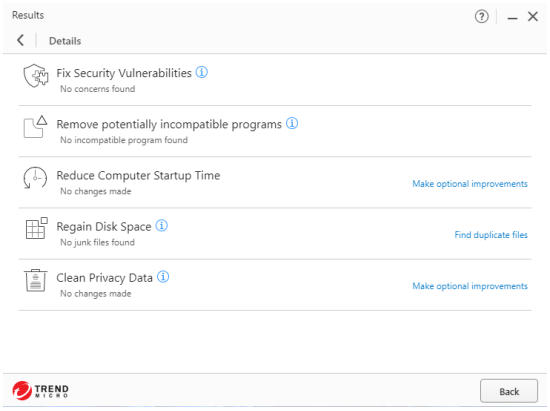

Figure 216. PC Health Checkup Details

6. Details include the following:

   - Fix Security Vulnerabilities
   - Remove potentially incompatible programs
   - Reduce Computer Startup Time
   - Regain Disk Space
   - Clean Privacy Data

7. Again, click **Make Improvements** to make the improvements; the results will be displayed.

8. Click **Back** to return to the **Optimization Level** window. The level will be adjusted to show your improvements.

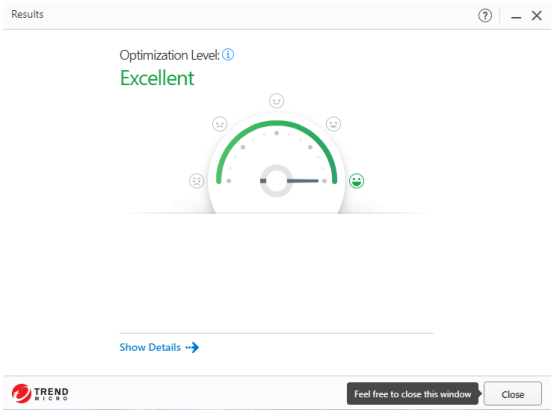

Figure 217. Optimization Level: Excellent

9. Click **Close** to close the **Optimization Level** window. This returns you to the **Device Settings** window.

Configure PC Health Checkup

To configure PC Health Checkup:

1. Back in the main **Console** screen, click **Device > Security Settings > Configure.** The **Protection Settings** screen appears, with **Security & Tuneup Controls > Scan Preferences** shown by default.

2. Click **PC Health Checkup** to configure its settings.

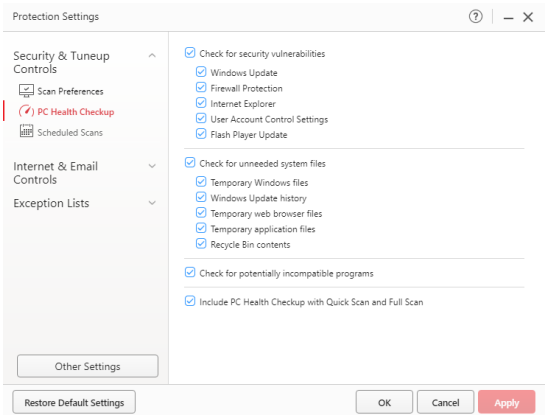

Figure 218. PC Health Checkup Settings

3. You can define how **PC Health Checkup** works by checking/unchecking a **Security Vulnerability** or **Unneeded System Files** item. All items are checked by default.

>Check for security vulnerabilities

- Windows Update
- Firewall Protection
- Internet Explorer
- User Account Control Settings
- Flash Player Update

>Check for unneeded system files

- Temporary Windows Files
- Windows Update history
- Temporary web browser files
- Temporary application files
- Recycle Bin contents

>Check for potentially incompatible programs. Uncheck to disable this in your PC Health Checkup.

>Include PC Health Checkup with Quick Scan and Full Scan. Uncheck this to disable PC Health Checkup with Quick and Full scans.

4. Click **Apply** to apply any changes.

Security Report: PC Health Checkup

Once you have conducted one or more PC Health Checkups, you can view a **PC Health Checkup Security Report.**

To view a PC Health Checkup Security Report:

1. Open the Trend Micro Security Console.

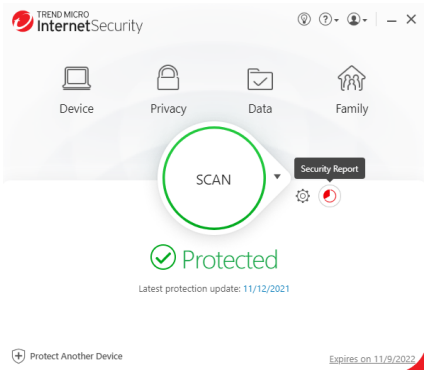

Figure 219. Security Report Tool

2. Click the **Security Report** tool. The **Security Report** appears, with **Security Threats** selected by default.

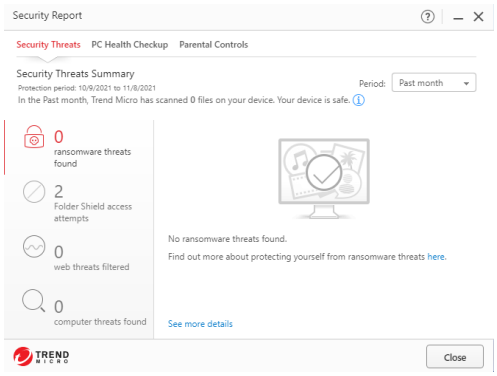

Figure 220. Security Threats

3. Click the **PC Health Checkup** menu item to display a **Report**.

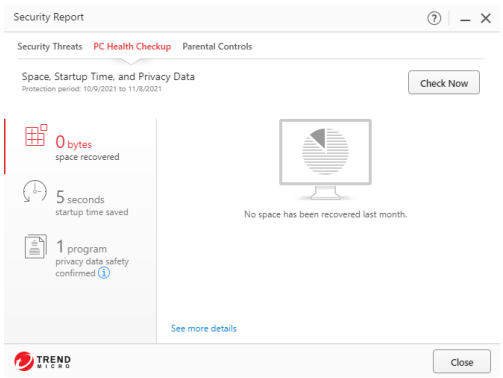

Figure 221. PC Health Checkup Report

4. Click **See more details** to obtain tabular data on Security and PC Health Checkup results.

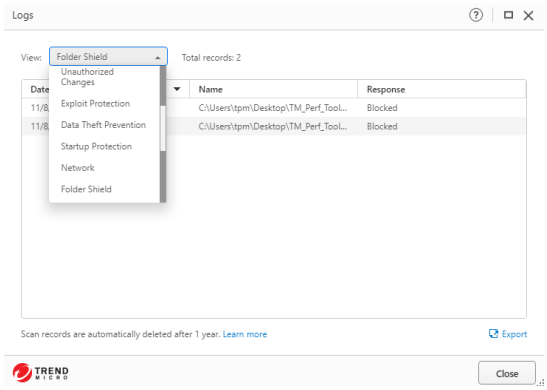

Figure 222. PC Health Checkup Logs

5. Use the **View** drop-down menu to view different logs, including **Regain Disk Space** and **Clean Privacy Data.**

6. Click **Export** to export the log in .CSV or .TXT format.
7. Click **Parental Controls** to see the report on Parental Controls.

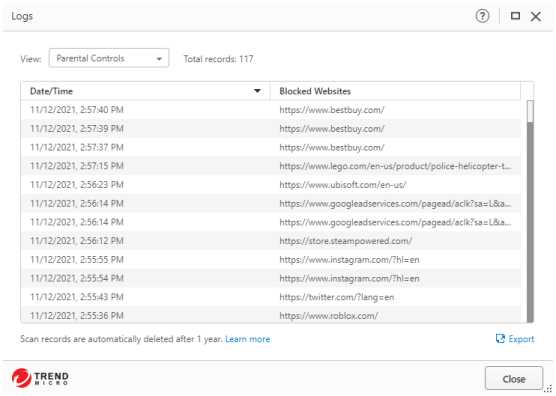

Figure 223. Security Report for Parental Controls

8. Monthly **Security Reports** are automatically generated by Trend Micro Security and emailed to you at the email address you used to create your account. Your monthly report includes
   - A list of Computers Protected in your account
   - A Threat Summary, including the various types of threats detected
   - A PC Health Checkup, including amount of space recovered and seconds saved at startup
   - Parental Controls, including violations of web and usage rules
   - An invitation and button to protect other devices, the number of which depends upon your active Trend Micro licenses.

Device: Protect Another Device

Trend Micro Internet Security provides a subscription for three Windows or Mac devices.

Go to Protect Another Device: PCs, Macs, Android and iOS Mobile Devices for more details.

Privacy: Privacy Scanner: Social Network Privacy & Web Browser Privacy

The Trend Micro Security **Privacy Scanner** works with Facebook, Twitter, and LinkedIn and supported PC browsers (Microsoft Edge, Internet Explorer, Chrome, and Firefox). It's turned on by default in Trend Micro Internet and Maximum Security. The default setting also turns on the Trend Micro Toolbar, which can be used to launch the Privacy Scanner.

NOTE: Make sure the Trend Micro Toolbar is already enabled in your browser before you try to use the Privacy Scanner. See Enable Trend Micro Toolbar for details.

To use the Privacy Scanner:

1. Double-click the Trend Micro Security shortcut on the desktop to open the **Trend Micro Security Console**. The **Trend Micro Security Console** appears.

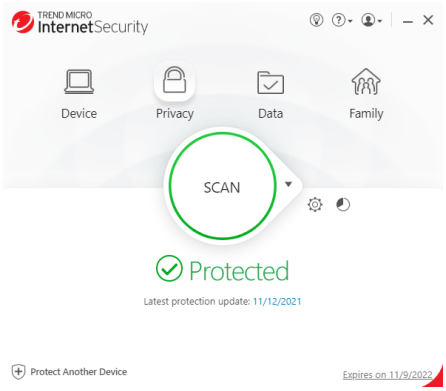

Figure 224. Trend Micro Security Console > Privacy

Do one of two things:

2. In the main **Console** window, click the **Privacy** icon. The **Privacy** window appears.

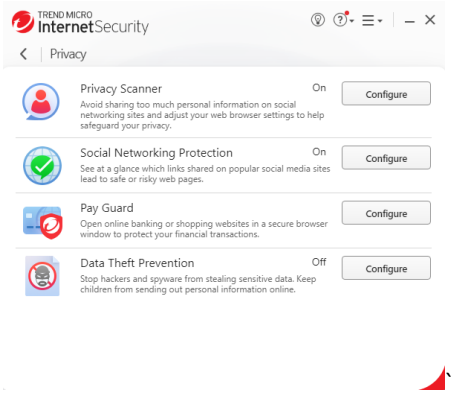

Figure 225. Privacy

3. Click **Configure** in the **Privacy Scanner** panel. The **Privacy Scanner** window appears.

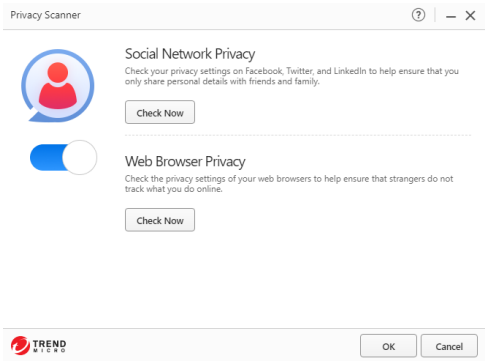

Figure 226. Privacy Scanner window

4. Ensure the slider is **On** and click **Check Now** in the **Social Network Privacy** panel.

   OR:

5. Open your browser and select the **Trend Micro Toolbar > Check your online privacy**.

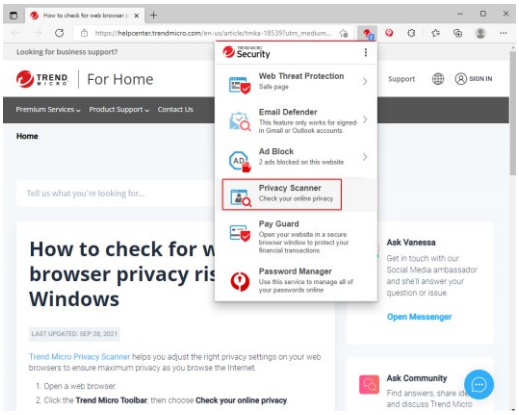

Figure 227. Privacy Scanner - Check your online privacy

6. Both actions take you via your browser to the **Trend Micro Privacy Scanner** webpage, with the **Facebook** sign-in panel shown by default.

Facebook Privacy Settings

To check your Facebook Privacy Settings:

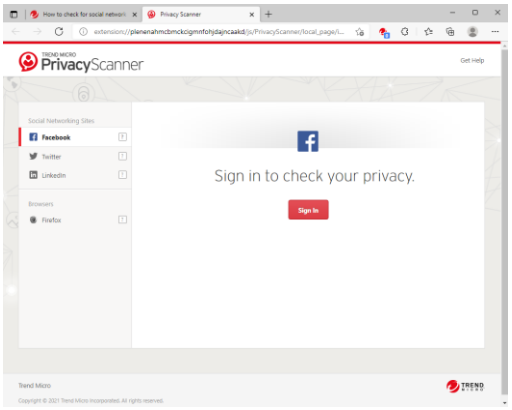

Figure 228. Trend Micro Privacy Scanner | Facebook

1. In the **Privacy Scanner** page, click **Sign In**. Trend Micro Security automatically takes you to the Facebook login website.

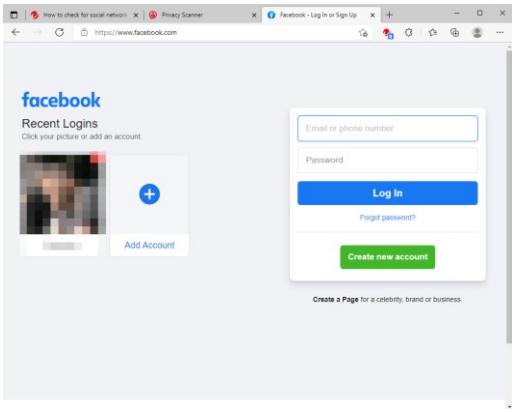

Figure 229. Facebook Login Webpage

2. Sign in to your Facebook account. The **Facebook News Feed** page displays, showing Trend Micro Security's **Privacy Scanner for Facebook**.

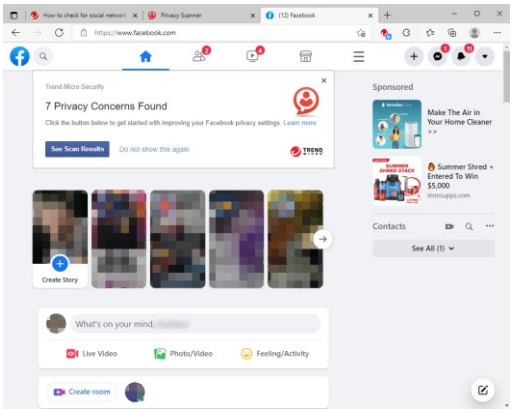

Figure 230. Facebook > Check My Privacy

3. Click **See Scan Results**. Facebook returns the results, indicating when you have privacy concerns.

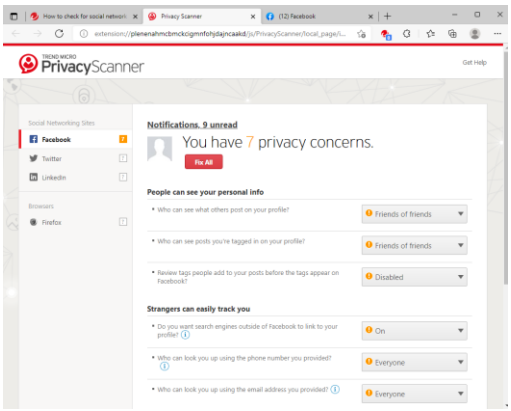

Figure 231. Facebook Privacy Concerns

4. If you have concerns, click **Fix All** to fix all the concerns at once using the Trend Micro Security recommended privacy settings, or select the drop-down settings menu to fix them manually. In this example, we'll choose **Fix All**. The **Fix** popup appears.

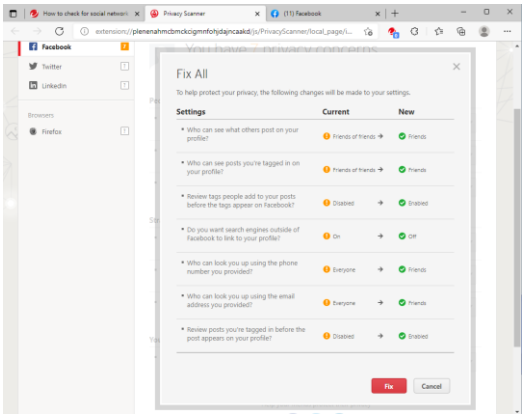

Figure 232. Fix All | Editor

5. Click **Fix** for the settings with Privacy Concerns. Trend Micro Security changes your settings and returns the result. In this case, since you accepted the default recommendations, it returns “Nice work! You don’t have any privacy concerns, but your friends might need some help...”

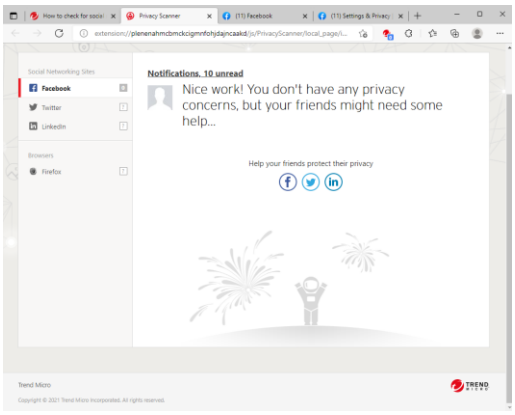

Figure 233. Nice work!

6. Click the **Facebook** icon to share a link Trend Micro Security and the Privacy Scanner to your friends on **Facebook**. The **Share Link** screen appears, allow you to share the post on Facebook.

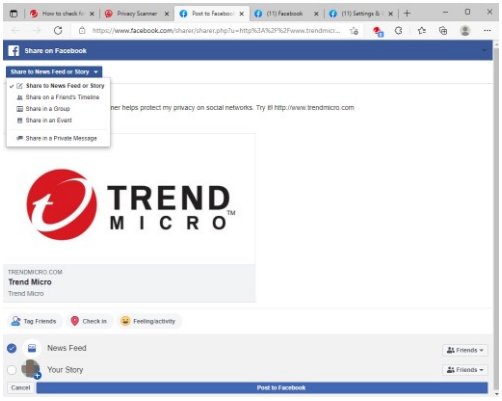

Figure 234. Share to Facebook

Upper-left popup:

- Share to News Feed or Story
- Share on a Friend's Timeline
- Share in a Group
- Share in an Event
- Send on a Page You Manage
- Share in a Private Message

7. Choose an option, or simply click **Post to Facebook.** The link is posted according to your choice.

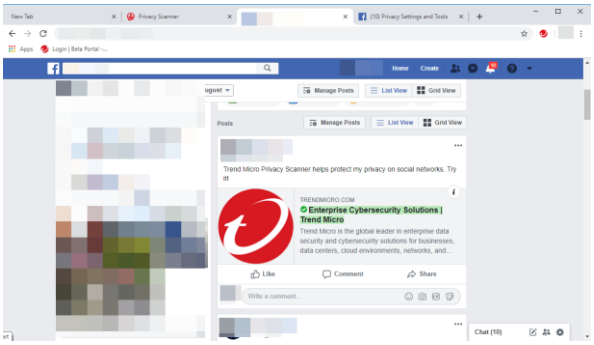

Figure 235. Trend Micro - Shared Link

Facebook App Privacy Settings

Note that the Privacy Scanner also scans Facebook Apps for their privacy settings. When you use a social networking app on your Facebook page, such as a game, your privacy settings determine who can see your posts.

To check the privacy settings of your app or game:

1. Use **Privacy Scanner** to perform a Privacy Scan of Facebook, as explained in the previous section. Trend Micro Security provides the result.

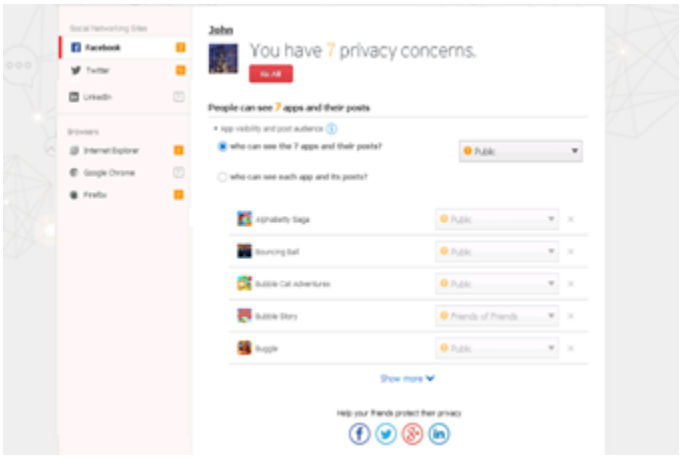

Figure 236. Apps (Games) With Privacy Concerns

2. Select **Fix All**, then **Fix** in the popup, to fix all your app privacy settings at once, or select "Who can see each app and its posts?", then fix each app setting in turn. Facebook tells you "Nice work! You don't have any privacy concerns, but your friends might need some help."

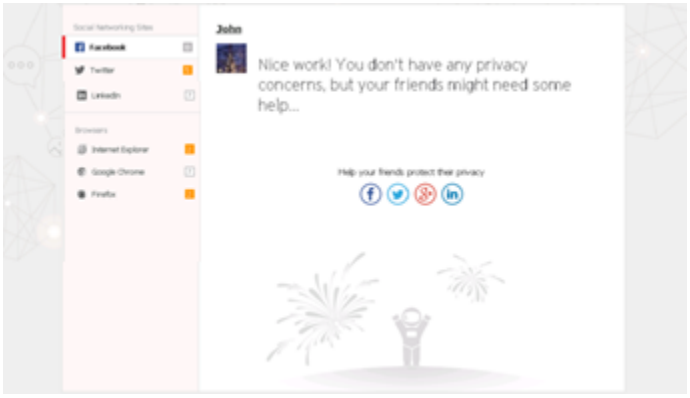

Figure 237. Nice Work! You don't have any privacy concerns.

Twitter Privacy Settings

To check your Twitter Privacy Settings:

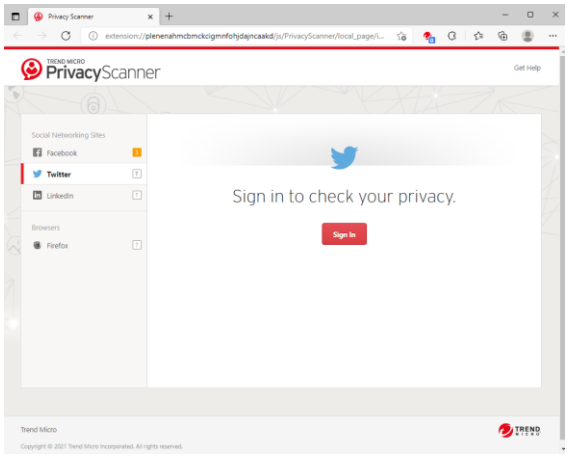

Figure 238. Privacy Scanner | Twitter

1. Click the **Twitter** tab in **Trend Micro Privacy Scanner**. The **Twitter Log In** page opens in your browser. Click the tab to access it.

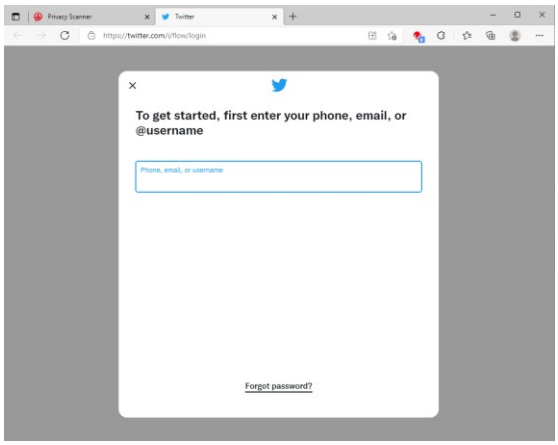

Figure 239. Log in to Twitter

2. Sign in to your Twitter account. Your **Twitter Settings** page appears.

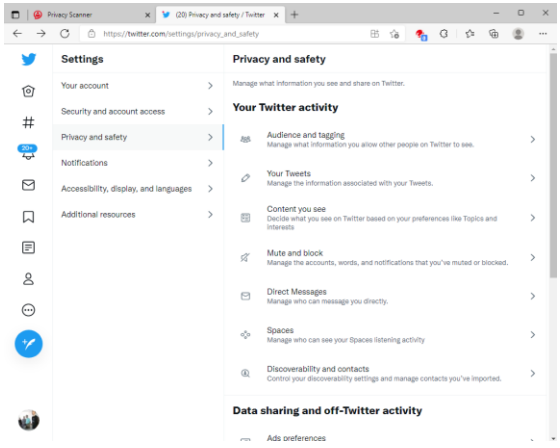

Figure 240. Twitter > Settings

3. Tap the **Privacy Scanner** tab. The Trend Micro Privacy Scanner returns the result.

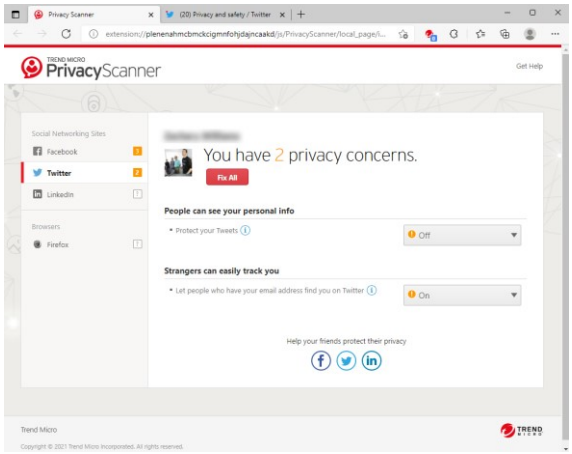

Figure 241. Twitter Privacy Concerns

4. As you did for Facebook, click **Fix All** or use the editor to edit specific settings. The editor appears.

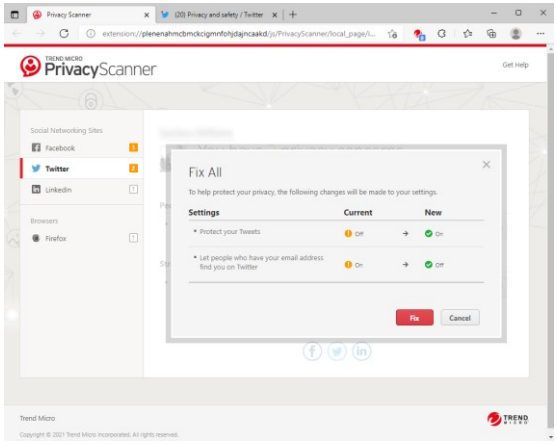

Figure 242. Fix All | Settings

5. The **Privacy Scanner** returns the result: "Nice work! You don't have any privacy concerns, but your friends might need some help…"

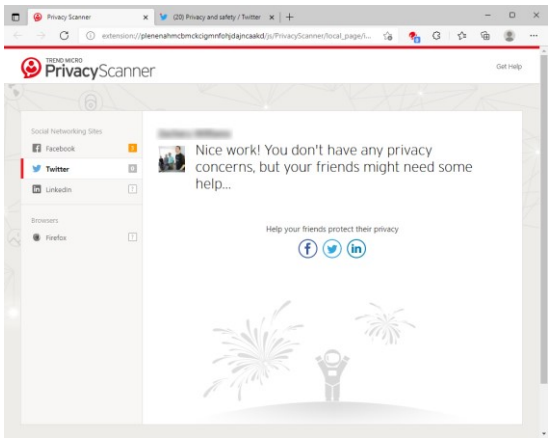

Figure 243. Privacy Scanner: No Privacy Concerns

6. As you did for Facebook, you can click the Twitter icon to post a link to help your friends protect their privacy.

LinkedIn Privacy Settings

To check your LinkedIn Privacy Settings:

1. Click **LinkedIn** in the **Privacy Scanner** list to begin a privacy scan of LinkedIn. The **LinkedIn Sign In** page appears.

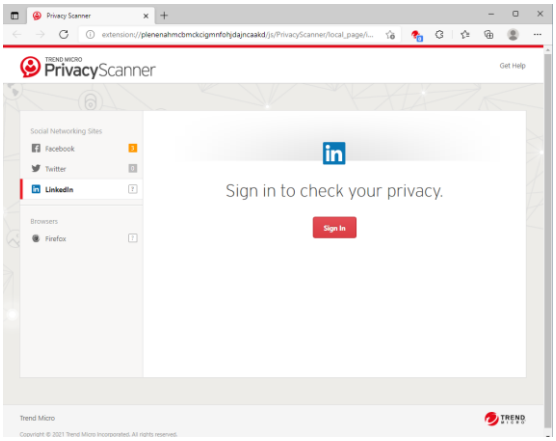

Figure 244. LinkedIn Sign In

2. Click **Sign in** to sign in to Linked In.

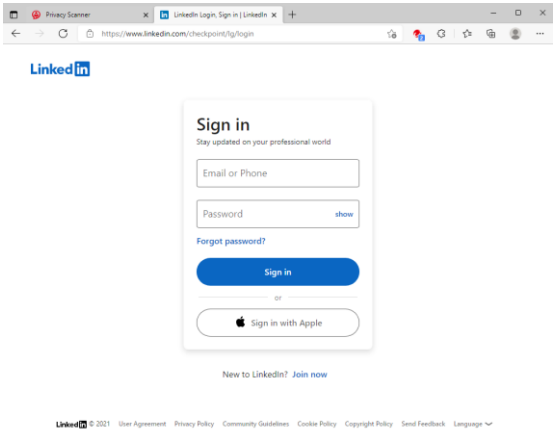

Figure 245. Sign In to LinkedIn

3. Enter your LinkedIn email address and password and click **Sign In.** Linked In opens and a **Privacy Scanner** panel appears in your LinkedIn page.

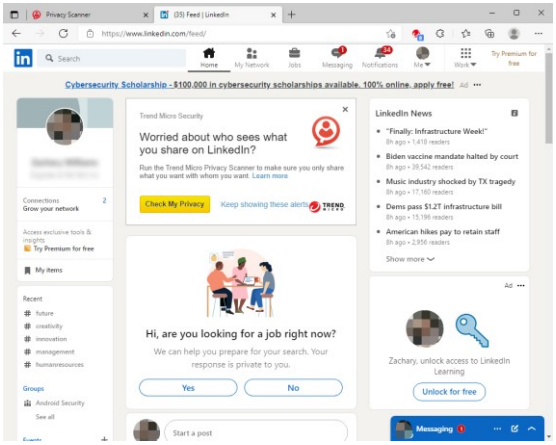

Figure 246. LinkedIn > Check My Privacy

4. Click **Check My Privacy** to begin a privacy scan of LinkedIn. **Privacy Scanner** scans your privacy settings and returns the result.

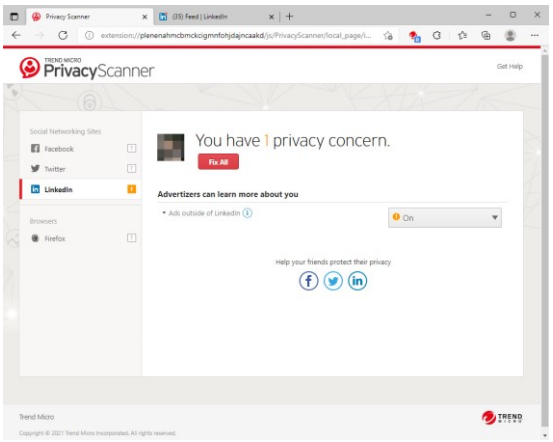

Figure 247. LinkedIn > 4 Privacy Concerns

5. As before click **Fix All** or use the editor to edit each manually. For the **Fix All** option, the **Fix All** dialog appears.

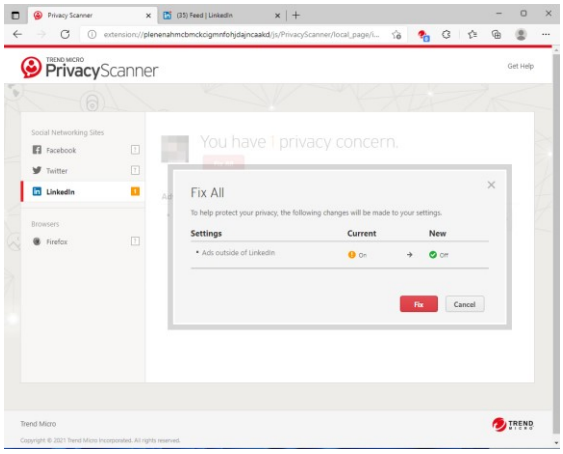

Figure 248. Fix All

6. Click **Fix** to fix all the privacy concerns.

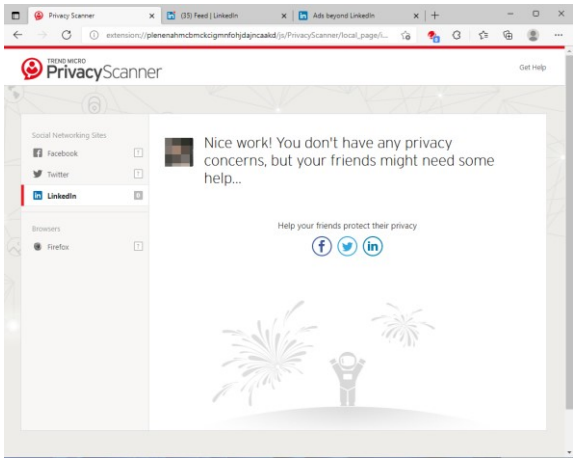

Figure 249. Nice Work! No Privacy Concerns

7. Privacy Scanner returns the result and the familiar “Nice Work!” page appears, where you can again help your friends protect their privacy by clicking the **LinkedIn** icon to post a link.

8. Trend Micro Security provides ongoing protection for Facebook, Twitter, Google+, and LinkedIn. At any time, particularly when the social networking site changes any privacy policies, you can run another **Privacy Scan** on your social networking pages to check your privacy settings.

Web Browser Privacy Settings

Trend Micro Security **Privacy Scanner** scans your Web browsers, including **Microsoft Edge, Internet Explorer, Google Chrome,** and **Mozilla Firefox**, to ensure maximum privacy as you’re browsing the internet.

1. To initiate a browser scan, simply open your preferred Web browser; for example, Microsoft Edge.

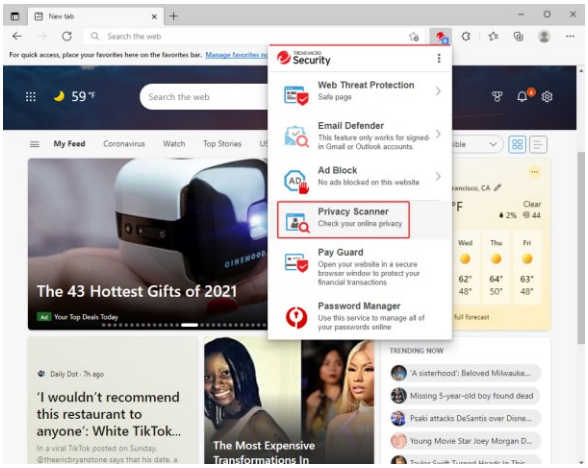

Figure 250. Microsoft Edge

2. In the **Trend Micro Toolbar,** select **Privacy Scanner**. The **Trend Micro Privacy Scanner** portal appears, with **Facebook** selected by default.

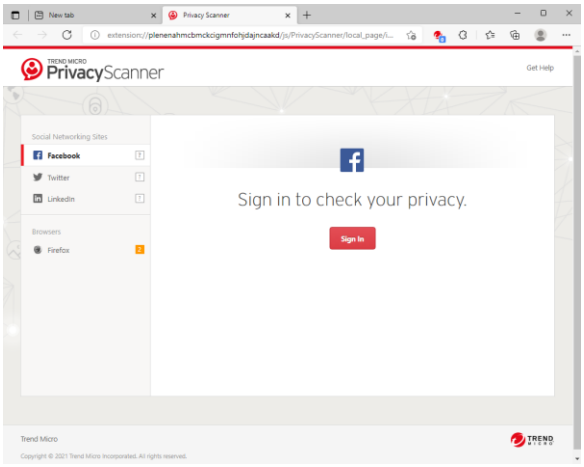

Figure 251. Trend Micro Privacy Scanner Portal

3. Click the installed Web browser you wish to check in the **Browsers** section; for example, **Firefox.** The **Privacy Scanner** shows when you have privacy concerns.

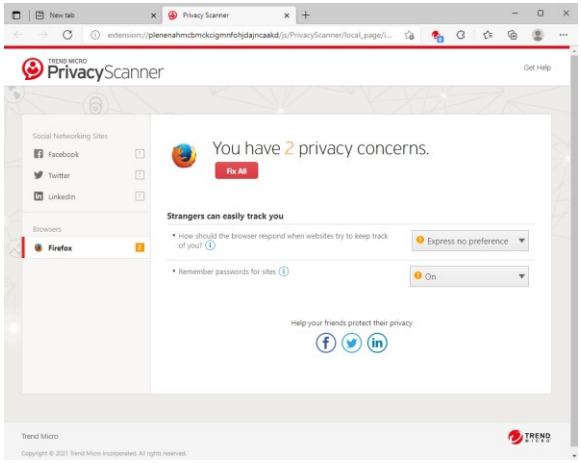

Figure 252. Privacy Scanner > Firefox

4. Click **Fix All** to fix all the privacy concerns, or manually edit them. When you click **Fix All**, the **Fix All** dialog appears.

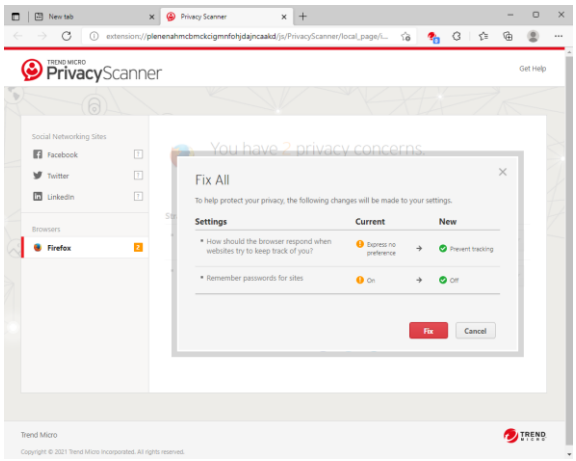

Figure 253. Fix All

5. Click **Fix** to fix the privacy concerns. **Privacy Scanner** resets the privacy settings in your browser.

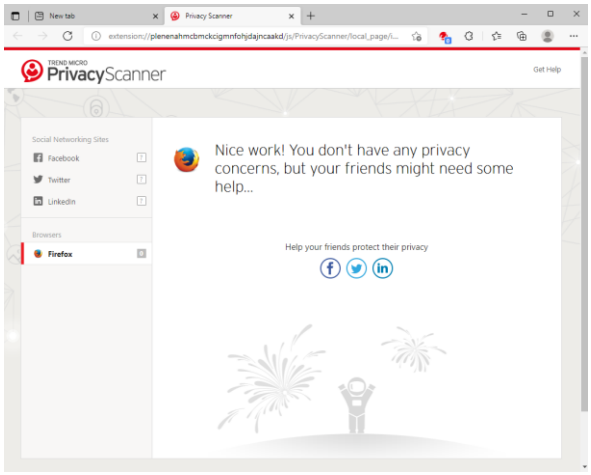

Figure 254. Nice Work!

6. Firefox is more secure with the changed privacy settings, saying "Nice Work! You don't have any privacy concerns, but your friends might need some help…"
7. Repeat this process for each of your installed browsers.
8. Note that you can reset your privacy settings for any supported browser (**Microsoft Edge, Internet Explorer, Chrome,** or **Firefox**) from *within that browser* for any of the *other* supported browsers installed on your computer.

Privacy: Data Theft Prevention

Data Theft Prevention prevents hackers and spyware from stealing sensitive data like credit card numbers, passwords, and email addresses. It can also stop children from accidentally sending out personal information through Outlook email, via instant messaging, or to untrustworthy websites.

To activate **Data Theft Prevention** in Trend Micro Security Internet Security (or Maximum and Premium Security) you must first create an email address and password. See the previous section for **Trend Micro Security Antivirus+** to obtain instructions on doing this.

To activate Data Theft Prevention:

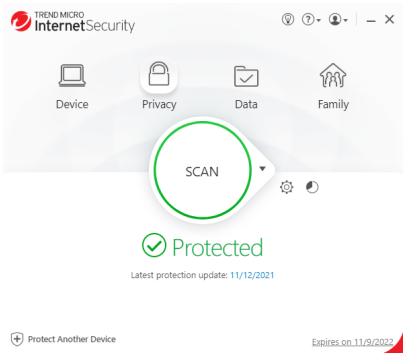

Figure 255. Trend Micro Internet Security Console

1. Click **Privacy** icon in the Console. The **Privacy** screen appears, showing the tools available.

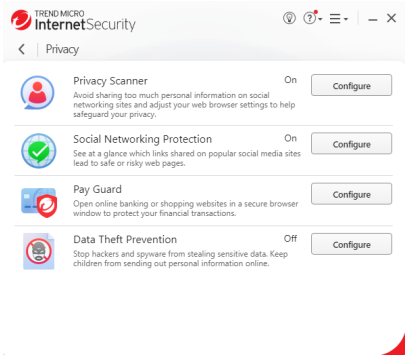

Figure 256. Privacy Options

2. Click **Configure** in the **Data Theft Prevention** panel. Trend Micro Internet Security provides you with an introduction to **Data Theft Prevention.**

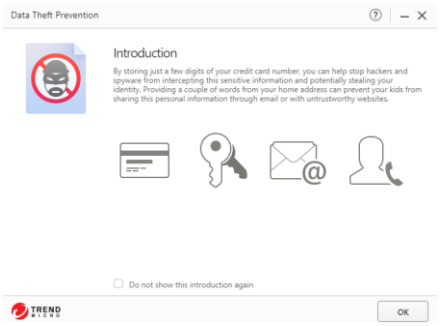

Figure 257. Data Theft Prevention Introduction

3. Click **OK** to close the introduction. The **Password** screen appears. A password is required to use **Data Theft Prevention** or **Parental Controls** in Trend Micro Security.

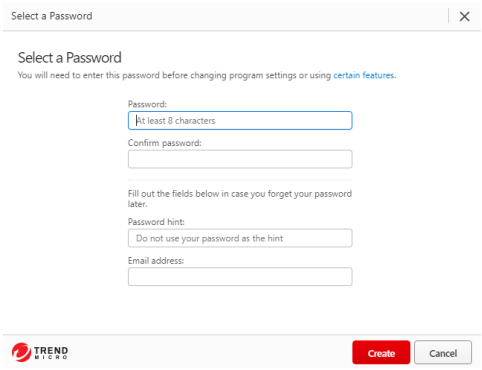

Figure 258. Select a Password

4. Enter a password and confirm it. Fill out the **Password hint** and **Email address**, in case you forget your password later. This will enable Trend Micro to send you a new password. Then click **Create**. The **Data Theft Prevention** settings screen appears, with the toggle set to **Off** by default.

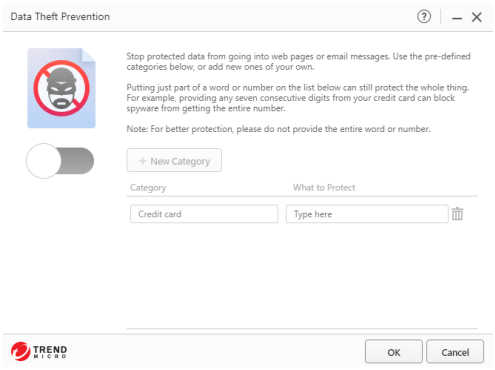

Figure 259. Data Theft Prevention

5. Click the slider to **On** to enable **Data Theft Protection.**
6. Trend Micro Security Internet Security provides you with some suggested categories such as **Phone number** and **Credit card.** You can edit any existing category name by typing over it. For better protection, don't provide the entire word or number.
7. In the **What to Protect** column, type the actual data you wish to protect; for example, in the phone number field you might type 899-999
8. After you save it, Trend Micro Security hides it from view by using asterisks. Simply click in the field to make it visible.
9. Click **+New Category** to add a new category.
10. Click the trashcan in the right-hand column of **What to Protect** to delete any category.
11. Click **Ok** to save your changes.

DTP Limitations

- Data Theft Prevention won't protect the receiving data via POP3 traffic.
- Data Theft Prevention monitors HTTP traffic (ports 80, 81, 8080, and any proxy server port you configure in your Microsoft® Internet Explorer® settings), but not HTTPS traffic (i.e., encrypted information cannot be filtered, such as webmail).
- Data Theft Prevention uses SMTP on TCP port 25/587 and is blocked as spec. TLS and SSL encryption authentication don't block as spec. Most free webmail programs provide TLS and SSL encryption authentication such as Hotmail, Gmail, and Yahoo! Mail.
- Data Theft Prevention doesn't monitor "IMAP" traffic as spec. An IMAP server is generally used with programs such as Microsoft Exchange Server, Hotmail, Gmail, AOL Mail.
- Data Theft Prevention can protect a maximum of 20 entries that have different data and categories.

Data: Secure Erase

Deleting a file just removes the directory information used to find it, not the actual data. The **Secure Erase** function provided in Trend Micro Internet Security (and also in Maximum and Premium Security) overwrites the unwanted file with data, so no one can retrieve the contents; while **Permanent Erase** overwrites the unwanted files making seven passes (overwriting the files 21 times, meeting US Government Security Standards).

To enable Secure Erase / Permanent Erase:

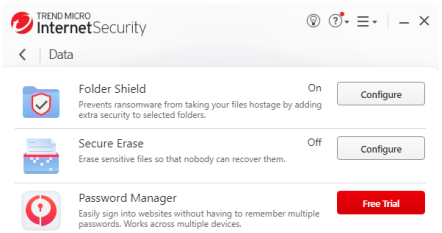

Figure 260. Secure Erase

1. In the main **Console**, click **Data**, then **Configure** for **Secure Erase.** The **Secure Erase Introduction** window appears.

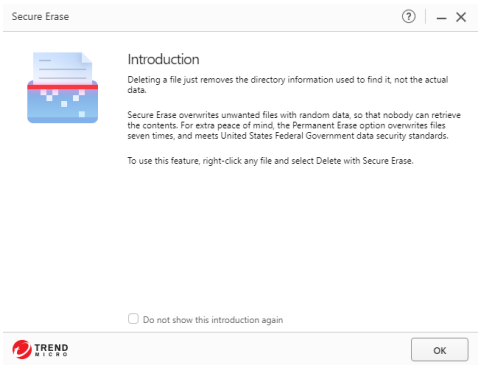

Figure 261. Secure Erase Introduction

2. Click **OK** to close the **Introduction** window. The **Type of Erase** window appears, with **Quick Erase** selected by default.

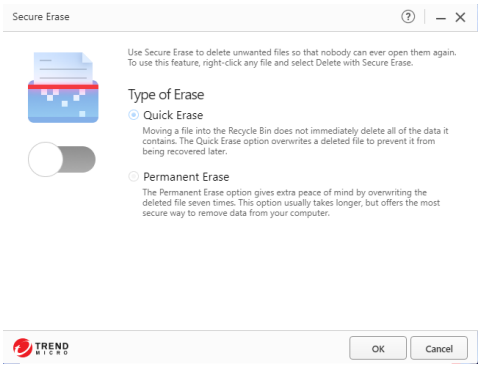

Figure 262. Type of Erase

3. Move the toggle to **On** to enable the function.

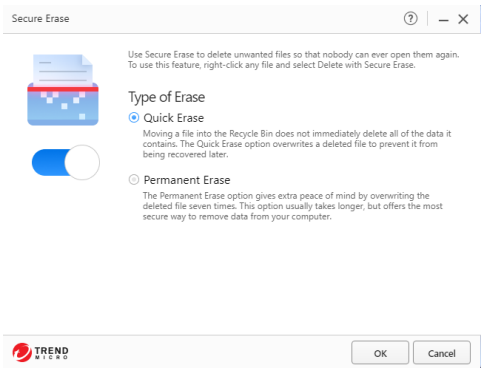

Figure 263. Secure Erase On

4. Keep **Quick Erase** or select the **Permanent Erase** button.
5. Click **OK** to save your changes.

To Secure/Permanent Erase a file:

1. Right-click a folder or file to perform a **Quick/Permanent Erase**. A file processing popup appears. Select **Show more options**.

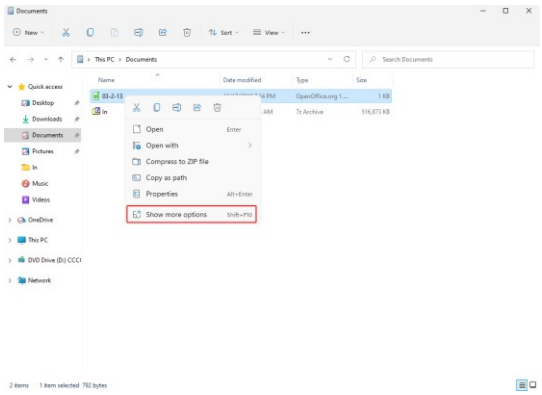

Figure 264. Right-click File > Show more options

2. A file processing popup appears. Select **Show more options**.

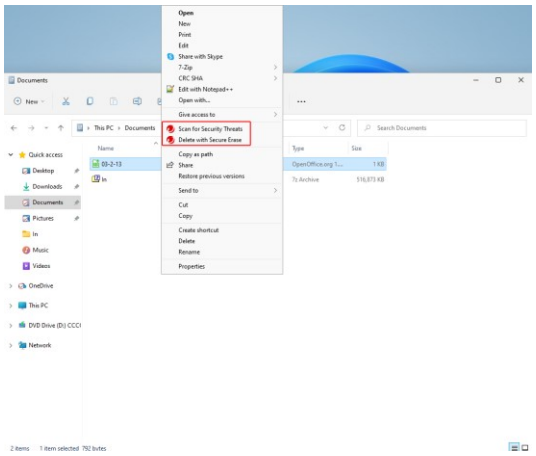

Figure 265. Scan for Security Threats | Delete with Secure Erase

3. Select **Delete with Secure Erase / Permanent Erase.**
4. The folder or file is securely deleted.

Data: Password Manager - Free Trial

Trend Micro™ Password Manager lets you easily sign into websites without having to remember multiple passwords. A **Free Trial for Password Manager**—which allows you to save up to 5 passwords—is available for download from the Trend Micro Internet Security Console.

Note: **A full, unlimited version of Trend Micro Password Manager is automatically installed with Trend Micro Maximum and Premium Security. See the following chapter for details:** **Data: Password Manager - Full Version**

Features include:

- **URL and Password Management -** Automatically capture your websites and password login credentials in a complete secure environment
- **Multi-user Access** – Multiple users can use Password Manager on the same computer.
- **Web Console Management** – Password Manager lets you use a Web Management Console to manage your passwords, notes, and other credentials. The Web Management Console also provides a password strength indicator, to increase the security of your accounts.
- **Cloud Storage and Synchronization -** Credentials are available across all devices where Password Management is installed
- **Password Generator -** Automatically generate strong passwords with custom criteria for increased login security
- **Secure Notes Management -** Store and manage Secure Notes regarding your accounts, logins, and procedures.
- **Password and Data Encryption –** All passwords entered in supported browsers are encrypted. AES 256-bit Encryption ensures the highest security for your data.
- **Secure Browser -** Use the Secure Browser on the PC and Mac to ensure security and privacy for online financial transactions.
- **Profile for Auto-Form Filling -** Create a Profile to enable auto-form filling when filling out online forms.
- **Mobile Support -** iOS and Android smartphones and tablet devices are fully supported.

To Download and Install Password Manager:

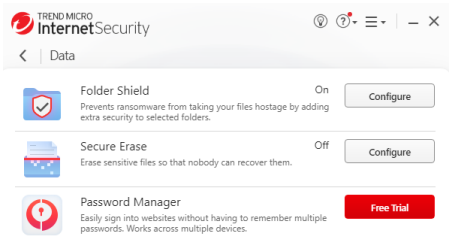

Figure 266. Data > Password Manager Free Trial

5. In the main Console, click **Data**, then **Free Trial** for **Password Manager**. Your default browser launches the **Password Manager Software** page.

Figure 267. Password Manager Software

6. Click **Get it for free.** The **Password Manager Download** page appears.

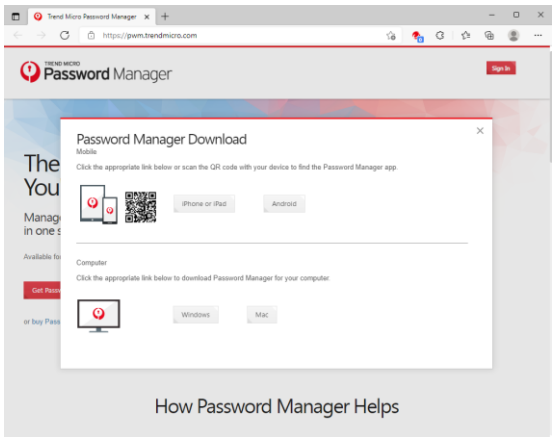

Figure 268. Password Manager Download

7. Choose the platform you're on and click the download button. **Password Manager** downloads. In Microsoft Edge, click **Open file** to install the Password Manager. The **User Account Control** window appears

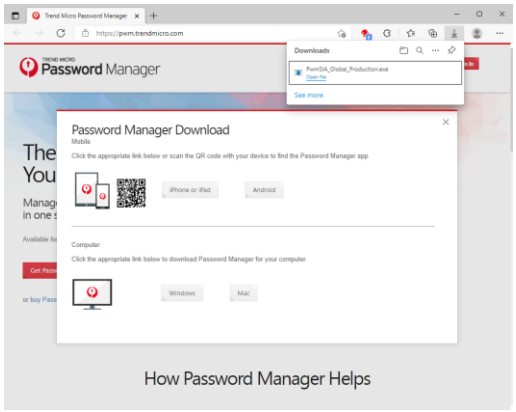

Figure 269. Microsoft Edge – Open file

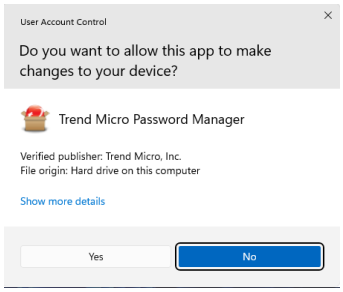

Figure 270. User Account Control

8. Click **Yes** to continue. Password Manager **Downloader** downloads the file.

Figure 271. Password Manager Downloader

9. The installer then presents you with the **Privacy and Personal Data Collection Disclosure.**

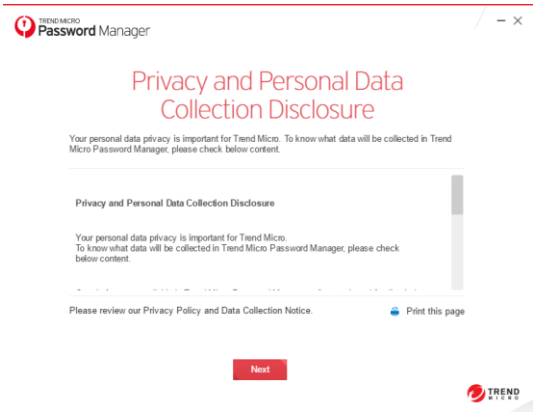

Figure 272. Privacy and Personal Collection Disclosure

10. Read the Privacy and Personal Data Collection Disclosure and click **Next**.

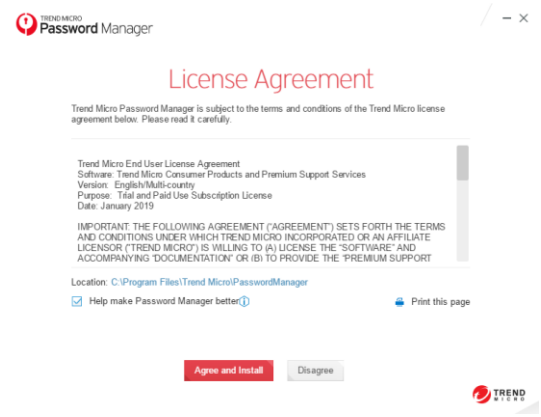

Figure 273. License Agreement

11. The installer picks the default location for installation. You can click the link to change the location, but Trend Micro doesn't recommend this.

12. Note the checkbox **Help make Password manager better** is checked by default. This provides technical data to Trend Micro to help improve the product; no personal data is shared. If you wish to opt out of this feedback, uncheck the checkbox.
13. Read the **License Agreement.** If you agree, click **Agree and install.** The installation proceeds and a progress dialog appear, showing you the progress of the installation.

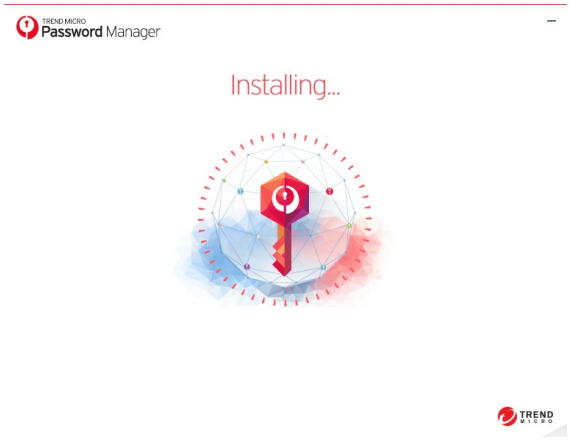

Figure 274. Password Manager Installation Progress

14. When the installation is complete, a wizard appears to help you get started.

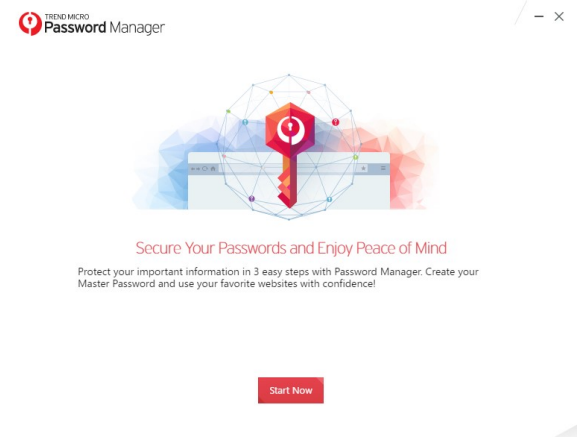

Figure 275. Start Now

15. Click **Start Now** to begin the configuration. A window appears in your preferred browser to get the browser extension.

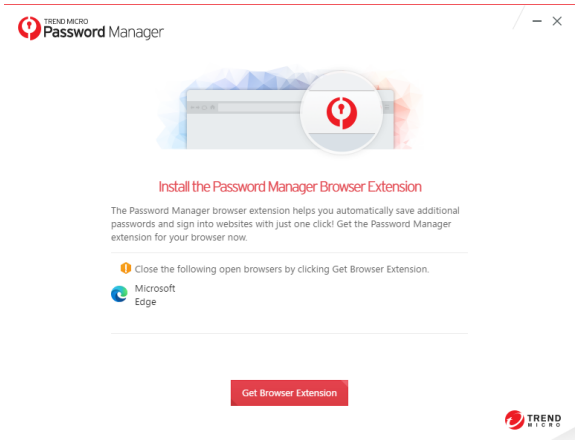

Figure 276. Get Browser Extension

16. Click **Get Browser Extension.** This will close your open browser and begin to install the extension.

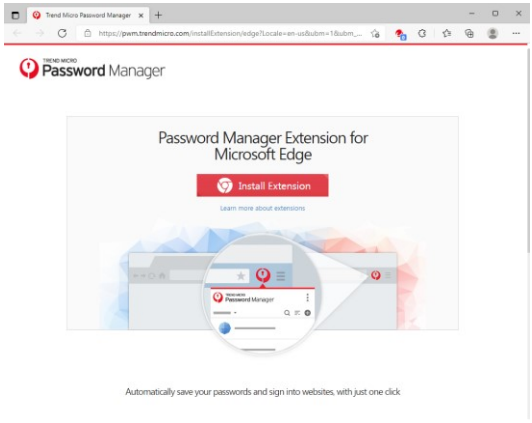

Figure 277. Install Extension

17. The Chrome Web Store page appears. Click **Add to Chrome**.

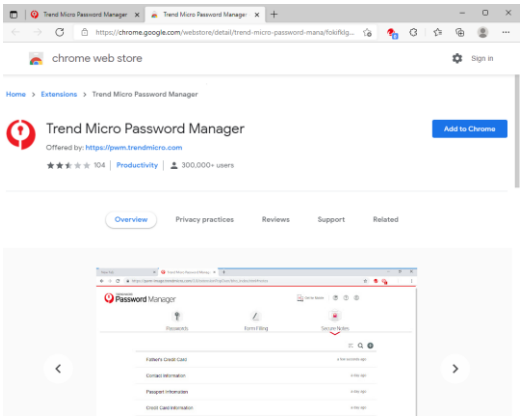

Figure 278. Chrome Web Store - Trend Micro Password Manager

18. Click **Add extension.** A popup appears to add the extension to your browser.

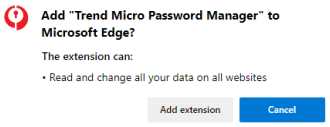

Figure 279. Add Extension

19. Click **Add Extension.** The extension is added to your browser.

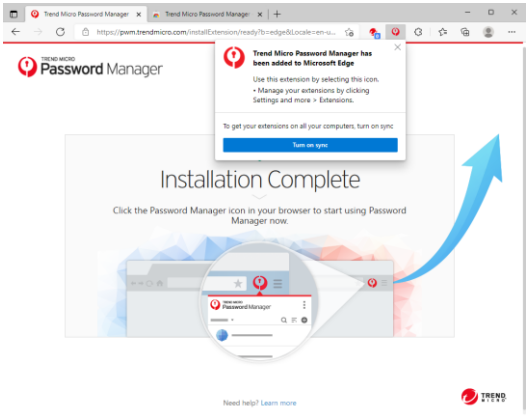

Figure 280. Installation Complete

20. When the installation is complete, a screen appears for you to sign into your **Trend Micro Account.**

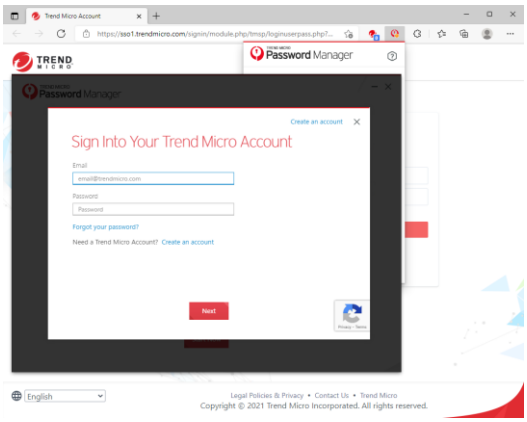

Figure 281. Sign Into Your Trend Micro Account

21. Enter the same email address and password you used to register Trend Micro Internet Security (and to create an account) and click **Next**. (This will facilitate your easy upgrade to a **Paid** edition of Password Manager, should you decide to purchase a subscription.) The **Select Your Version screen** appears.

Figure 282. Use the Free Version

22. **Use the free version** is selected by default. Click **Next**. The **Protect Your Passwords** screen appears.

Figure 283. Protect Your Passwords

23. Click **Next**. The **Create Your Master Password** screen appears.

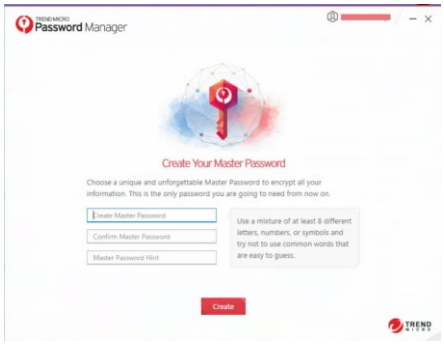

Figure 284. Create Your Master Password

24. Use between 6 and 20 characters and at least two kinds of characters among letters, numbers, and symbols.
25. Confirm your **Master Password** and provide yourself a **Password Hint** to help you remember it and click **Create**. You're now ready to start using Password Manager.
26. Click the **Password Manager** icon in your browser. The **Password Manager** popup appears.

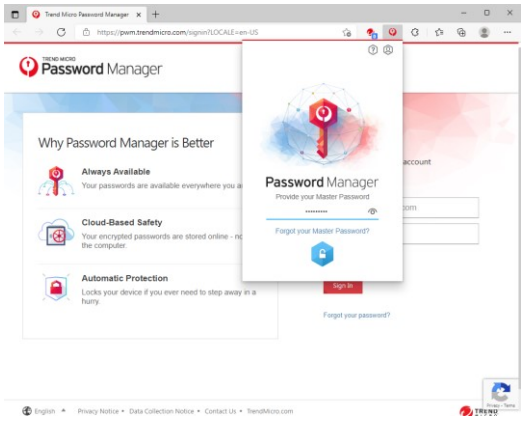

Figure 285. Provide your Master Password

27. Enter your **Master Password** and click the **Lock** icon. The **Password Manager** extension opens, click **Download Now** to install the Password Manager in every device.

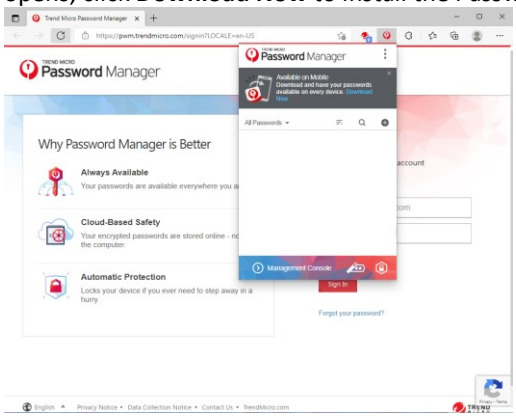

Figure 286. Password Manager Extension

28. For smart phones simply **scan the QR Code** with a code scanner and it will take you to Google Play or the Apple App Store. Click **Windows** or **Mac** for your desktop or laptop devices.

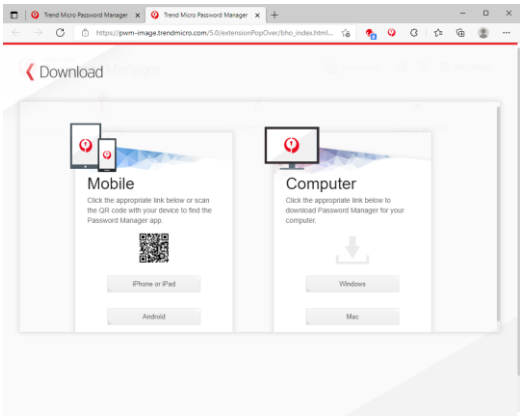

Figure 287. Download

29. Otherwise, simply sign in to any website and Password Manager will save your password—up to 5 passwords for the Free version.
30. For example, go to facebook.com, enter your login ID and password, and sign in.

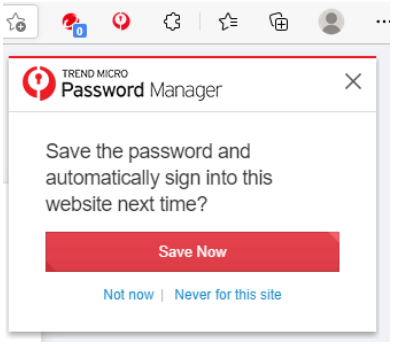

Figure 288. Save Now

31. Password Manager captures your login ID and password. Click **Save Now** to save it to Password Manager.
32. In the future, simply go to the same website login page and Password Manager will prompt you to click **Sign In** to sign into your account.

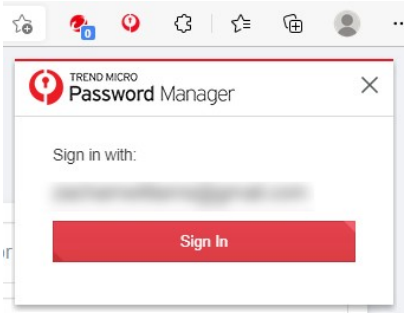

Figure 289. Sign In

33. You may also go directly to Password Manager by clicking the Password Manager icon in your browser. This opens your accounts list. Simply click the account listing to take you to the account webpage, where you can click the above **Sign In** button to sign in.

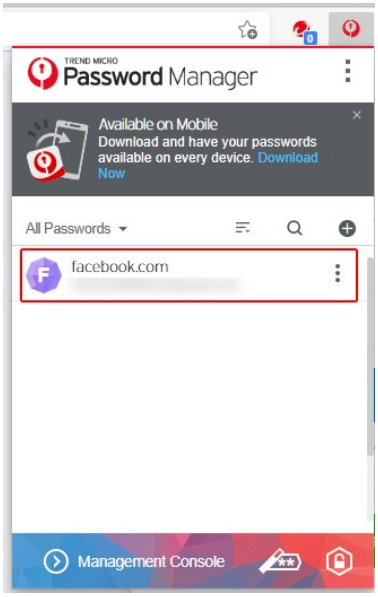

Figure 290. Facebook Captured

34. Repeat the process for up to four additional passwords in the Free version.

NOTE: You can upgrade to a Paid edition of Password Manager at any time and retain your five stored passwords. Upgrading to Trend Micro Maximum or Premium Security will also provide you with a full 1-year subscription to Password Manager.

35. For full instructions on using **Trend Micro Password Manager**, the *Trend Micro™ Password Manager Product Guide* is available for download from the Trend Micro Support site at Trend Micro Password Manager Support.

Family: Parental Controls

The **Parental Controls** tool in Trend Micro Internet and Maximum Security lets you protect your children from inappropriate websites, limit their time on the internet, and see detailed reports about what they do online.

To enable **Parental Controls** in Trend Micro Security Internet Security, you first have to enter an email address and password. See the previous section on **Data Theft Prevention** to obtain instructions on doing this.

Note: **The instructions below are tailored to Windows 11 and 10 users. The process for creating a new user account in Windows 7 or 8.1 is similar, but not identical.**

To enable Parental Controls:

1. Click the **Family** icon in the Trend Micro Security Console. The **Family > Parental Controls** screen appears.

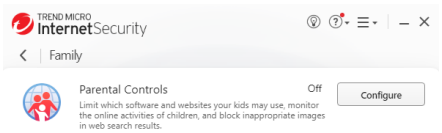

Figure 291. Family > Parental Controls

2. Click **Configure**. The **Parental Controls** Introduction screen appears.

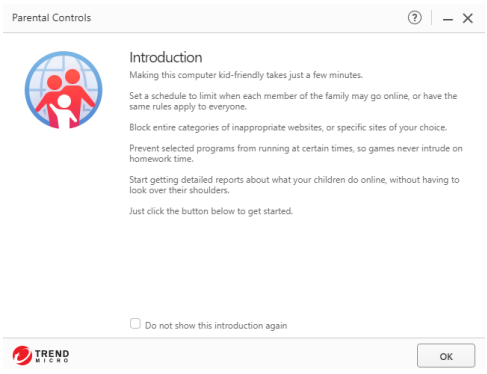

Figure 292. Parental Controls Introduction

3. Read the instructions and click **OK** to continue. A screen appears for you to enter your Password.

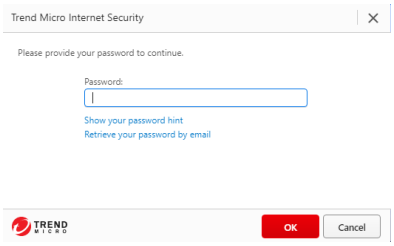

Figure 293. Enter Password

4. Enter your Password and click **OK**. The **Parental Controls Get Started** screen appears.

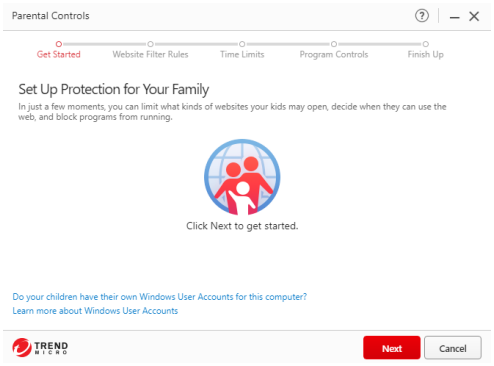

Figure 294. Parental Controls Get Started

5. **Important note**: At the bottom of the screen you're asked **Do your children have their own Windows User Accounts for this computer?** If they don't, click the link on the question to create them, so your various settings can be assigned to the proper child. The **Parental Controls > Add Windows Account** screen appears.

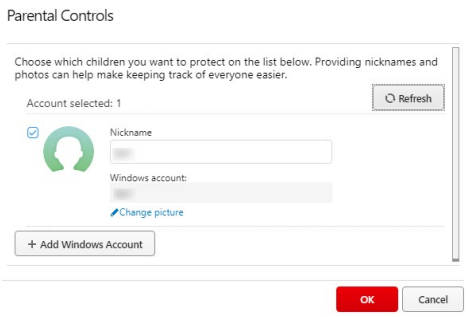

Figure 295. Parental Controls

6. In the lower left-hand corner, click **Add Windows Account.** The **User Accounts** Control Panel appears.

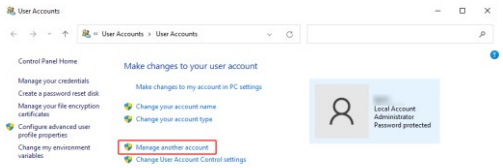

Figure 296. Windows User Accounts

7. Click **Manage another account.** The **Manage Accounts** screen appears.

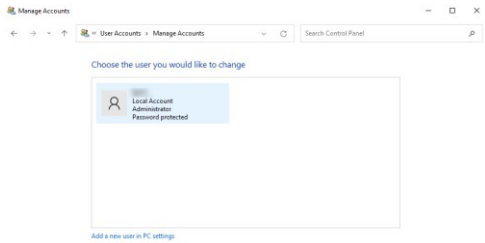

Figure 297. Manage Accounts

8. Click **Add a new user in PC settings.** The **Accounts > Family & other users** screen appears.

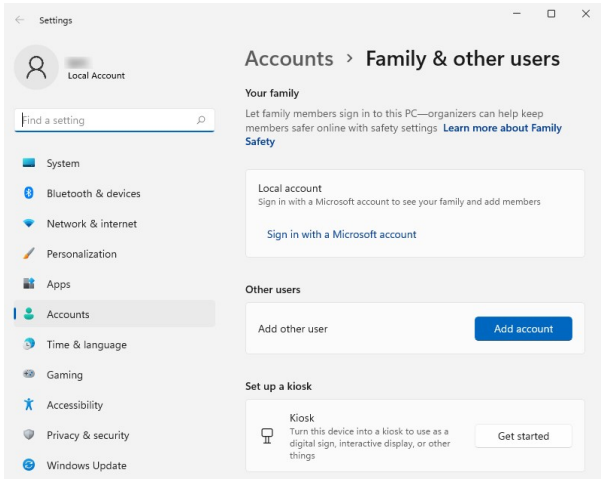

Figure 298. Accounts > Family & other people

9. Click **Add account**. A screen appears, asking “How will this person sign in?”

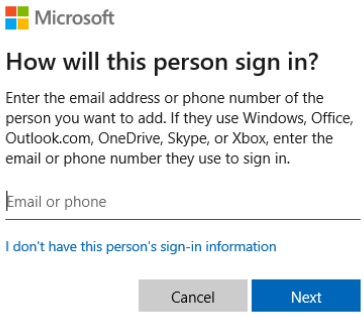

Figure 299. How will this person sign in?

10. To simplify this example, we'll start your child without a Microsoft Account. (You can change to a Microsoft Account later.)
11. Click "**I don't have this person's sign-in information**." The **Create account** screen appears.

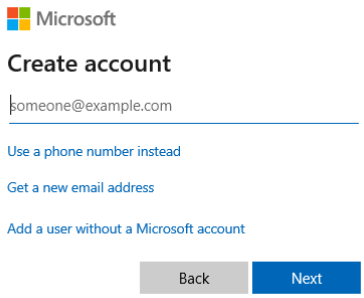

Figure 300. Let's create your account

12. Click **Add a user without a Microsoft account.** A screen appears, saying "Create an account for this PC."

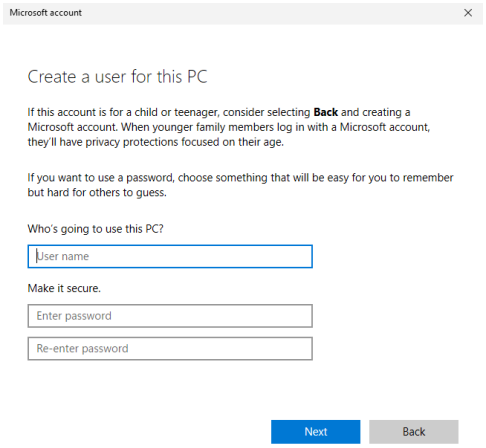

Figure 301. Create an account for this PC

13. Type a name for the account (e.g., Mary), enter a password and confirm it, then provide a password hint and click **Next**. The **Accounts > Family & other users** screen appears, confirming the creation of the account for Mary.

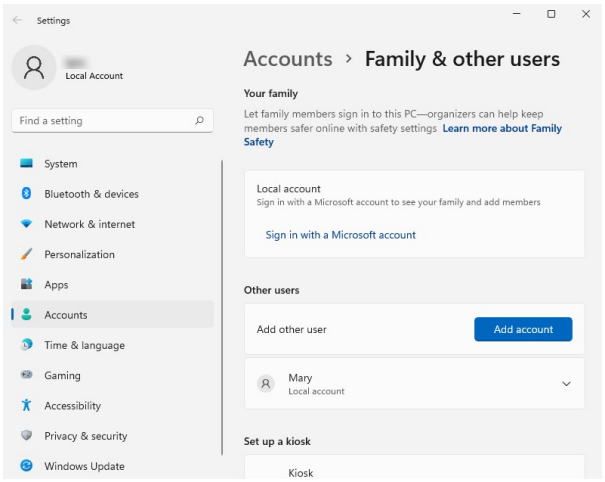

Figure 302. Local Account created

14. Back in the **Manage Accounts** screen, you'll see Mary added to the list of accounts on this PC.

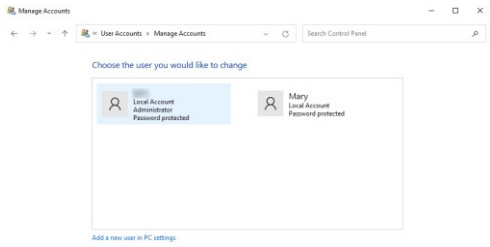

Figure 303. Local Account - Mary

15. Close the **Manage Accounts** window by clicking the **Close Box (X)** in the upper-right-hand corner.
16. Back in the **Parental Controls > Add Windows Account** window, click the **Refresh** link if the new account is not showing**.** The **Mary** account now appears in the list.

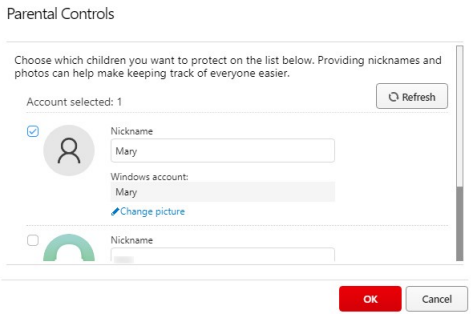

Figure 304. New Windows Account Listed

17. Uncheck the account you're logged on to, check the **Mary** account, and click **OK**. A popup appears, telling you "You have not set the rules for one or more users. Let's set it up now."

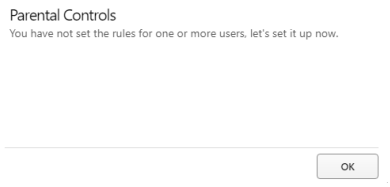

Figure 305. Set Up Rules Popup

18. Click **OK**. The **Website Filter Rules** window appears.

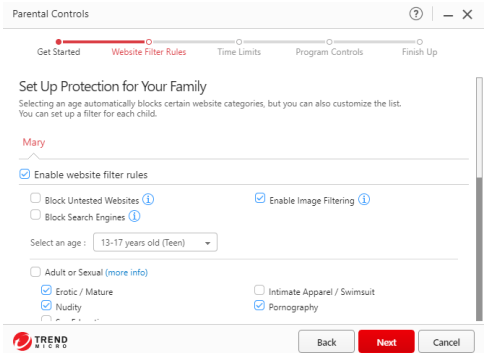

Figure 306. Website Filter Rules

19. Check **Block Untested Websites** if you wish. This will block your children from using websites Trend Micro has not tested yet.

20. In the **Select An Age** popup, choose the age the filter will apply to from the **Select an age** pop-up. For example, choose **Ages 3-7 (Child).** (You can also define a **Custom** age bracket.)

    For a child this age, all categories and subcategories are checked. Scroll down to see the full category/subcategory listings.

    You can check or uncheck a category or subcategory to redefine the filter. You can also obtain more information on a category by clicking the **more info** link; a definition list will pop up.

21. Click **Next** to define the **Time Limits.** The **Time Limits** window appears.

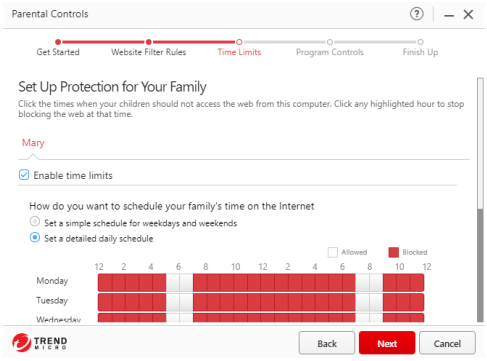

Figure 307. Time Limits

22. Using your mouse pointer, select the weekday and weekend hours your kids **should not** access the web by holding your mouse down and stroking across the hours, then scroll down and indicate the number of hours your children may use this computer.

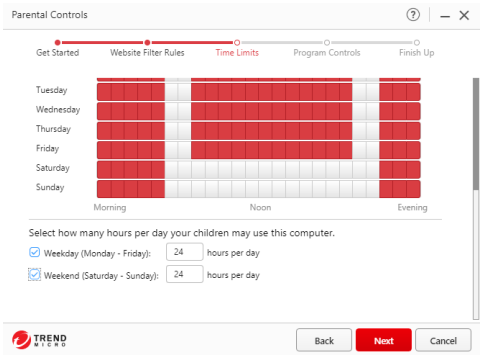

Figure 308. Allowed Hours on Computer

23. Upwards in the window you may also **Set a simple schedule for weekdays and weekends**, applying the same schedule across all days at once.

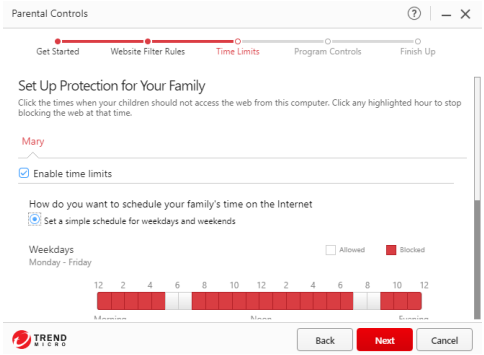

Figure 309. Detailed Daily Schedule

24. Click **Next**. A screen appears, letting you set the child's program controls.

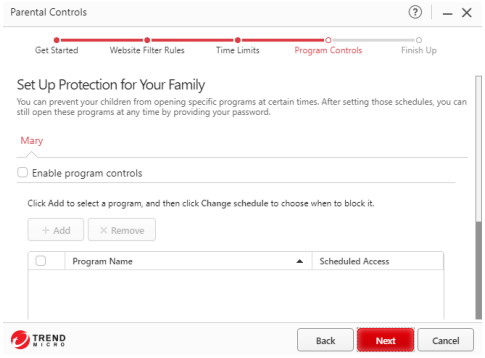

Figure 310. Program Controls

25. Check **Enable program controls**, then click **Add** to add the programs you want to control the usage of.

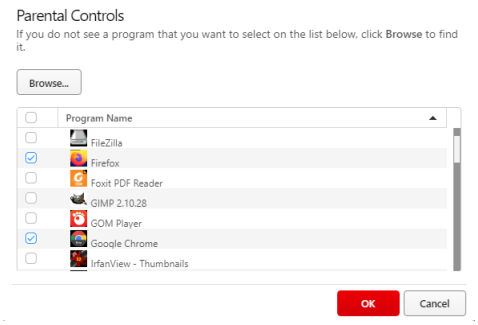

Figure 311. Program List

26. Select the program you want to control from the list, or click **Browse** to find it.

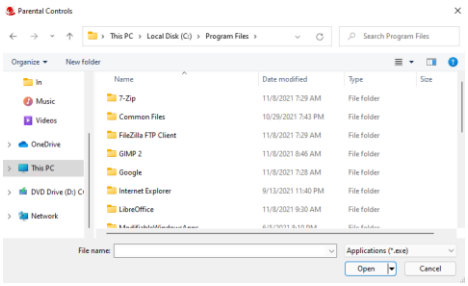

Figure 312. Browsing for Programs to Add to Program Controls

27. Navigate to the program in the **Programs Folder**, select it from its own folder (e.g., Internet Explorer), and click **Open**. Trend Micro Security adds it to the list of controlled programs.

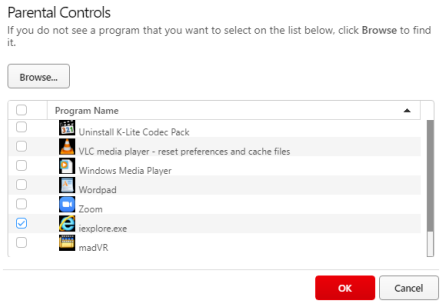

Figure 313. Programs in List | IE Added

28. Check the program checkbox and click **OK**.

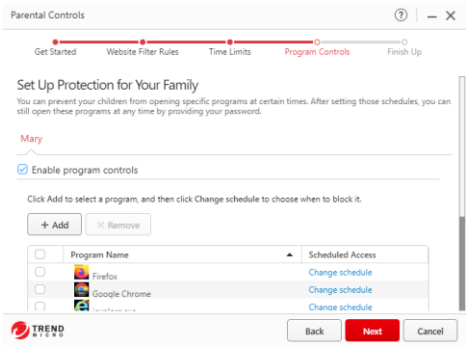

Figure 314. Program List Updated

29. The program is added to the **Parental Controls** window. You can now set the times the program may be used. Click **Change Schedule** in the **Scheduled Access** field. The schedule appears.

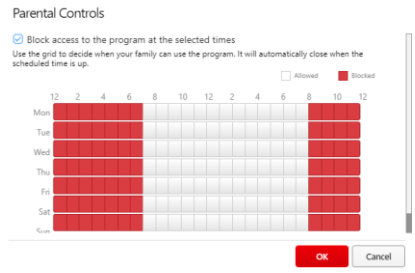

Figure 315. Access Schedule

30. **Block access to the program at the selected times** and **all hours** are selected by default. *Deselect* the hours in the week the child will be permitted use of the program, then click **OK**. When the wizard window appears, click **Next**.

31. A screen appears, indicating that protection has been activated for **Mary**, applying the **Pre-teen Website Filter**, giving the **Time Limits** and **Program Controls**.

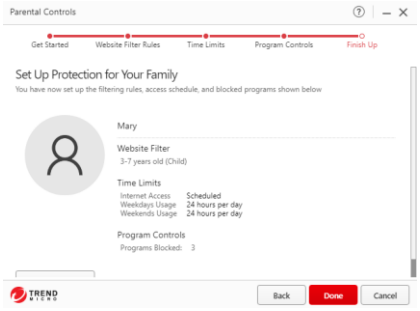

Figure 316. "Mary" Protection Criteria

32. Click **Done** to finish adding the parental control for this child. The main **Parental Controls** window reappears.

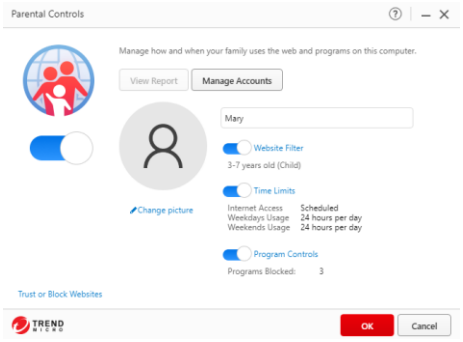

Figure 317. Sliders are "On"

33. In **Parental Controls,** the slider buttons should be **On**. If not, slide to **On**, then click **OK**. The rule set is now applied to the **Mary** account.
34. Note that the link **Trust or Block Websites** allows you to set exceptions to your rules. This function was covered in the previous **Trend Micro Antivirus+ Security** section. Go to Exception Lists: Websites for details.
35. Note also that you can turn the **Website Filter**, **Time Limits,** and **Program Controls** functions on or off by using the appropriate slider. You can also edit the functions by clicking the hotlinks and making your changes in the respective editor.
36. Click **OK** to close the **Parental Controls** window, then click the respective **Close** boxes to close the **Parental Controls** window and the **Trend Micro Security Console.**
37. In the Windows Menu, click **Account Icon**, then select **Mary** to switch to her account; then sign in using the password you created for her account.

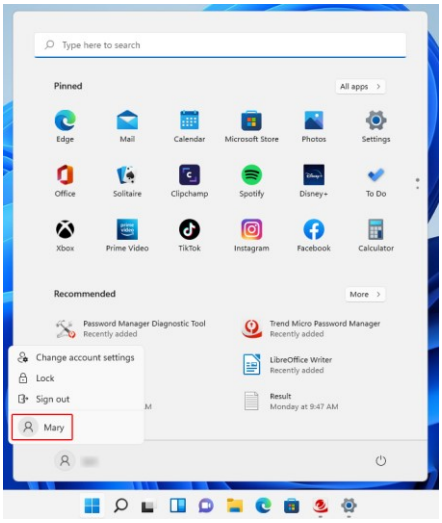

Figure 318. Switching to "Mary" Account

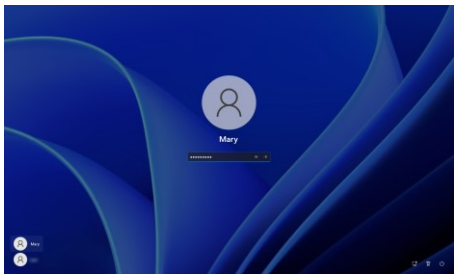

Figure 319. Mary Login

38. Using your browser, attempt to go to a website at a time prohibited by the account rules. Trend Micro Security will block access to the web and provide a **No Web Surfing Allowed** notification, indicating the user cannot use the web at this time.

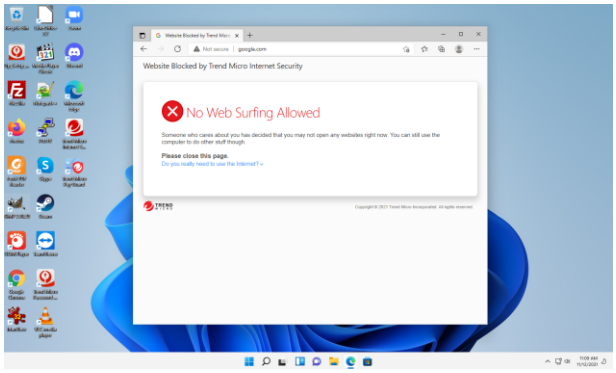

Figure 320. No Web Surfing Allowed

39. During the hours allowed for surfing, if the user attempts to browse to a site not permitted by the rules, Trend Micro Security will block access to the site and provide an **Off Limits** notification for the user in the browser.

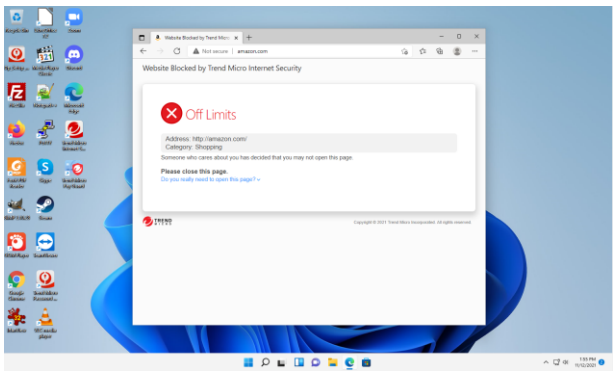

Figure 321. Trend Micro Security Off Limits Notification in Browser

40. If the user tries to use a blocked program during the hours you've chosen to block it, a popup appears saying **Program Accessed Blocked.**

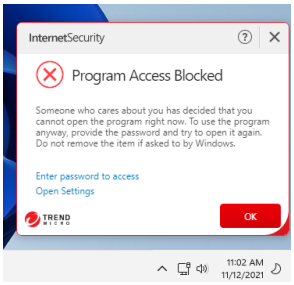

Figure 322. Program Access Blocked

41. Finally, if the user tries to open websites during the hours you've chosen to block internet usage, a popup appears saying **No Web Surfing Allowed**.

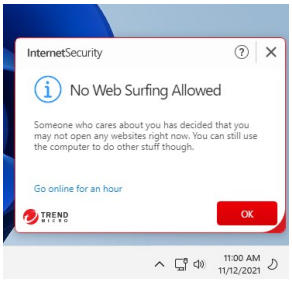

Figure 323. No Web Surfing Allowed

42. If the user knows the Trend Micro Security password on the computer, they can override the block. Naturally, for their own safety, kids being monitored should not be given access to this password.

Security Report: Parental Controls

Once you've enabled Parental Controls, Trend Micro Security Internet Security provides a security report that can give you basic information about how many times your kids have attempted to access prohibited sites and the kinds of website violations they are.

To view the Parental Controls Security Report:

1. Open the Trend Micro Security Console.

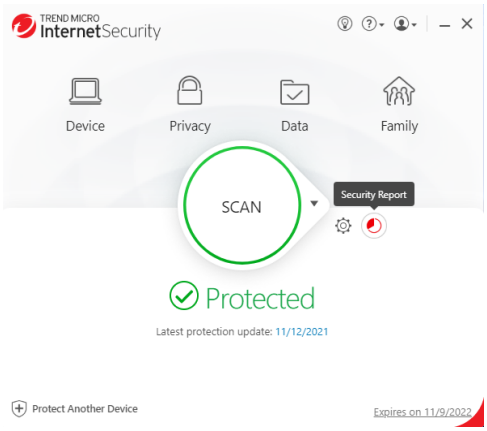

Figure 324. Console > Security Report

2. Click the **Security Report** icon. The **Password** popup appears.

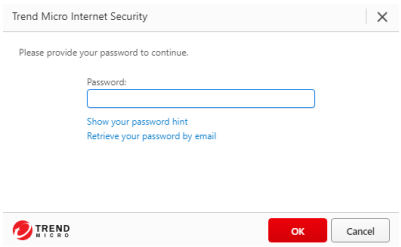

Figure 325. Password Screen

3. Enter your password and click **OK**. The **Security Report** window appears, with **Security Threats** selected by default.

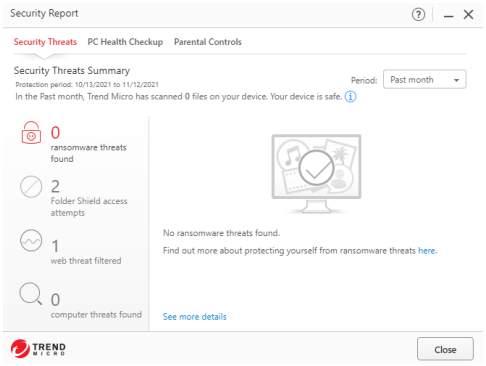

Figure 326. Security Reports > Security Threats

4. Click the **Parental Controls** tab to show the **Parental Controls Security Report**. The **Parental Controls Security Report** appears.

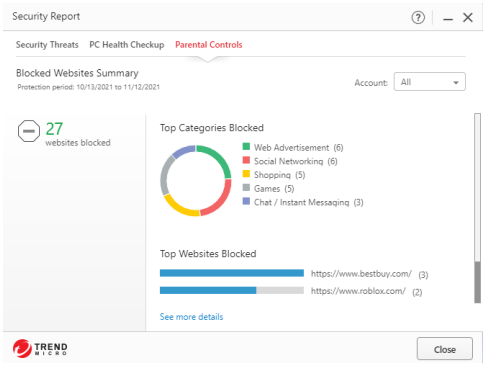

Figure 327. Parental Controls Security Report

5. The report will show the **Top Categories** and **Websites Blocked.** Use the **Account** pop-up to show the report for **All users**, or for a specific user account; e.g., “Mary.”

Note: **The administrator will receive a monthly Security Report via email, which includes Parental Controls data.**

6. Click **See More Details**, to display the **Parental Controls** log.

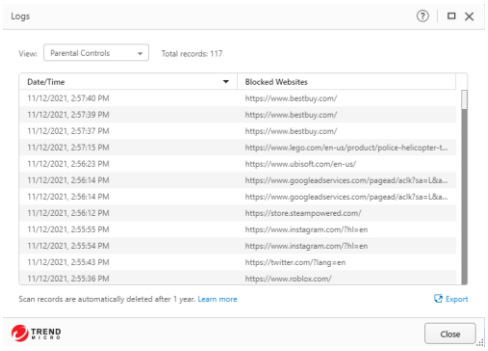

Figure 328. Parental Controls Logs

7. Note that any data older than a year ago will be deleted automatically.
8. Click **Export** to export the Parental Controls log in .CSV or .TXT format.

Chapter 6: Trend Micro Maximum Security

This chapter provides detailed instructions for configuring and using Trend Micro Maximum Security.

Protection Overview

Trend Micro Maximum Security is functionally the most robust edition of Trend Micro Security, providing everything previously described in the Trend Micro Security Antivirus+ and Internet Security chapters, while adding more protections and tools. To enable all its functions, you need a paid version of Trend Micro Maximum Security.

Figure 329. Trend Micro Maximum Security - Welcome Screen

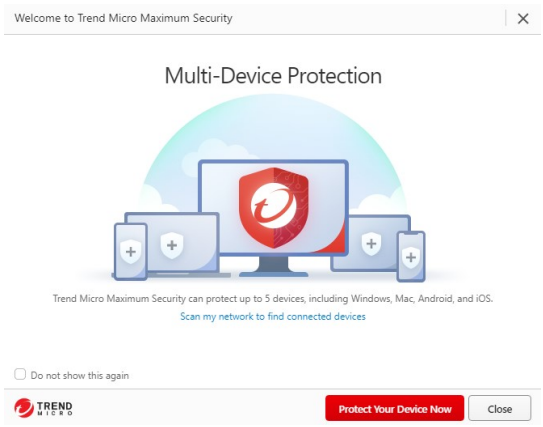

Figure 330. Trend Micro Maximum Security - Protect Another Device Now

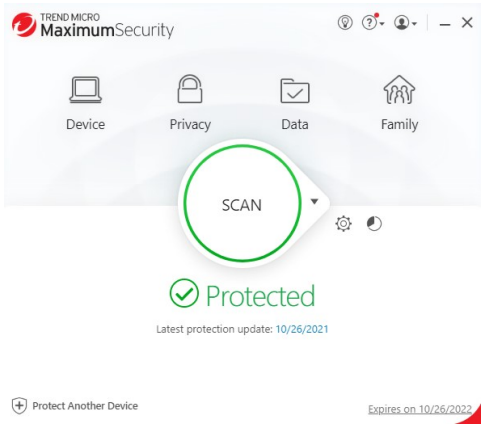

Figure 331. Trend Micro Maximum Security Console

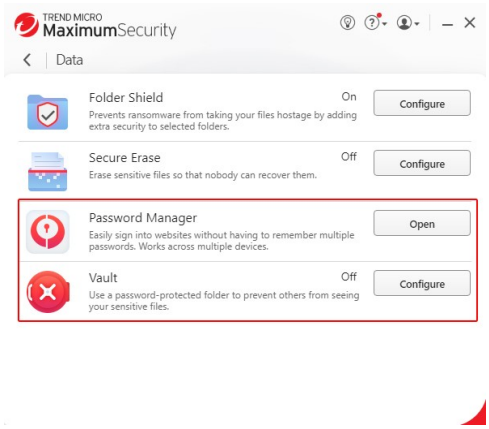

Figure 332. Data > Password Manager | Vault

Note: **Trend Micro Maximum Security's Additional Features:**

Data: Password Manager (auto-installed) and Vault.

Additional Seats: Trend Micro Security Maximum users can also protect from five to ten devices, depending on the purchase level, choosing among PC, Mac, Android, and iOS devices.

ADDITIONAL TOOLS FOR TREND MICRO SECURITY MAXIMUM SECURITY PAID VERSION

Password Manager – Auto-installed

Your installation of Trend Micro Maximum or Premium Security also auto-installs a copy of Trend Micro Password Manager onto your computer. Using Password Manager, you can easily sign into websites without having to remember multiple passwords. Generate strong passwords that are harder to crack and replace weak ones that you're using because they're easy to remember. Use the Secure Browser to access banking and other financial sites, to protect yourself against keyloggers.

Vault

Users can enable a password-protected folder that can secure sensitive files. If the computer is lost or stolen, the vault can be sealed shut by remote control until the computer is returned to its rightful owner.

Device: Protect Another Device

Trend Micro Maximum Security provides a subscription for five to ten devices, depending on the subscription, across Windows, Mac, Android, and iOS devices.

Go to Protect Another Device: PCs, Macs, Android and iOS Mobile Devices for more details.

Data: Password Manager - Full Version

Trend Micro™ Password Manager helps you manage and secure all your online credentials, ensuring an easy and safe online experience, while offering a faster, more secure, and convenient way to access web sites. Using a single Master Password, users have instant access to all their login credentials, no matter where they're located or what device they're using.

A full 1-year subscription of Password Manager is auto-installed with Trend Micro Maximum Security. You can opt out of the auto-installation.

To Start Using Password Manager:

Note: **The instructions below assume you registered Trend Micro Maximum Security when you installed it, creating a Trend Micro Account, and you're signed in.**

1. Open the **Trend Micro Security Console** and click the **Data** icon. The **Data** screen appears.

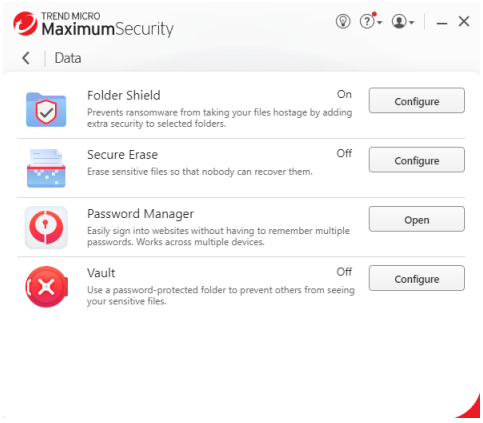

Figure 333. Data > Password Manager > Open

2. Click **Open** in the **Password Manager** panel. The **Password Manager Introduction** screen appears.

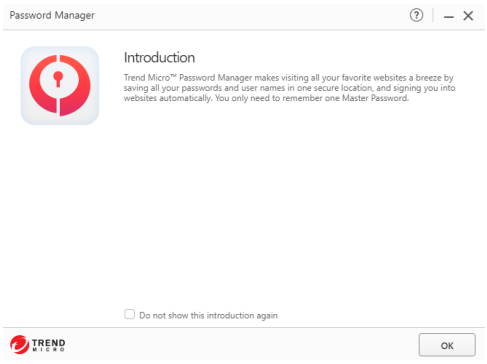

Figure 334. Password Manager Introduction

3. You may check “Do not show this introduction again” if you choose. Click **OK** to close the introduction. A screen appears to **Secure Your Passwords and Enjoy Peace of Mind.**

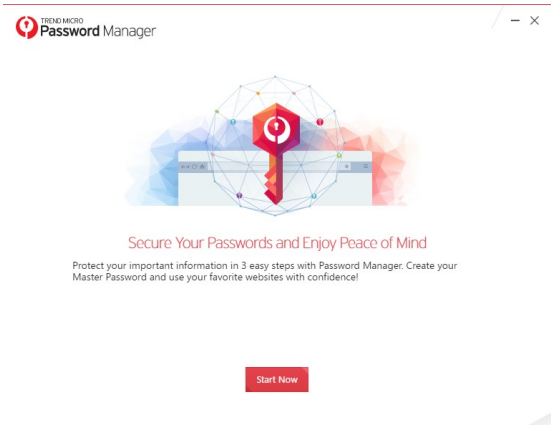

Figure 335. Secure Your Passwords and Enjoy Peace of Mind

4. Click **Start Now.** A screen appears to **Protect Your Passwords with Password Manager.**

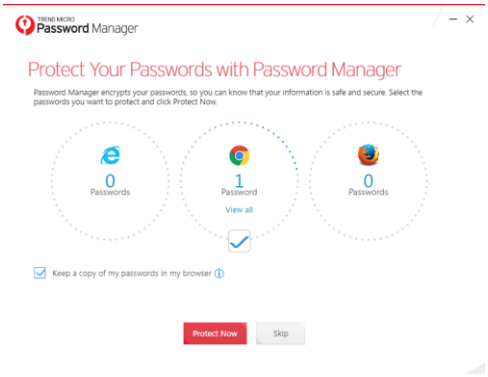

Figure 336. Protect Your Passwords with Password Manager

5. This screen will import your browser passwords into Password Manager. Trend Micro recommends you uncheck the option “Keep a copy of my passwords in my browser.”
6. Click **Protect Now.** A window appears for you to **Create Your Master Password.**

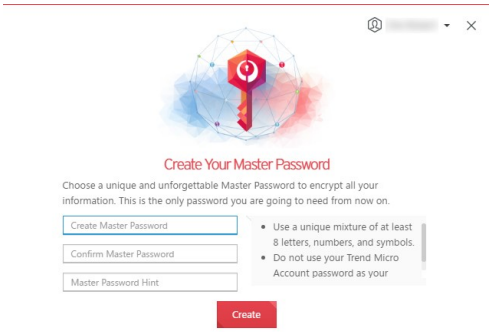

Figure 337. Create Your Master Password

7. Use a mixture of at least 8 different letters, numbers, or symbols and try not to use common words that are easy to guess, then provide yourself a hint and click **Create**. A window appears for you to get the Password Manager browser extension.

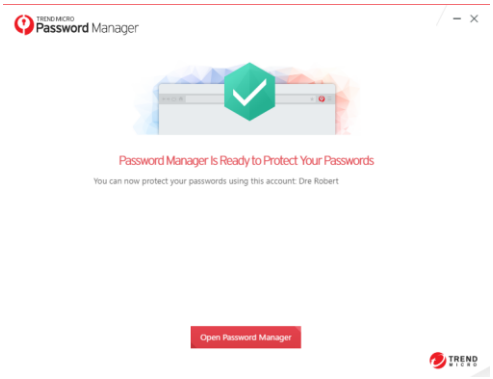

Figure 338. Open Password Manager

8. Click **Open Password Manager**. Your default browser opens for you to install the extension (in this case Microsoft Edge) and a popup appears to install Password Manager Extension in Microsoft Edge.

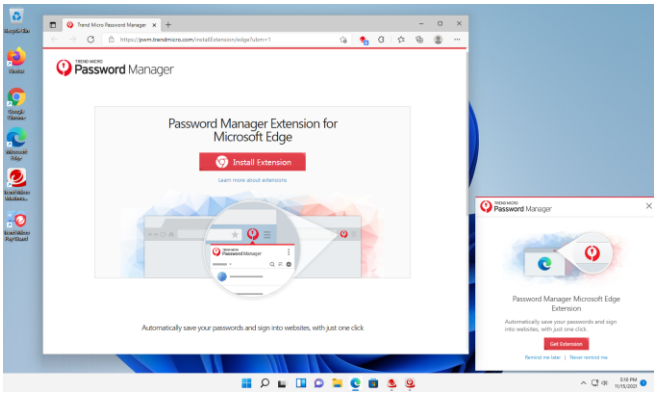

Figure 339. Install Password Manager Extension (for Edge)

9. Click **Install Extension.** The **Chrome Web Store** appears.

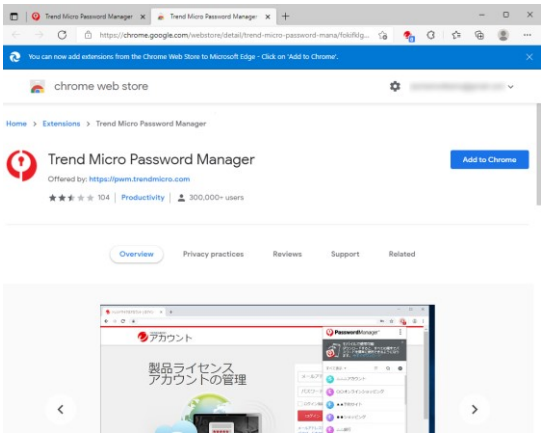

Figure 340. Chrome Web Store | Trend Micro Password Manager

10. Click **Add to Chrome**. A popup appears to add the extension.

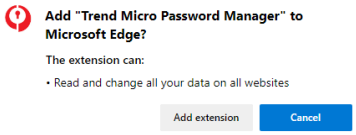

Figure 341. Add Extension

11. Click **Add Extension.** The Password Manager extension is added to your browser.

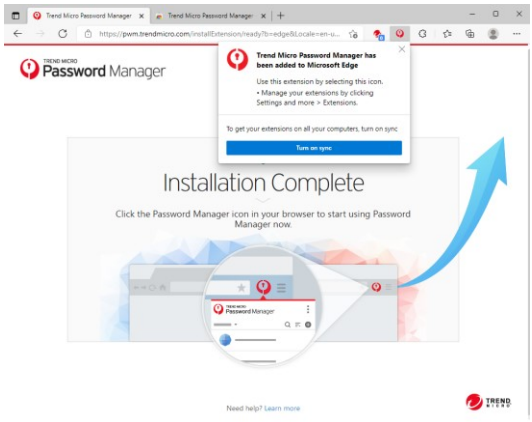

Figure 342. Installation Complete

12. Click the icon to see the active **Password Manager** extension in your browser.

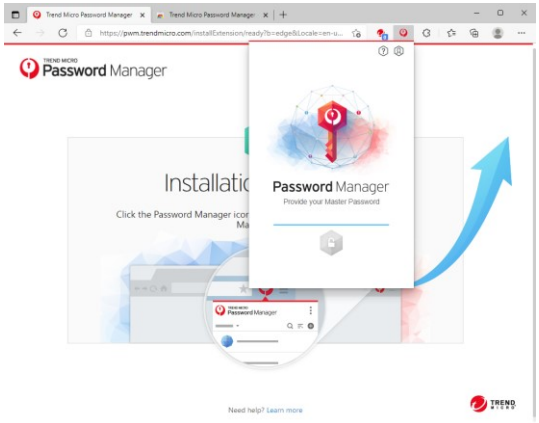

Figure 343. Provide your Master Password

13. Provide your **Master Password**, then click the **Unlock** icon to log in.

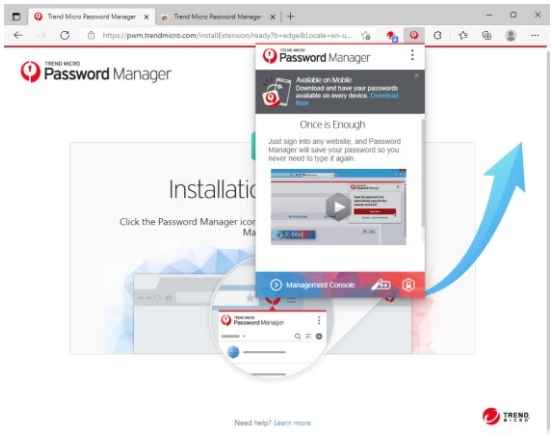

Figure 344. Password Manager Extension

14. The **Password Manager** extension opens. Click **Download Now** to install Password Manager to other devices.

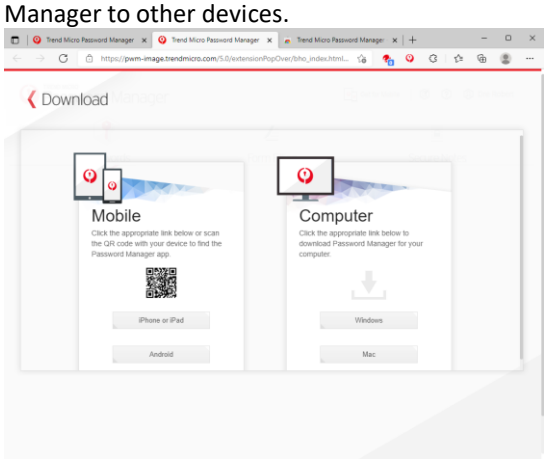

Figure 345. Download

15. The **Password Manager** Download page opens, with a QR code to download Password Manager to your smartphone. Simply scan the QR Code with a code scanner and it will take you to Google Play or the Apple App Store. Click the **Windows** or **Mac** link for desktop and laptop devices.

16. A two-factor authentication notification appears in the Password Manager Extension if the said security feature is not enabled.

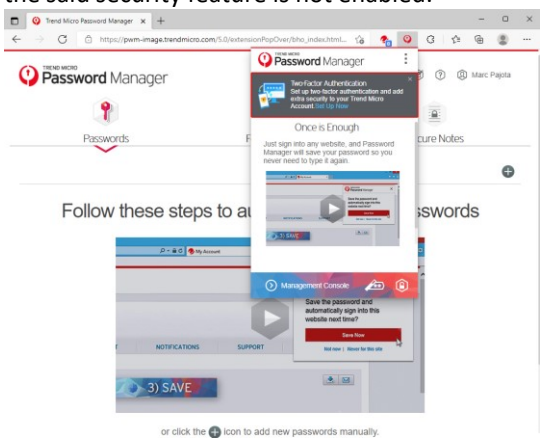

Figure 346. Two-Factor Authentication Notification

17. Click **Set Up Now**. The Trend Micro Account Sign In page appears. Input your Trend Micro Account and click **Sign In**.

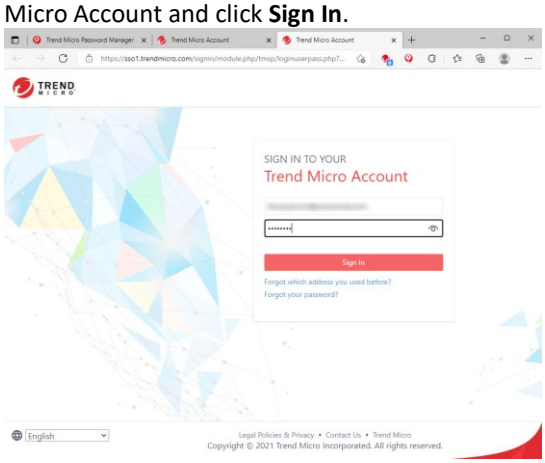

Figure 347. Trend Micro Account Login Page

18. The Trend Micro Account dashboard page appears. Click the **Profile** tab.

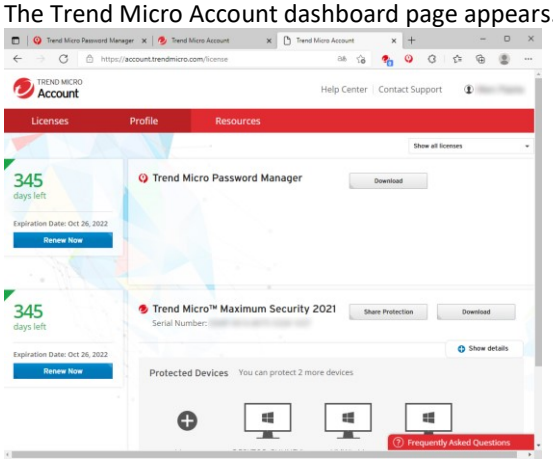

Figure 348. Trend Micro Account Dashboard

19. The Account Profile page appears. Click Two-factor Authentication.

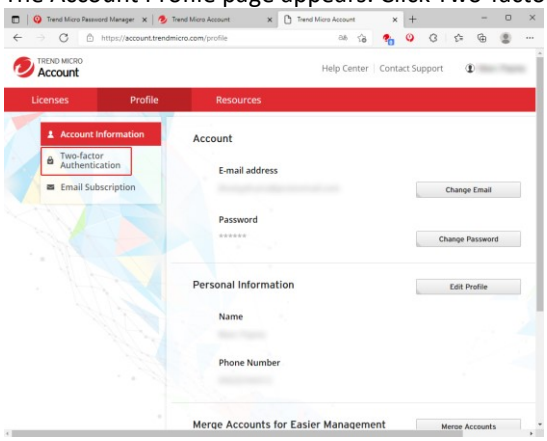

Figure 349. Trend Micro Account Dashboard | Profile

20. The **Set Up Two-factor Authentication** page appears. The two-factor authentication is an added security for your Trend Micro Account by sending first a confirmation code to

your email address or mobile device when you try to sign in.

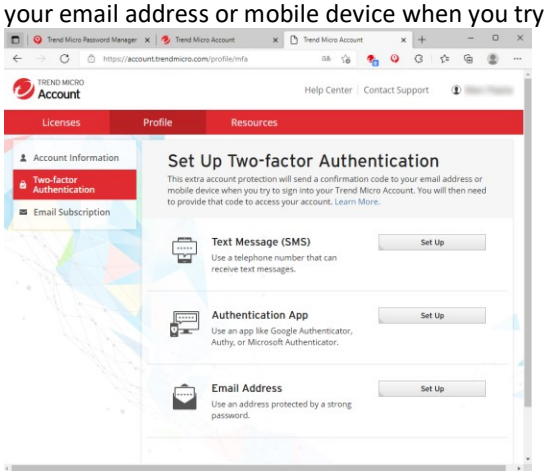

Figure 350. Set Up Two-Factor Authentication

21. Two-factor authentication can be set up via SMS, authentication programs like Google Authenticator, or an email address. Launch your selected mode by clicking **Set Up** and following the on-screen instructions.

Install Password Manager in Pay Guard

To Install Password Manager in Pay Guard:

1. Once you've activated your **Trend Micro Password Manager** account as given above, you may also install **Password Manager** in **Pay Guard**.
2. Double-click the **Pay Guard** icon on your Desktop. The **Pay Guard** window appears, with a popup window suggesting **Add the Password Manager extension to Pay Guard to access your passwords. Browser will restart.**

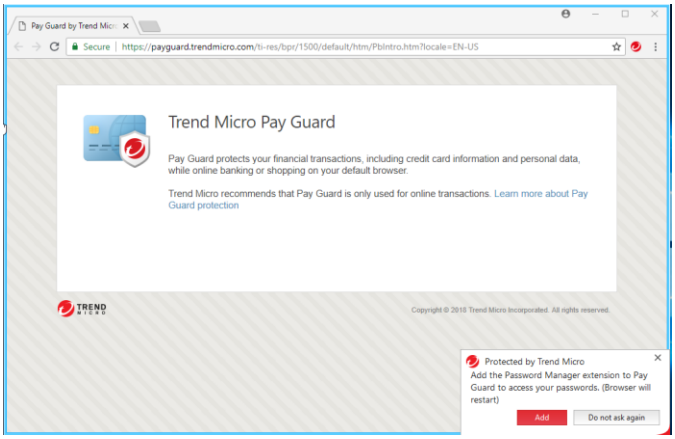

Figure 351. Pay Guard > Install Password Manager

3. Click **Add** to add the Password Manager extension. A window open for you to install the extension.

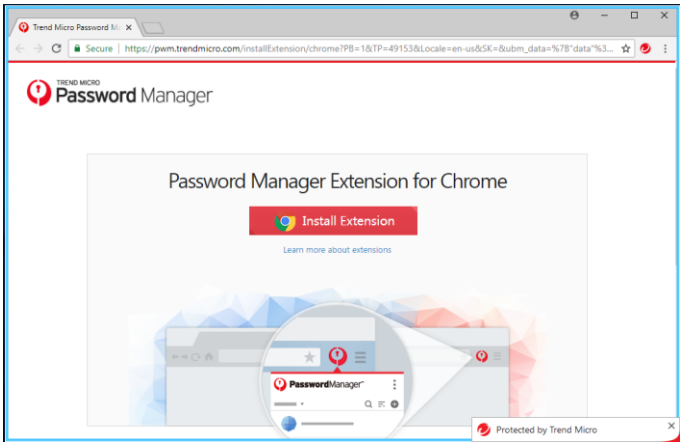

Figure 352. Install Extension

4. Click **Install Extension.** In our example, because Chrome is the default browser, you're taken to the Chrome store to install the extension.

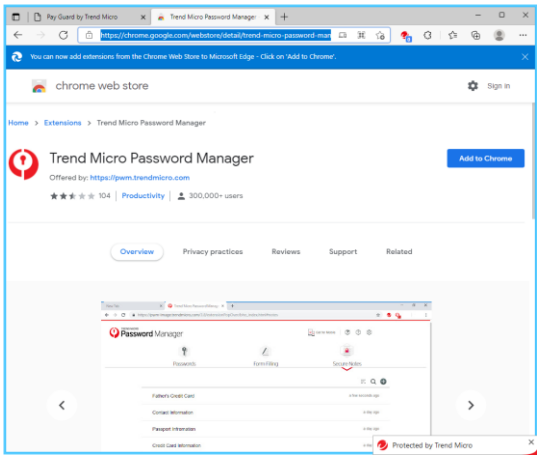

Figure 353. Add Password Manager

5. Click **Add to Chrome.** A popup appears, asking **Add "Trend Micro Password Manager"?**

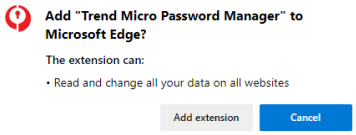

Figure 354. Add Extension

6. Click the **Add extension** button. The **Password Manager** extension installs and reboots your **Pay Guard** browser, showing **Installation Complete.**

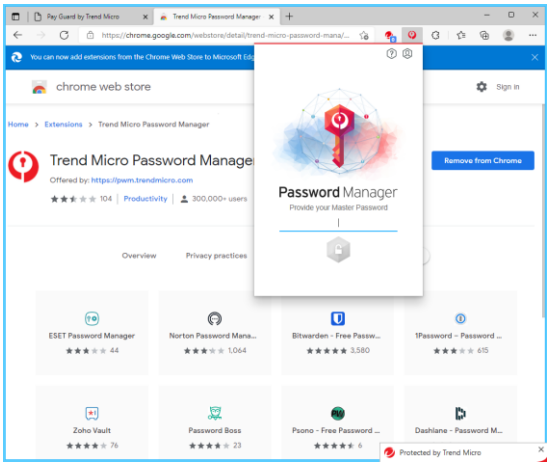

Figure 355. Installation Complete

7. You're now ready to use Password Manager in your full default browser or in **Pay Guard.**

Using Password Manager

To Use Password Manager:

1. Using your default browser or **Pay Guard**, simply sign in to any website and **Password Manager** will save your password.
2. For example, go to www.facebook.com.com, enter your login ID and password, and sign in.

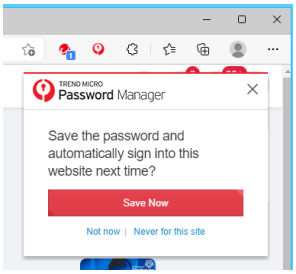

Figure 356. Save Now

3. Password Manager captures your login ID and password. Click **Save Now** to save it to Password Manager.
4. In the future, simply go to the same website login page and Password Manager will prompt you to click **Sign In** to sign into your account.

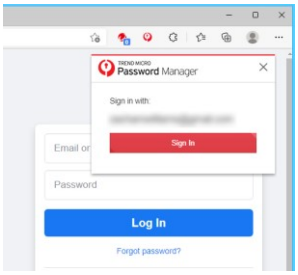

Figure 357. Sign In

5. You may also go directly to Password Manager by clicking the Password Manager icon in your browser. This opens your accounts list. Simply click the account listing to take you to the account webpage, where you can click the above **Sign In** button to sign in.

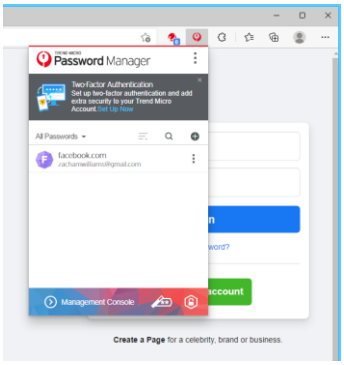

Figure 358. Facebook Captured

6. Note, that you can also import passwords from your browser by clicking the **Tools** icon in the upper-right corner and selecting **Settings.**

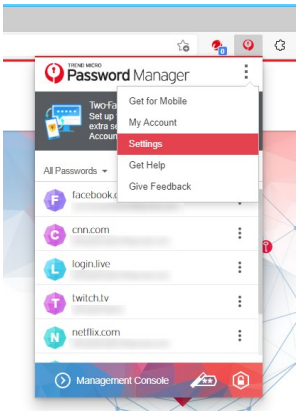

Figure 359. Password Manager > Tools > Settings

7. The **Settings** page appears. Click **Data**. To export all your passwords, form filling data and secure notes click **Export**. Take note that Password Manager does not protect the

exported file. To import saved passwords from other password managers click **Import**.

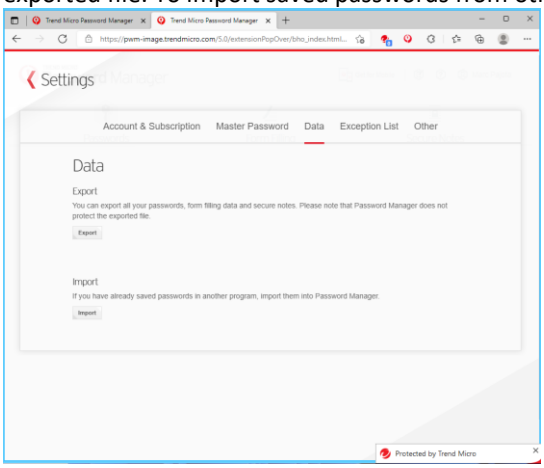

Figure 360. Settings > Data

8. Log off **Password Manager** by clicking the **Lock** icon in the lower right-hand corner of the **Password Manager** popup.
9. That's it! You now know how to get started with **Password Manager**.
10. For full instructions on using **Trend Micro Password Manager**, the *Trend Micro™ Password Manager Product Guide* is available for download from the Trend Micro Support site at Trend Micro Password Manager Support, then click on the Windows, Mac, Android, or iOS tabs for the platform(s) you're interested in.

Data: Vault

Vault is a password-protected folder that can protect your sensitive files. Using a password, files inside the Vault are kept invisible until you enter the password. If your computer is stolen, Vault can also seal itself shut by remote control, so that even using the password you cannot open the Vault—that is, until the computer is returned to its rightful owner, who then must report that the computer has been found.

To set up Vault:

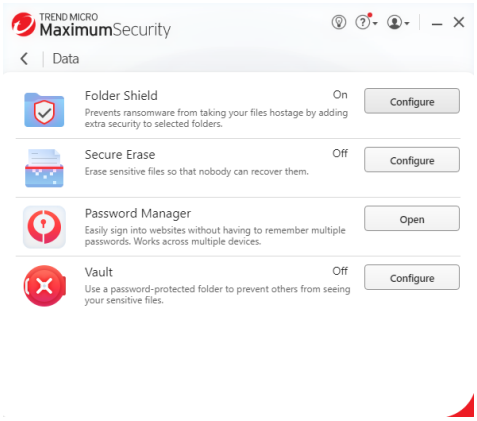

Figure 361. Data > Vault > Configure

1. In the Trend Micro Security Console, click the **Data** icon, then **Configure** in the **Vault** panel. The **Introduction** to **Vault** appears.

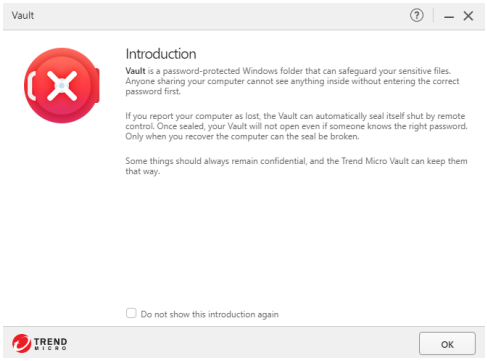

Figure 362. Data > Introduction to Vault

2. Click **OK** to close the Introduction. The **Select a Password** screen appears.

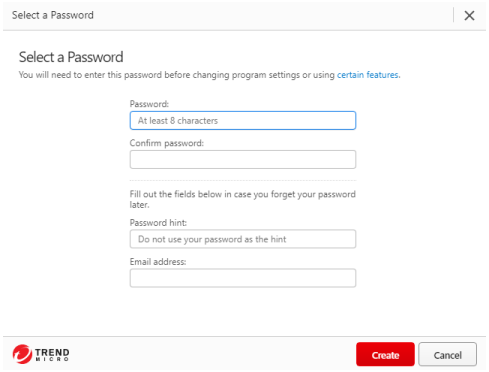

Figure 363. Select a Password

3. Enter a password and confirm it, then provide a hint and your email address and click **Create**. A setup dialog appears, telling you that you have successfully set up the **Vault** and to double-click its desktop icon to start using it.

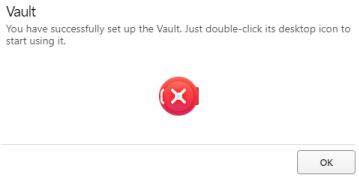

Figure 364. Vault Set Up

4. Click **OK** to close the dialog. The **Vault** window appears, with the slider turned to **On**, and instructions on reporting a loss and regaining access to the **Vault**.

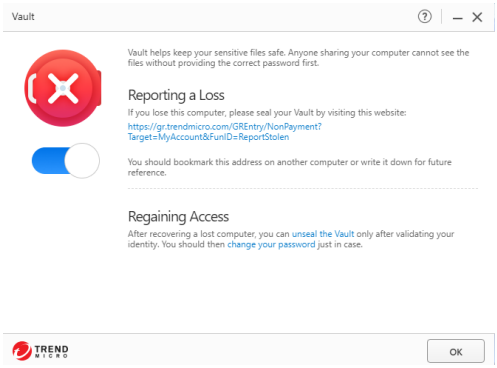

Figure 365. Vault

5. The **Vault** desktop icon also appears on your desktop.

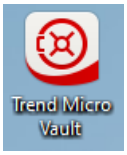

Figure 366. Vault Desktop Icon

6. You can now use the **Vault** to protect your sensitive files, to seal the vault if your computer is stolen or misplaced, and to regain access to the vault if you've turned it off.
7. To open the **Vault**, double-click the desktop icon. The password window appears.

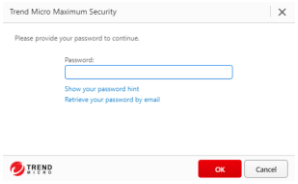

Figure 367. Vault > Password Protection

8. Enter your password and click **OK**. This opens the **Vault.**

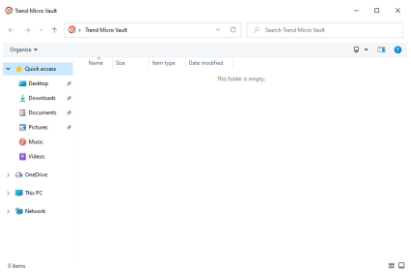

Figure 368. Trend Micro Vault

9. Drag files and folders you wish to protect into the **Vault**, then close it.

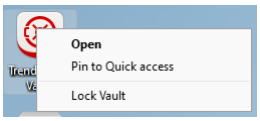

Figure 369. Lock Vault Menu Item

10. Right-click the **Vault** and select **Lock Vault** to lock it. A dialog appears, warning you that locking the vault does not automatically block access to files currently open. Make sure you close all files that need protection before you lock the Vault.

Figure 370. Trend Micro Vault Warning

11. Click **OK** to close the dialog.
12. In the Trend Micro Console Vault window, note the link http://account.trendmicro.com/report_stolen/ for reporting a loss.

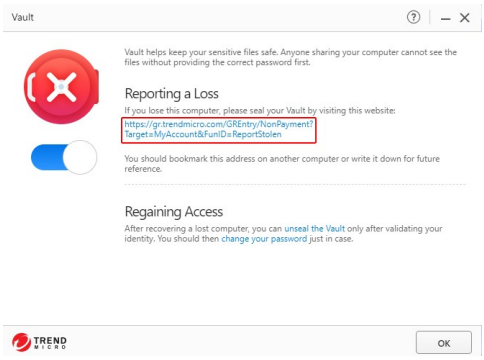

Figure 371. Reporting a Loss

13. You should bookmark this link on another computer or write it down for future reference. Clicking it takes you to the Trend Micro Vault **Report Stolen** webpage, where you can report the loss.

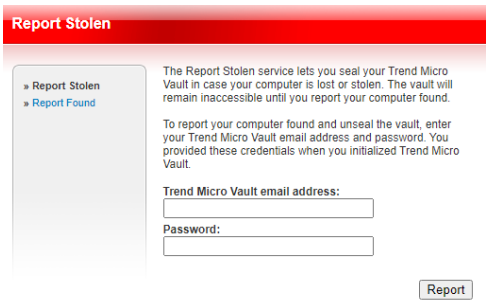

Figure 372. Report Stolen Service

14. In the **Report Stolen** webpage, enter your Trend Micro Vault email address and password and click **Report** to seal the vault. Once you do, your Vault-protected folders and files cannot be opened.
15. Once you recover the computer, open the Trend Micro Security console, click **Data > Trend Micro Vault**, re-enter your password, then click the link **Unseal the Trend Micro Vault** in the **Regaining Access** paragraph.

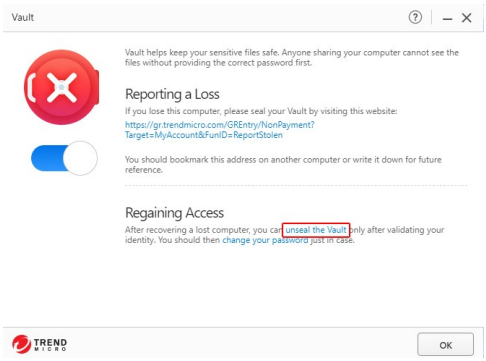

Figure 373. Regaining Access

16. This takes you to the Trend Micro Vault Report **Report Found** webpage, where you can unseal the Vault.

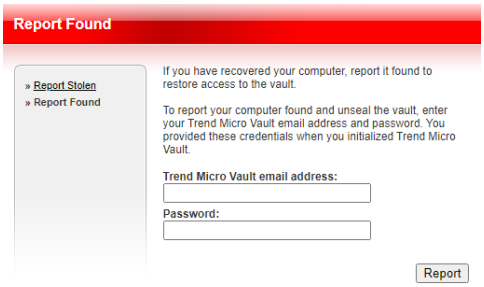

Figure 374. Report Found

17. Enter the **Trend Micro Vault email address** and **Password** and click **Report**. This unseals the Vault and you're notified by Trend Micro Security.
18. For your safety, you should now change your Trend Micro Security password.

Chapter 7: Trend Micro Security Feedback, Get Help, Identity, and Tools

All Trend Micro Security editions provide **Feedback, Get Help, and Identity** menus in the Console.

Feedback

To Provide Feedback:

1. Open the **Trend Micro Security Console.**

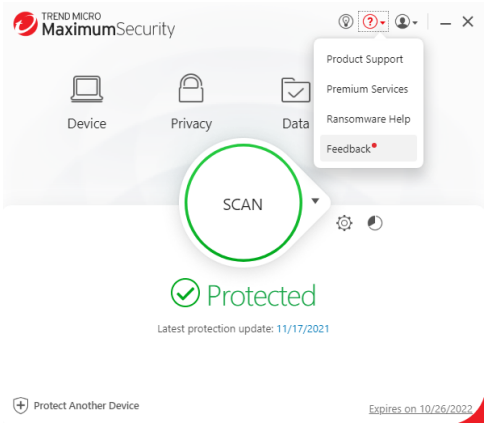

Figure 375. Feedback

2. Click the **? Icon > Feedback**.

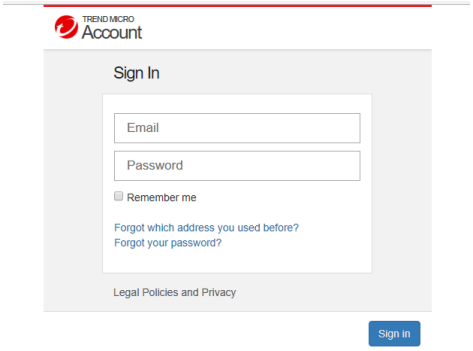

Figure 376. Account Sign In

3. Enter the email address and password you used to register Trend Micro Security and click **Sign In.**

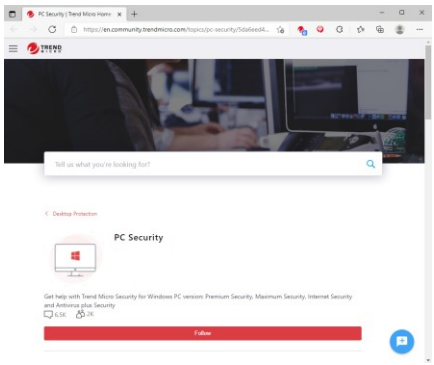

Figure 377. Trend Micro Home Users Community - DEV

4. Click **New Post** to begin a new conversation and to post your feedback. Your feedback will be posted on the **Trend Micro Home Users Community - DEV** website, where you'll obtain responses from Trend Micro developers and other users.

Help > Product Support

To get Help (?) > Product Support:

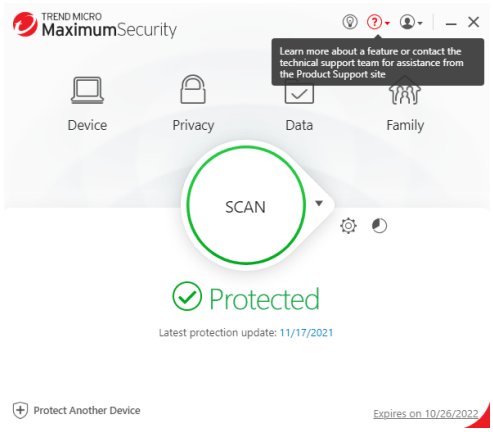

Figure 378. ? (Help)

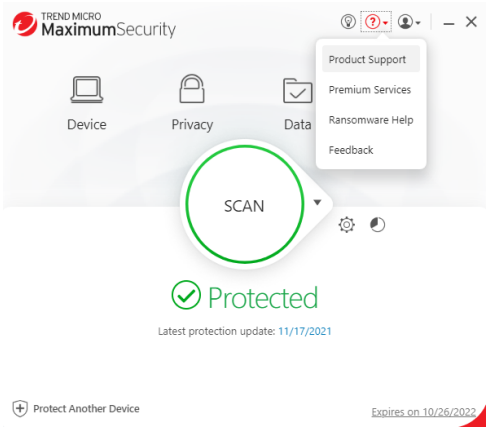

Figure 379. Get Help

1. Click **? Icon** in the Console, then choose **Product Support** in the drop-down menu. The **Product Support** page appears.

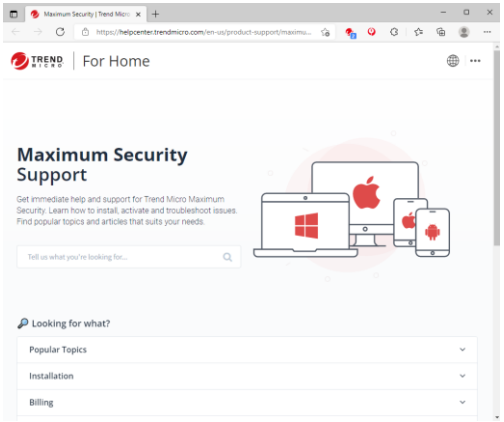

Figure 380. Trend Micro Maximum Security Support (image subject to change)

2. Here you can get access to training videos, this product guide, and a wide range of support topics to help you get the most out of your security software. Use the drop-down menus for **Support Topics** and **Related Product Support** to obtain relevant information, or click the **Discussion Forums** link for the latest discussion and support.

Help > Premium Services

To access Premium Services:

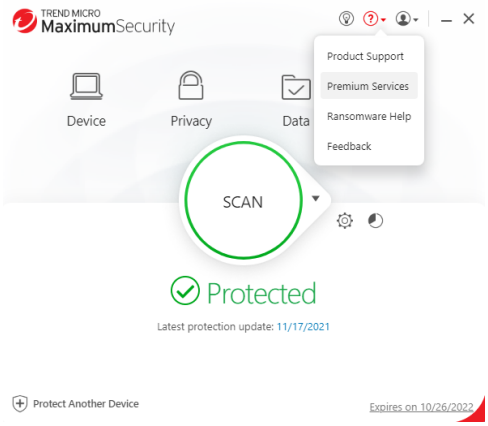

Figure 381. ? (Help) > Premium Services

1. Choose **Premium Services** in the **? (Help)** menu. The **Premium Services for Home Users** webpage appears.

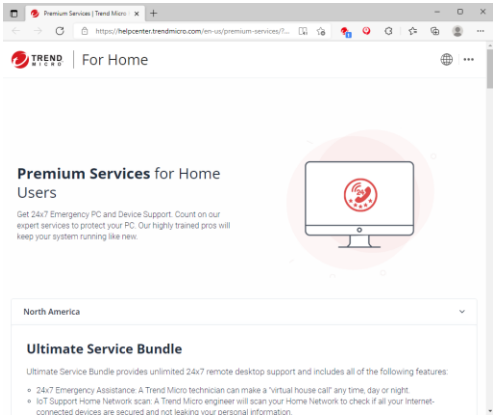

Figure 382. Premium Service (image subject to change)

2. Here you can obtain answers to frequently asked questions about Premium Service and to purchase a plan to enable a Trend Micro technician to make a "virtual house call" any time, day or night, to help you with any problems you may have with your computer.
3. Select the region you inhabit for the correct plan and pricing.

Help > Ransomware Help

To get help with ransomware:

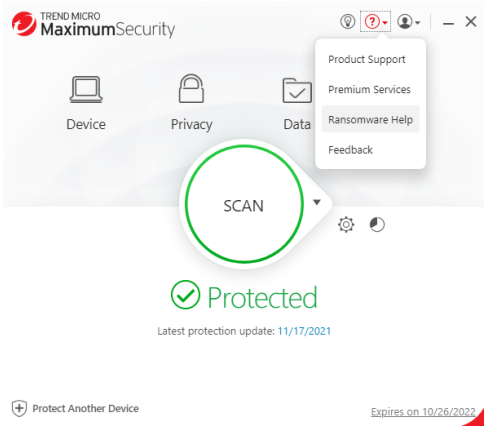

Figure 383. Ransomware Help

1. Choose **Ransomware Help** in the **? (Help)** menu. The **Ransomware Help** webpage appears.

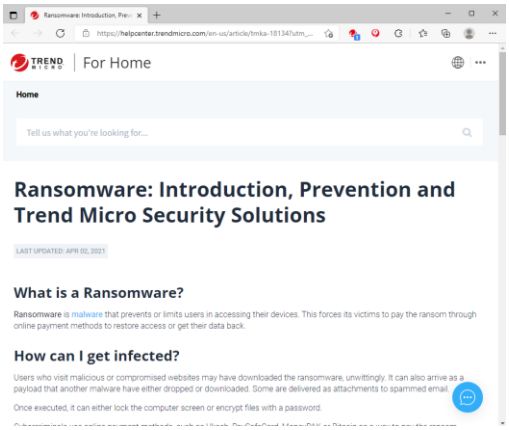

Figure 384. Ransomware Help Webpage (Image subject to change)

2. Here you can get information on ransomware, including advice on what to do if you're under a ransomware attack. See the **Ransomware Hotline** entry for information on getting live help from a Trend Micro Support Specialist.

ID > Account

To check your Account:

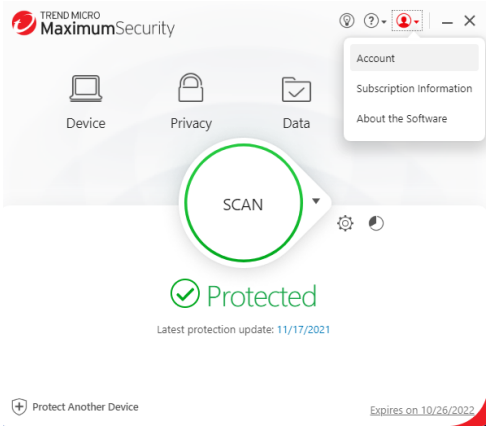

Figure 385. Account

1. Click the **ID** (**Identity)** menu, then choose the **Account** menu item in the Console. The **Trend Micro Account** webpage appears.

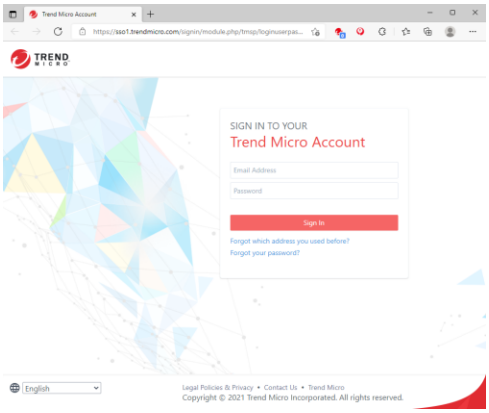

Figure 386. Trend Micro Account Webpage

2. In the **Trend Micro Account** page you can sign in to your account if you've already purchased Trend Micro products or services, manage all of your subscriptions in one place, stay up-to-date and protected by getting the latest protection for your devices or those of friends and family, and update your account.

ID > Subscription Information

To check your subscription:

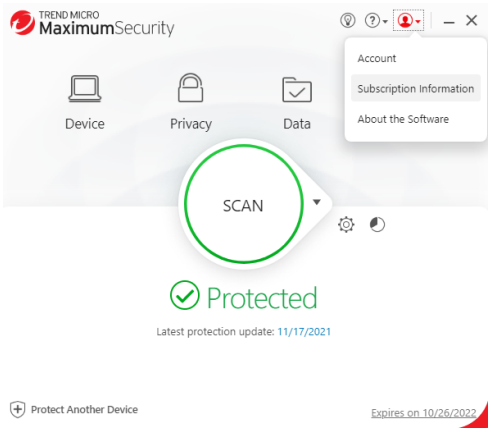

Figure 387. ID > Subscription Information

1. Select **ID (Identity) > Subscription Information** menu item in the Console. The **Subscription Information** screen appears.

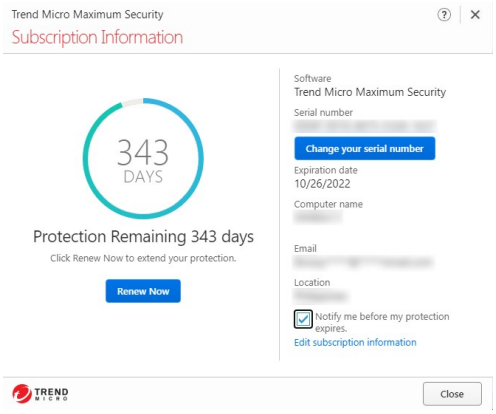

Figure 388. Subscription Information

2. In the **Subscription information** screen, you can view the days of protection remaining in your subscription, renew it, view the edition of Trend Micro Security installed on your computer, change your serial number, view your Expiration Date, your Computer Name, the email address the software is registered to, your location, and whether you've chosen to receive the latest news and offers from Trend Micro. Click **Edit subscription information** to edit it.

ID > About the Software

To check your software and get updates manually:

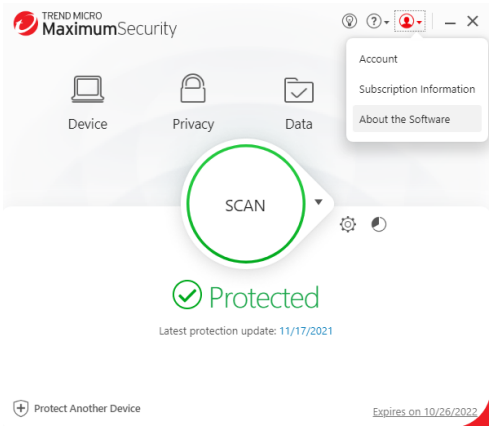

Figure 389. About the Software

1. Select the **ID > About the Software** menu item in the Console. The **About the Software** screen appears and automatically queries the Trend Micro servers to provide any available updates of your software.

Figure 390. About Your Software

2. In the **About Your Software** screen you can view the version of your software and even the version of the components by clicking **Component Versions.**

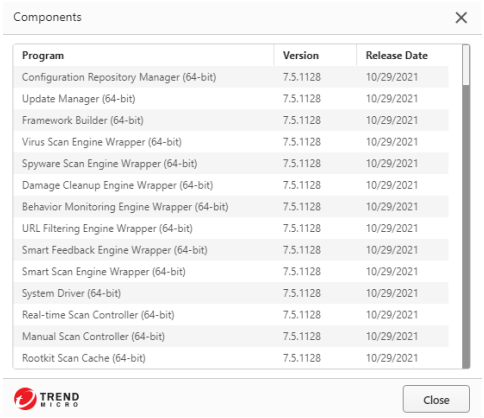

Figure 391. Component Versions

3. Click the **Serial Number** link to change it. A screen appears for you to Enter the Serial Number.

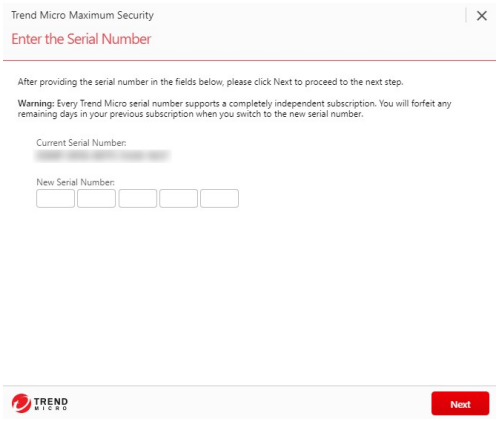

Figure 392. Enter the Serial Number

4. Click **Next** to update your software with the new serial number. Your new serial number and its subscription is applied to your software.

The Trend Micro Tools

The Trend Micro Tools are a set of utilities to perform various functions, from managing your subscription to troubleshooting.

To use the Trend Micro Tools:

1. Click **Windows Menu > All apps** and navigate down to "T" in the menu; then click the **Trend Micro Maximum Security**.

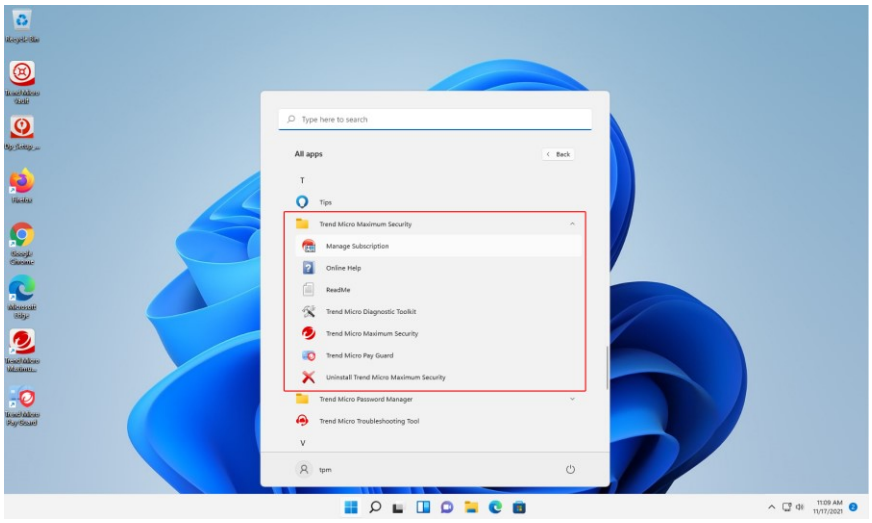

Figure 393. Trend Micro Troubleshooting Tool

2. Many functions work just as they do from the **Trend Micro Security Console.** Below are brief descriptions of key additional tools.

Trend Micro Security:

Manage Subscription

1. Click **Manage Subscription** and the **Trend Micro Account** page appears, where you can log into your account to manage your subscription(s).

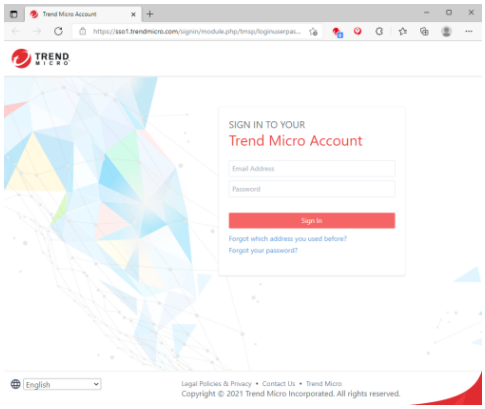

Figure 394. Manage Subscription > Trend Micro Account

Online Help

1. Click **Online Help** and the **Support** page appears, where you can obtain help about your software.

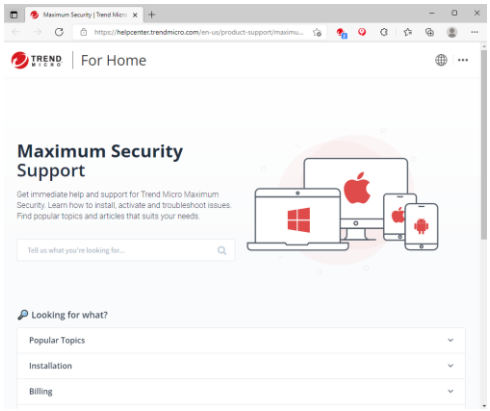

Figure 395. Support

Pay Guard

1. Click **Trend Micro Pay Guard** and the **Pay Guard** browser launches, to help you bank and shop online securely.

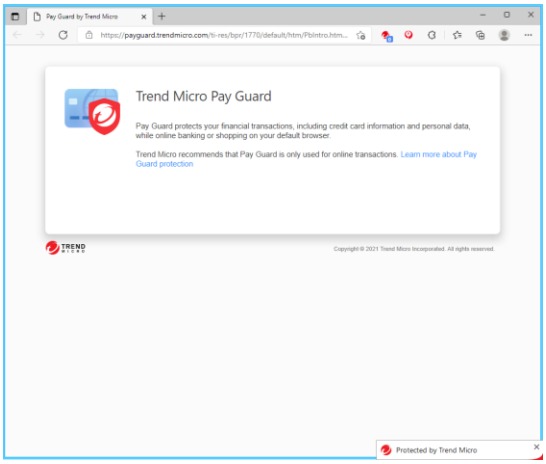

Figure 396. Trend Micro Pay Guard

ReadMe

1. Click the **ReadMe** menu item and choose the document reader you wish to use. The **ReadMe** document appears.

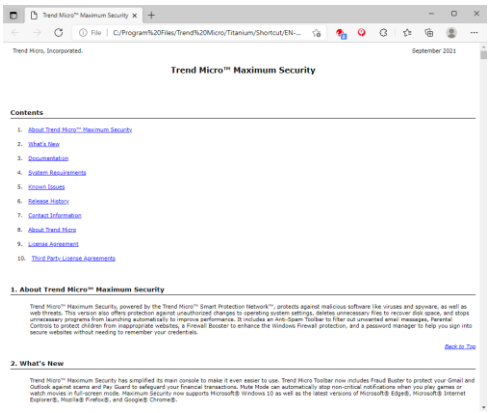

Figure 397. ReadMe

2. Click the various items in **ReadMe** to show the contents.

Trend Micro Diagnostic Toolkit

1. Click **Trend Micro Diagnostic Toolkit** to open it. The **Diagnostic Toolkit** opens.

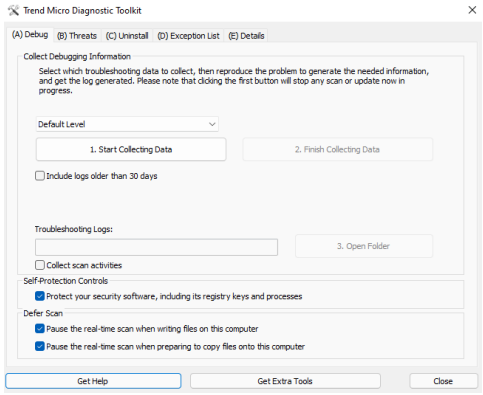

Figure 398. Trend Micro Diagnostic Toolkit

2. You'll use the **Diagnostic Toolkit** to help diagnose any problems you may encounter when using Trend Micro Security. These tools include the debugging, uninstall, exception list, and details functions. A Trend Micro Support Specialist will generally work with you to conduct your diagnosis.

Trend Micro [Edition] Security:

1. Select **Trend Micro [Edition] Security** to launch the Console.

Uninstall Trend Micro [Edition] Security:

1. Select **Uninstall Trend Micro [Edition] Security** to uninstall the program.

Trend Micro Password Manager:

Password Manager Diagnostic Tool

1. Select **Widows Menu > All apps > Trend Micro Password Manager.**

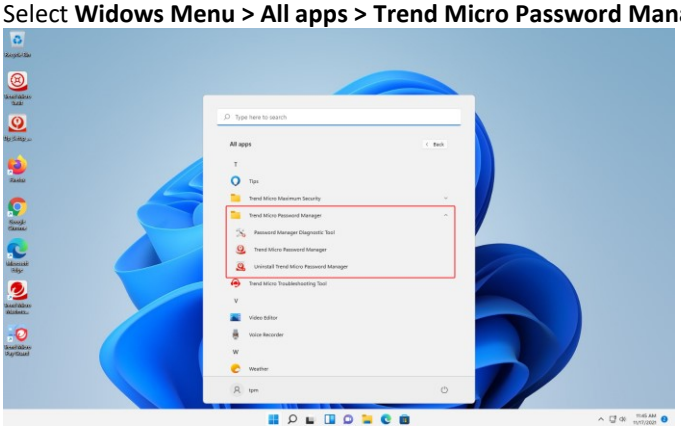

Figure 399. Trend Micro Password Manager

2. Select **Trend Micro Password Manager > Password Manager Diagnostic Tool** to open it.

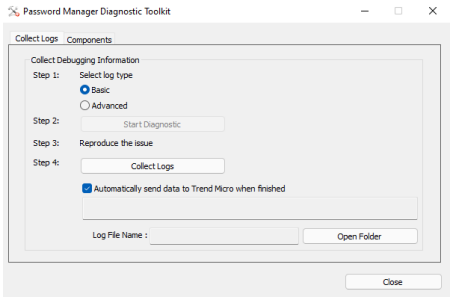

Figure 400. Password Manager Diagnostic Toolkit

3. As with Trend Micro Security, the **Password Manager Diagnostic Toolkit** can help you diagnose any problems you may have with Password Manager and is usually used in conjunction with a Trend Micro Support Specialist.

Trend Micro Password Manager

1. Select **Trend Micro Password Manager** to open the Login webpage for the web console in your default browser.

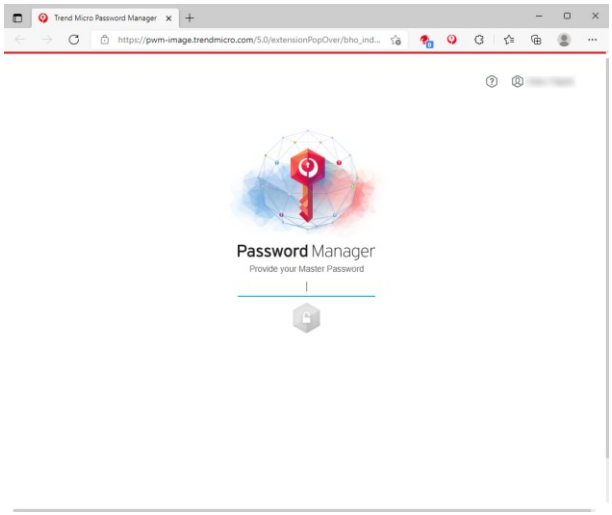

Figure 401. Password Manager Web Login Page

Uninstall Trend Micro Password Manager

1. Select **Uninstall Trend Micro Password Manager** to uninstall the program.

Trend Micro Troubleshooting Tool:

1. Click **Trend Micro Troubleshooting Tool** to open it.

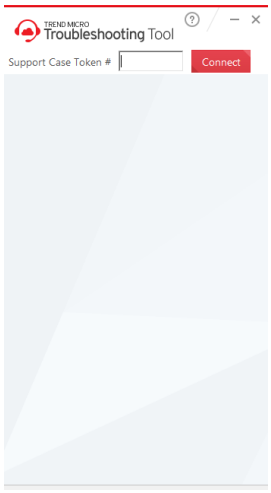

Figure 402. Trend Micro Troubleshooting Tool

2. You use the **Trend Micro Troubleshooting Tool** during a troubleshooting session with a Trend Micro Support Specialist. The specialist will provide you with a **Support Case Token**, which will link the specialist's session directly to your computer.

About Trend Micro

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables users to enjoy their digital lives safely. For more information, visit www.trendmicro.com.