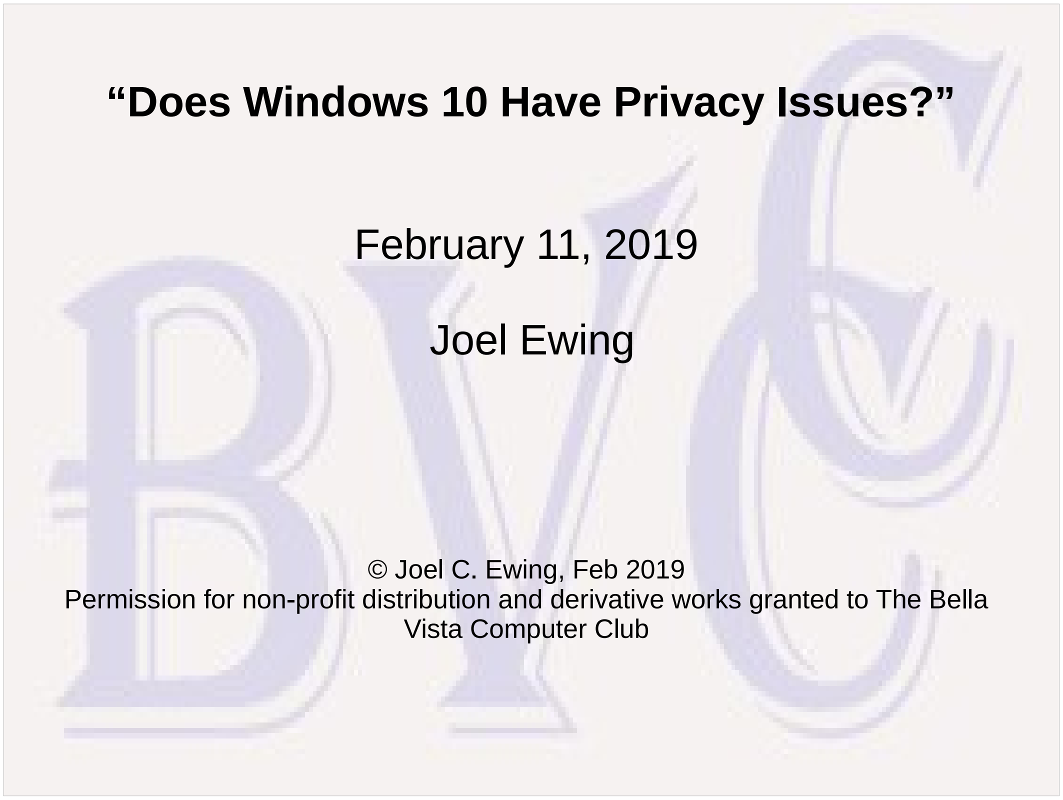
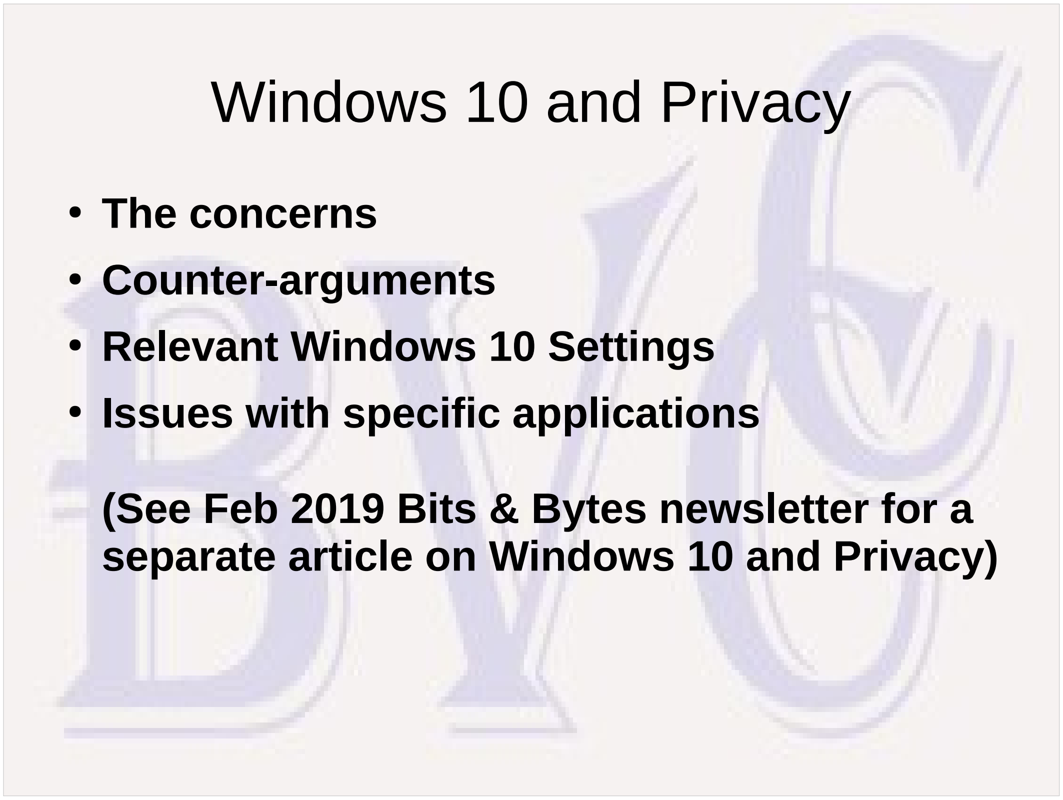


“Does Windows 10 Have Privacy Issues?”

February 11, 2019

Joel Ewing

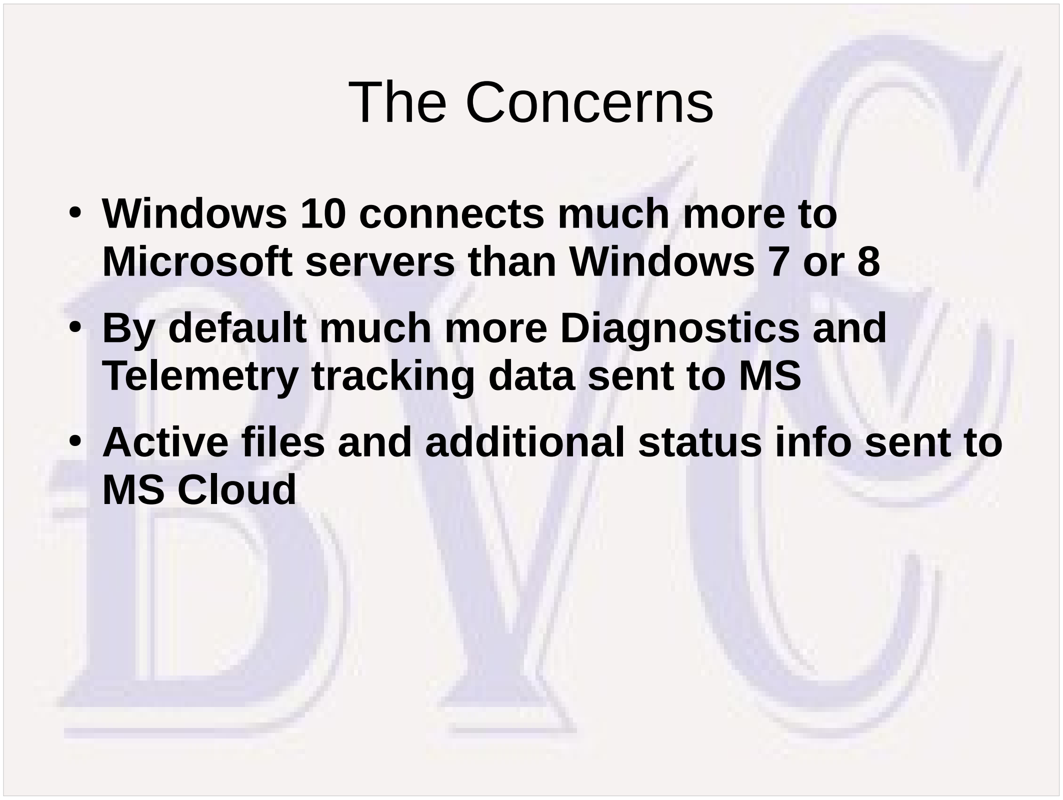
© Joel C. Ewing, Feb 2019
Permission for non-profit distribution and derivative works granted to The Bella Vista Computer Club



Windows 10 and Privacy

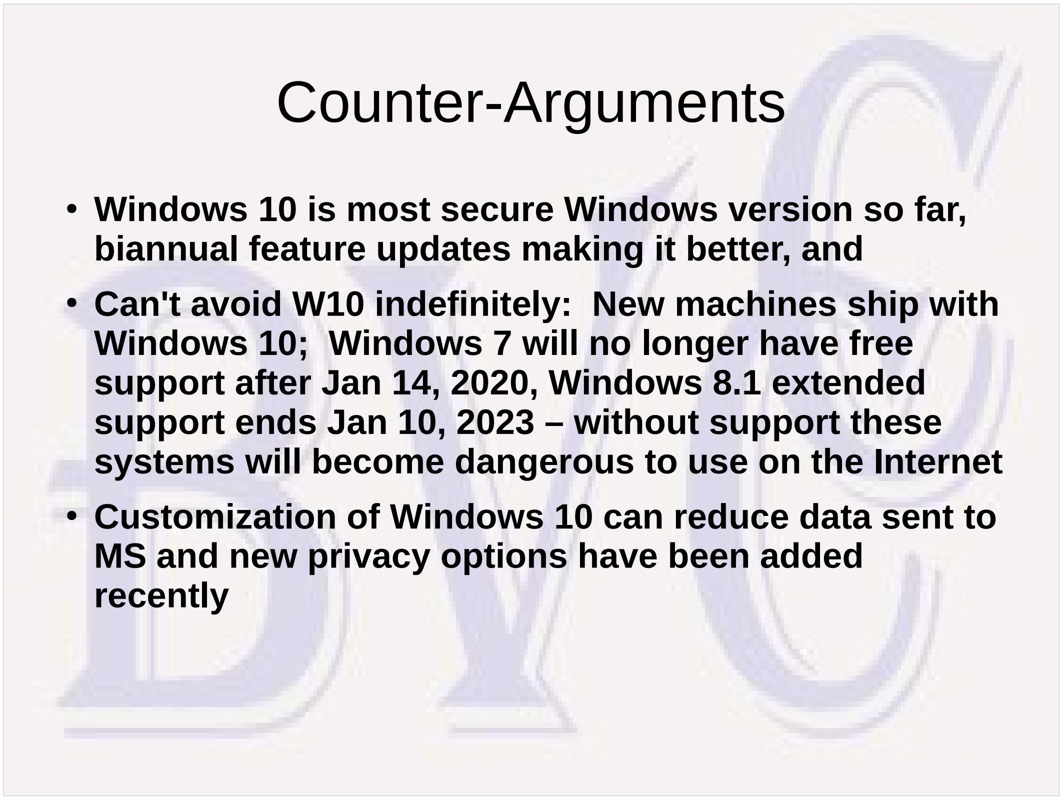
- **The concerns**
- **Counter-arguments**
- **Relevant Windows 10 Settings**
- **Issues with specific applications**

(See Feb 2019 Bits & Bytes newsletter for a separate article on Windows 10 and Privacy)



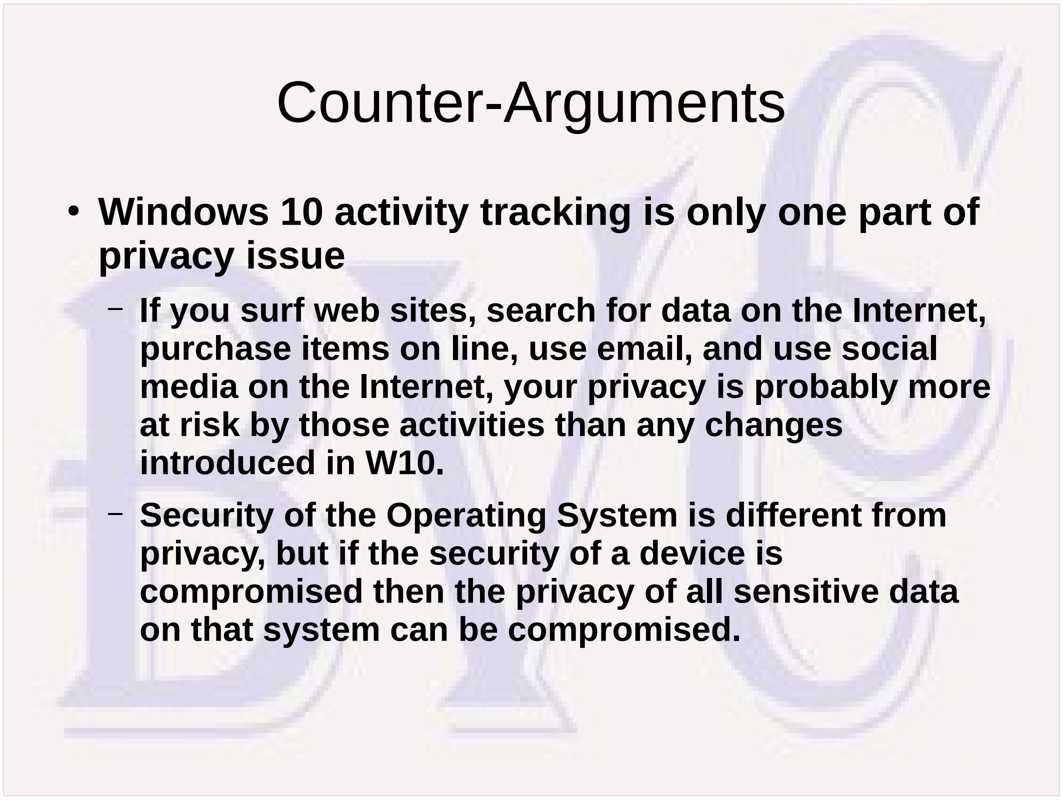
The Concerns

- **Windows 10 connects much more to Microsoft servers than Windows 7 or 8**
- **By default much more Diagnostics and Telemetry tracking data sent to MS**
- **Active files and additional status info sent to MS Cloud**



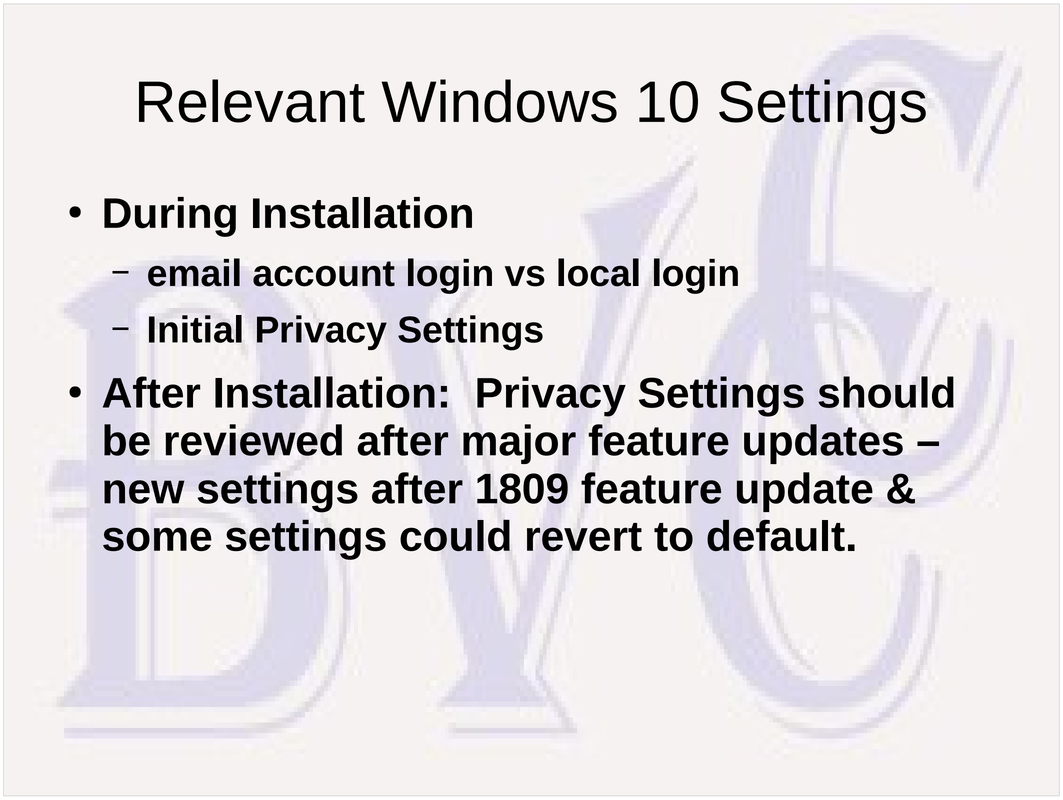
Counter-Arguments

- Windows 10 is most secure Windows version so far, biannual feature updates making it better, and
- Can't avoid W10 indefinitely: New machines ship with Windows 10; Windows 7 will no longer have free support after Jan 14, 2020, Windows 8.1 extended support ends Jan 10, 2023 – without support these systems will become dangerous to use on the Internet
- Customization of Windows 10 can reduce data sent to MS and new privacy options have been added recently



Counter-Arguments

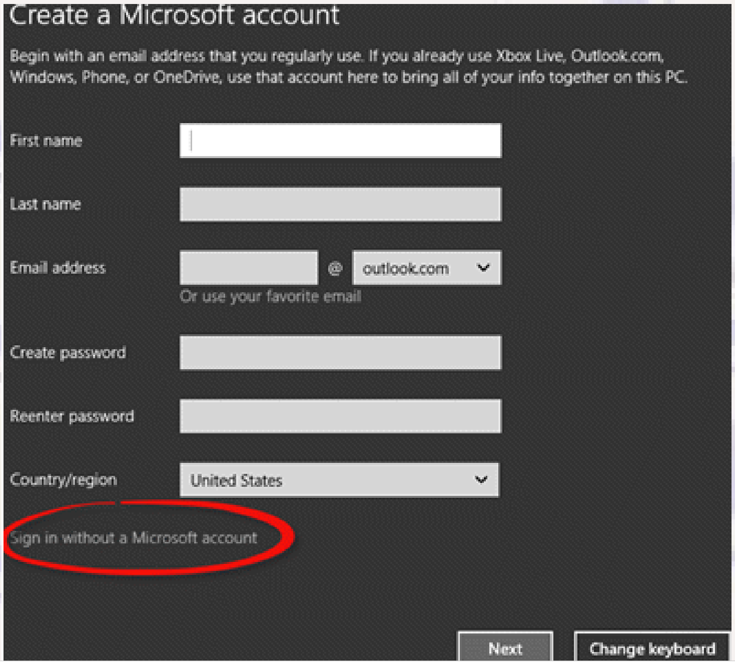
- **Windows 10 activity tracking is only one part of privacy issue**
  - **If you surf web sites, search for data on the Internet, purchase items on line, use email, and use social media on the Internet, your privacy is probably more at risk by those activities than any changes introduced in W10.**
  - **Security of the Operating System is different from privacy, but if the security of a device is compromised then the privacy of all sensitive data on that system can be compromised.**



Relevant Windows 10 Settings

- **During Installation**
  - **email account login vs local login**
  - **Initial Privacy Settings**
- **After Installation: Privacy Settings should be reviewed after major feature updates – new settings after 1809 feature update & some settings could revert to default.**

Choice of Login Account



Create a Microsoft account

Begin with an email address that you regularly use. If you already use Xbox Live, Outlook.com, Windows, Phone, or OneDrive, use that account here to bring all of your info together on this PC.

First name

Last name

Email address @ outlook.com

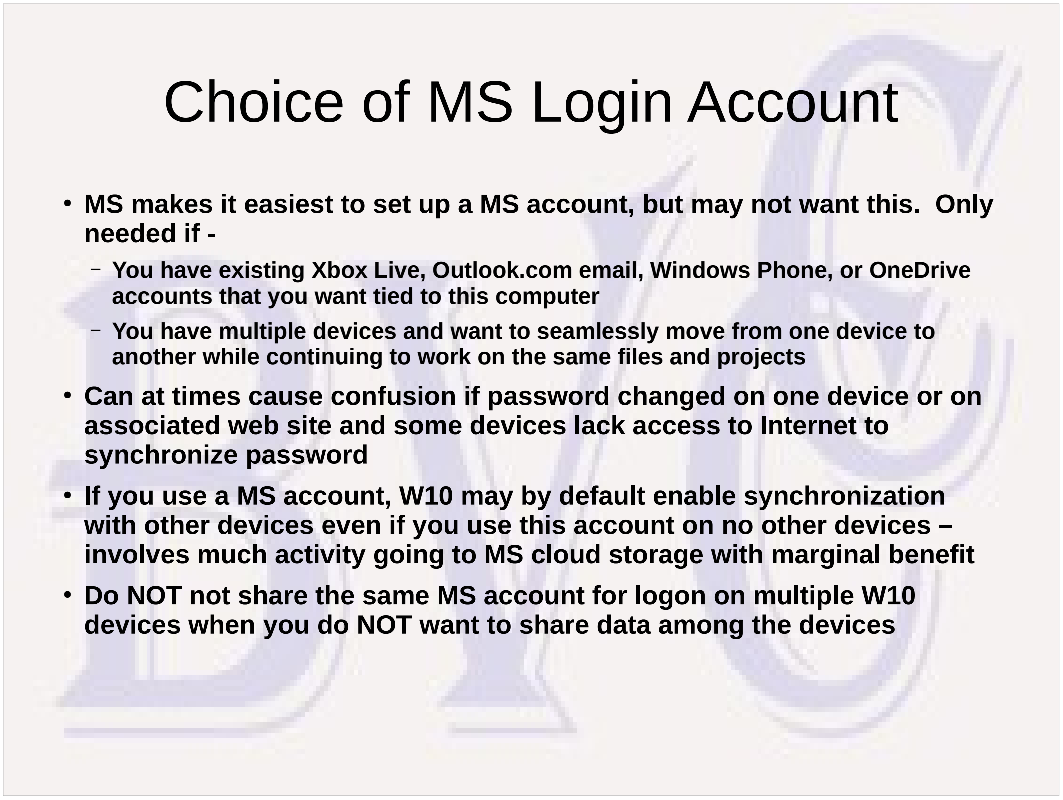
Or use your favorite email

Create password

Reenter password

Country/region: United States

Sign in without a Microsoft account

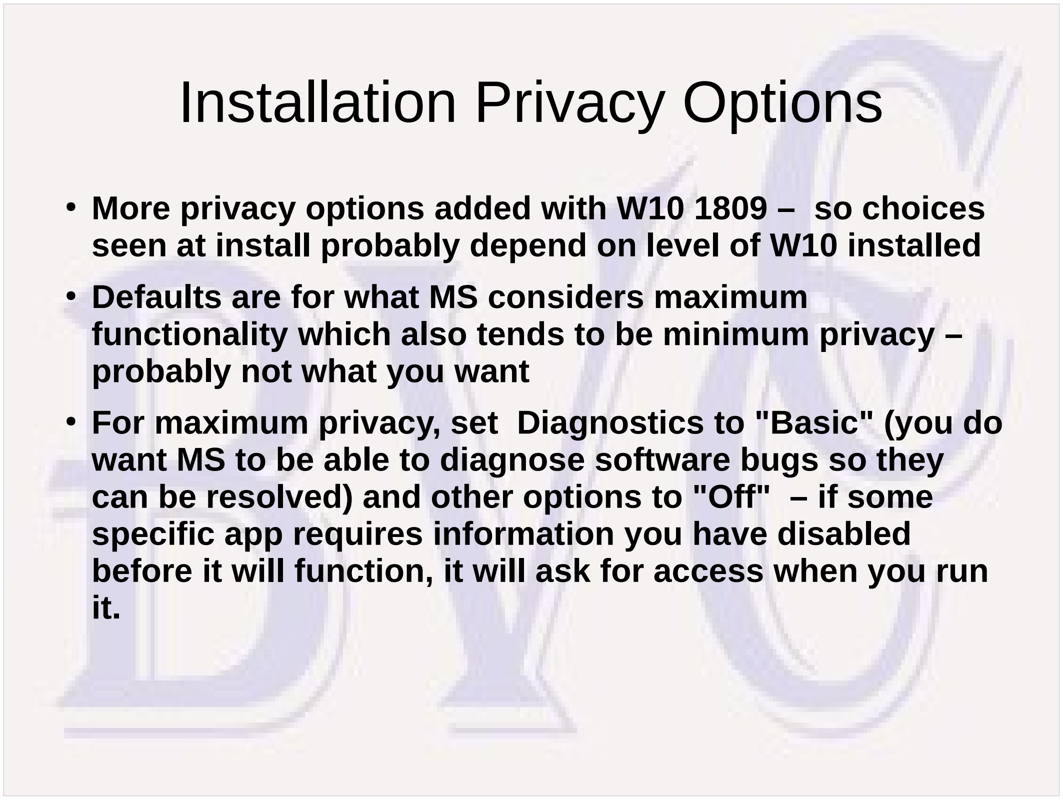


Choice of MS Login Account

- MS makes it easiest to set up a MS account, but may not want this. Only needed if -
  - You have existing Xbox Live, Outlook.com email, Windows Phone, or OneDrive accounts that you want tied to this computer
  - You have multiple devices and want to seamlessly move from one device to another while continuing to work on the same files and projects
- Can at times cause confusion if password changed on one device or on associated web site and some devices lack access to Internet to synchronize password
- If you use a MS account, W10 may by default enable synchronization with other devices even if you use this account on no other devices – involves much activity going to MS cloud storage with marginal benefit
- Do NOT not share the same MS account for logon on multiple W10 devices when you do NOT want to share data among the devices

Choice of Local Login Account

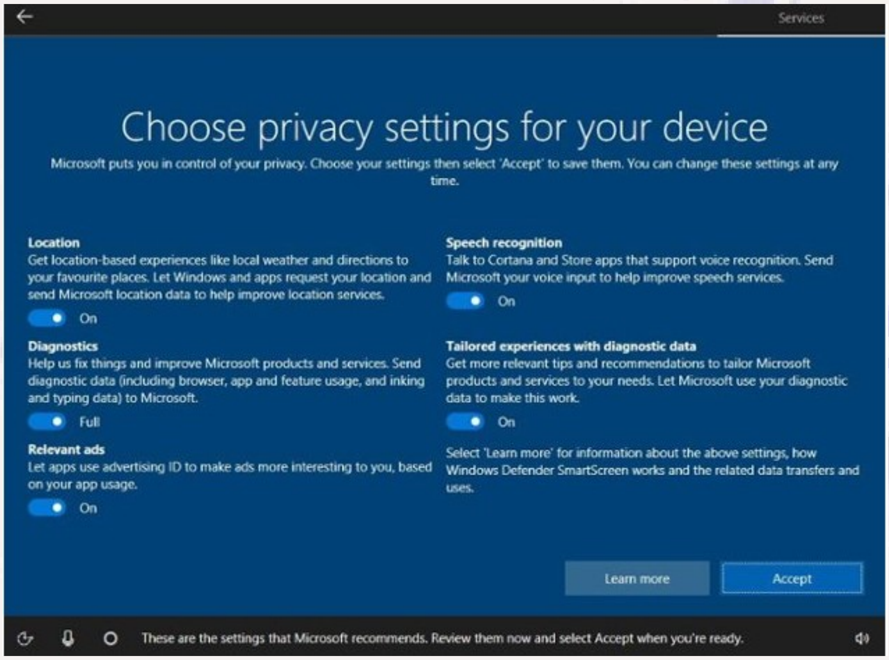
- **Select the barely-visible "sign in without a Microsoft account" option**
- **Allows specification of a simple username and password as on earlier Windows versions**
- **Even if you normally want to use a Microsoft account for logon, having a local admin login account as a backup can be useful**



Installation Privacy Options

- **More privacy options added with W10 1809 – so choices seen at install probably depend on level of W10 installed**
- **Defaults are for what MS considers maximum functionality which also tends to be minimum privacy – probably not what you want**
- **For maximum privacy, set Diagnostics to "Basic" (you do want MS to be able to diagnose software bugs so they can be resolved) and other options to "Off" – if some specific app requires information you have disabled before it will function, it will ask for access when you run it.**

Installation Privacy Options



Choose privacy settings for your device

Microsoft puts you in control of your privacy. Choose your settings then select 'Accept' to save them. You can change these settings at any time.

Location
Get location-based experiences like local weather and directions to your favourite places. Let Windows and apps request your location and send Microsoft location data to help improve location services.
On

Diagnostics
Help us fix things and improve Microsoft products and services. Send diagnostic data (including browser, app and feature usage, and inking and typing data) to Microsoft.
Full

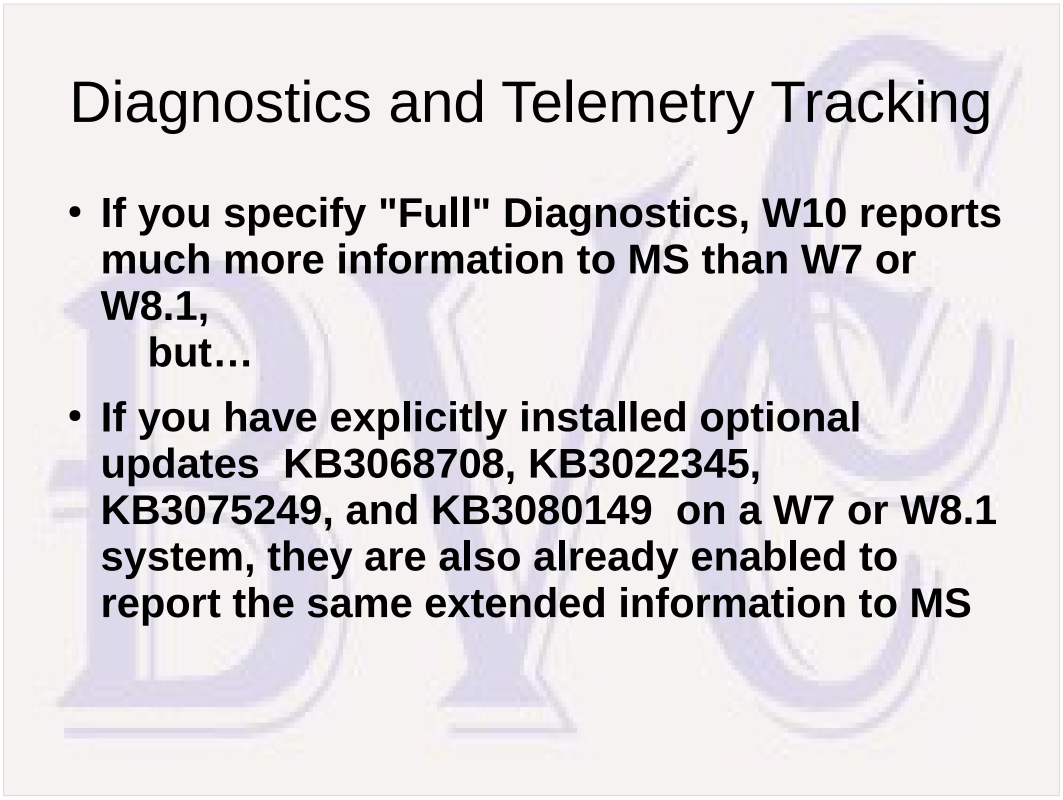
Relevant ads
Let apps use advertising ID to make ads more interesting to you, based on your app usage.
On

Speech recognition
Talk to Cortana and Store apps that support voice recognition. Send Microsoft your voice input to help improve speech services.
On

Tailored experiences with diagnostic data
Get more relevant tips and recommendations to tailor Microsoft products and services to your needs. Let Microsoft use your diagnostic data to make this work.
On

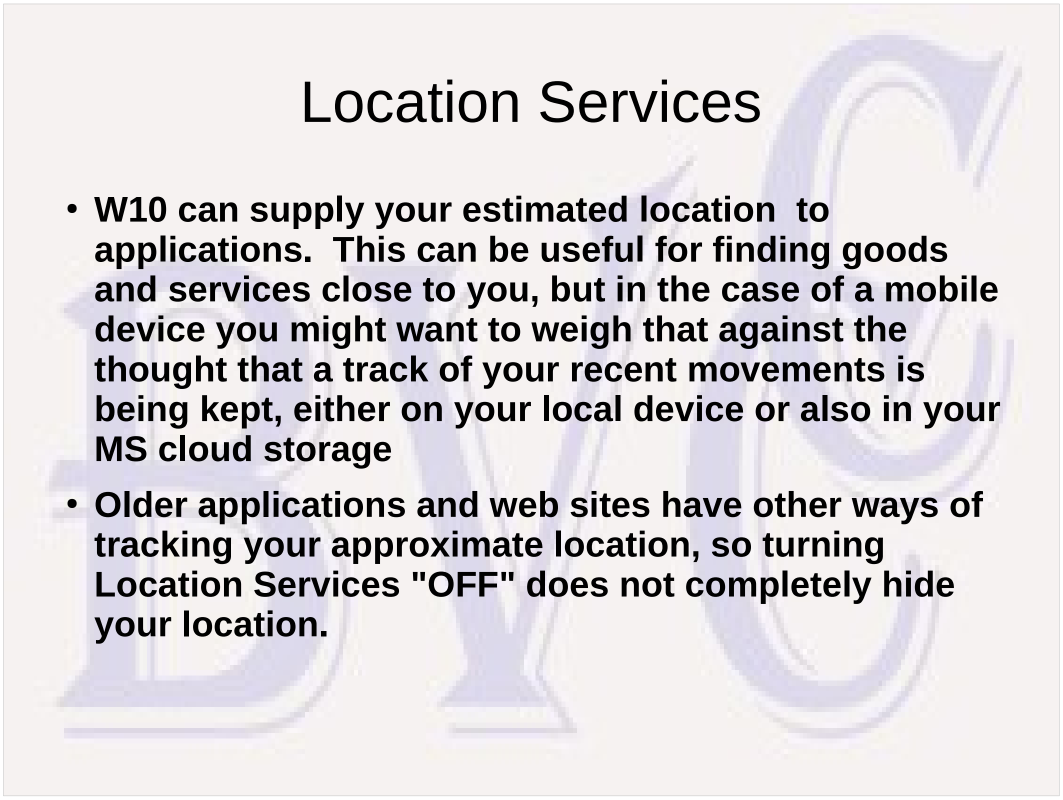
Select 'Learn more' for information about the above settings, how Windows Defender SmartScreen works and the related data transfers and uses.

These are the settings that Microsoft recommends. Review them now and select Accept when you're ready.



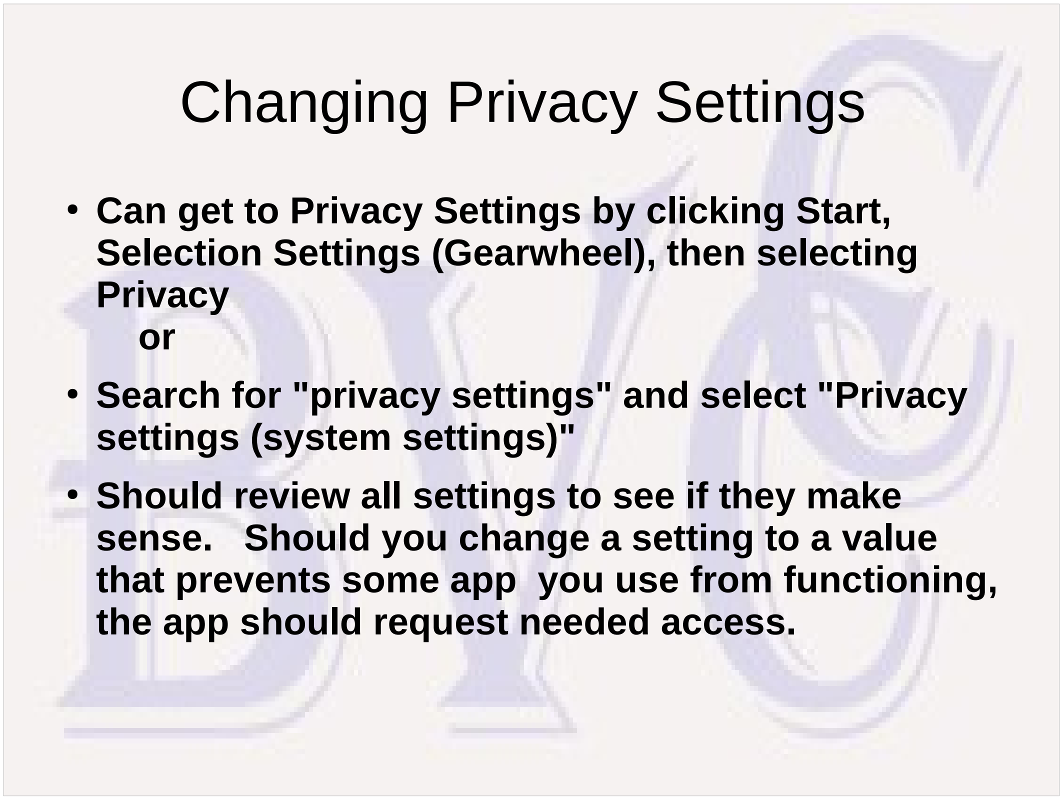
Diagnostics and Telemetry Tracking

- **If you specify "Full" Diagnostics, W10 reports much more information to MS than W7 or W8.1,**
  but…
- **If you have explicitly installed optional updates KB3068708, KB3022345, KB3075249, and KB3080149 on a W7 or W8.1 system, they are also already enabled to report the same extended information to MS**



Location Services

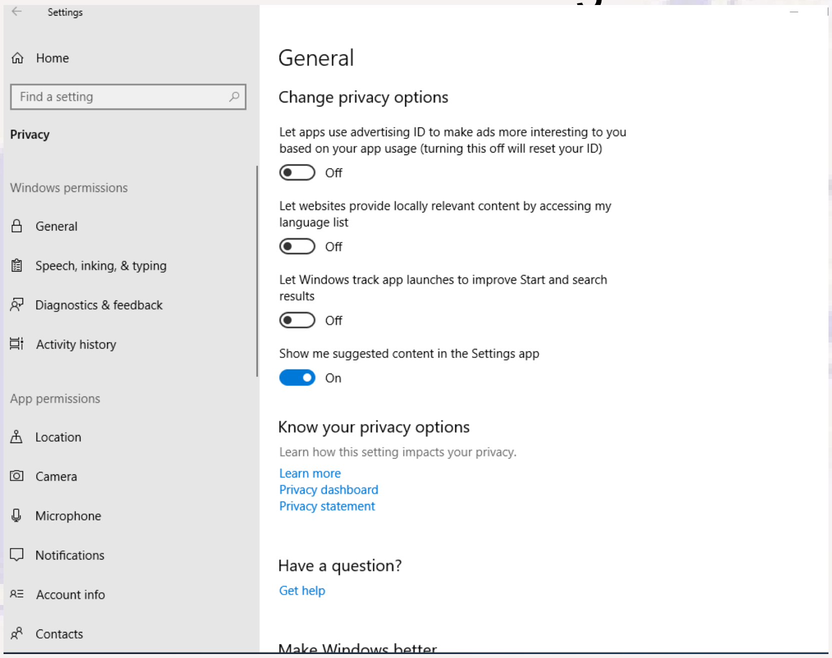
- W10 can supply your estimated location to applications. This can be useful for finding goods and services close to you, but in the case of a mobile device you might want to weigh that against the thought that a track of your recent movements is being kept, either on your local device or also in your MS cloud storage
- Older applications and web sites have other ways of tracking your approximate location, so turning Location Services "OFF" does not completely hide your location.



Changing Privacy Settings

- **Can get to Privacy Settings by clicking Start, Selection Settings (Gearwheel), then selecting Privacy**
  or
- **Search for "privacy settings" and select "Privacy settings (system settings)"**
- **Should review all settings to see if they make sense.   Should you change a setting to a value that prevents some app you use from functioning, the app should request needed access.**

General Settings



General

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app usage (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

Know your privacy options

Learn how this setting impacts your privacy.

Learn more
Privacy dashboard
Privacy statement

Have a question?

Get help

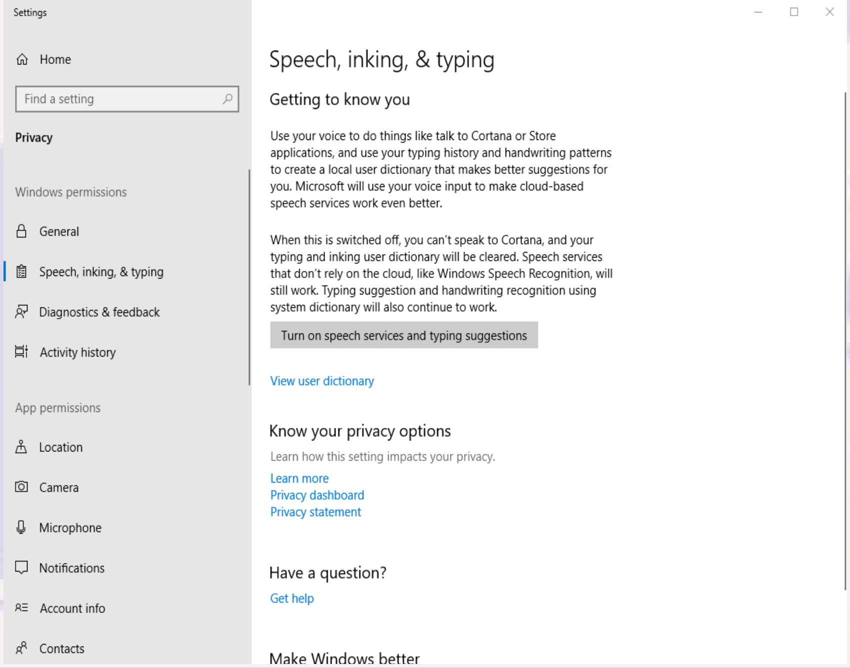
Make Windows better

Turning off Advertising ID doesn't turn off all ads, just some targeted ads.

Language list reveals some info about you, but could allow a web site that supports multiple languages to default to a language you can read.

App tracking reveals a lot about how you use your computer, but if you ask for help while running an app, it makes it more likely the answer is relevant.

Speech, inking, & typing



Speech, inking, & typing

Getting to know you

Use your voice to do things like talk to Cortana or Store applications, and use your typing history and handwriting patterns to create a local user dictionary that makes better suggestions for you. Microsoft will use your voice input to make cloud-based speech services work even better.

When this is switched off, you can't speak to Cortana, and your typing and inking user dictionary will be cleared. Speech services that don't rely on the cloud, like Windows Speech Recognition, will still work. Typing suggestion and handwriting recognition using system dictionary will also continue to work.

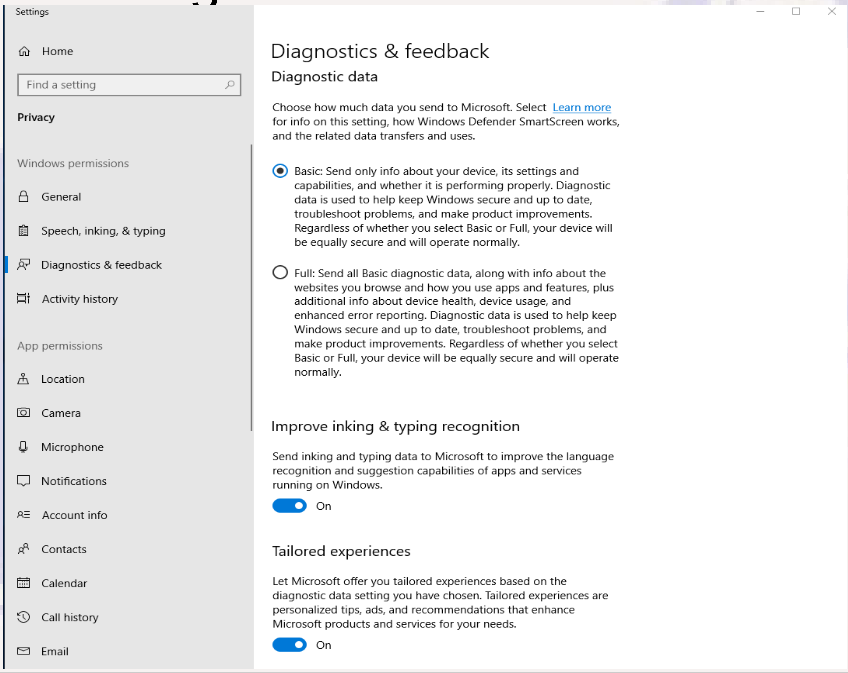
Know your privacy options

Learn how this setting impacts your privacy.

Have a question?

Make Windows better

Diagnostics & Feedback



Diagnostics & feedback

Diagnostic data

Choose how much data you send to Microsoft. Select Learn more for info on this setting, how Windows Defender SmartScreen works, and the related data transfers and uses.

● Basic: Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements. Regardless of whether you select Basic or Full, your device will be equally secure and will operate normally.

○ Full: Send all Basic diagnostic data, along with info about the websites you browse and how you use apps and features, plus additional info about device health, device usage, and enhanced error reporting. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements. Regardless of whether you select Basic or Full, your device will be equally secure and will operate normally.

Improve inking & typing recognition

Send inking and typing data to Microsoft to improve the language recognition and suggestion capabilities of apps and services running on Windows.

On

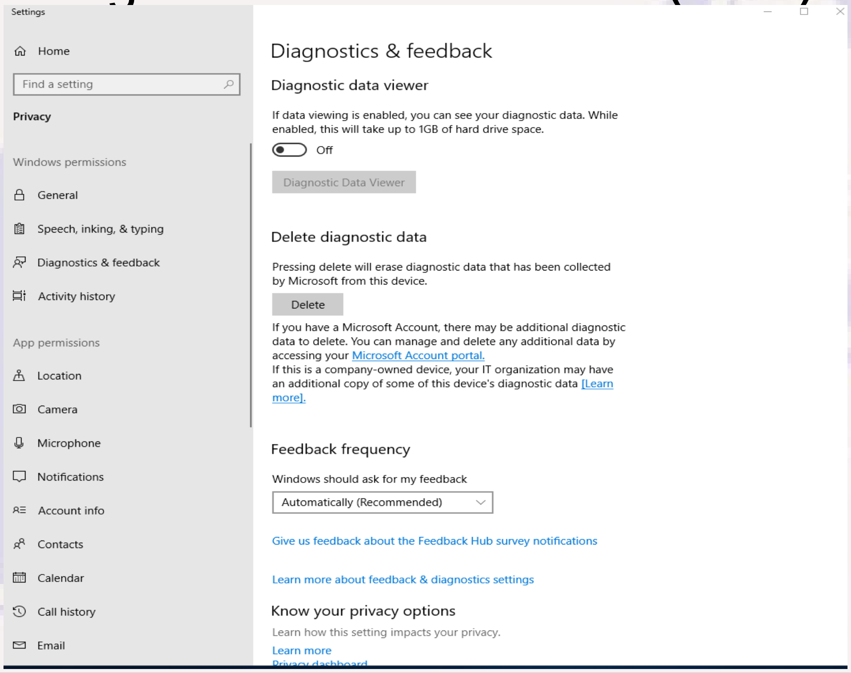
Tailored experiences

Let Microsoft offer you tailored experiences based on the diagnostic data setting you have chosen. Tailored experiences are personalized tips, ads, and recommendations that enhance Microsoft products and services for your needs.

On

You want MS to have enough info to fix problems with Windows 10, but probably not more than that.

Diagnostics & Feedback (cont)



Diagnostics & feedback

Diagnostic data viewer

If data viewing is enabled, you can see your diagnostic data. While enabled, this will take up to 1GB of hard drive space.

Off

Delete diagnostic data

Pressing delete will erase diagnostic data that has been collected by Microsoft from this device.

If you have a Microsoft Account, there may be additional diagnostic data to delete. You can manage and delete any additional data by accessing your Microsoft Account portal.
If this is a company-owned device, your IT organization may have an additional copy of some of this device's diagnostic data [Learn more].

Feedback frequency

Windows should ask for my feedback

Automatically (Recommended)

Give us feedback about the Feedback Hub survey notifications

Learn more about feedback & diagnostics settings

Know your privacy options

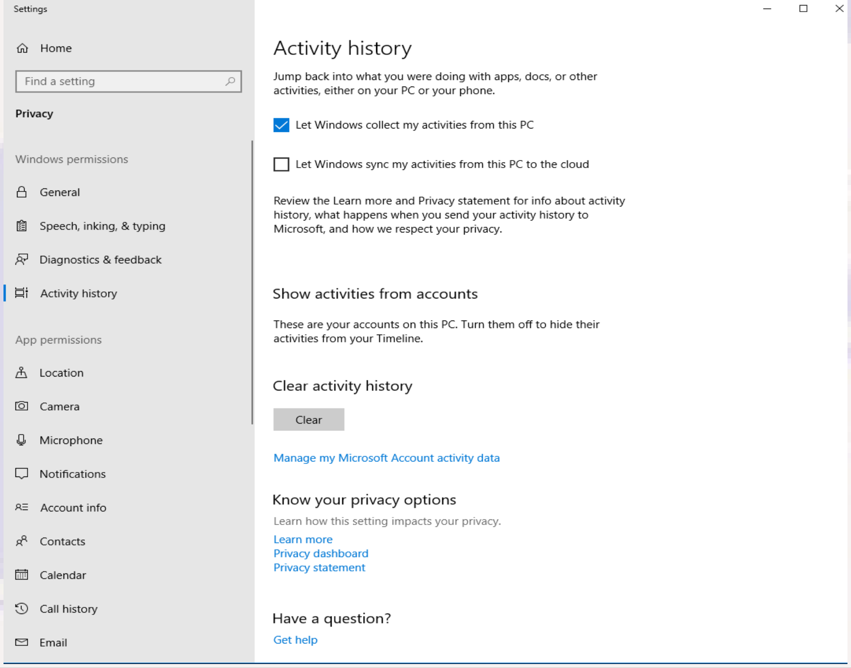
Learn how this setting impacts your privacy.

Learn more
Privacy dashboard

If 1 GB of hard drive space is not an issue, viewing diagnostic data might be interesting.

Provides ability to delete diagnostics data that has been collected.

Activity History



Activity history

Jump back into what you were doing with apps, docs, or other activities, either on your PC or your phone.

☑ Let Windows collect my activities from this PC

□ Let Windows sync my activities from this PC to the cloud

Review the Learn more and Privacy statement for info about activity history, what happens when you send your activity history to Microsoft, and how we respect your privacy.

Show activities from accounts

These are your accounts on this PC. Turn them off to hide their activities from your Timeline.

Clear activity history

Clear

Manage my Microsoft Account activity data

Know your privacy options

Learn how this setting impacts your privacy.

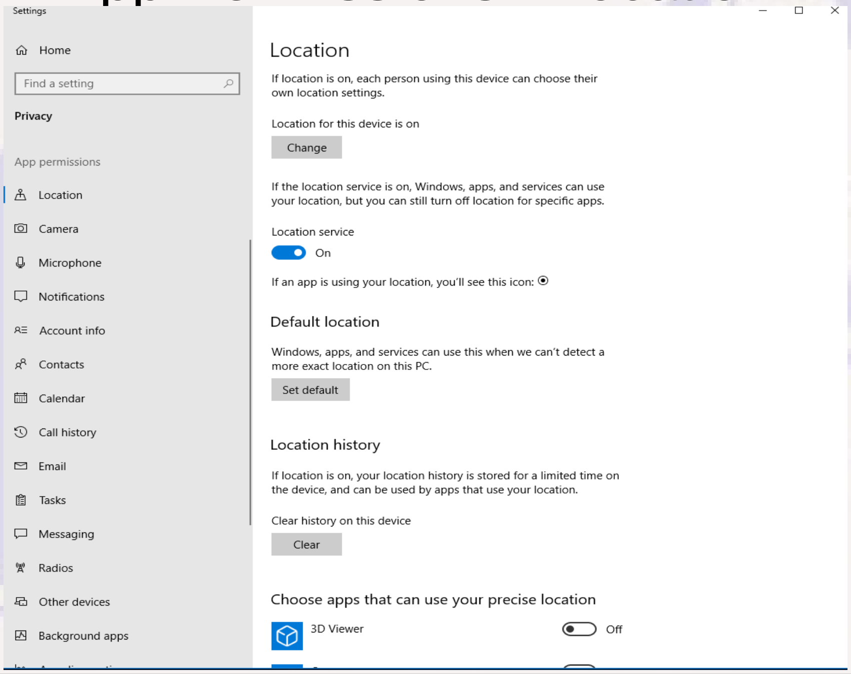
Learn more
Privacy dashboard
Privacy statement

Have a question?

Get help

There are no accounts shown because this W10 system has only a local login account.

App Permissions - Location



Location

If location is on, each person using this device can choose their own location settings.

Location for this device is on

Change

If the location service is on, Windows, apps, and services can use your location, but you can still turn off location for specific apps.

Location service

On

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

Default location

Windows, apps, and services can use this when we can't detect a more exact location on this PC.

Set default

Location history

If location is on, your location history is stored for a limited time on the device, and can be used by apps that use your location.

Clear history on this device

Clear

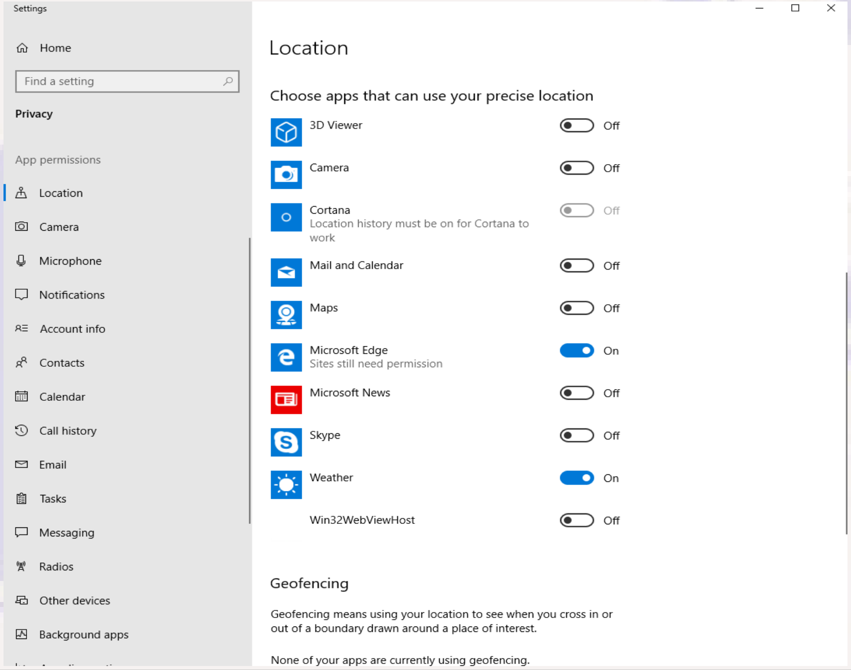
Choose apps that can use your precise location

3D Viewer — Off

This illustrates the typical pattern for App Permissions: You can turn off access for all apps globally, or leave global access on and disable access for specific apps that have asked for access. Would recommend also turning off access for all listed apps if you turn off global access Reason: If a denied app requests access when you run it and you agree, it probably turns on global access, which may allow other apps access as well unless you turned them off.

Note apps installed from MS Store play by the rules. Apps installed from other sources may not.

Permissions - Location



Settings

Home

Find a setting

Privacy

App permissions

Location

Camera

Microphone

Notifications

Account info

Contacts

Calendar

Call history

Email

Tasks

Messaging

Radios

Other devices

Background apps

Location

Choose apps that can use your precise location

3D Viewer Off

Camera Off

Cortana Off
Location history must be on for Cortana to work

Mail and Calendar Off

Maps Off

Microsoft Edge On
Sites still need permission

Microsoft News Off

Skype Off

Weather On

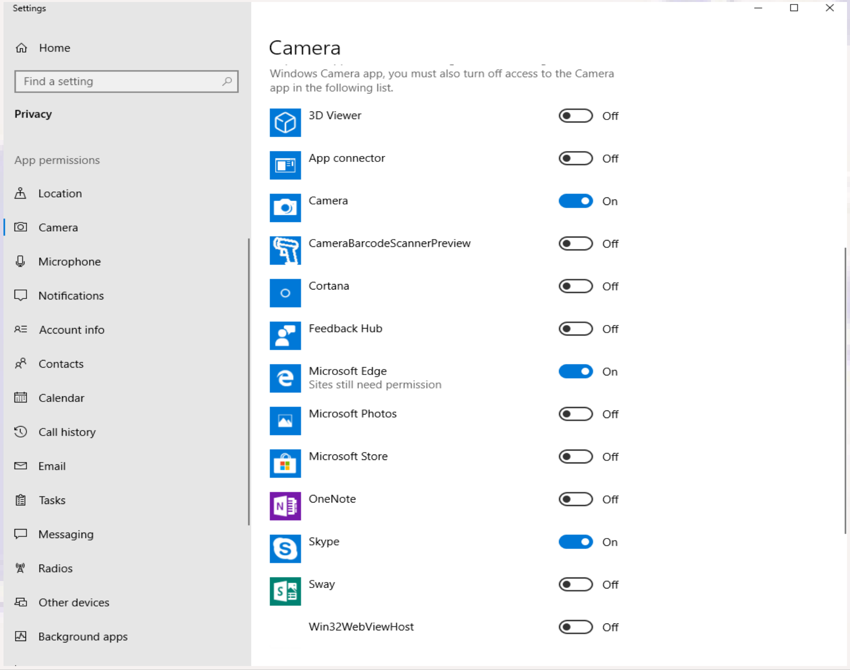
Win32WebViewHost Off

Geofencing

Geofencing means using your location to see when you cross in or out of a boundary drawn around a place of interest.

None of your apps are currently using geofencing.

Permissions - Camera



Camera

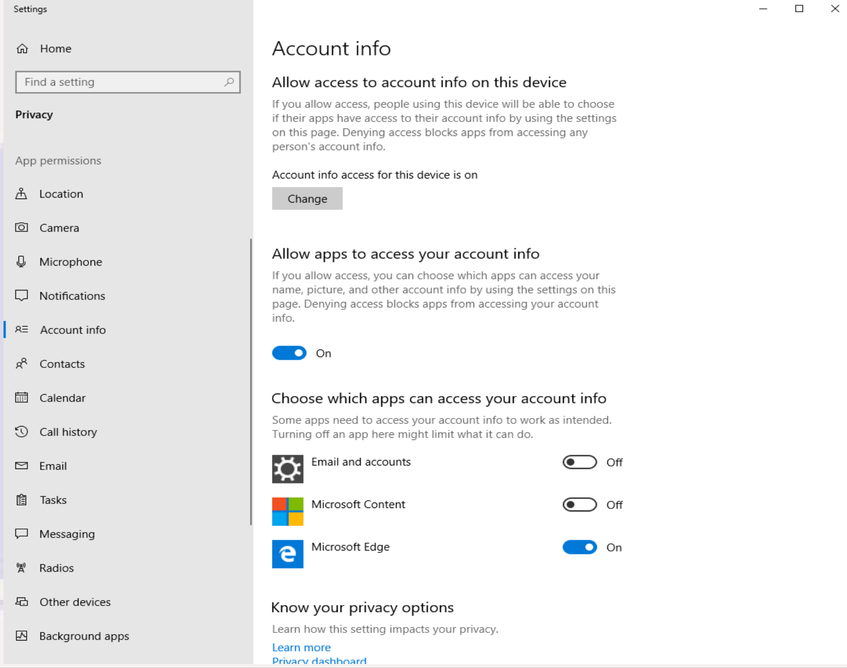
Windows Camera app, you must also turn off access to the Camera app in the following list.

3D Viewer	Off
App connector	Off
Camera	On
CameraBarcodeScannerPreview	Off
Cortana	Off
Feedback Hub	Off
Microsoft Edge Sites still need permission	On
Microsoft Photos	Off
Microsoft Store	Off
OneNote	Off
Skype	On
Sway	Off
Win32WebViewHost	Off

There are rogue apps and malware in existence that can access a camera without turning on the "camera active" LED. If you want an extra line of defense, keep something opaque over the camera when not intentionally using it.

Permissions for Camera and microphone access are only effective for newer apps that play by the rules. If you need a more positive way to disable these devices and rarely use them, use the "Device Manager" application to disable these devices when not in use and enable them only when you actually need to use them.

Permissions – Account Info



Account info

Allow access to account info on this device

If you allow access, people using this device will be able to choose if their apps have access to their account info by using the settings on this page. Denying access blocks apps from accessing any person's account info.

Account info access for this device is on

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	Off
Microsoft Content	Off
Microsoft Edge	On

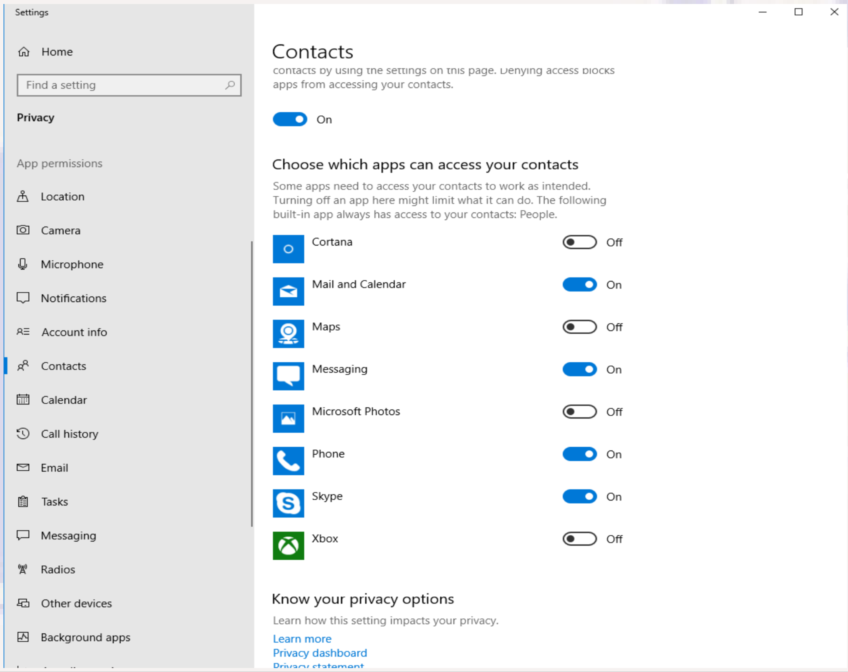
Know your privacy options

Learn how this setting impacts your privacy.

Learn more

Privacy dashboard

Permissions – Contacts



Contacts

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.

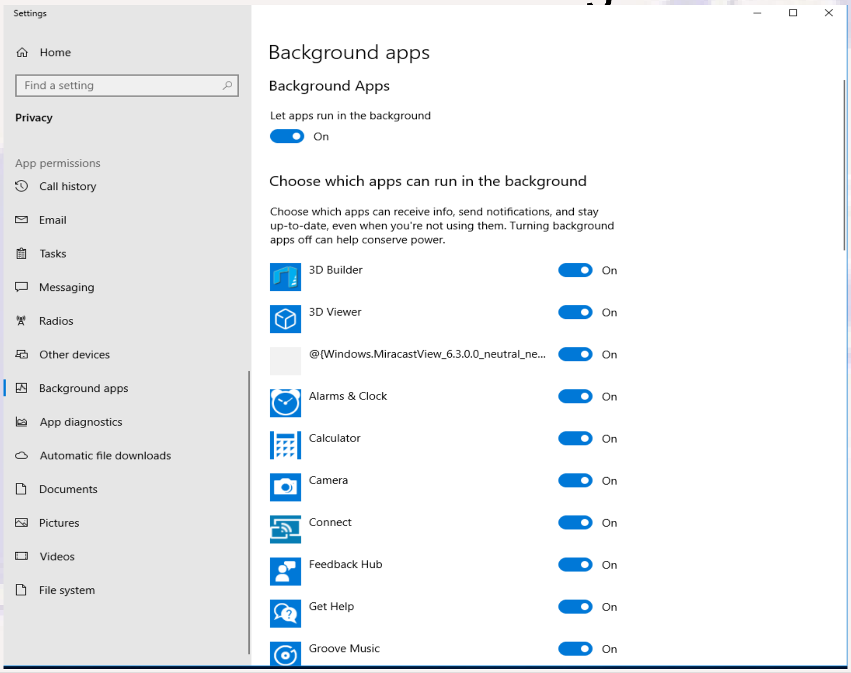
Cortana	Off
Mail and Calendar	On
Maps	Off
Messaging	On
Microsoft Photos	Off
Phone	On
Skype	On
Xbox	Off

Know your privacy options

Learn how this setting impacts your privacy.

Learn more
Privacy dashboard
Privacy statement

Permissions – Background



Settings

Home

Find a setting

Privacy

App permissions

Call history

Email

Tasks

Messaging

Radios

Other devices

Background apps

App diagnostics

Automatic file downloads

Documents

Pictures

Videos

File system

Background apps

Background Apps

Let apps run in the background

On

Choose which apps can run in the background

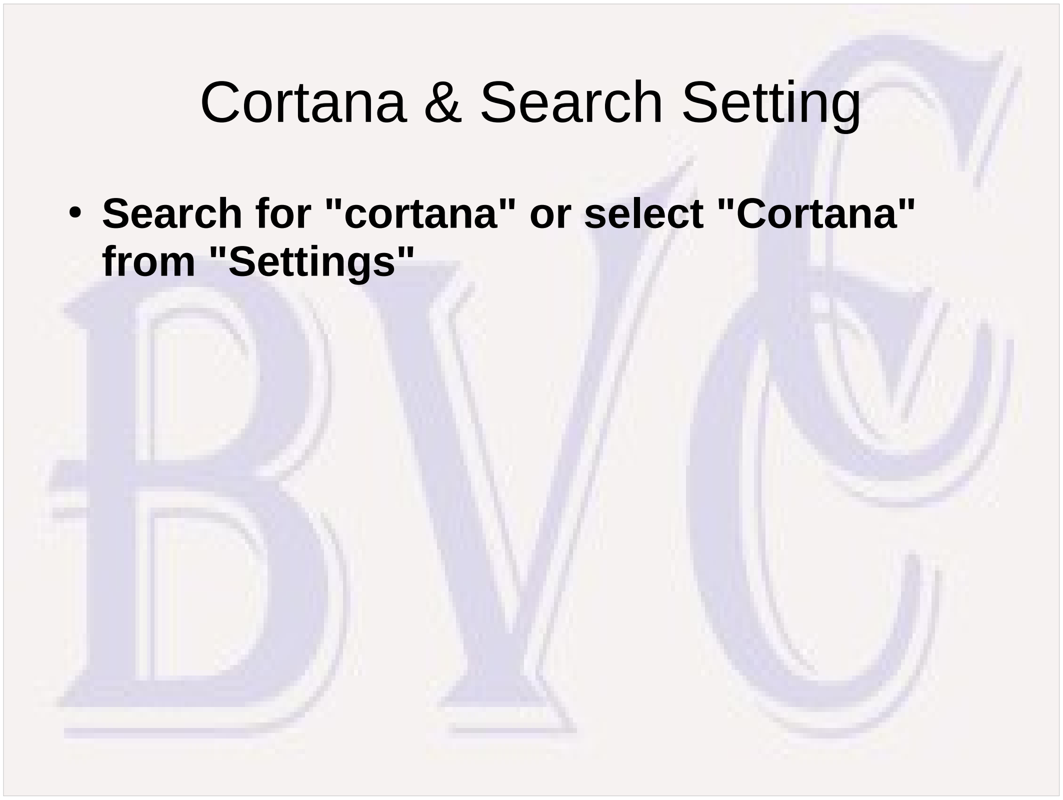
Choose which apps can receive info, send notifications, and stay up-to-date, even when you're not using them. Turning background apps off can help conserve power.

3D Builder	On
3D Viewer	On
@{Windows.MiracastView_6.3.0.0_neutral_ne...	On
Alarms & Clock	On
Calculator	On
Camera	On
Connect	On
Feedback Hub	On
Get Help	On
Groove Music	On

Apps running in background increase power consumption on a mobile device.

Some apps like "Alarms & Clock" seem obvious candidates that should run all the time.

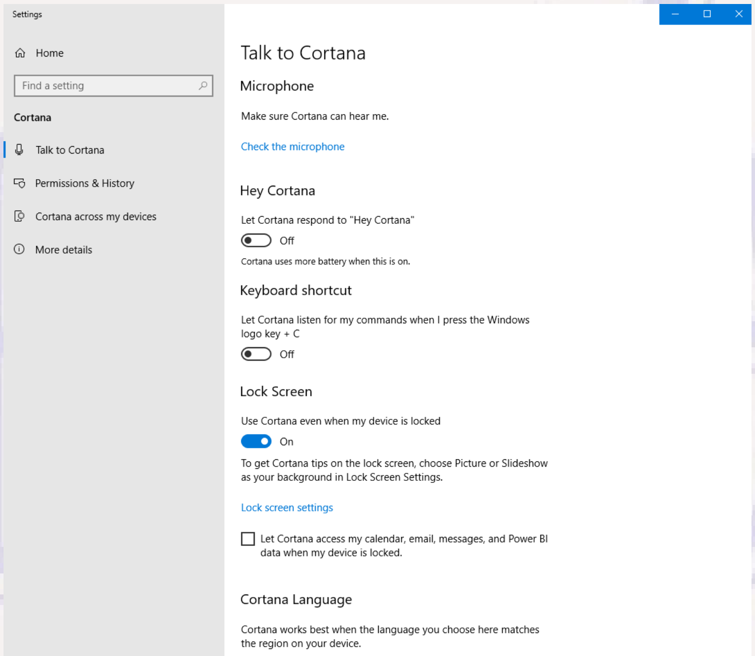
Others like "Calculator" and "3D Viewer" seem unreasonable to run in background when you are not viewing it, and yet that is the default.



Cortana & Search Setting

- **Search for "cortana" or select "Cortana" from "Settings"**

Talk To Cortana



Talk to Cortana

Microphone

Make sure Cortana can hear me.

Check the microphone

Hey Cortana

Let Cortana respond to "Hey Cortana"

Off

Cortana uses more battery when this is on.

Keyboard shortcut

Let Cortana listen for my commands when I press the Windows logo key + C

Off

Lock Screen

Use Cortana even when my device is locked

On

To get Cortana tips on the lock screen, choose Picture or Slideshow as your background in Lock Screen Settings.

Lock screen settings

□ Let Cortana access my calendar, email, messages, and Power BI data when my device is locked.

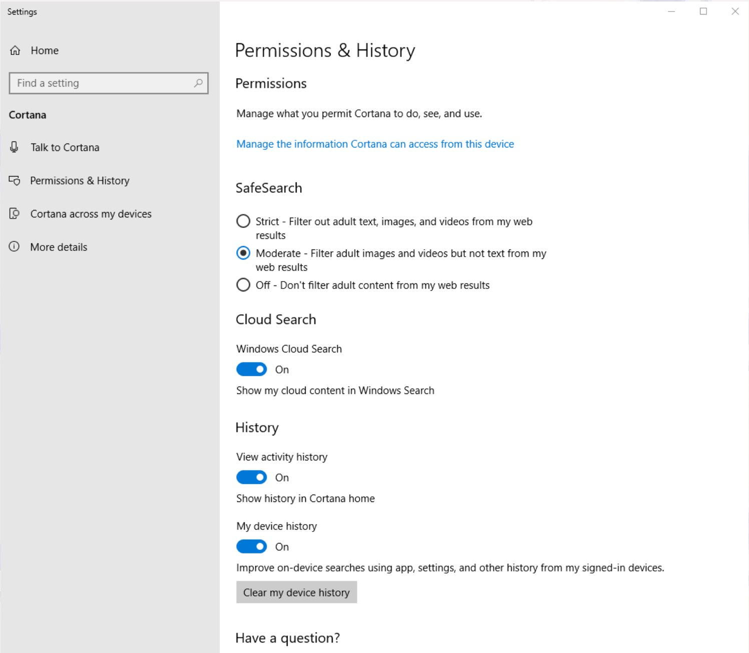
Cortana Language

Cortana works best when the language you choose here matches the region on your device.

If you don't have a microphone, or don't want to talk to your computer, turn off support

If you leave support on, you probably don't want Cortana to respond to voice commands when your computer is locked.

Cortana Permissions & History



Permissions & History

Permissions

Manage what you permit Cortana to do, see, and use.

Manage the information Cortana can access from this device

SafeSearch

○ Strict - Filter out adult text, images, and videos from my web results

● Moderate - Filter adult images and videos but not text from my web results

○ Off - Don't filter adult content from my web results

Cloud Search

Windows Cloud Search

On

Show my cloud content in Windows Search

History

View activity history

On

Show history in Cortana home

My device history

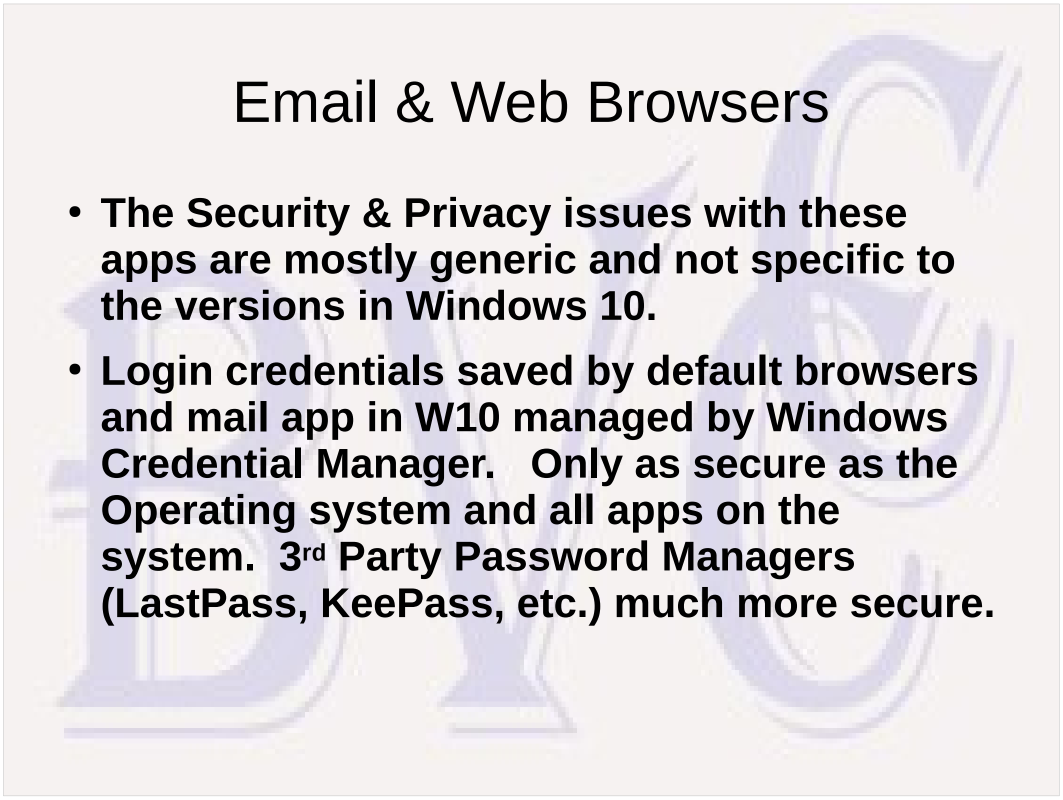
On

Improve on-device searches using app, settings, and other history from my signed-in devices.

Have a question?

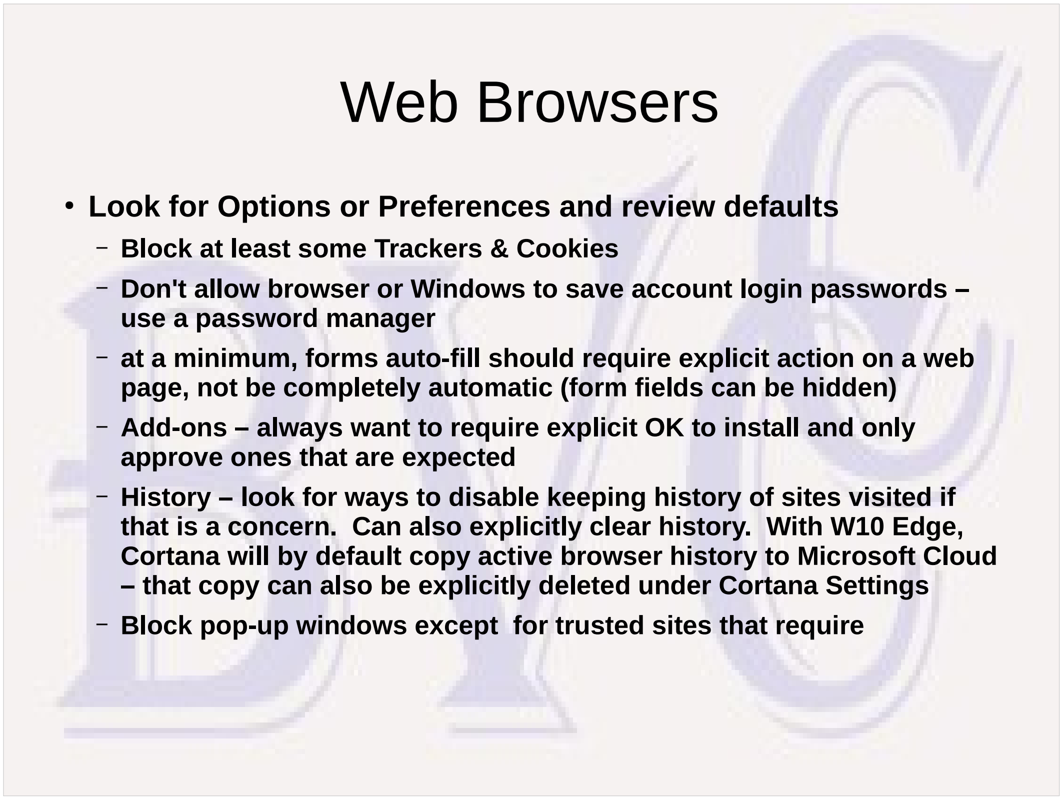
Various search and history options.

Also way to delete Cortana history.



Email & Web Browsers

- **The Security & Privacy issues with these apps are mostly generic and not specific to the versions in Windows 10.**
- **Login credentials saved by default browsers and mail app in W10 managed by Windows Credential Manager. Only as secure as the Operating system and all apps on the system. 3rd Party Password Managers (LastPass, KeePass, etc.) much more secure.**



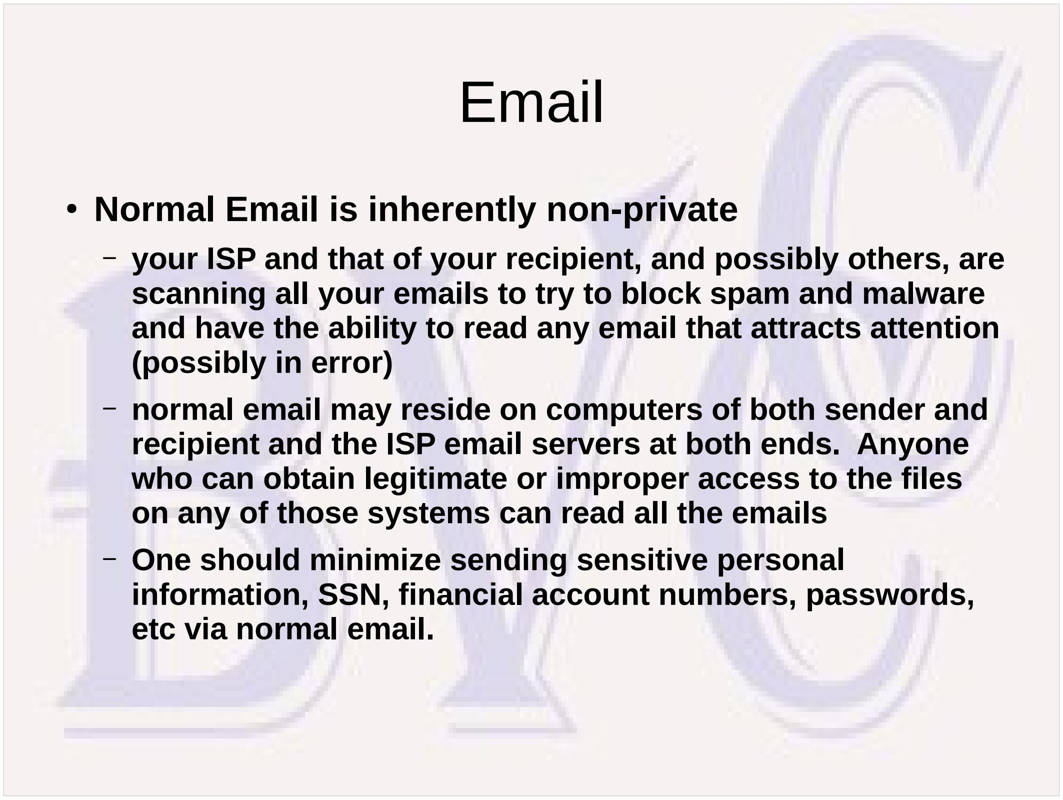
Web Browsers

- Look for Options or Preferences and review defaults
  - Block at least some Trackers & Cookies
  - Don't allow browser or Windows to save account login passwords – use a password manager
  - at a minimum, forms auto-fill should require explicit action on a web page, not be completely automatic (form fields can be hidden)
  - Add-ons – always want to require explicit OK to install and only approve ones that are expected
  - History – look for ways to disable keeping history of sites visited if that is a concern. Can also explicitly clear history. With W10 Edge, Cortana will by default copy active browser history to Microsoft Cloud – that copy can also be explicitly deleted under Cortana Settings
  - Block pop-up windows except for trusted sites that require

W10 Credentials Manager not as secure as Password managers – access to system or files by a rogue app can extract login credentials.

Password Managers encrypt credentials so that credentials are secure even if containing files are obtained.

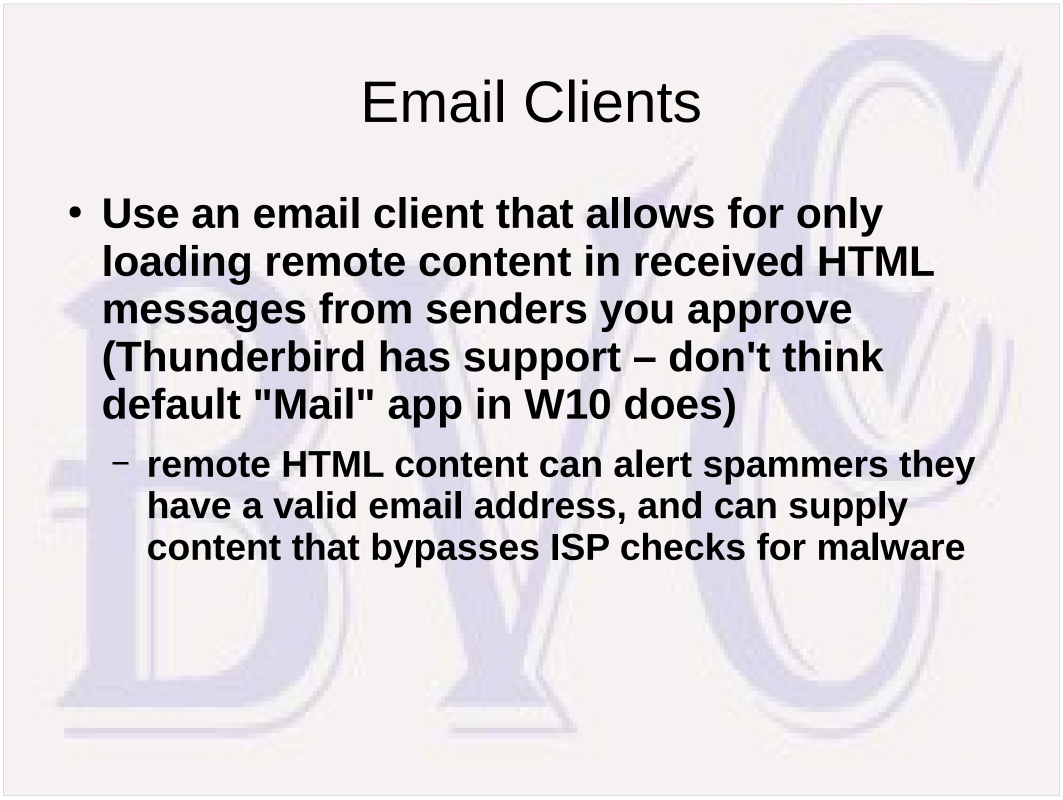
Firefox encrypts saved login credentials iff a master password is used, but the encryption key is saved and can be found. Takes more work but login credentials can still be extracted.



Email

- **Normal Email is inherently non-private**
  - **your ISP and that of your recipient, and possibly others, are scanning all your emails to try to block spam and malware and have the ability to read any email that attracts attention (possibly in error)**
  - **normal email may reside on computers of both sender and recipient and the ISP email servers at both ends. Anyone who can obtain legitimate or improper access to the files on any of those systems can read all the emails**
  - **One should minimize sending sensitive personal information, SSN, financial account numbers, passwords, etc via normal email.**

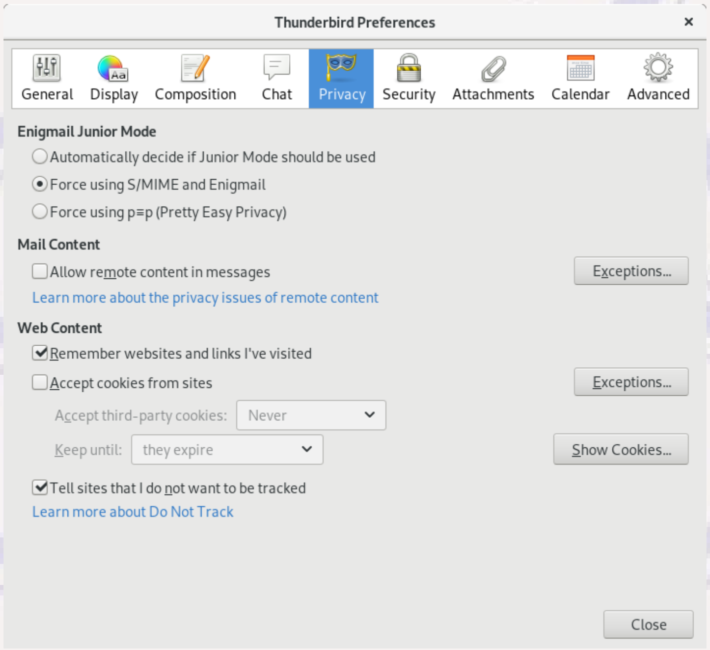
There actually is a standard for securely encrypted and signed email that can guarantee privacy, and some email clients like Thunderbird have support for it; but it can be tricky to set up and use. To exchange encrypted emails, every user must set up a private key which only he possesses and carefully guards, a public key which he shares with all who need to send encrypted email to him or who need to verify his signature on securely signed emails from him, and an email client that will manage his keys and the public keys from others and do the required encryption/decryption.



Email Clients

- Use an email client that allows for only loading remote content in received HTML messages from senders you approve (Thunderbird has support – don't think default "Mail" app in W10 does)
  - remote HTML content can alert spammers they have a valid email address, and can supply content that bypasses ISP checks for malware

TB Privacy Settings



Enigmail Junior Mode

○ Automatically decide if Junior Mode should be used
● Force using S/MIME and Enigmail
○ Force using p≡p (Pretty Easy Privacy)

Mail Content

□ Allow remote content in messages   Exceptions...

Learn more about the privacy issues of remote content

Web Content

☑ Remember websites and links I've visited
□ Accept cookies from sites   Exceptions...

Accept third-party cookies: Never
Keep until: they expire   Show Cookies...

☑ Tell sites that I do not want to be tracked

Learn more about Do Not Track

Enigmail options not there by default – only present if encrypted email support installed with TB.

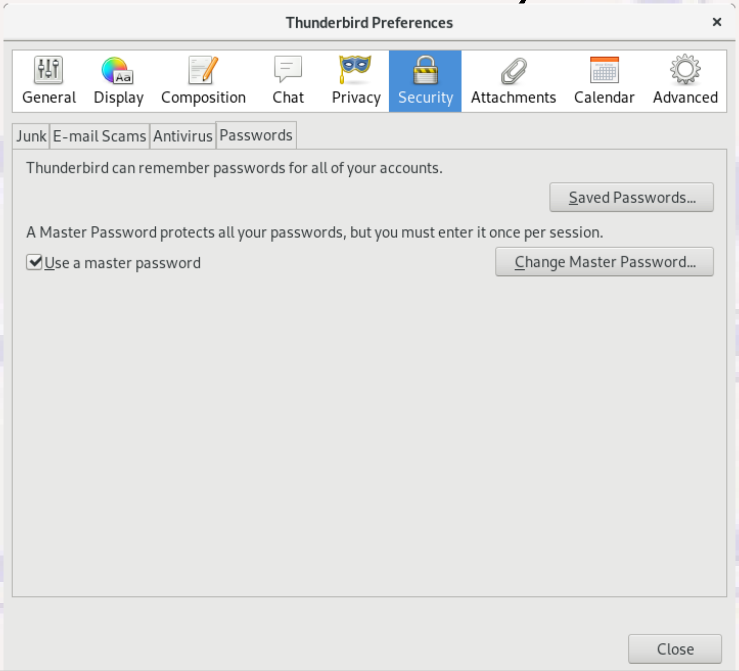
Remote content not allowed here means TB will give you option of allowing loading of remote content when viewing a specific email

Cookies shouldn't be needed to display HTML formatted emails – seems questionable to allow. Might affect behavior if you go to a link in the email, but then that's a bad idea for other reasons

Email Clients

- **Logins & Passwords – email clients check frequently for new email and must have some way to store and re-use email account login info to be practical, but some methods are safer than others.**
  - **W10 Mail app uses W10 Credentials Manager.**
  - **Thunderbird must have a Master Password to be secure and is insecure without it (which allows anyone with access to your system or the files on your system to obtain your email logins)**
  - **login credential security with Webmail depends on how credentials are secured with your browser**

TB Security

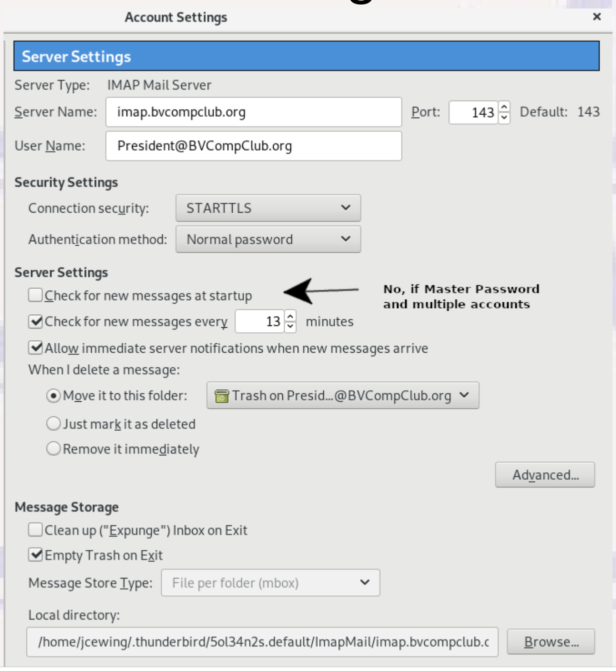


Thunderbird can remember passwords for all of your accounts.

A Master Password protects all your passwords, but you must enter it once per session.

☑ Use a master password

TB Account Setting w Master Pwd



Account Settings ×

Server Settings

Server Type: IMAP Mail Server

Server Name: imap.bvcompclub.org Port: 143 Default: 143

User Name: President@BVCompClub.org

Security Settings

Connection security: STARTTLS

Authentication method: Normal password

Server Settings

☐ Check for new messages at startup

No, if Master Password and multiple accounts

☑ Check for new messages every 13 minutes

☑ Allow immediate server notifications when new messages arrive

When I delete a message:

● Move it to this folder: Trash on Presid...@BVCompClub.org

○ Just mark it as deleted

○ Remove it immediately

Message Storage

☐ Clean up ("Expunge") Inbox on Exit

☑ Empty Trash on Exit

Message Store Type: File per folder (mbox)

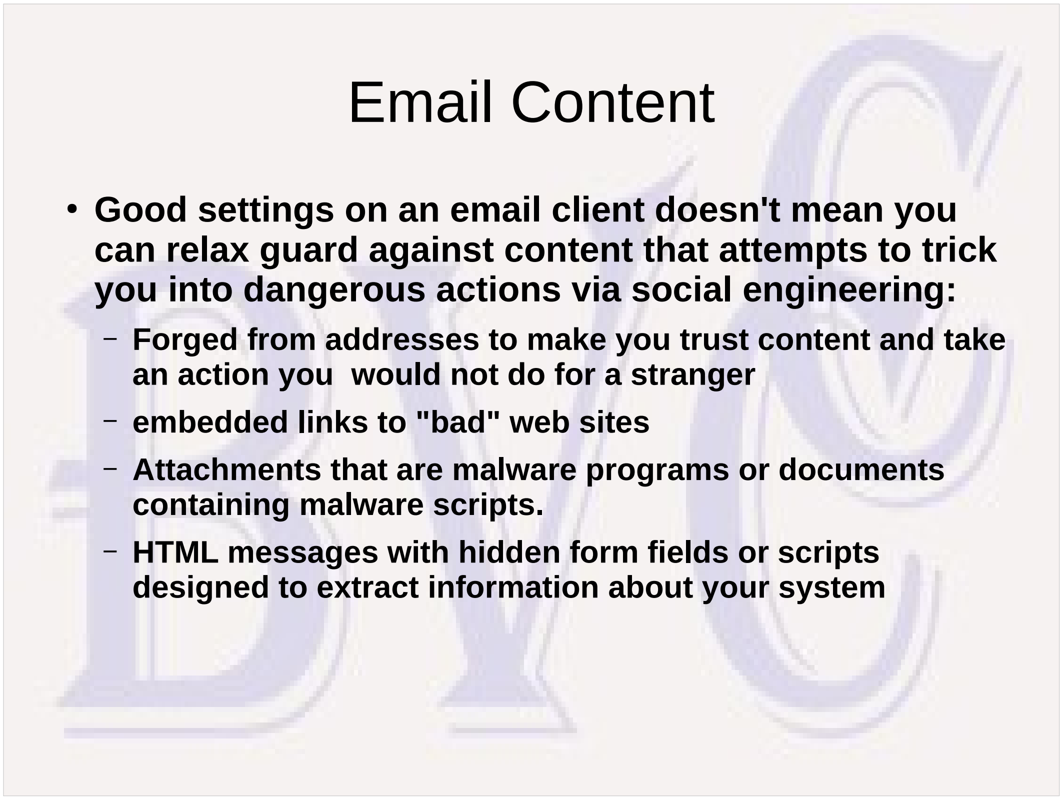
Local directory:

/home/jcewing/.thunderbird/5ol34n2s.default/ImapMail/imap.bvcompclub.c

If you use a Master Password with Thunderbird and you have multiple email accounts defined, want to uncheck "Check for new messages at startup" for all accounts; otherwise, will be flooded with multiple requests for the master password at startup. With that feature unchecked, the first email account INBOX folder you attempt to look at will result in a single request to supply the master password.

Email

- **Return Receipts**
  - **Email protocol allows the sender to request a return receipt when email is opened by recipient. Rarely used by legitimate emails these days.**
  - **Default behavior should be to ask if a receipt should be sent and only OK a receipt under special circumstances when certain of sender's identity.**
  - **Avoid setting for auto-receipts or reflex manual sending of a requested receipt because spammers love to know they have reached a valid email address**



Email Content

- Good settings on an email client doesn't mean you can relax guard against content that attempts to trick you into dangerous actions via social engineering:
  - Forged from addresses to make you trust content and take an action you would not do for a stranger
  - embedded links to "bad" web sites
  - Attachments that are malware programs or documents containing malware scripts.
  - HTML messages with hidden form fields or scripts designed to extract information about your system