

APCUG 2019 Winter Virtual Technology Conference (VTC31) 3 mini-presentations

1. Microsoft Security Center Windows 10
2. New **Privacy** Updates Windows 10
3. Password Managers for all devices

Jere Minich

APCUG Advisor Region 5

jminich@apcug.org



Microsoft Security Center

Windows 10 Version 1809

MS Security Center - What is it?

- Cyber attacks have changed.
- Hackers can now take over PC's and lock down files.
- These types of attacks are called Ransomware.
- To mitigate these types of attack, Microsoft has a feature which allows enabling **Core Isolation** and **Memory Integrity** to prevent such attacks.
- 'Windows Defender Security Center' offers these features:
 - named in Settings **Device Security**.

Update & Security

Windows Update

Delivery Optimization

Windows Security

Backup

Troubleshoot

Recovery

Activation

Find my device

For developers

Windows Security

Windows Security is your home to view and manage the security and health of your device.

Open Windows Security

Protection areas

Virus & threat protection
No actions needed.

Account protection
No actions needed.

Firewall & network protection
No actions needed.

App & browser control
No actions needed.

Device security
No actions needed.

Device performance & health
No actions needed.

Family options
Manage how your family uses their devices.

Keep your PC safe

Windows Security has options to help keep you protected online, maintain your device's health, run periodic scans, manage your threat-protection settings, and more.

Get more info about Windows Security

Have a question?

Add Microsoft account security info

How to use Windows Security

Turn on Windows Defender Firewall

Exclude a folder from a scan

Get help

Make Windows better

Give us feedback

Security Features for Everyone

- **Core isolation** - provides added protection against malware by isolating computer processes from the operating system.
- **Security processor** - provides additional encryption for the device.
 - manufacturer and version numbers, as well as about the security processor's status.
- **Secure boot** - prevents a dangerous type of malware - **rootkit**—from loading on startup of the PC.
 - Support.Microsoft.com - <http://bit.ly/2MThSdS>

What is Core Isolation?

- Windows uses hardware virtualization features to create a secure area of system memory.
 - **It is isolated from the normal operating system.**
- Windows can run system processes and security software in this secure area.
 - This protects important operating system processes from being tampered with by anything running outside the secure area.
- ‘Virtualization’ hides the physical characteristics of a PC from the users;
 - an additional layer of protection

What is Security Processor?

Two critical vulnerabilities — dubbed “Meltdown/Spectre” — affect nearly every (CPU) device made in the past 20 years.

- **Security Processor** - a trusted execution environment subsystem.
- Responsible for creating, monitoring and maintaining the security environment.
- Many devices that run Windows 10 have Trusted Platform Module (**TPM**) chipsets.
 - CPU manufacturers are releasing firmware updates via Windows 10 Updates.

What is Secure Boot?

- When a PC starts, it first finds the operating system 'bootloader'.
- PCs without Secure Boot simply run whatever bootloader is on the PC's hard drive.
 - There's no way for the PC to know it's a trusted operating system or a rootkit.
- When a PC equipped with UEFI starts, the PC first verifies that the firmware is digitally signed,
 - (UEFI {**Unified Extensible Firmware Interface**} replaces the Basic Input/Output System (BIOS) firmware interface originally present in all IBM PC's)
 - reducing the risk of firmware rootkits.
- If Secure Boot is enabled, the firmware examines the bootloader's digital signature to verify that it hasn't been modified.

How to Enable Core Isolation

1. Sign in as an Administrator.
2. Click 'Start'
3. Click on 'Settings'
4. Click on 'Update & Security'
5. Click On 'Windows Security'
6. Click on 'Device security'.

All Screenshot slides are from my Laptop.

Windows Settings

Find a setting



System

Display, sound, notifications, power



Devices

Bluetooth, printers, mouse



Phone

Link your Android, iPhone



Network & Internet

Wi-Fi, airplane mode, VPN



Personalization

Background, lock screen, colors



Apps

Uninstall, defaults, optional features



Accounts

Your accounts, email, sync, work, family



Time & Language

Speech, region, date



Gaming

Game bar, captures, broadcasting, Game Mode



Ease of Access

Narrator, magnifier, high contrast



Cortana

Cortana language, permissions, notifications



Privacy

Location, camera



Update & Security

Windows Update, recovery, backup



Settings



Start

← Settings

Home

Find a setting

Update & Security

Windows Update

Delivery Optimization

Windows Security

Backup

Troubleshoot

Recovery

Activation

Find my device

For developers

Click Here

Windows Security

Windows Security is your home to view and manage the security and health of your device.

Open Windows Security

Protection areas

Virus & threat protection
No actions needed.

Account protection
No actions needed.

Firewall & network protection
No actions needed.

App & browser control
No actions needed.

Device security
No actions needed.

Device performance & health
No actions needed.

Family options
Manage how your family uses their devices.

Click Here

Keep your PC safe

Windows Security has options to help keep you protected online, maintain your device's health, run periodic scans, manage your threat-protection settings, and more.

Get more info about Windows Security

Have a question?

Add Microsoft account security info

How to use Windows Security

Turn on Windows Defender Firewall

Exclude a folder from a scan

Get help

Make Windows better

Give us feedback

The Final Screen for Core Isolation

Windows Security

←

≡

Home

Virus & threat protection

Account protection

Firewall & network protection

App & browser control

Device security

Device performance & health

Family options

Device security

Security that comes built into your device.

Core isolation

Virtualization-based security is running to protect the core parts of your device.

[Core isolation details](#)

The words here say I have already turned these **'ON'**.

Security processor

Your security processor, called the trusted platform module (TPM), is providing additional encryption for your device.

[Security processor details](#)

Secure boot

Secure boot is on, preventing malicious software from loading when your device starts up.

[Learn more](#)

Your device meets the requirements for standard hardware security.

[Learn more](#)

Windows Community videos

[Learn more about Device security](#)

Have a question?

[Get help](#)

Help improve Windows Security

[Give us feedback](#)

Change your privacy settings

View and change privacy settings for your Windows 10 device.

[Privacy settings](#)

[Privacy dashboard](#)

[Privacy Statement](#)

Windows Defender Exploit Guard.

- [Exploit protection](#) - protects the operating system and applications from many types of exploits,
 - is enabled by default.
 - All Windows 10 users now have exploit protection.
- [Controlled Folder Access](#), which protects PC files from ransomware.
 - It's not enabled by default for all files
 - it requires some configuration.
- Enable this feature, to allow applications access before they can access files in your personal file folders.



Home



Virus & threat protection



Account protection



Firewall & network protection



App & browser control



Device security



Device performance & health



Family options



Block



Warn



Off

[Privacy Statement](#)

SmartScreen for Microsoft Store apps

Windows Defender SmartScreen protects your device by checking web content that Microsoft Store apps use.



Warn



Off

[Privacy Statement](#)

Isolated browsing

Windows Defender Application Guard opens Microsoft Edge in an isolated browsing environment to better protect your device and data from malware.

[Install Windows Defender Application Guard](#)[Learn more](#)

Exploit protection

Exploit protection is built into Windows 10 to help protect your device against attacks. Out of the box, your device is already set up with the protection settings that work best for most people.

[Exploit protection settings](#)[Privacy Statement](#)[Learn more](#)[Privacy settings](#)[Privacy dashboard](#)[Privacy Statement](#)**Click Here****Scroll Down to Exploit Protection****Click Here**



Home



Virus & threat protection



Account protection



Firewall & network protection



App & browser control



Device security



Device performance & health



Family options



Settings

Exploit protection

See the Exploit protection settings for your system and programs. You can customize the settings you want.

System settings Program settings

Control flow guard (CFG)

Ensures control flow integrity for indirect calls.

Use default (On) ▼

Data Execution Prevention (DEP)

Prevents code from being run from data-only memory pages.

Use default (On) ▼

Force randomization for images (Mandatory ASLR)

Force relocation of images not compiled with /DYNAMICBASE

Use default (Off) ▼

Randomize memory allocations (Bottom-up ASLR)

Randomize locations for virtual memory allocations.

Use default (On) ▼

High-entropy ASLR

Increase variability when using Randomize memory allocations (Bottom-up ASLR)

[Export settings](#)

Have a question?

[Get help](#)

Help improve Windows Security

[Give us feedback](#)

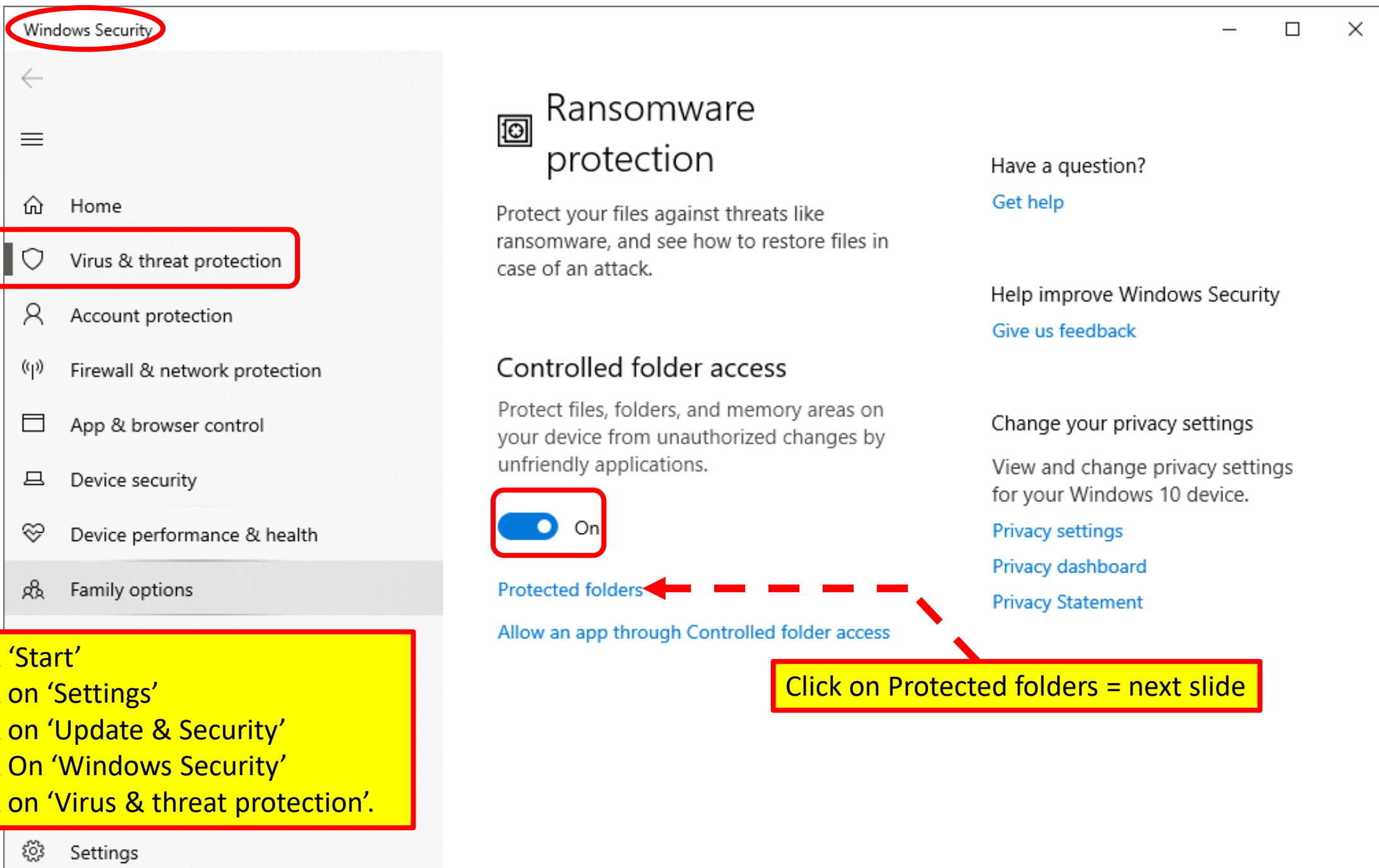
Change your privacy settings

View and change privacy settings for your Windows 10 device.

[Privacy settings](#)

[Privacy dashboard](#)

[Privacy Statement](#)



1. Click 'Start'
2. Click on 'Settings'
3. Click on 'Update & Security'
4. Click On 'Windows Security'
5. Click on 'Virus & threat protection'.

Click on Protected folders = next slide

Windows Security



Home

Virus & threat protection

Account protection

Firewall & network protection

App & browser control

Device security

Device performance & health

Family options

Protected folders

Windows system folders are protected by default. You can also add additional protected folders.

+ Add a protected folder

Documents

C:\Users\Jere Standard\OneDrive\Documents

Documents

C:\Users\Public\Documents

Pictures

C:\Users\Jere Standard\OneDrive\Pictures

Pictures

C:\Users\Public\Pictures

Videos

C:\Users\Public\Videos

Videos

C:\Users\Jere Standard\Videos

Music

C:\Users\Jere Standard\Music

Music

C:\Users\Public\Music

Desktop

C:\Users\Jere Standard\Desktop

Desktop

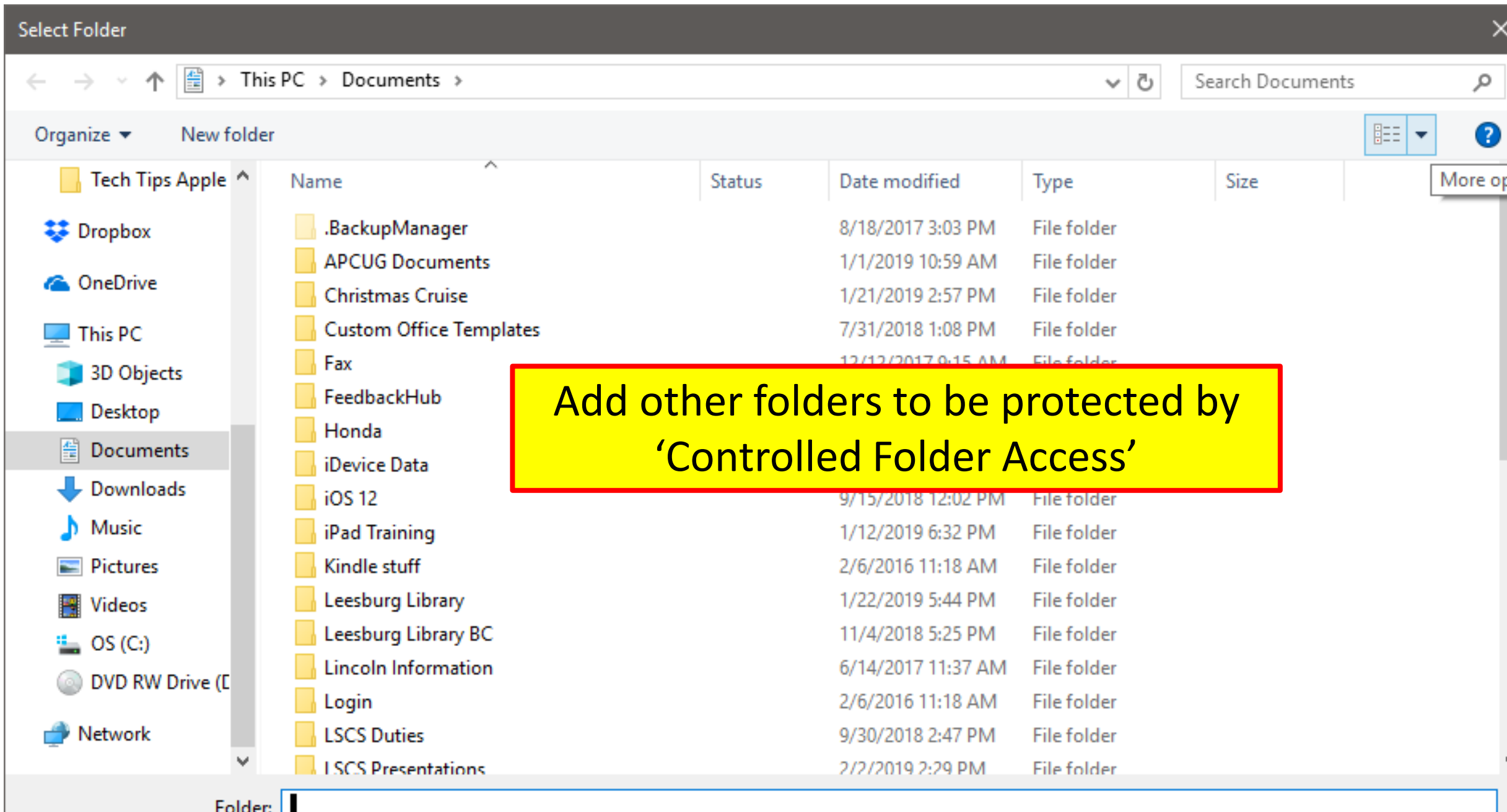
C:\Users\Public\Desktop

Favorites

C:\Users\Jere Standard\Favorites

Click on 'Add a protected folder';
opens 'File Explorer'. (Next Slide)

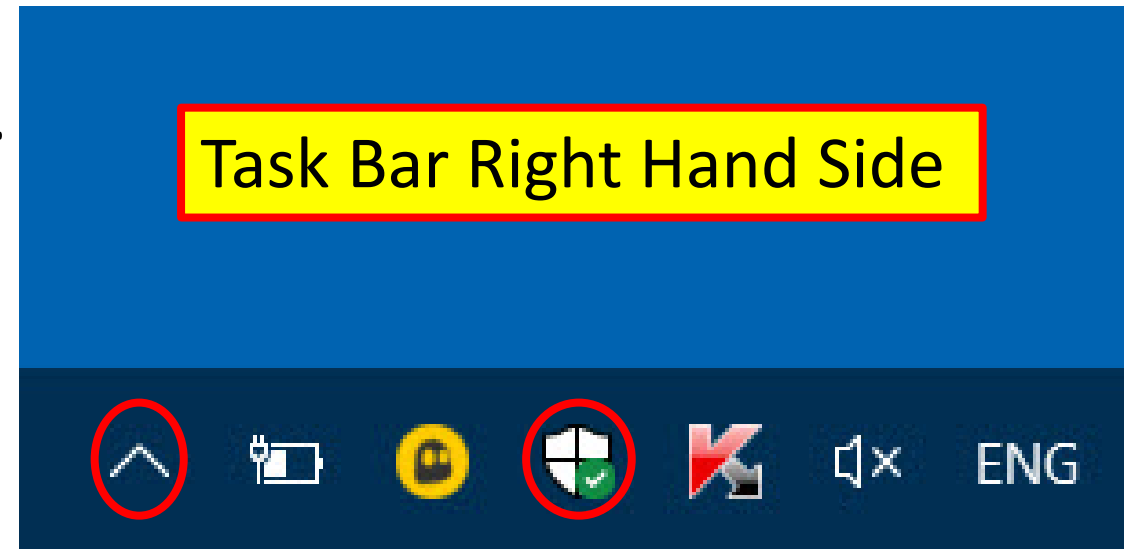
These are the folders I have
protected on my PC.



Add other folders to be protected by
'Controlled Folder Access'

Microsoft Security Essentials

- provides real-time protection for home PC's that guards against viruses, spyware, and other malicious software.
- a free download from Microsoft that is simple to install, easy to use, and always kept up to date so you can be assured your PC is protected by the latest technology.
- the PC is secure - when green, good.
- runs in the background;
 - without interruptions.





Home



Virus & threat protection



Account protection



Firewall & network protection



App & browser control



Device security



Device performance & health



Family options

Security at a glance

See what's happening with the security and health of your device and take any actions needed.



Virus & threat protection
No action needed.



Account protection
No action needed.



Firewall & network protection
No action needed.



App & browser control
No action needed.



Device security
View status and manage hardware security features



Device performance & health
No action needed.



Family options
Manage how your family uses their devices.

Go Back to Setting > Windows Security

1. Select Each Category

2. Make your desired security settings.



Settings



Home



Virus & threat protection



Account protection



Firewall & network protection



App & browser control



Device security



Device performance & health



Family options

Security at a glance

See what's happening with the security and health of your device and take any actions needed.



Virus & threat protection

No action needed.



Account protection

No action needed.



Firewall & network protection

No action needed.



App & browser control

No action needed.



Device security

View status and manage hardware security features



Device performance & health

No action needed.



Family options

Manage how your family their devices.

Select "No action needed"
These settings may not be what
you want.



Home



Virus & threat protection



Account protection



Firewall & network protection



App & browser control



Device security



Device performance & health



Family options

Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Have a question?

[Get help](#)

Help improve Windows Security

[Give us feedback](#)

Change your privacy settings

View and change privacy settings for your Windows 10 device.

[Privacy settings](#)

[Privacy dashboard](#)

[Privacy Statement](#)

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.



On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.



On

[Privacy Statement](#)

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.



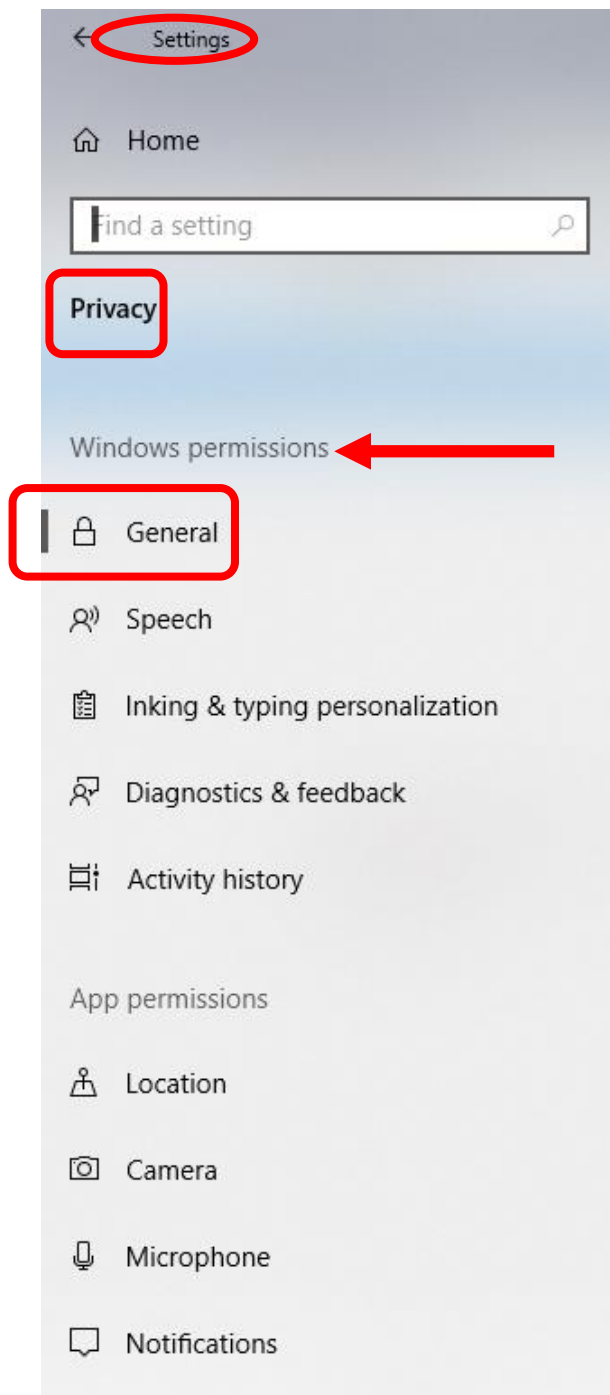
On

New Privacy Updates

Windows 10 Version 1809

Privacy settings after updating Windows 10

- It's important to make sure privacy settings are right.
- Review or choose privacy settings after each Windows update,
 - sign in with an 'administrator' account.
- 'Preselected' settings - are based on before updating Windows.
 - Adjust them by turning any toggle "ON" or "OFF".
- Change them at any time by selecting:
 - **Start > Settings > Privacy.**
- <https://privacy.microsoft.com/en-US/windows10privacy>
 - <http://bit.ly/2MXDVQW>



General

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app activity (Turning this off will reset your ID.)



Off

Let websites provide locally relevant content by accessing my language list



Off

Let Windows track app launches to improve Start and search results



Off

Show me suggested content in the Settings app



On

Resets your Advertising ID

It won't block ads in apps, but future advertisements you see won't be personalized, based on App Activity.

← Settings

Home

Find a setting

Privacy

Windows permissions

General

Speech

Inking & typing personalization

Diagnostics & feedback

Activity history

App permissions

Location

Camera

Microphone

Notifications

Account info

Contacts

Calendar

Call history

Email

Tasks

Activity history

Jump back into what you were doing on your device by storing your activity history, including info about websites you browse and how you use apps and services.

☒ Store my activity history on this device

Jump back into what you were doing, even when you switch devices, by sending Microsoft your activity history, including info about websites you browse and how you use apps and services.

☐ Send my activity history to Microsoft

Review the [Learn more](#) and [Privacy Statement](#) to find out how Microsoft products and services use this data to personalize experiences while respecting your privacy.

Show activities from these accounts

These are your accounts on this device. Turn them off to hide their activities from your timeline.

jerethrive10@gmail.com

Off

Clear activity history

Clear history for jerethrive10@gmail.com

[Manage my Microsoft account activity data](#)

I have shown 2 examples.
(General & Activity History)
Check them all under Windows permissions.

Checked by default

Click here to manage MS account activity data.

Know your privacy options
[Learn how this setting impacts your privacy.](#)
[Learn more](#)
[Privacy dashboard](#)
[Privacy statement](#)

Have a question?
[Get help](#)

Make Windows better
[Give us feedback](#)

MS Account activity data

The following data can be adjusted/ edited/ viewed in Account Activity Data.

- Browsing History
- Location Activity
- Voice Activity
- Media Activity
- Apps and services
- Cortana's Notebook
- MS Health Activity
- Ad Settings
- Search History
- Promotional communications
- SKYPE
- Xbox
- LinkedIn
- Product and service performance data
- Product and service activity
 - Microsoft Says:
- When we do collect data, we will use it to benefit you and to make your experiences better.

Set app permissions

- A handy list of your installed apps and set permissions for each app.
- Choose what Apps can: access your camera, precise location, your contacts, your account info., run in the background, etc.
 - run in the background - can help conserve power when on battery.
- How to get there:
 1. Go to Settings > Privacy > Apps Permissions
 2. Select an App
 3. Move, Modify or Uninstall each App.

← Settings

Home

Find a setting

Privacy

Windows permissions

General

Speech

Inking & typing personalization

Diagnostics & feedback

Activity history

App permissions

Location

Camera

Microphone

Location

Allow access to location on this device

If you allow access, you will enable Windows to use your device's capabilities to determine your location and Microsoft will use your location data to improve location services. People using this device will be able to choose if their apps have access to location by using the settings on this page. Denying access blocks Windows from providing location to Windows features, Microsoft Store apps, and most desktop apps.

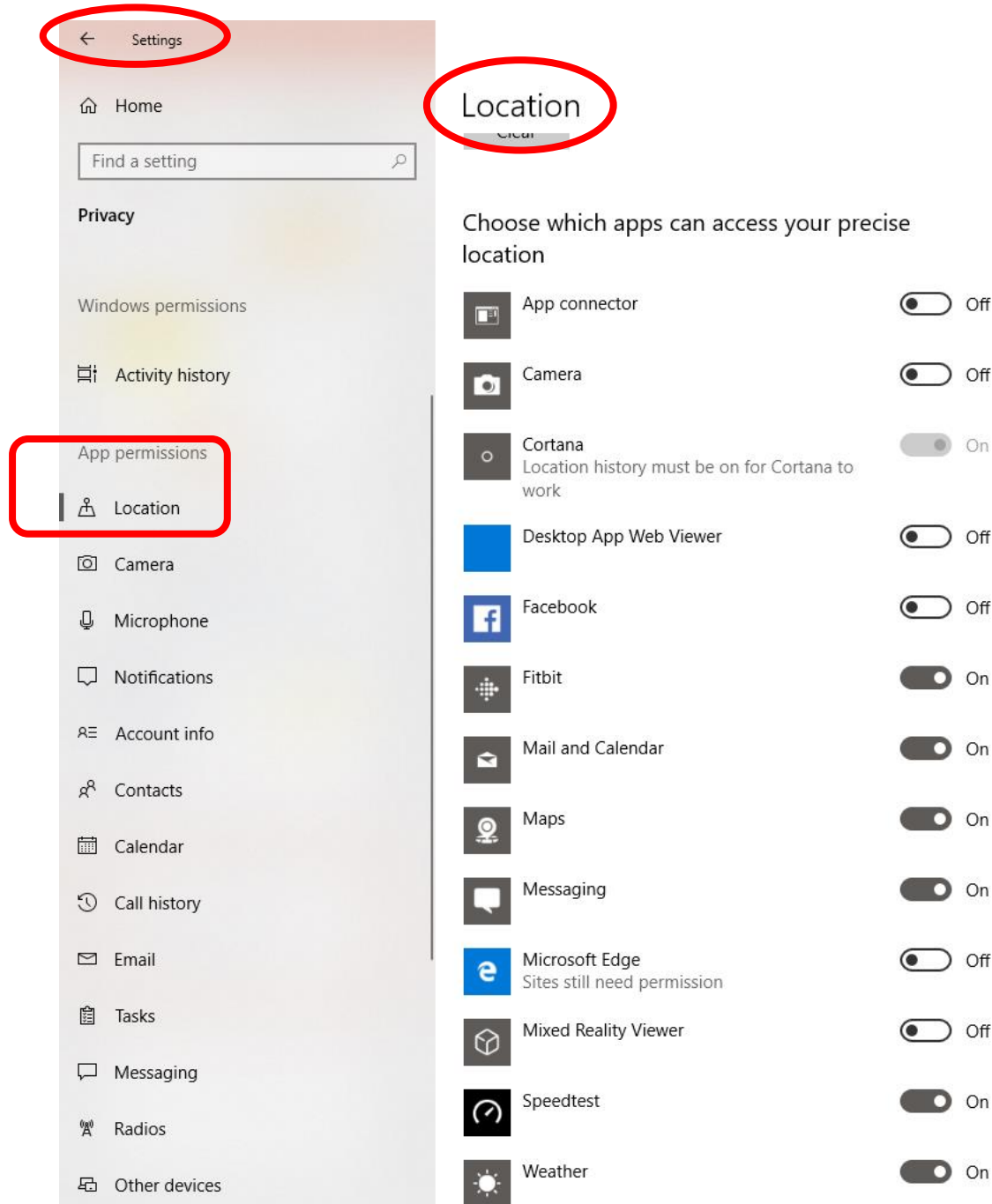
Allow apps to access your location

If you allow access, you can use the settings on this page to choose which apps can access your device's precise location and location history to enable location-based experiences such as directions and weather. If you are signed in with a Microsoft account on this device, your last known location is saved to the cloud, and shared with other devices where you are signed in with your Microsoft account. Denying access only blocks the apps listed on this page from accessing your location.

☒ On

Some desktop apps may still be able to determine your location when settings on this page are off. Find out why

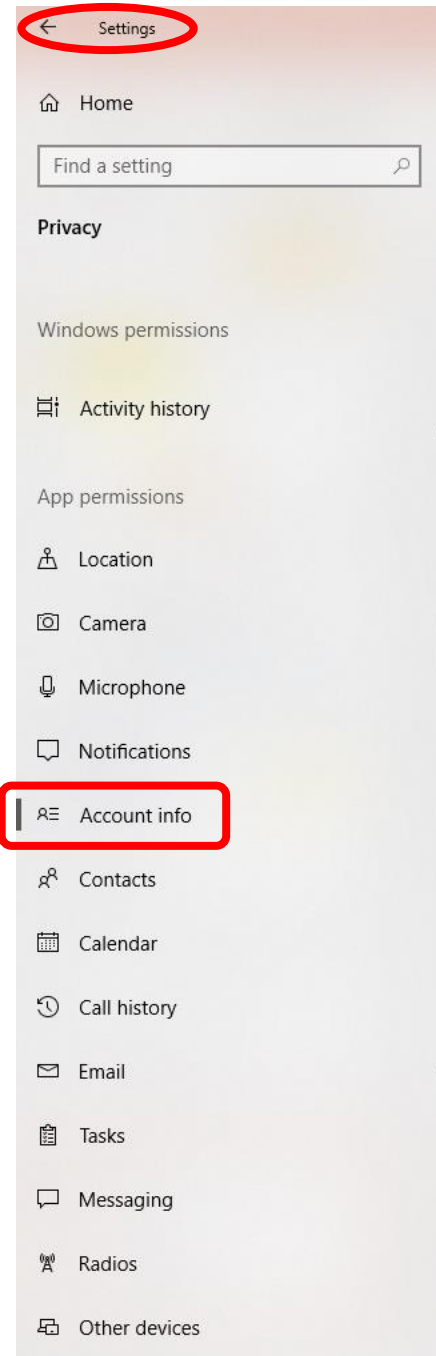
If an app is using your location, you'll see this icon: 📍



This list of Apps are ones who want access to your location.

If the App requires this info, it will alert with a popup, and allow changes to this setting.

Screenshot from my Laptop.



Account info





Allow apps to access your account info

If you allow access, you can choose which apps can access your name, picture, and other account info by using the settings on this page. Denying access blocks apps from accessing your account info.

☒ On

Choose which apps can access your account info

Some apps need to access your account info to work as intended. Turning off an app here might limit what it can do.

	Email and accounts	<input type="checkbox"/> Off
	Microsoft Content	<input checked="" type="checkbox"/> On
	Microsoft Edge	<input checked="" type="checkbox"/> On
	Speedtest	<input type="checkbox"/> Off

Apps that want access to your account information. e.g.:

- record of your sign-in (date and time),
- info about the service you signed into,
- your sign-in name,
- your IP address (location),
- your operating system,
- browser version.

If the App requires this info, it will alert with a popup, and allow changes to this setting.

← Settings

Home

Find a setting

Privacy

Windows permissions

General

Speech

Inking & typing personalization

Diagnostics & feedback

Activity history

App permissions

Location

Camera

Microphone

Notifications

Account info

Contacts

Calendar

Call history

Email

Contacts










Allow apps to access your contacts

If you allow access, you can choose which apps can access your contacts by using the settings on this page. Denying access blocks apps from accessing your contacts.

☒ On

Choose which apps can access your contacts

Some apps need to access your contacts to work as intended. Turning off an app here might limit what it can do. The following built-in app always has access to your contacts: People.

	Cortana	<input type="checkbox"/> Off
	Fitbit	<input type="checkbox"/> Off
	Mail and Calendar	<input checked="" type="checkbox"/> On
	Maps	<input type="checkbox"/> Off
	Messaging	<input type="checkbox"/> Off
	Photos	<input type="checkbox"/> Off
	PowerPoint Mobile	<input type="checkbox"/> Off
	Skype	<input type="checkbox"/> Off
	Xbox	<input type="checkbox"/> Off

This list will indicate all the Apps that want access to your Contacts.

If the App requires this info, it will alert with a popup, and allow changes to this setting.

Know your privacy options

Learn how this setting impacts your privacy.

Learn more

Privacy dashboard

Privacy statement

Have a question?

Get help

Make Windows better

Give us feedback

← Settings

🏠 Home

Find a setting 🔍

Privacy

App permissions

📅 Calendar

🕒 Call history

✉ Email

📋 Tasks

💬 Messaging

📻 Radios

📱 Other devices

🖼 Background apps

📁 App diagnostics

☁ Automatic file downloads

📄 Documents

🖼 Pictures

📺 Videos

📁 File system

Tasks

Allow apps to access your tasks

If you allow access, you can choose which apps can access your tasks by using the settings on this page. Denying access blocks apps from accessing your tasks.

☒ On

Choose which apps can access your tasks

Some apps need to access your tasks to work as intended. Turning off an app here might limit what it can do. The following built-in apps always have access to your tasks: Mail and Calendar.

Check each App permissions category and set your own **privacy**.

Password Managers

Any Device.

Password Managers

- People use very weak passwords.
 - And reuse them on different websites.
- **How are you supposed to use strong, unique passwords on all the websites you use?**
- The solution is a **password manager.**

Password managers

What do they Do?

- Store login information for all the websites in use.
 - User ID and Password.
 - Two-Factor Authentication
- Help log into the Web Site automatically.
- Encrypt your password database:
 - with a master password
 - only one you have to remember.

How do password managers Work?

- A software app or Browser extension that is used to store and manage:
 - the **passwords** for various online accounts.
- Store the **passwords** in an encrypted format.
- Provide secure access to all the **password** information
 - Controlled by a **user**-devised master **password**.
- Passwords are saved to a protected 'vault'.
- Far safer than reusing passwords or writing them down.

Why Browser-Based Password Managers Aren't Ideal

- Web browsers - all have integrated password managers.
 - Chrome, Mozilla Fire Fox, Edge, Safari, Opera.
- They can't compete with dedicated password managers.
- Example:
 - Chrome stores your passwords on your computer in an unencrypted form.
 - People could access the password files on the PC and view them, unless you encrypt your computer's hard drive.
- Mozilla Firefox has a “master password” feature:
 - encrypts your saved passwords with a single “master” password,
 - storing them on your computer in an encrypted format.
 - The browser software doesn't generate random passwords.
 - No cross-platform syncing (Firefox password manager can't sync to iOS devices).

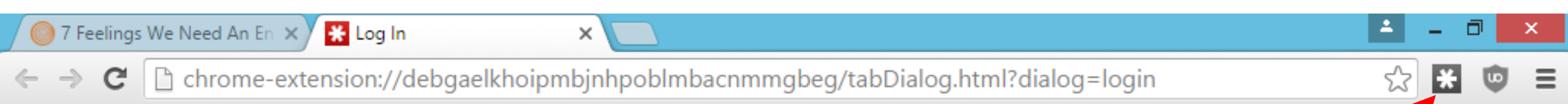
Types of password managers include:

- Locally installed software applications.
 - reside on the user's personal computer or mobile device.
 - in the form of a software app.
- Online services accessed through a specially designed website
 - content is login protected and user-specific.
 - a website that securely stores login details.
 - used on any computer with a web browser.
 - user trusts the hosting site.
- Locally accessed hardware devices that serve as keys
 - a form of token-based password manager.
 - such as smart cards or secure USB flash devices.
 - still require software loaded on the PC.

LastPass:

The password manager I have used for 6 years.

- A cloud-based password manager with:
 - extensions, (added to my Browser Mozilla Firefox)
 - mobile apps, (on my iPad and iPhone)
 - desktop apps.
- For all the browsers and operating systems you could want.
 - Windows (browser Extension)
 - iOS, Android, Mac (App)
- It's extremely powerful:
 - two-factor authentication options
 - stores your passwords in the cloud, (must have internet to use)
 - on LastPass's servers in an encrypted form, (they can not read it)
 - the extension or app locally decrypts and encrypts them when you log in,



To Activate Last Pass:

Your Email Address

Your Master Password
At least 16 Characters

This Icon turns Red
on your Browser
Address Bar after
you log in to
LastPass

What Pass Word Managers Do

Example from my Laptop



Sign in

Your Email address

[Change](#)

Password

[Forgot your password?](#)

.....



Sign in

☐ Keep me signed in. [Details](#) ▼

or

Get a sign-in code in your email

[Conditions of Use](#)

[Privacy Notice](#)

[Help](#)

© 1996-2018, Amazon.com, Inc. or its affiliates

Sign In

Sample 'Log in' to a greeting card web site

email address:

Your Email address

password:

••••••••••

[Forgot password?](#) [reset password](#)

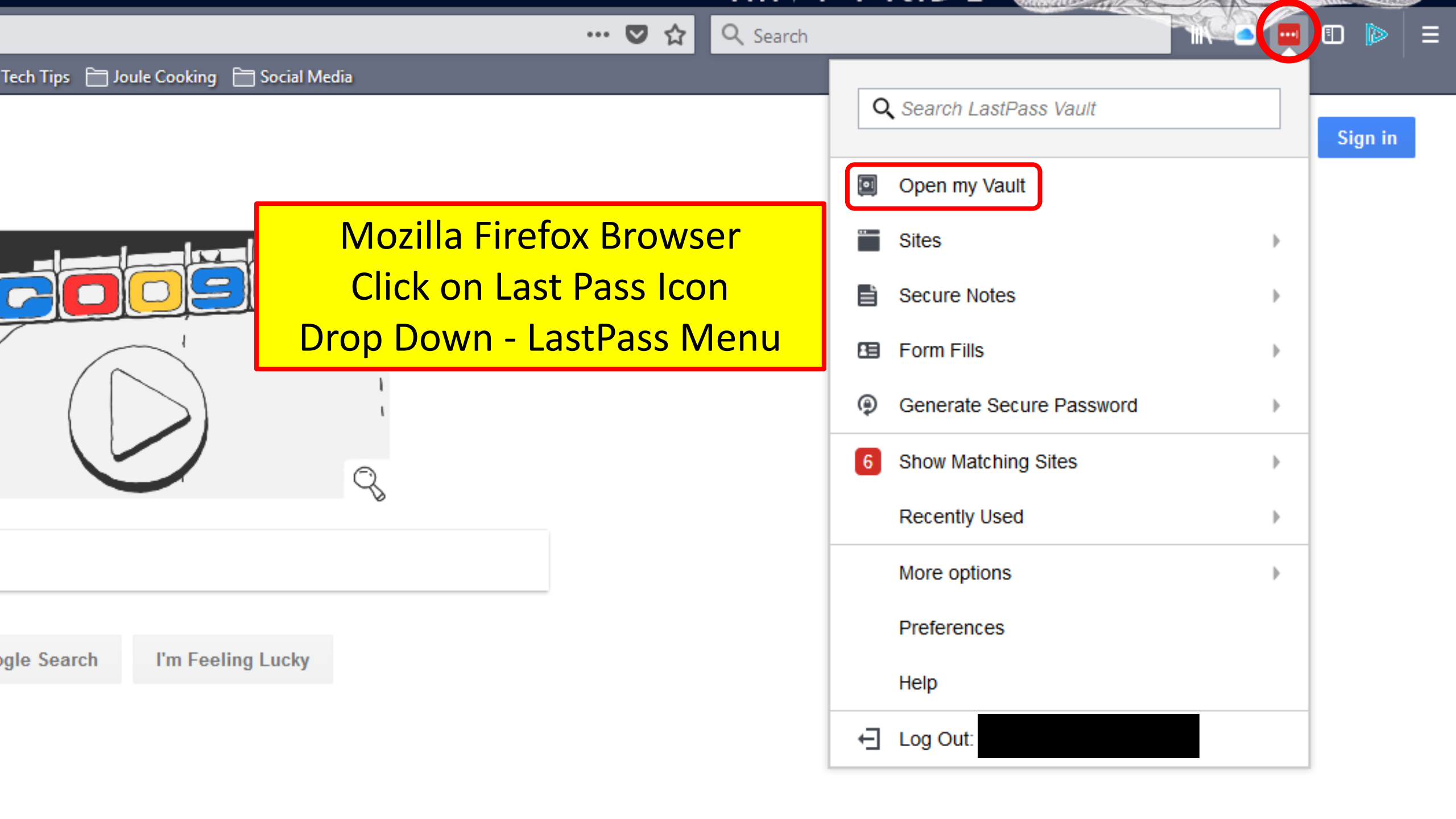
☐ Remember me.
(not recommended on public computers)

sign in >

Not a member yet? [Learn about member benefits](#)

question

- Call us Friday
- Email C
- Visit our frequen



Mozilla Firefox Browser
Click on Last Pass Icon
Drop Down - LastPass Menu

Search LastPass Vault

Open my Vault

Sites

Secure Notes

Form Fills

Generate Secure Password

6 Show Matching Sites

Recently Used

More options

Preferences

Help

Log Out: [redacted]

Sign in

← Collapse



Sites



Secure Notes



Form Fills



Sharing Center



Security Challenge

47%

LastPass...



search my vault

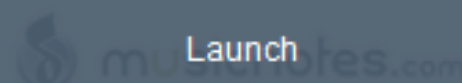
Sites

Favorites (4) ▼

We have 132 Web Sites and
104 Secure Notes in Last Pass



ancestry.com



musicnotes.com



(none) (148) ▼



lookout.com



vzw.com

xm-rad

Welcome to your vault!

Your vault is a safe place to store passwords, notes, profiles for online shopping, and even documents.
And no matter where you work, you can access your vault from any device.

[Show me around](#)

Secure Notes

Secure Notes (2) ▼

Apple Watch

Edit Note



Name:

Folder:

Note Type:

Advanced Settings:

Add Attachment

Model MU652LL/A
SN FH7Y180FKDH2
Order Number: W514721862
Ordered on: Jan 18, 2019

Apple Watch Series 4 GPS,
40mm Silver Aluminum Case with Seashell Sport Loop

Sample Page in Last Pass to Edit
a Secure Note.



Cancel

Save

The best free password manager 2018

- **LastPass.** Free, secure password creation and storage for all your accounts. ...
- **Dashlane.** Superb password security for all web browsers and devices. ...
- **RoboForm.** A superb desktop password manager with free mobile apps. ...
- **KeePass Password Safe.** A customizable password manager for more experienced users. ...

What do these Password Managers Offer:

They offer additional features including:

- **Auto-fill functionality**, so you don't have to waste time entering individual usernames and passwords.
- **Online syncing across devices** for a more streamlined user experience.
- **Two-factor authentication**, so you can bolster your account's security with an additional code required to finish the login process.
- **Secure sharing features**, so you can share information with trusted friends and family members.

Reviews | Software | Security | Password Managers

The Best **Free** Password Managers for 2019

A password like '123456' may be easy to remember, but it's also equally easy to guess or hack. These are the best free password managers that can help you keep track of strong, unique passwords for every secure site you use.



By Neil J. Rubenking October 16, 2018 1:24PM EST



142 SHARES

PCMag reviews products [independently](#), but we may earn affiliate commissions from buying links on this page. [Terms of use.](#)

Product	LastPass	LogMeOnce Password Management Suite Premium	Myki Password Manager & Authenticator	1U Password Manager	Avira Password Manager	Enpass Password Manager	KeePass 2.34	oneID	Symantec Norton Password Manager
Lowest Price	Free LastPass SEE IT	Free LogMeOnce SEE IT	\$0.00 MSRP	\$0.00 MSRP	\$0.00 MSRP	\$0.00 MSRP	\$0.00 MSRP	\$0.00 MSRP	\$0.00 MSRP
Editors' Rating	★★★★★ EDITORS' CHOICE	★★★★★	★★★★☆	★★★★☆	★★★★☆	★★★★☆	★★★★☆	★★★★☆	★★★★☆
Import From Browsers	✓	✓	✓	✓	—	—	✓	—	✓
Two-Factor Authentication	✓	✓	✓	✓	✓	—	✓	✓	—
Fill Web Forms	✓	✓	—	—	—	—	—	—	✓

The End

- This presentation will be available from YouTube APCUG Video - <https://www.youtube.com/user/APCUGVideos>
- Comments, Questions or request a personal copy:
 - If requesting a personal Copy;
 - Please tell me when you viewed this presentation.
 - jminich@apcug.org