Bits & Bytes

Arkansas' Premier Computer Club

February 2019

Bella Vista Computer Club - John Ruehle Center

Highlands Crossing Center, 1801 Forest Hills Blvd Suite 208 (lower level), Bella Vista, AR 72715

Website: http://www.BVCompClub.org Email: editor@bvcompclub.org

HOW TO FIND US

All meetings are on the lower level of the Highlands Crossing Center in Bella Vista. You may use entrance A on the West side or entrance C on the South side and take the elevator or stairs to the lower level. Turn left (West) to reach the General Meeting room, right for the John Ruehle Training Center. Additional information is on our web site.

MEETINGS

Board Meeting: February 11, 6:00 pm, John Ruehle Training Center

General Meeting: February 11, (2nd Monday), 7:00 pm, Community Room 1001.
Program: Joel Ewing will present a program on "Does Windows 10 Have Privacy Issues?"

Bring a guest! New Members and Guests are always welcome at the General Meeting

Genealogy SIG: February 16 (meets 3rd Saturday of the month).

MEMBERSHIP

Single membership is $20; $10 for each additional family member. Join by mailing an application (from the web site) with check, or complete an application

HELP CLINICS

Saturday, February 2, 9am – noon
Wednesday, February 20, 9am – noon
Saturday, March 2, 9am – noon

Help clinics are a free service for BVCC club members, held in the Training Center

Bring your tower, laptop, tablet or smartphone for problem solving.

CLASSES

"Computer Security for Regular People, Part 2" – Justin Sell, Tuesday, February 19, 6:30 – 8:30 pm
Part 1 will be offered again on 3rd Tuesday in February.

Advance sign up required for classes: Contact Grace: email to edu@bvcompclub.org, text 469-733-8395, call 479-270-1643, or sign up at the General Meeting. Classes are **free to Computer Club members** and are at our John Ruehle Training Center.

Check the monthly calendar and announcements for any last minute schedule changes at http://bvcompclub.org .

Windows 10 and Privacy

By Joel Ewing, President, Bella Vista Computer Club
President (at) bvcompclub.org
Bits & Bytes, February 2019
www.bvcompclub.org

The research that produced this article was done in response to concerns expressed by several of our members. A search on the Internet can locate comments by some who argue that Windows 10 engages in activity that looks highly suspicious – that if one migrates from older versions of Windows to Windows 10, Microsoft could be seeing entirely too many details of your personal activity and put your privacy at risk. These views don't tend to be based on serious analysis.[1] The general gist of the criticism of Windows 10 is "I have observed the connection attempts from my computer to sites controlled by Microsoft and they are so frequent as to suggest spyware". There tends to be minimal analysis on the nature of the connections, what data may actually be involved, and what Windows options may have been chosen that are causing them.

It is true that Microsoft is by default collecting much more data about your usage of Windows 10 than with previous versions of Windows, but there are also ways to disable significant parts of this data collection if that seems too intrusive to you. A good overview of Windows 10 options can be found at https://www.avg.com/en/signal/windows-10-privacy-everything-you-need-to-know-to-keep-windows-10-from-spying-on-you .

If you use the Internet in any significant way – browsing the web, exchanging email, engaging in social media, searching the web, making on-line purchases – your privacy is already greatly exposed no matter what Operating System you run, in ways unknown and to parties unknown who may have no motivation to guard your data. Many web sites have no known physical location, no permanent presence, and no business relationship with you, and no motivation to treat data about you with care if is a salable commodity. Microsoft at least has a strong motivation to not abuse the trust of its users, as any such abuse would inevitably be reported someday and could destroy their future customer base.

By all expert accounts, Windows 10 is a more secure platform than prior versions of Windows, and its forced update model and reasonably adequate built-in anti-virus defenses are more likely to keep it secure. By far, the most serious and damaging privacy threat is a system whose security can be breached. If that happens to your computer, you can lose the privacy of anything stored on that system and must assume that all your sensitive data could be in the hands of someone with evil intent.

Microsoft at least tells you what types of data they are collecting and how they intend to use the data[2]. Most of that usage is to improve the Windows platform reliability or add function in some way. One announced use that does seem questionable is that some data may be used for targeted advertising and marketing. I would prefer an option to opt out of all advertising, not just targeted advertising, but I haven't seen an option for that. Of course

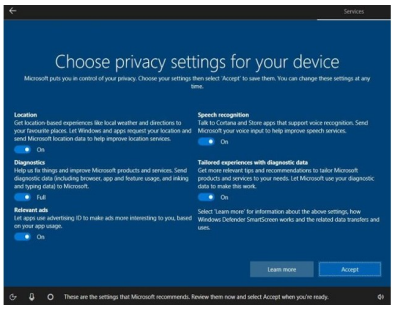
1 https://www.zdnet.com/article/when-it-comes-to-windows-10-privacy-dont-trust-amateur-analysts/
2 Microsoft Privacy Statement https://privacy.microsoft.com/en-US/privacystatement

the reality is that any app you install on top of Windows may have its own internal rules for advertising, targeted or otherwise.

While I am uncomfortable about providing too much personal data to Microsoft, it is not not so much a distrust of Microsoft as a concern that too much data from too many people at one location makes that location such an extremely attractive target to attack – that someone, someday will find a way to compromise and abuse the data. So as a matter of principle, I want to reduce the amount of that data unless it is mandatory to support some function that is valuable to me.

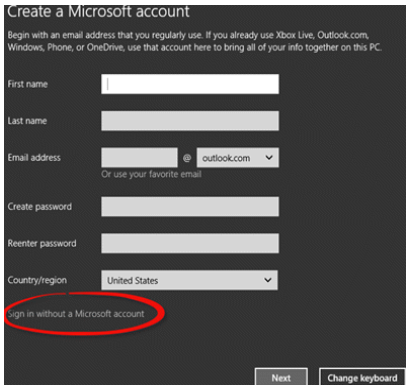
THE NATURE OF THE EXPOSURE[3]

Initial Windows 10 Configuration



When initially configuring Windows 10 you will be asked to set a number of new privacy options. The defaults are designed to give the most "enhanced" behavior of Windows, but this is likely more data than you wish to provide to Microsoft. As a good first start, you may want to turn all these options off. They can all be changed later later if need be (search for Privacy Settings).

While it is possible to initially install Windows 10 using a local account instead of a Microsoft account, this is subtly hidden at the bottom of a "Create a Microsoft Account" screen as "Sign in without a Microsoft account". Microsoft makes it easier to set up Windows 10 with a Microsoft outlook.com logon account, which is then associated with Microsoft cloud storage on one of their servers. This makes it possible to synchronize your Windows 10 activity and settings on this device with your Windows 10 activity on other devices on which you use that same account logon, allowing you to move from one device to another and continue work that is in progress. This requires making copies of your recent "active" files and recent actions on Microsoft servers, resulting in activity to Microsoft servers to keep that data synchronized. You are dependent on Microsoft to keep that data suitably secure. If this is a feature that is useless to you, you should at a minimum disable synchronization, and possibly consider setting up a local-only login instead of an outlook.com login for Windows 10..



Specific Apps

To make Cortana a powerful digital assistant, your location, your language, and your requests to Cortana are collected and whatever Cortana does to produce results could end up stored in some Microsoft server. Microsoft says that will treat your data as confidential and not share with outsiders; but does admit there are circumstances where they must allow access by law enforcing agencies

Other Apps that run under Windows 10 may be given access to your location, information about your hardware, and information derived from a microphone or camera. Writing tools such as OneNote may extract information from your typing or voice to improve dictionaries that may reside on Microsoft servers. Generally when installing new apps that require such access, you will be given an option to approve or deny such access, but the function of

3 https://www.thewindowsclub.com/privacy-issues-in-windows-10 and other sources such as https://www.avg.com/en/signal/windows-10-privacy-everything-you-need-to-know-to-keep-windows-10-from-spying-on-you .

the App may be reduced if access is not granted. Since installing additional apps could always introduce additional privacy exposures, this is one of many reasons why you should avoid installation of Apps from un-trusted sources and frivolous or "cute" apps you don't really need. Those exposures from added Apps existed on previous Windows versions, but perhaps weren't always as visible.

Diagnostics and Telemetry Tracking

Windows 10 enhanced the Diagnostics and Telemetry Tracking feature that was also present in Windows 7 and 8.1 and this feature defaults to "Full" tracking. Those enhancements have also been added into Windows 7 and 8.1 as optional updates KB3068708, KB3022345, KB3075249, and KB3080149. If you manually selected those optional updates for installation, then Windows 7 and Window 8.1 have this same potential data exposure just like Windows 10. The level of tracking can be customized to reduce tracking data, but the default option must be manually changed.

Location Services

Windows 10 can supply an estimate of your location to apps that are allowed to access Location Services. Even laptops and desktops that do not have GPS or hardware to obtain location information from cell towers to directly determine their location have ways to indirectly approximate your location fairly closely. Your devices will communicate on the Internet with an IP address that is assigned by your Internet Provider. Your assigned IP address by itself will typically narrow your location at least to a specific town. Almost every home and business these days has a WiFi network. Everyone passing through your neighborhood with a smart mobile devices with GPS and WiFi capability can see the presence of your WiFi signal even if they cannot access your network, and the presence of your WiFi signal is used to update databases maintained by Apple, Google, Microsoft and perhaps others to map the approximate location of your WiFi signal. That data allows connection to or mere proximity to a WiFi network to be sufficient in many cases to zero in on your location. As an experiment on my laptop, I went to Privacy → Location to set my Default Location on Windows 10, and without manually doing anything it estimated the location of my laptop on my home WiFi within 500 feet of my actual location. That must mean my WiFi signal ID, or maybe that of one of my neighbors, has been mapped that closely in the various databases. My ISP-assigned IP address rarely changes, so I wouldn't rule out the possibility that my current IP address could also be associated that closely to my actual location in some database.

HOW TO IMPROVE PRIVACY IN WINDOWS 10

Some of the tips below are specific to particular apps on Windows 10 and not issues with the Windows 10 Operating System itself. Some of these setting could already be set the right way depending on what privacy options were selected when Windows 10 was initially configured.

Reducing Telemetry in Windows 10

To set telemetry in the Windows 10 Home or Windows 10 Pro editions (the two most common editions) to the lowest possible level is not possible. There are procedures you can find on-line that claim to do this, but they only work on other less-common editions of Windows 10. It is, however, fairly simple to scale back the amount of Telemetry data sent to Microsoft from the default "Full" to a "Basic" level: search for "Privacy Settings" and select that, select "Feedback & diagnostics", Change "Diagnostic data" to "Basic".

Reducing Customized Advertising

Under the same "Privacy" settings as above, select "General" and set "Let apps use advertising ID" to "Off". This prevents different apps under Windows from being able to easily correlate information as being related to the same user. It doesn't prevent apps from retaining information specific within that app (like cookies in web browsers) that retain user history that can still be used for targeted advertising: it just makes it slightly less pervasive.

Reducing Cortana's Presence

I don't like the idea of talking to my computer, especially on a laptop that might be used in a public place. For me, typing is a more secure and precise way of communicating. A Search for "Cortana" should find "Cortana & Search settings". On that screen I run with "Hey Cortana" and "Keyboard shortcut" both turned "Off". The idea of allowing Cortana to leak information to an unauthorized user while my computer is locked also seems like a bad idea, so if audio communication with Cortana is enabled, I would also turn Off use of Cortana on a "Lock Screen".

Cortana is designed to keep track of your most recent activity with the idea of storing that information in MS Cloud storage associated with your outlook.com Windows 10 logon. Should you use the same logon on a different computer, you can then resume your interrupted activity on a different device. If this is a capability you don't need, you can reduce your exposure by going to "Privacy Settings", "Activity History" and being sure that "Let Windows sync my activities from this PC to the cloud" is NOT checked. If you only check "Let Windows collect my activities from this PC" that activity data will only be kept locally on your PC. The Activity History screen is also where you can Clear your activity history.

If you don't need Cortana to respond to voice commands, you can "Turn off speech services and typing suggestions" or verify that it is off. That option is found on "Privacy Settings" under "Speech, inking, & typing".

Camera and Microphone Access

These privacy setting only affect access by new Windows Store apps and not third-party apps like Skype for Desktop or Google Chrome. If you want to disable all access by all apps, then you need to use the Device Manager to disable these devices rather than use these privacy options.

If you do not normally use the camera or microphone on hardware that has those devices, they may be turned off for new Windows Store apps from the "Camera" and "Microphone" settings under "privacy Settings" and only turned on when there is a need to use them. Alternatively, if they are used frequently, they may be left on but only enabled for specific applications.

Should your computer become compromised by malware, there is malware in existence which can hack a web cam and even view data from the web cam without turning on the "camera active" LED. There is one simple protection against a camera hack that is 100% effective – just tape something opaque over the camera and only remove it when you actually need to use the camera.

Restricting Location Services

Although you can turn Location Services completely off, that may disable some useful functionality in Windows, like suggesting store branches that are nearer to you. Another option is to leave Location Services on, but only

enable access from specific apps. All those options are specified in the "Location" section of "Privacy Settings", which may be found by searching for "Privacy Settings".

Note that restricting use of Location Services doesn't prevent web sites or apps that communicate over the Internet from deducing your approximate location from your IP address, or from retaining explicitly given information about your location from prior visits to the site.

Bluetooth Access

Some computers (typically laptops) have hardware support for Bluetooth devices (typically limited to mice, keyboards, and audio devices including smart phones). If your device has hardware support for Bluetooth but you do not use it with Bluetooth devices, you can turn off the Bluetooth radio by going to "Privacy Settings", "Radios", and turn Off the "Let apps control radios" option. The privacy exposure from a rogue Bluetooth device should be fairly minimal, but some of my sources mentioned this.

Turning Off Access to Hotspot 2.0 Networks?

Many U.S. Airports now support Hotspot 2.0 WiFi networks, and that service will come to more locations. If you have a device with WiFi hardware, the "Network & Internet" settings will include a "WiFi" tab where Hotspot 2.0 network access my be turned On or Off. I'm still looking for a clear description on how secure these networks are, and whether they are free to use or if that depends somehow on your ISP service. Until I find a clearer description, I'm not convinced of their security or whether they are safe without an independent VPN service. While you do know that a Hotspot 2.0 network is a legitimate WiFi hot spot for the location and is encrypted, it is unclear whether your encrypted WiFi data is uniquely encrypted or still viewable by others on the same WiFi network.

Using a Local Account For a Windows 10 Logon

The initial Windows 10 setup makes it appear as if a Microsoft account is mandatory. A Microsoft account is required to access Windows Store or OneDrive cloud storage. However, having that Microsoft account also be your Windows 10 logon is only required if you want synchronization of files, settings, and browser history across multiple Windows 10 devices.

If you have no need to synchronize your activity across multiple Windows 10 devices, you do not have to use an outlook.com account to logon to Windows 10. If you have Windows 10 set up that way but want to change it to a local logon, for a procedure to change it see
https://www.howtogeek.com/230543/how-to-revert-your-windows-10-account-to-a-local-one-after-the-windows-store-hijacks-it/

Even If you want to keep a Microsoft account as your Windows 10 logon, it may be useful to add an additional local-only administrative account with a different password as an emergency logon. There can be some confusing cases when a Microsoft account password is changed and some devices using that account aren't able to connect to the Internet to synchronize with the change. A Backup administrative logon account can also be useful if you always use a short PIN to logon to your main account, and then suddenly find yourself in a boot-recovery situation where use of the PIN is not allowed, and realize the real password can no longer be found.

Web Browsers and Email Clients

Although there may be some specific issues associated with the versions of these apps included in Windows 10. the issues associated with these apps are mostly generic ones that affect most browsers and email clients, not just those running under Windows 10. Web browsing and email are the two apps most likely to expose you to Internet privacy and security threats, so they will be separately discussed.

PRIVACY SETTINGS IN WEB BROWSERS

Your Internet Service Provider (ISP) and any Internet routers between you and the web sites you visit are in a position to monitor what web sites you are visiting; and, unless you only visit secure encrypted web pages (https), your ISP and anyone in control of routers through which your traffic passes can even read the actual data being sent. The trend is for all web sites to move away from non-secure web pages, but we are not there yet. Secure web pages encrypt the data being transmitted, but can't hide what web sites you contact.

Web sites and services that you frequent on the Internet (think Google, Amazon, Facebook) can partially identify you through your IP address and cookies or explicitly identify you through your logon and retain a history of your activity on their sites. There is a good chance these sites know much more about your personal interests and beliefs than Microsoft ever will.

Each web browser used (Firefox, Chrome, Edge, Safari, etc.) has settings or preferences which likely need review and adjustment. The options and methods used to set them may be slightly different for each browser, but the types of things to look for are:

Trackers and Cookies. Ways to block at least some Trackers, and Cookies (Firefox can be set to block all and then will ask if a site should be made an exception). Many legitimate sites you may need to use will require the saving of cookies; so if a site you need to use and trust asks for permission to be an exception and save cookies you will need to grant approval.

Logins & Passwords. Browsers' default support for saving site login information should **NOT** be assumed to be secure – a password management application[4] should be used for that function It is safest just to disallow the browser saving any logon information. If Firefox is allowed to save logon information, it will explicitly ask if it should for each site, and approval should only be granted if it would be of little consequence to you if someone could get access to your credentials for the site – in other words, sites with no access to or control over financial data, no sensitive data (like email), and whose passwords don't suggest password patterns used for any of your sensitive accounts. Even if you specify a Master Password for Firefox, someone with access to the files on your computer and enough knowledge can still extract your login data from Firefox.

Forms & Autofill. As a convenience, browsers will remember field values for address-type fields to speed filling in typical fields like name, mail address, email address, city state, zip code, country, and phone number when ordering items on-line. Typing a name and/or an email may be sufficient to autofill the other values. The problem is that a web page can contain "hidden" fields, so this may be exploited to obtain more information than you think your are providing. It may look like you are only giving a name and email address to a deceptive web site when you are also giving them your mailing address and phone number in hidden fields. If this is a concern, you should turn off autofill of addresses.

---

4 LastPass, KeePass, and others.

Pop-up Windows. This is not so much a privacy issue as an annoyance, although pop-up windows can also be misused by some fraud attempts. Some sites have abused this feature for unwanted ads so much that you may want to Block pop-up windows by default. Many sites do use pop-up windows for legitimate purposes, so if you block them, you will have to authorize an exception the first time a legitimate site you trust indicates it needs to display a pop-up window to complete a function you requested.

Add-ons. A browser add on can add both good and bad or even dangerous features to your browser. You definitely want to enable any options that lets you know if any site tries to install an add-on to your browser that you didn't expect and request. If you don't trust the site or it is trying to install an add-on without explanation, it should be rejected.

History. Browsers keep a history of sites visited. This can be a useful thing on a private computer, but is bad on a public computer. Privacy settings can be used to either disable saving page history or to clear history. With Windows 10 Edge, Cortana will by default copy active browser history to the Microsoft Cloud associated with your Microsoft account. If you need to clear that copy as well, search for Cortana, select "Cortana & Search settings", select "Permissions & History", and select "Clear my device history"

PRIVACY SETTINGS FOR EMAIL CLIENTS

An email client is an app that runs on your local device and communicates with remote Internet servers to send and receive email. Another way of dealing with email is to use web mail – web site pages that are provided by the same company that provides the email account and that are accessed from a web browser to send and receive email. Most email clients tend to support more functions and have more customizable options than webmail and can be set to send and receive email from multiple email accounts. Webmail using a browser can become much more tedious if your have many email accounts – using webmail, you have to visit and logon to a different webmail site to check each separate email account.

Normal email is inherently non-private. You must assume that your Internet Service Provider (ISP) the ISP of your intended recipient, and possibly others are reading any emails you send, or at the very least scanning all your emails for keywords of interest or to determine whether you are sending spam or malware. Normally email sent between an end-user and his ISP, or between ISPs is encrypted in transit, but this is not always guaranteed, and email is not normally encrypted when it is at stored on an end-user's computer or an ISP server.

Logins & Passwords. Because of the frequency with which an email client like Thunderbird or Outlook needs to logon to check email accounts for email, it is pretty much essential that email clients be allowed to save logon credentials for sending and receiving email; but, be sure you activate whatever protection the email client provides for protecting that information. With Thunderbird, you must specify a Master Password before login credentials will be encrypted. Unlike Firefox, the encryption key used by Thunderbird to encrypt login credentials is derived directly from the master password and not stored anywhere, so with a Master Password your account information is fairly secure. Without a Master Password, anyone who can access the files on your computer can easily obtain your email login information and use your email accounts.

Mail Content. Email can contain malicious links and references to remote files and data or to dangerous attachments, and this is especially true of HTML-formatted emails. HTML formatting allows many ways for content to be hidden and disguised to escape notice. Preferences should be set to NOT "Allow remote content in messages" and NOT allow any auto-preview of attachments. You may then selectively allow individual emails

that you know can be trusted to access remote content. Downloading remote content for email from unknown sources is dangerous because references to remote content can be used to introduce malware to your computer or inform a spammer that he has reached a valid email address.

Unexpected attachments, even if they at first glance appear to be from a known party, should be treated as suspicious -- executable malware can be disguised under false names. Password protected attachments with a password provided in the email body is usually a sign of a con-artist trying to prevent email servers from auto-detecting and rejecting email with an attachment containing malware or a fraud offer. Fraud schemes use text hidden in images to circumvent spam detection.

Never completely trust web links received in emails. Some web sites (like Facebook) routinely send email with links, and when it refers to a posting by a known friend and takes you to that posting these are probably pretty safe; but keep in mind that bad people are always looking for ways to exploit your trust. Never supply logon information or other personal information to a site reached by following a link in an email.

Don't allow your email client to accept cookies via HTML. The legitimate purpose of HTML tags in email is to display nicely formatted email, not to save data from some Internet site.

Forged Email. It is easy to forge a From name on an email address, and with the right software trivial to forge both the From name and From email address. This does not require having any access to the actual email accounts of the individual whose name is forged, or that the individual have any of his personal email accounts compromised. With normal email, there is no easy option to auto-detect and reject such emails. The best defense is common sense – looking for subtle clues like an unknown email address in the From header, or a Reply-To address with an unknown email address, differences from the usual wording and formatting of emails from that friend, and awareness that any unreasonable or highly unusual requests from a supposed "friend" may indicate the email is not really from the party named in the From heading.

Return Receipts. Email protocol has a mechanism to request that a return receipt be sent to the sender when the email is opened by the recipient. Spammers very quickly subverted this feature as a device to find "good" email addresses for future spam, to the point that this is rarely used in legitimate email and email clients now default to no auto response. The setting I would recommend for Return Receipts (under "Advanced" in Thunderbird preferences) is "To allow return receipts for some messages" and to "Ask me" in all cases before sending a return receipt (this is probably the default). I don't see that many receipt requests any more, and only very rarely in special cases would I elect to send a requested return receipt. But, if some popular email client enabled auto-return receipts by default, all the spammers would quickly abuse this feature again.

Privacy of email. It is important to understand that the content of ordinary email is not really private. Copies of the email that reside on your local computer, the recipient's computer, and the email servers of the email providers for both parties are not encrypted and anyone who can gain legitimate or improper access to the files on those systems can read the emails. One should avoid sending sensitive personal information, a SSN, financial account numbers, passwords, etc. via normal email.[5]

---

5 If you need to send sensitive information to someone else over the Internet, consider setting up a temporary shared folder on some free Internet cloud storage service like DropBox, making the folder only accessible to you and the other party, and leaving a file in that folder only until the 2nd party has retrieved a copy.

There actually are standards for sending secure encrypted email and digitally-signed email over the Internet, but this is more cumbersome to use than ordinary email, not universally supported by all email clients, and not supported if you use a browser and web mail to access your email. It requires both individuals to setup their own individual public/private encryption keys, making their public keys available to the other party, and keeping their private keys under their direct physical control. Thunderbird supports this using Enigmail, and I have tested it with one of my sons to prove it actually works. When set up properly, it is completely secure from the sending computer to the receiving computer: only the intended recipient with knowledge of the private-key password of and possession of his private key file can decrypt and read the body of an email sent to him, and the recipient can also confirm from the senders public key and digital signature in the email that only the party who claims to have sent the email could have created the message.

CONCLUSIONS

There are settings in Windows 10 and in common apps that need to be changed from default values to maximize your security and privacy. With those proper precautions, privacy issues should not be a major reason for avoiding Windows 10.