MANAGING CHROME ADD-ONS

By John Krout, PATACS member

At the July 20, 2019 meeting of PATACS and OLLI OPCUG in Fairfax City, a question was raised pertaining to a recent Washington Post article reporting that many Firefox and Chrome browser add-ons were secretly reporting browser use. This means that some add-ons report the web sites you visit and possibly your name, email address and physical address, and a detailed description of your personal computer, without asking your permission to do so.

The clubs asked its members to look into this matter. Here is what I learned.

This info was prepared using Windows 10 and Chrome version 76.0.3809.100 (64-bit).

WHAT IS AN ADD-ON?

Web browsers provide various ways for third parties to add capabilities to the browsers. This is done by adding software to your computer. This could be either Java software to be executed within the browser, or an executable program or library. Some of those capabilities help you, some help the add-on publisher improve their software, some help the publisher learn about you, and some do all of that.

Chrome itself identifies two types of add-ons: **extensions and plug-ins**. Additionally, I suggest that it is important to view **cookies** as add-ons.

COOKIES

Cookies are blocks of data that are stored in your browser by a Web site. Many web sites deploy cookies to your browser. Some Web sites tell you that they do, and some do not.

Originally cookies were created for purposes such as retaining your login credentials, ID and password, for a frequently used web site such as your email provider's site, so you do not have to log in every time you visit that site. For years I have used that behavior, for instance, to access my account rapidly on Amazon.com.

Retailer web sites such as Amazon use a cookie as your *shopping cart*. The cookie in your browser remembers the products you have decided to purchase. That way, when you finally choose to pay for your purchases, the cookie tells Amazon what you want, so that Amazon can add up the prices and figure out the shipping cost and delivery dates.

Obviously, those cookies help you. You and many other people are never told that cookies are used to accomplish those useful things. At least not until you read this article.

Cookies exist because the Web was designed to be ***connectionless***, meaning that the Web server does not have any means on the server side to remember that your browser, or any other, is using the Web server. The server only knows that a browser asks for a specific Web page, and the Web server delivers that page to the browser. The Web server does not remember the pages you have accessed in the past, or your product choices, or your login ID and password.

Cookies on your computer provide that memory.

Cookies are sometimes installed without your express consent or knowledge, and these days often report a great deal of what you do with your browser to the cookie publisher. Usually the aim is to make money selling that info to advertisers, again without your consent or knowledge.

Clearly, cookies have a capability to communicate over the Internet. And cookies are now widespread. After just three weeks of ownership and very occasional use of my new desktop computer and the Firefox browser, I had over 600

Kilobytes of cookies on my hard drive. I told Firefox to prevent future cookie storage, but the 600K was installed before I told Firefox to do that.

I found that B&H Photo, a web site I access frequently when I need photo accessories, installs a cookie identifying the products I examined on that site. When I use CNN.com to look at news, that cookie informs CNN.com to load ads for those products from B&H. I got very tired of looking at those ads, and now I know how the ads are targeted at me.

Chrome also accumulates a huge number of cookies very quickly. Like many web browsers, Chrome's default behavior is to retain all cookies until the Web site owning the cookies instructs the browser to delete its cookies. That deletion usually happens around the Twelfth of Never.

A CONNECTION-CENTRIC APPLICATION EXAMPLE

An email client application such as Outlook establishes a connection so that the mail server is constantly aware that your Outlook software is connected, and also aware when you disconnect. That is how, when email addressed to you arrives at the email server, the email server can push email to your client application quickly.

Webmail, using a browser to access your email account, is not connection-centric. Instead, the browser keeps your login info in a cookie, and silently and frequently sends that to the email server. If email for you arrives in the email server, then it usually shows up in your webmail inbox within a minute or so.

HOW TO PREVENT COOKIES FROM BEING INSTALLED PERMANENTLY

You can set Chrome to permanently prevent cookies from being installed.

For some Web sites, this setting has a predictable and unwanted side effect: *you are prevented from using the site.* For instance, as mentioned above, webmail uses at least one cookie. If you have no cookie, then you cannot retrieve email. On Amazon.com, your login info is stored in a cookie, and your Shopping Cart is literally a cookie containing the identification of each product you have chosen to purchase. If you prevent such cookies from being installed and used, then you cannot make a purchase. Most retail web sites use the same approach.

I think most of us would not be happy to choose that cookie prevention approach.

So, Chrome provides another approach, a useful compromise. You can tell Chrome to allow cookies to be created, but then delete the recently created cookies each time you close your Chrome Web browser. That way the retailer cookies persist only as long as you need them, meaning while you are using the retailer web site. And when you restart Chrome, those cookies accumulated during your most recent use of Chrome are *gone*.

This compromise approach does mean that sites such as Amazon.com and your webmail site will not automatically recognize you when you open the browser and go to the site. You will be forced to log in every time you visit such a site. This is the price paid for no permanent cookies.

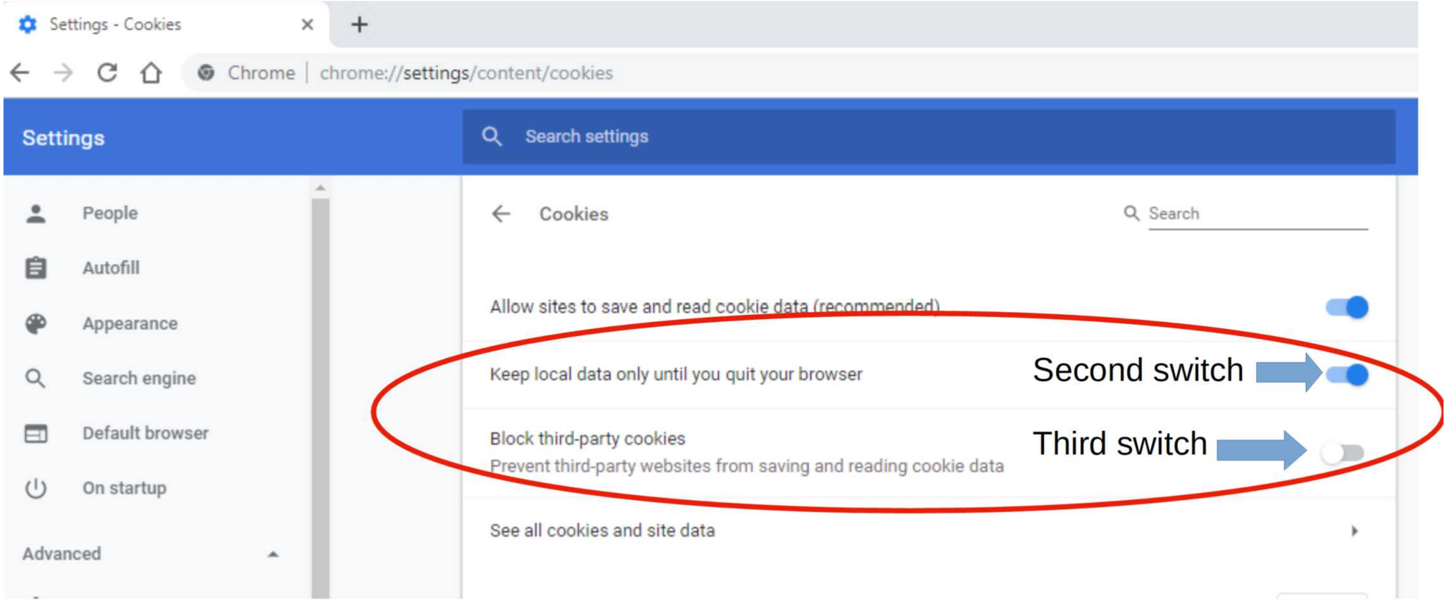
Obviously, shutting down the browser frequently minimizes the scope of the reports made by nasty cookies. Do not leave Chrome running overnight.

Here are the instructions for setting Chrome to delete all cookies created during your current use of Chrome, whenever you shut down Chrome:

1. Start the Chrome web browser

2. Go to this URL: Chrome://settings/content/cookies

A new web page appears, including three on/off switches, as shown in **Illustration 1.**



Allow sites to save and read cookie data (recommended)

Keep local data only until you quit your browser

Block third-party cookies
Prevent third-party websites from saving and reading cookie data

See all cookies and site data

Illustration 1.

3. The second switch is labeled **Keep Local Data until you quit your browser**. TURN THAT SWITCH ON, which is the position shown in Illustration 1.

4. The third switch is labeled **Block Third-Party Cookies**. TURN THAT SWITCH ON.

What does the phrase **Third-party cookies** mean? Sometimes when you browse to a web site containing advertisements, those ads are loaded from a third party's web server, and also contain cookies. That third party is frequently Doubleclick.net, but it can be many others as well. Almost inevitably, those third-party cookies track all your use of the browser, every page you visit, and report your data to the third party. All this is done without your knowledge or consent. Advertisers find this kind of info very useful for targeting ads that are likely to be of interest to you.

Turning on the third switch tells Chrome to stop loading third-party cookies.

Of course this is a never-ending battle, and the advertisers find increasingly sly and subtle ways to dodge around Chrome's prohibition. So the Chrome behavior might not succeed 100% of the time.

On the other hand, with the *second* switch set, the third party tracking cookies that do manage to dodge Chrome's prohibition won't be around long. They will be deleted when you shut down Chrome.

If you find yourself with no need to identify yourself to any Web site, then you can perhaps live with the consequences of turning off the *first* switch, the one which permits Web sites to install and read cookies. But I do not recommend it.

OTHER ADDONS

Chrome also supports other categories of add-ions: Plug-ins and Extensions.

CHROME PLUG-INS

A plug-in is a piece of software that manages Internet content that Chrome by itself is not designed to process. Probably the most widely used example is Adobe Flash, for displaying video. There are other video plug-ins as well, including Silverlight which is a Microsoft product, and QuickTime, which is an Apple product.

I am sure that the plug-ins all report some aspect of their use to their publishers, especially including crash reports. This makes sense. However, it probably means the publishers have at least considered adding a wider range of tracking capability to each plug-in.

Plug-ins are usually considered to be compiled programs or compiled software libraries that are downloaded to your computer by a Web site and can be run by Chrome when told to do so by a web site.

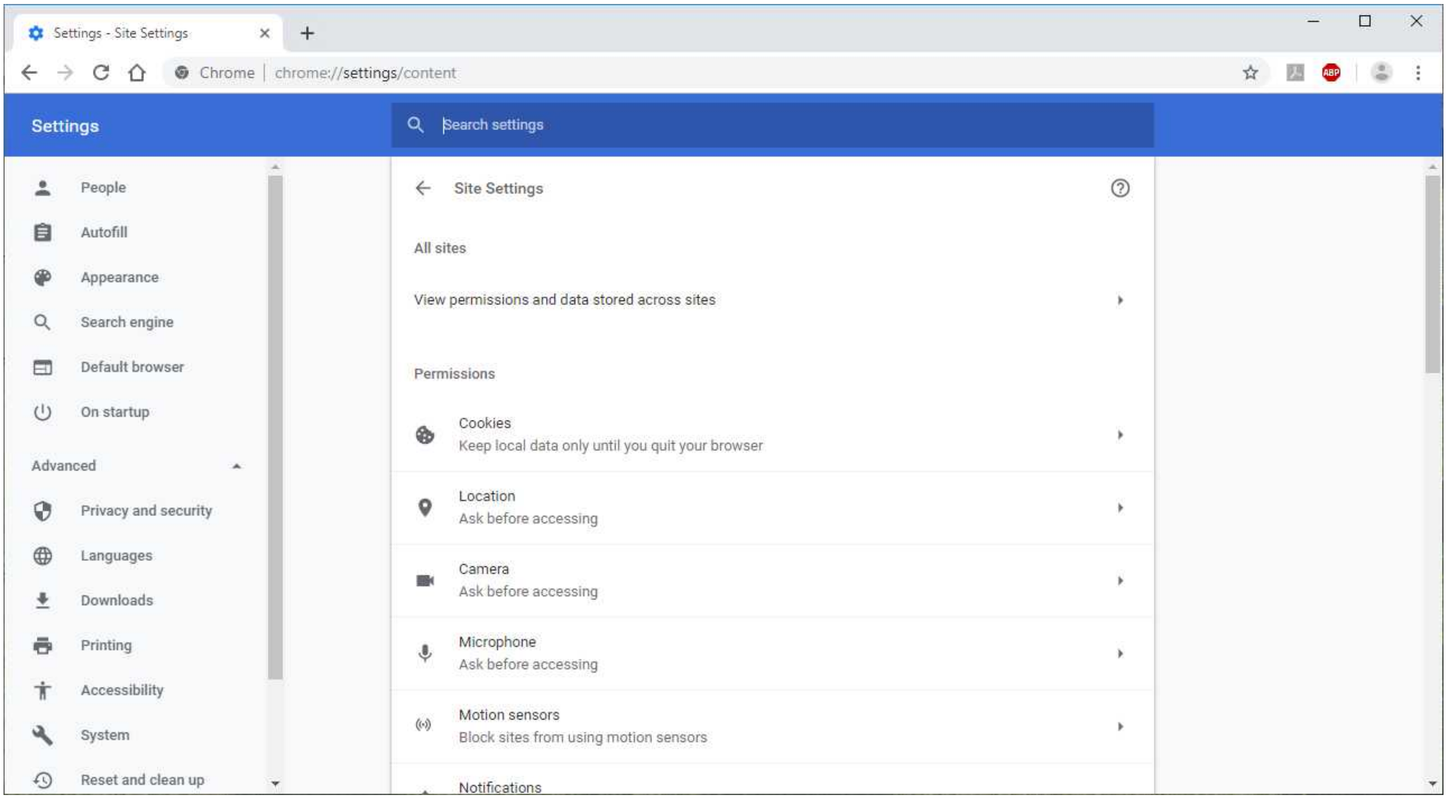
The risk associated with plug-ins is that nasty plug-ins can do really bad things. For instance, plug-ins can install viruses on your computer, or mine for bitcoins which uses a lot of CPU power and slows down your computer, or even encrypt your hard drive and demand that you pay ransom to decrypt it.

Here is how you can see a list of plug-ins currently in use in your Chrome browser.

1. Start Chrome.

2. Go to this URL: Chrome://settings/content

A new Web page appears, the top of which is shown in **Illustration 2**.



Site Settings

All sites

View permissions and data stored across sites

Permissions

Cookies
Keep local data only until you quit your browser

Location
Ask before accessing

Camera
Ask before accessing

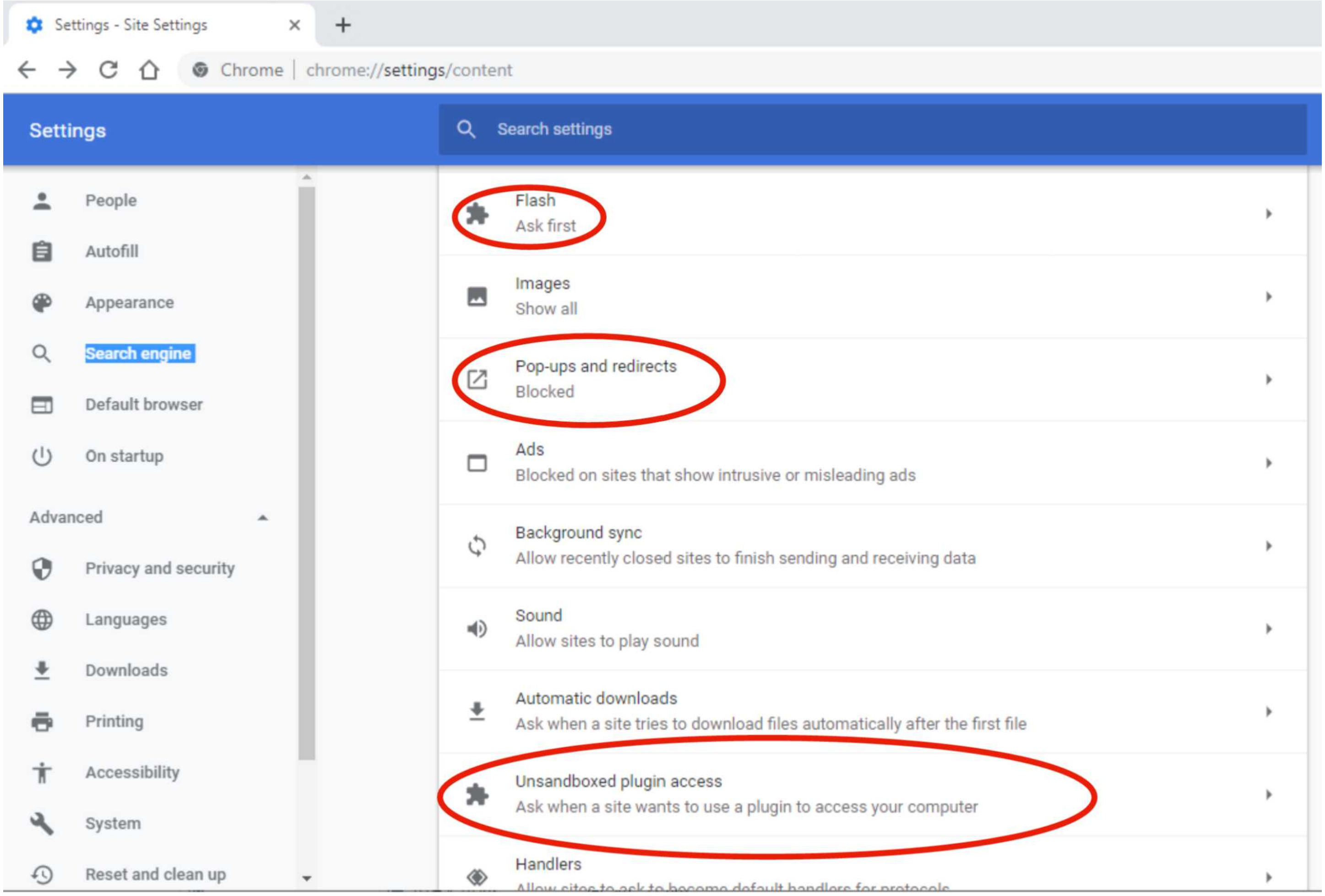
Microphone
Ask before accessing

Motion sensors
Block sites from using motion sensors

Notifications

Illustration 2.

3. Scroll to the middle of the list, as shown in **Illustration 3**.



Flash
Ask first

Images
Show all

Pop-ups and redirects
Blocked

Ads
Blocked on sites that show intrusive or misleading ads

Background sync
Allow recently closed sites to finish sending and receiving data

Sound
Allow sites to play sound

Automatic downloads
Ask when a site tries to download files automatically after the first file

Unsandboxed plugin access
Ask when a site wants to use a plugin to access your computer

Handlers
Allow sites to ask to become default handlers for protocols

Illustration 3.

There are Chrome settings here that you may wish to adjust:

Flash: the default setting is **Block**. I set mine to **Ask First**. This means the browser will ask me if I want to allow the web site to run Flash. This won't be possible much longer, since Chrome will soon drop support for Flash.

Pop-ups and redirects: these are usually third-party ad behaviors. The default is Block. Leave it set that way.

Unsandboxed plugin access: The default is **Ask when a site wants to use a plugin to access your computer**. The alternative is **Do not allow any site to use a plugin to access your computer**. That alternative is far more secure and comprehensive. I have to admit, that alternative setting has some appeal.

I circled each of those in Illustration 3.

I figure I would rather be told about uses of Plugins, especially because one financial services site that I use frequently requires Flash. Note that the alternative setting does not literally prohibit *installation* of plugins. It does prohibit *use* of plug-ins.

I admit I found the list of Plug-ins content on this Chrome page baffling. Cookies are plug-ins? Javascript is a plug-in? Not by my standards.

Clearly Flash is a plug-in. In my Chrome browser, Flash is listed on this page. On of the problems I ran into is that I need Flash for one financial services web site in particular, and I can only set Flash to be used *after the browser asks me* (I am not permitted to set permission in advance), and that setting will not persist after Chrome is shut down. I consider that to be a less than ideal approach for managing use of Flash.

However, Chrome, like Firefox, will soon cease using Flash, possibly because some extreme uses of Flash cause browser lockups or crashes.

More generally, this Chrome page, unlike Firefox, does not give you options to *uninstall* plug-ins. But you can disable them through this page, using the Unsandboxed Plugin access Do Not Use setting described above.

To change any of these settings, click on the tiny arrowhead appearing to the right of the setting name. That reveals the setting switch, which you can change.

CHROME EXTENSIONS

Extensions are Java software that can be run by Chrome. Chrome itself offers several Extensions for public use. I installed one provided by Chrome called AdBlockPlus, and I have written the installation steps for that Extension in a PATACS Posts article.

The simplest risk associated with Extensions is that, being Java software, they can possibly take significant time to execute, and therefore slow down Chrome.

Worse yet, Extensions can do things you might not want them to do, such as tracking your visits to all web sites, just like tracking cookies do. Nasty extensions might, for example, copy your contacts list when you access an email web site, and then send all of your contacts an email containing a link to a virus.

So it is important that you take a look at Chrome Extensions and know what each installed Extension is supposed to accomplish for you. If you find some that you do not recognize, and are not easily understood by their title or description, you can search via Google or any assistant of your choice to determine the purpose and reputation of the unrecognized Extension. Or, if you don't have time to do that, you can disable the unrecognized Extension.

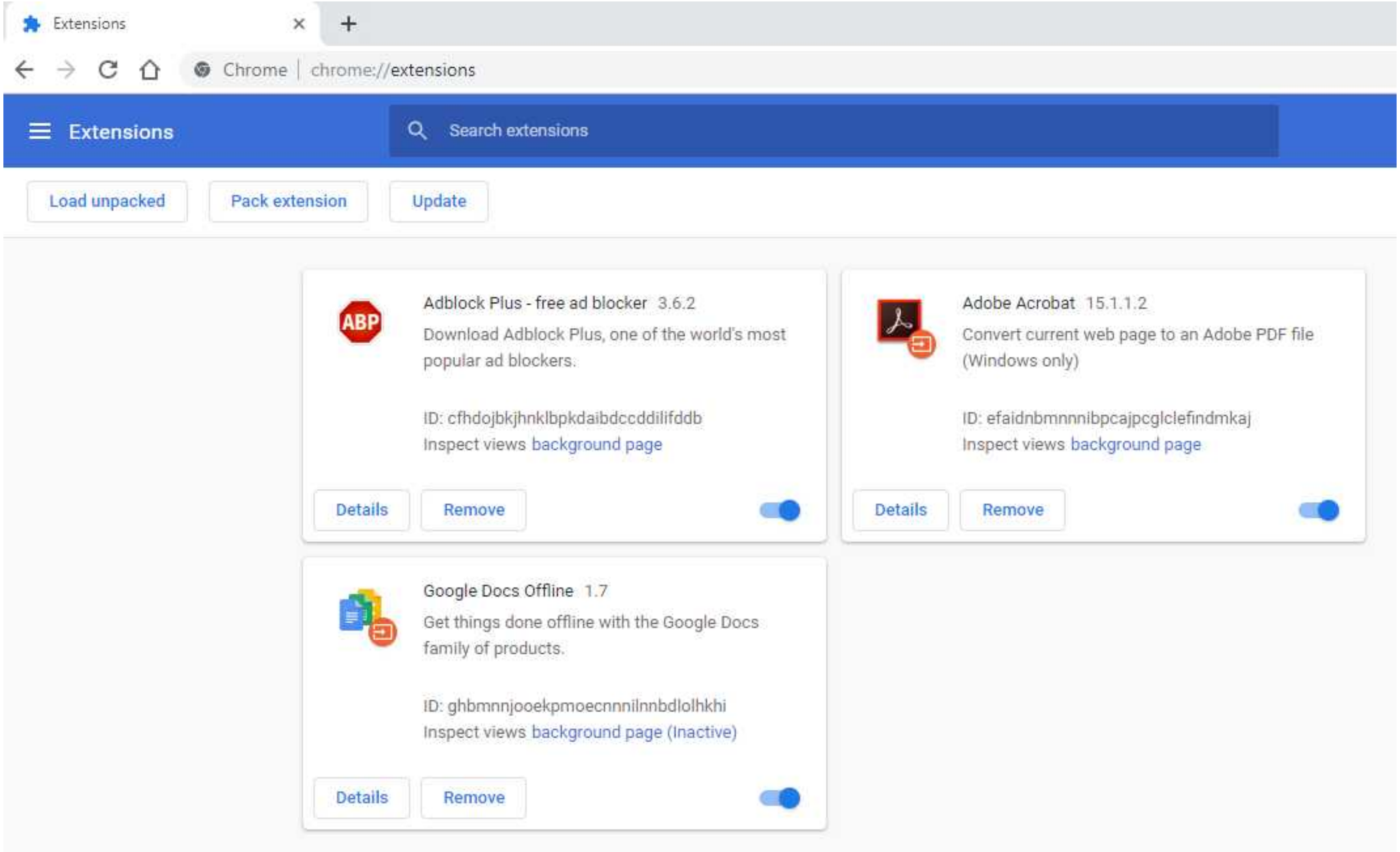
What I found is that Chrome will show you a list of all installed Extensions, and enable you to disable or remove each Extension individually.

Here is how you can tell Chrome to show you a list of all installed Extensions:

1. Start Chrome.

2. Go to this URL: Chrome://extensions.

A new page appears, as shown in **Illustration 4**.



Adblock Plus - free ad blocker 3.6.2
Download Adblock Plus, one of the world's most popular ad blockers.

ID: cfhdojbkjhnklbpkdaibdccddilifddb
Inspect views background page

Adobe Acrobat 15.1.1.2
Convert current web page to an Adobe PDF file (Windows only)

ID: efaidnbmnnnibpcajpcglclefindmkaj
Inspect views background page

Google Docs Offline 1.7
Get things done offline with the Google Docs family of products.

ID: ghbmnnjooekpmoecnnnilnnbdlolhkhi
Inspect views background page (Inactive)

Illustration 4.

This page does not provide a way to disable all Extensions at once. But you *can* disable each Extension individually.

In the lower right corner of each Extension description block, there is an on/off switch in the ON position by default. You can click on the switch to disable the Extension.

I tried clicking on the Details button but the additional info did not add anything to my understanding of the purpose of each Extension.

To remove the Extension permanently, you can click the Remove button.

Of the three Extensions shown to me by Chrome, I know I installed AdBlockPlus and Adobe Acrobat. I did *not* install Google Docs Offline, and I have no use for that. I believe it was included with Chrome when I installed the browser.

THE SLEDGEHAMMER

There is also a way to start Chrome so that it disables all Extensions.

If you have installed a valuable Extension like AdBlockPlus, disabling all Extensions does disable those Extensions you explicitly installed and want to use. In my case, I found it prohibits use of AdBlockPlus. The only advantage I can see in the option to disable all Extensions is that it will disable any Extensions installed without your explicit approval while you are browsing using Chrome, but at the expense of disabling all Extensions that are doing something good for you.

I would prefer to give you a method simply to prevent the installation of any Extension without your explicit approval, without also disabling the Extensions you have installed and want to use, but Chrome does not seem to offer such a method.

You may get the notion that I think this startup option is a sledgehammer, not a precision tool for controlling Extensions. You are correct about that. But here it comes anyway, just in case you decide you need it.

HOW TO DISABLE ALL CHROME EXTENSIONS

if you decide that you want to disable ALL Extensions, good and bad, then you need these instructions. Otherwise you can skip this part.

Find the Chrome icons on your computer screen. Also find the Google Chrome item in your Start menu.

There may be a shortcut on the screen, and possible a pinned shortcut on the Task Bar at the bottom of the screen. Additionally, the is almost always a Google Chrome item in the Start menu.

In Windows, each icon has a text property that tells the computer how to find and start up Chrome. You will modify that property to tell Chrome to disable all Extensions.

Note: this must be done while Chrome is NOT running. And you have to make the changes separately *for each one of the icons, and the menu item*. Doing one change does NOT affect all.

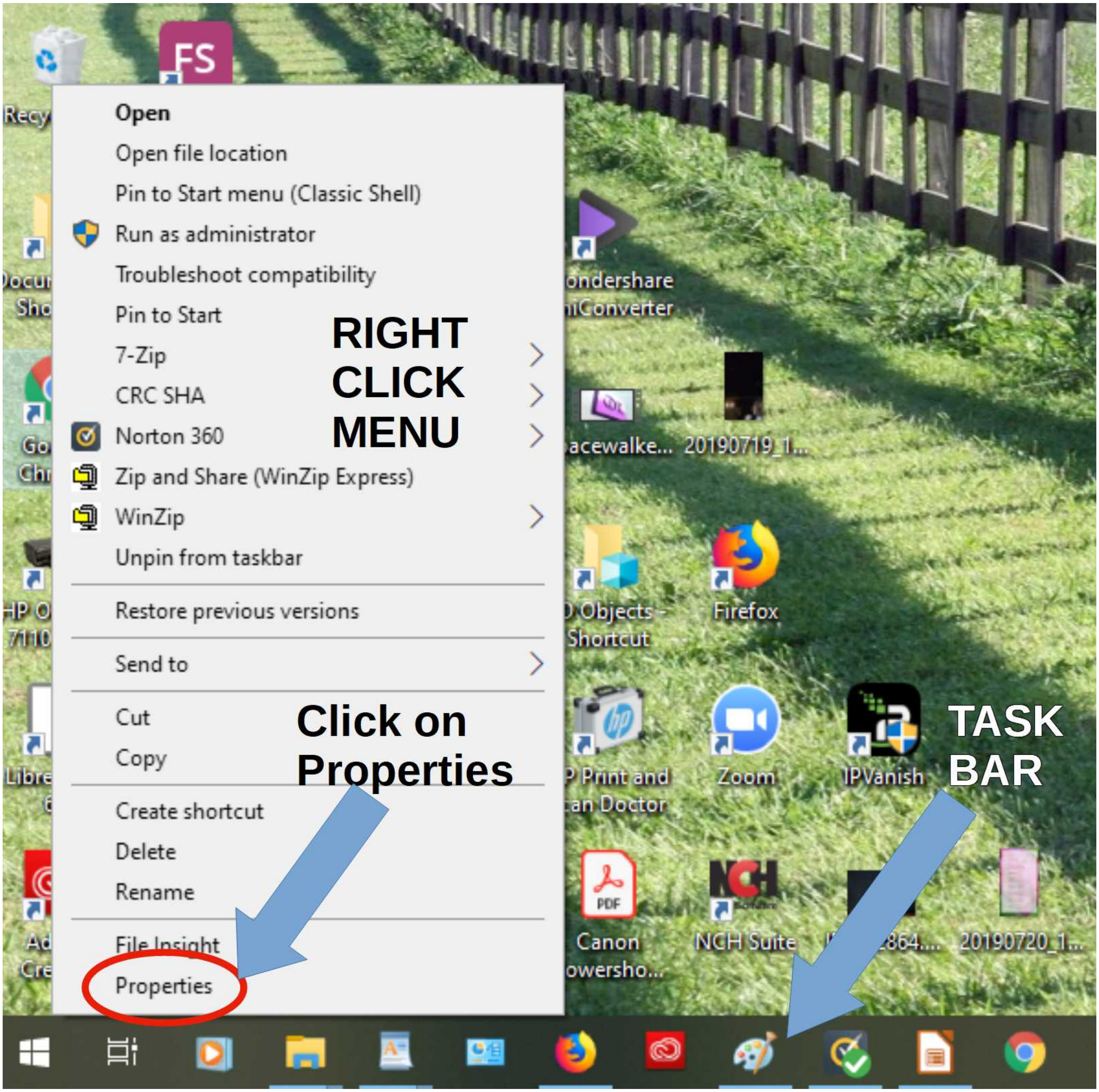
Here is how you can see and alter the startup instructions, to disable extensions in Chrome:

1. Open a pop-up menu for Chrome, as shown in **Illustration 5**:

    Shortcut in Task bar: hold down the Shift key and, while holding that key, right-click on the Chrome icon

    Shortcut on Screen: right click on the Chrome icon.

    Menu item: right-click on the Google Chrome menu item.



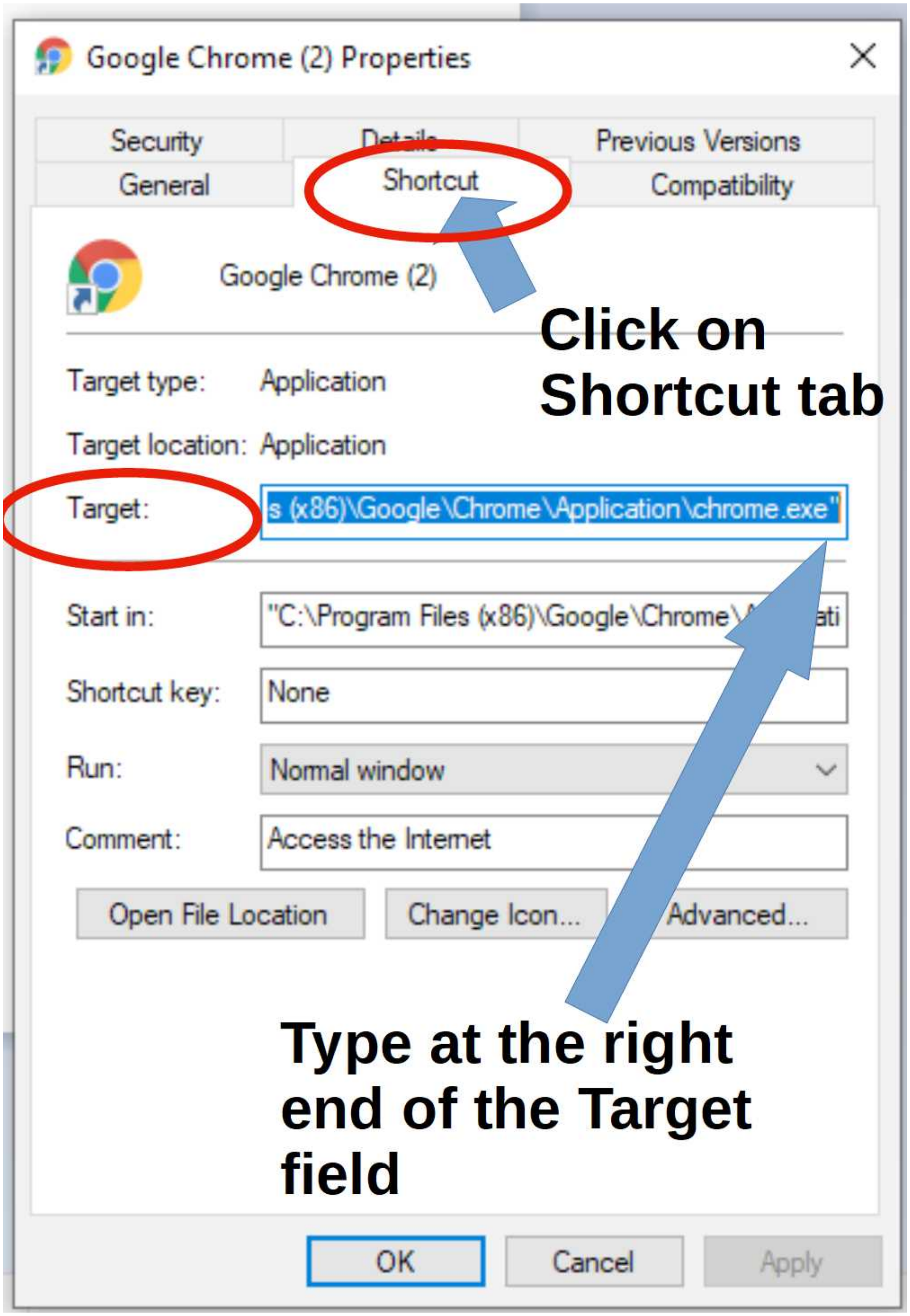
RIGHT CLICK MENU

Click on Properties

TASK BAR

Illustration 5.

2. In the pop-up menu, choose Properties; that word is usually at the bottom of the menu. A dialog window appears, as shown in **Illustration 6**.



Target type: Application

Target location: Application

Target: s (x86)\Google\Chrome\Application\chrome.exe"

Start in: "C:\Program Files (x86)\Google\Chrome\ ati

Shortcut key: None

Run: Normal window

Comment: Access the Internet

Click on Shortcut tab

Type at the right end of the Target field

Illustration 6.

3. In the dialog window, click on the Shortcut tab, and find the Target field. There is a string in the field contained in quotes. The end of the string reads: Chrome.exe”

4. After the double-quotes at the end of Chrome.exe, type a space and --**disable-extensions**

5. At the bottom of the dialog window, click on the OK button to save the changes you have made.

That’s it.

I hope I have made it easy to understand and to implement. I admit I have my doubts, mainly because I think the design and organization of these Chrome settings could be explained with greater clarity by the Chrome development team.

About the Author: John Krout was a president of the Washington Area Computer User Group (WAC), one of the clubs that later merged to become the Potomac Area Technology and Computer Society. He writes frequently for PATACS Posts, the club newsletter, and occasionally provides presentations at PATACS meetings in Fairfax City VA. Recently he wrote on the subject of converting Android or iPhone voicemails to audio files. He lives in Arlington VA. He works as a tech writer for the Thales Group, supporting the use of the company’s automated fingerprint identification hardware in a major federal government computer system.