

Windsor Senior Computer Users' Group

Common Internet Browser Mistakes







Ross Guistino
July 10, 2017

Today's Agenda

- ▶ What's a Browser vs a Search Engine
- ▶ How to recognize legitimate links vs ads
- ▶ Search engine scams
- ▶ Microsoft Support Scam
- ▶ Resetting your Home Page
- ▶ Resetting your default Search Engine
- ▶ Determining what to click when downloading a file
- ▶ Adobe "options"
- ▶ Java "options"
- ▶ How to look up real vs fake news
- ▶ The use of Ctrl–Alt–Del

Browser vs Search Engine

A browser is an application that allows you to do things on the internet. It is the vehicle that you use to “browse” the internet. All of the topics that I talk about today apply to whichever browser you use. Examples of internet browsers are:

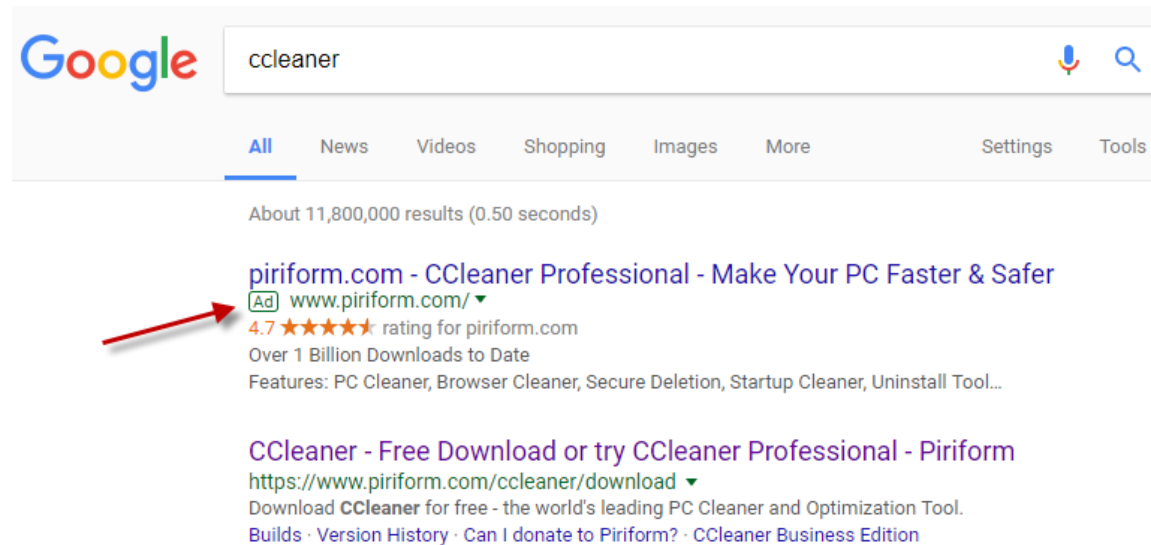
- Google Chrome 
- Mozilla Firefox 
- Microsoft Internet Explorer (Win7 & 8.1) 
- Microsoft Edge (Win10) 
- Apple Safari 
- Opera 

A search engine is the web page that you use to search for things on the internet. Examples of internet search engines are:



Of all of these search methods, the ones to avoid are Yahoo due to their excessive ads and poor search results, and Ask.com due to the sneaky way they infiltrate your web browser and install unwanted software. Avoid like the plague.

Ads



Look at the two search results above; they both will bring you to a download of Ccleaner, but with one very important difference. The first one has an Ad tag next to it. Though the website is legitimate, it will bring you to a very different page than the search result below it.

Take away: Never click the first few search results which are usually ads paid for by the vendor so that their website goes to the top of the list. Skip over anything with an Ad symbol.

Ads

In relation to the previous slide showing the search results, the first search item with the Ad icon takes you to a page advertising Ccleaner →

Piriform®

Microsoft
CERTIFIED
Partner

Over
1 Billion
Downloads



- Automated cleaning for an instantly faster PC
- Protects your online privacy
- Fixes system errors, freezes & crashes
- Restores PC speed, power & stability

Works with Windows 10, 8, 7, Vista & XP

Search



BUY NOW
\$24.95 reduced from \$32.95

FREE DOWNLOAD

(Free trial)



Download CCleaner - The world's most popular PC cleaner!



FREE

PROFESSIONAL

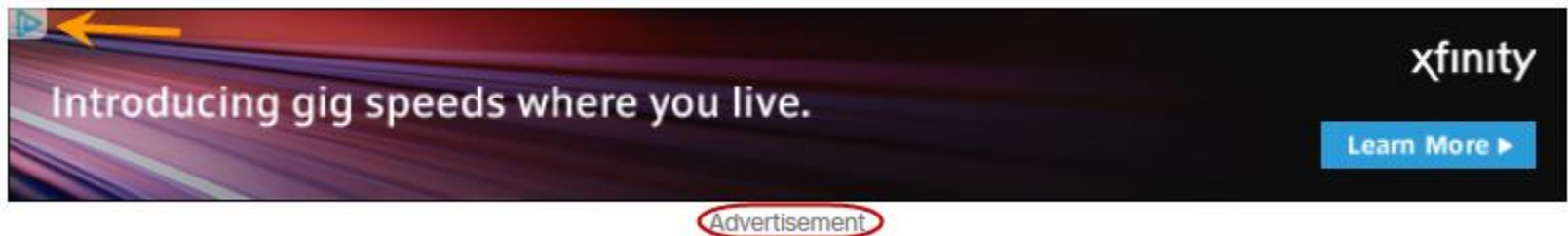
PROFESSIONAL PLUS

	FREE	PROFESSIONAL	PROFESSIONAL PLUS
Faster Computer	✓	✓	✓
Privacy Protection	✓	✓	✓
Complete Cleaning	✗	✓	✓
Real-time Junk Monitoring	✗	✓	✓
Automatic History Cleaning	✗	✓	✓
Automatic Updating	Manual	✓	✓
Defragmentation			✓
File Recovery			✓
Hardware Analysis			✓
	Download	Free Trial Buy Now	Buy Now £69.95 £29.95

Whereas the second search result without the Ad icon opens this, a page that takes you directly to the file download page ←

Ads

Sometimes internet ads can be obvious, such as the Xfinity ad shown here where it not only has the tell-tale blue sideways triangle but also says “Advertisement” below it. The take away here is to never click on anything with the triangle or that says advertisement.



Search Engine Scams

One of the most prolific search engine scams is a piece of software called Mysearch.com. This fake search engine gets installed in the background when you inadvertently think you're installing something legitimate. A common way of getting mysearch.com installed is when you are looking for a map. If you go to Google and search for maps, one of the first links is this:

Maps & Driving Directions - Enter Your Address & Location

Ad www.directionsandmap.com/driving/directions ▼

Get Maps & Driving Directions!

Traffic Updates · Driving Distance · Print Directions

Types: Printable, Driving, Walking, Fastest Route, Satellite

[Driving Directions](#)

[Route Planner](#)

[Printable Directions](#)

[Traffic Alerts](#)

If you proceed to click on it, you will be asked to install software to assist you with directions to your destination. It will also install a bogus search function called mysearch.com. If you read the fine print, they tell you what they will be doing to your browser. Here's the fine print:

<http://legal.directionsandmap.com/home/terms?source=g-ccc1-googlesearch>.

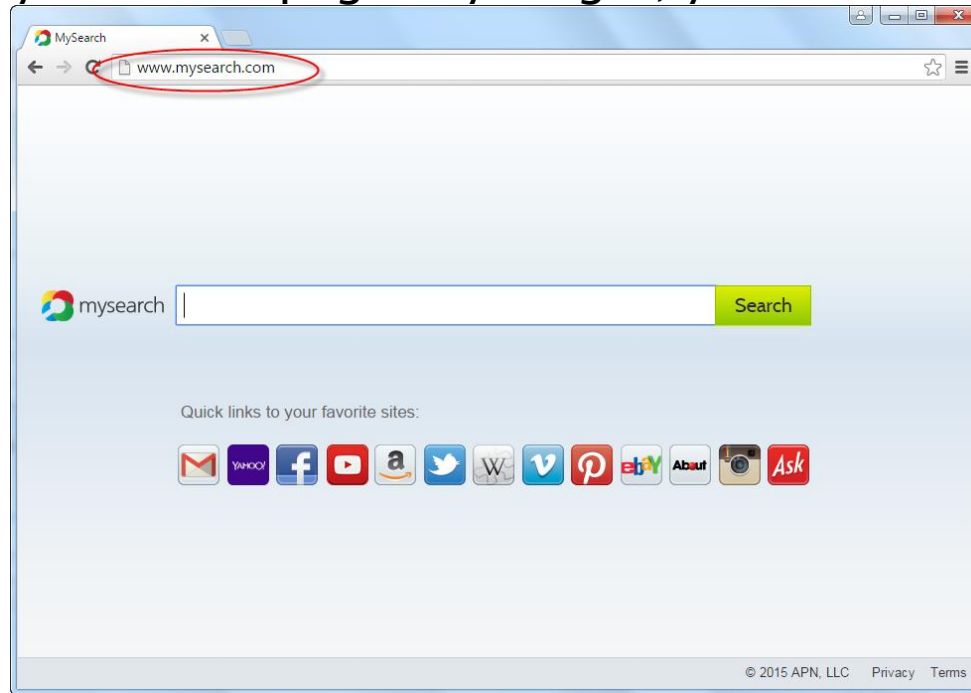
Do you really need software that is based in the Cayman Islands?

Take away: You should never have to install software for maps. *Never.*

Simply go to www.googlemaps.com.

Search Engine Scams

Many people like to set Google as their home page. However, if one day you see something like this when you start your browser, you do NOT have Google as your home page any longer, you have the Mysearch bogus search engine:



To remove mysearch you must do several things:

1. Uninstall it in your Programs Control Panel
2. Remove it from your browser's add-ons menu
3. Reset your browser's Home Page and/or Search Engine

Microsoft Support Scam

Many of you have heard of someone getting a call from “Microsoft” and paying up to \$400 to repair their computer, and often times giving the stranger complete control of their computer. In some instances you may come across a web page that pops up and instructs you to call for Microsoft support. And in most instances, that number is (844) 308-6819. Do a Google search on that number and you’ll see page after page of the same number attached to multiple company names, all different, but with the same number. This is NOT the real Microsoft support. A similar number is given if you search for HP printer support.

If you need support for your product, Dell, Compaq, HP, etc., it is best to go directly to the vendor’s website. Do not do a Google search for support because chances are good that you’ll get a bogus support website or phone number. Remember, vendors both good and bad, pay Google to put their websites at the top of the search list.

Here is a video of a person who played along with the support technician. The video is 26 minutes but will give you an idea of how easy it is to fall for this scam if you didn’t know any better.

<http://www.wired.co.uk/article/malwarebytes>

Setting Your Home Page

If your home page has been hijacked by malware, here is how to reset it:
In **Chrome**: 1. Go to the page you want to make as your home page, for example, www.google.com. Make sure that there are no other tabs open except for the page you want as Home page.

2. Click on the settings menu (3 stacked dots)
3. Click Settings
4. Under On Startup, click Open a specific page or set of pages
5. Click “Use current pages”
6. Close Chrome and reopen

In **Firefox**: 1. Go to the page you want to make as your home page, for example, www.google.com. Make sure that there are no other tabs open except for the page you want as Home page.

2. Click the settings menu (3 stacked lines)
3. Click Options
4. Click “Use Current Page”
5. Close Firefox and reopen

Setting Your Home Page

- In **Edge**:
1. Go to the page you want to make as your home page, for example, www.google.com. Make sure that there are no other tabs open except for the page you want as Home page.
 2. Click on the settings menu (3 horizontal dots)
 3. Click Settings
 4. Under Open Microsoft Edge with, click the downward arrow and choose "A specific page or pages"
 5. Type in the web page you wish to have as the home page (www.google.com for example)
 6. Close Edge and reopen

- In **Internet Explorer**:
1. Go to the page you want to make as your home page, for example, www.google.com. Make sure that there are no other tabs open except for the page you want as Home page.
 2. Click the settings menu (the nut icon)
 3. Click Internet Options
 4. Click "Use Current", click OK
 5. Close Internet Explorer and reopen

Setting Your Default Search Engine

If your browser's home page was hijacked, you must not only reset your home page, but also your default search engine. Here's how:

In Chrome: 1. Click on the settings menu (3 stacked dots)

2. Click Settings

3. Under Search engine, click the arrow to the right of "Manage search engines"

4. Click on the three stacked dots to the right of the search engine you wish to make as your default, click Make default

5. Close Chrome and reopen

In Firefox: 1. Click the settings menu (3 stacked lines)

2. Click Options

3. Click Search from the left-hand column

4. Click the downward arrow under Default Search Engine and choose your default search engine. If your choice isn't listed, click on "Add more search engines..." at the bottom of the page.

5. Click on the search engine you'd like as your default

6. Click the green "Add to Firefox" button

7. Close Firefox and reopen

Setting Your Default Search Engine

If your browser's home page was hijacked, you must not only reset your home page, but also your default search engine. Here's how:

In Edge: 1. Click on the settings menu (3 horizontal dots)

2. Click Settings

3. Scroll down and click on "View advanced settings"

4. Scroll down and click on "Change search engine"

5. Click on the search engine you wish to use, example Google

6. Click Set as default button at the bottom of the list

7. Close Edge

In Internet Explorer: 1. Click the settings menu (the nut icon)

2. Click Manage Add-ons

3. Click Search Providers

4. If your search engine is in the list, click it, then click the "Set as default" button at the bottom of the window. If your search engine is not listed, then click "Find more search providers...", click on the search engine you wish to use, then click the Add button next to it.

5. Close Internet Explorer and reopen

Downloading the right file

Many times I'm looking for a specific file to download and as usual I'll bring up Google to search for it. More often than not I'll be taken to the CNET site which is both a help and a hindrance if you don't know what to look for when using this site. For example, here's what you get when you search for Ccleaner: <http://download.cnet.com/ccleaner/>

Which is the correct link for Ccleaner?

Start Download
3 steps for a faster install

▼ **Start Download**

 1. [Click to Start Download](#)
 2. **Run** and Install
 3. **Scan** for Issues
- Mac Optimizer

[Home](#) > [Windows Software](#) > [Utilities & Operating Systems](#) > [Maintenance & Optimization](#) > CCleaner

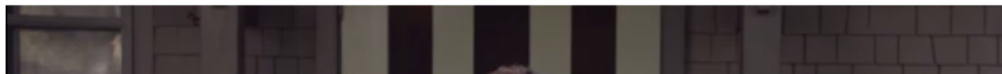


Download Editors' Rating:

Very good

Average User Rating:

out of 6764 votes



START DOWNLOAD

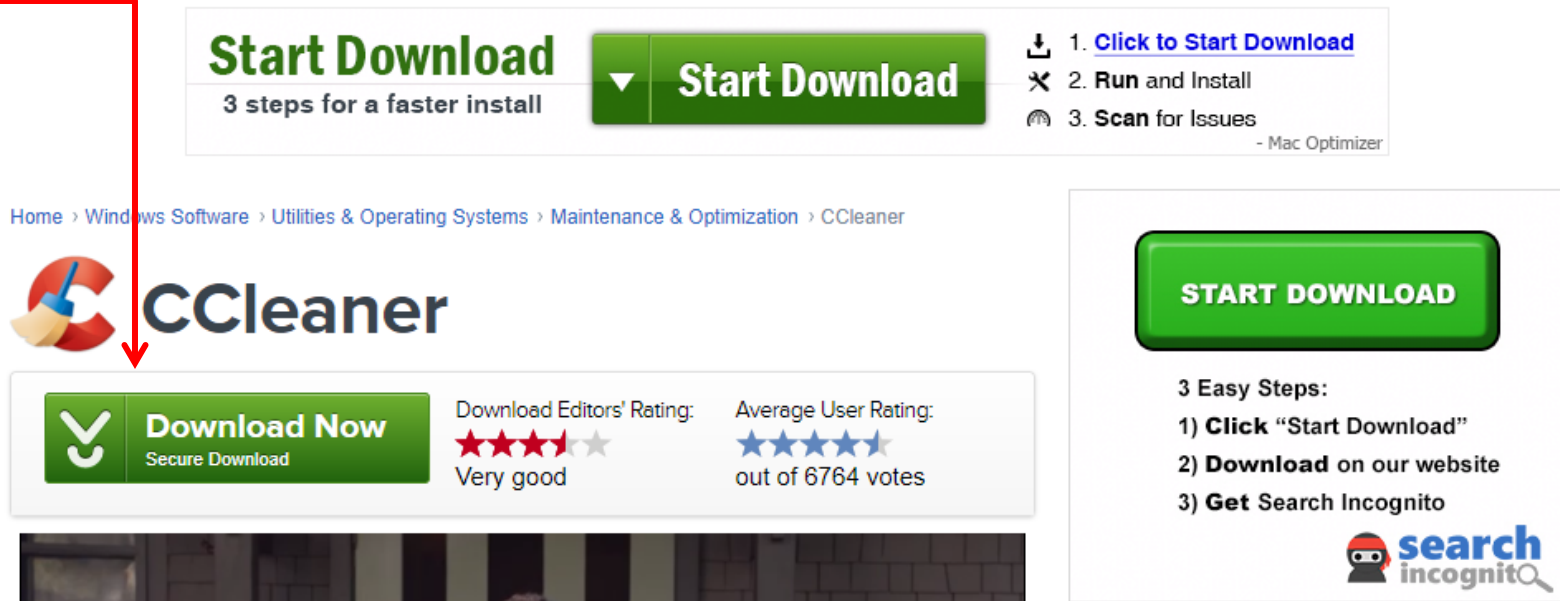
3 Easy Steps:

- 1) **Click** "Start Download"
- 2) **Download** on our website
- 3) **Get** Search Incognito



Downloading the right file

The correct link is this one. Many websites that offer free items will fill their page with ads that help pay for the website. Read each section carefully to see exactly what you're clicking on. Don't assume that the big green "Start Download" button is the correct item. Out of these three download buttons, two are ads and one is the correct one. This is a common play.




The screenshot shows the CCleaner website with three distinct download buttons and a list of steps. A red arrow points from the text above to the 'Download Now' button.


Start Download
3 steps for a faster install

Start Download

1. [Click to Start Download](#)
2. **Run** and Install
3. **Scan** for Issues
- Mac Optimizer

Home > Windows Software > Utilities & Operating Systems > Maintenance & Optimization > CCleaner

 **CCleaner**


 **Download Now**
Secure Download

Download Editors' Rating: ★★★★★
Very good

Average User Rating: ★★★★★
out of 6764 votes

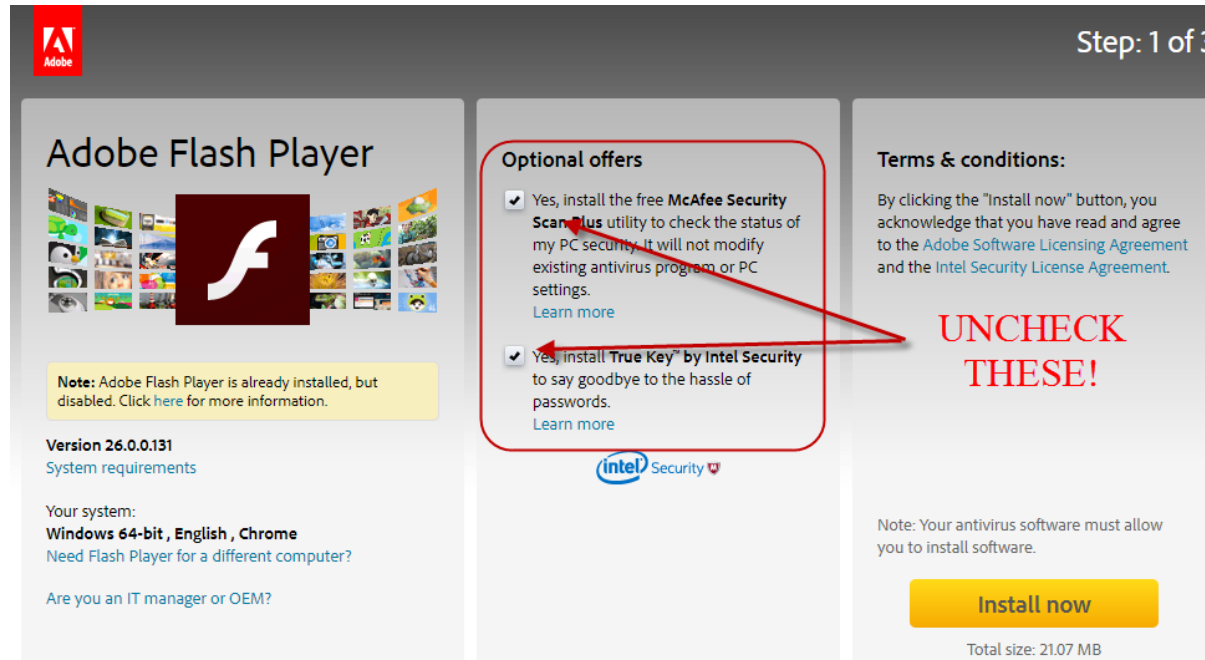
START DOWNLOAD

3 Easy Steps:
1) **Click** "Start Download"
2) **Download** on our website
3) **Get** Search Incognito



Adobe Options

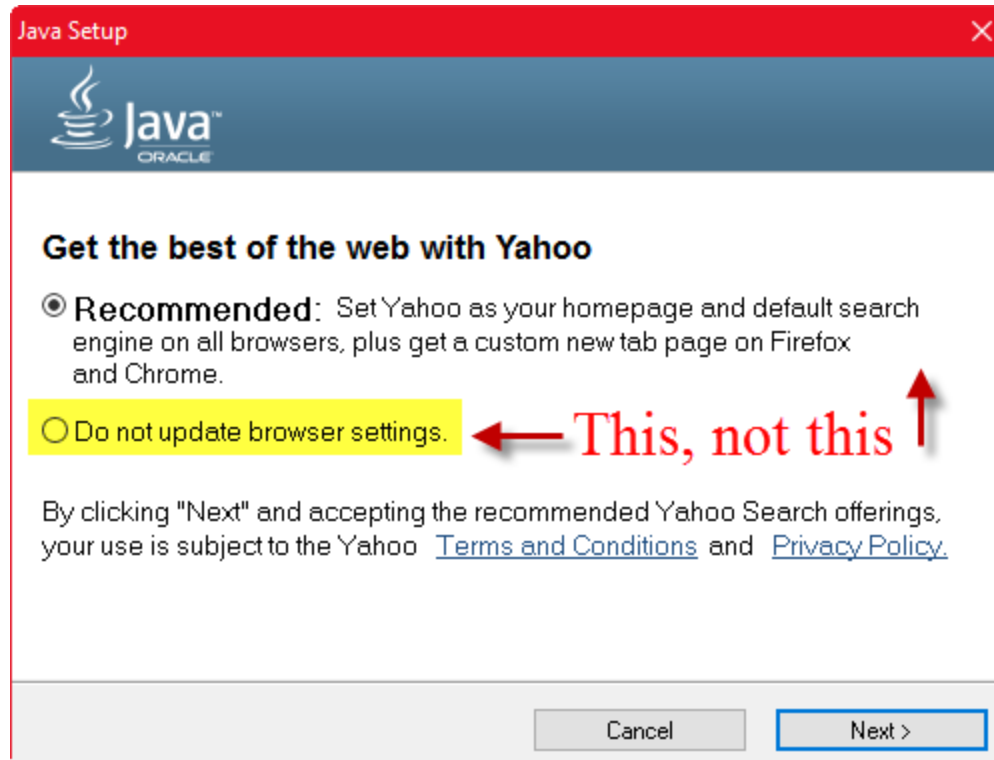
If you need to update Adobe Flash or Reader, you'll be faced with this:



Unless you want garbage-ware installed automatically, you must uncheck the boxes. Remember: You never want “optional offers”.

Java Options

If you need to update Java, you'll be faced with this:



Unless you want garbage-filled Yahoo installed automatically, you must click the “Do not update” option!

Truth or Fiction?

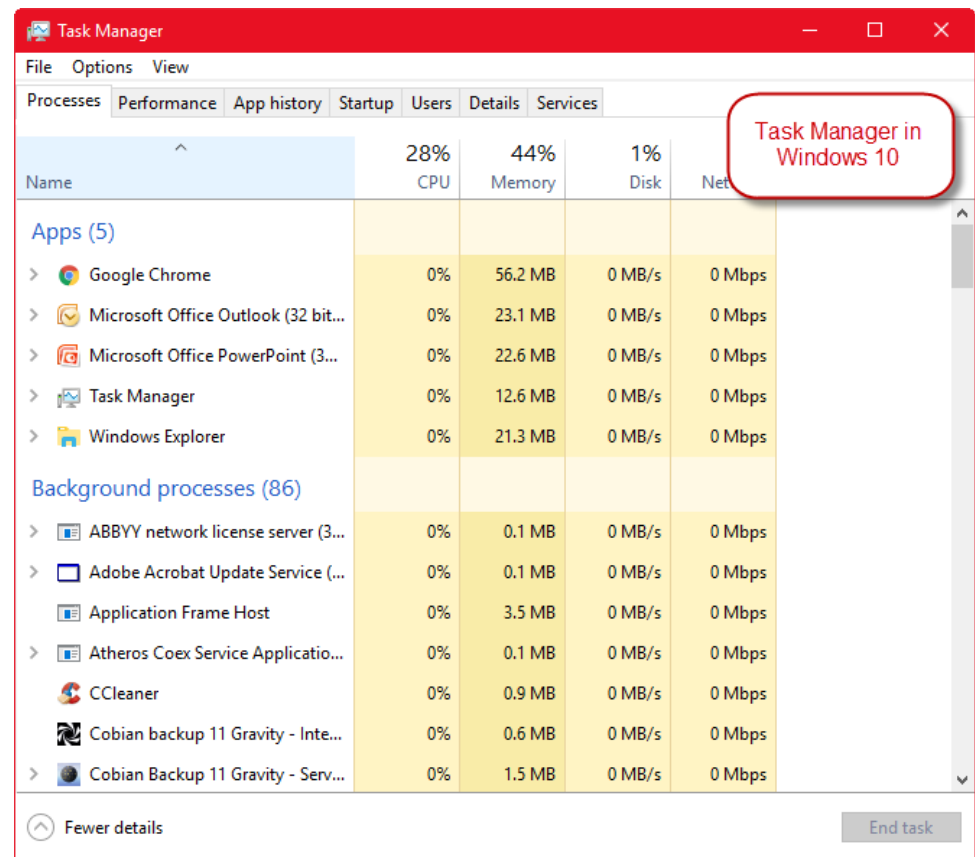
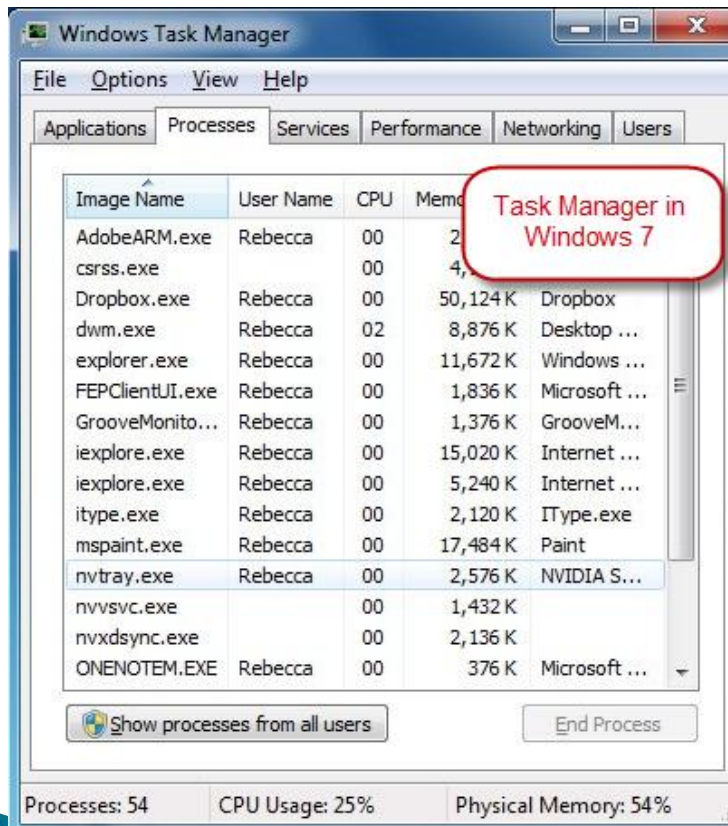
We all get emails from friends or see posting on Facebook about something that just seems too good to be true. How do I determine what's real or not when I encounter these types of posts? I go to one of several websites:

1. www.truthorfiction.com
2. www.hoax-slayer.com
3. www.snopes.com

And for news, a good site is: <http://www.politifact.com/>

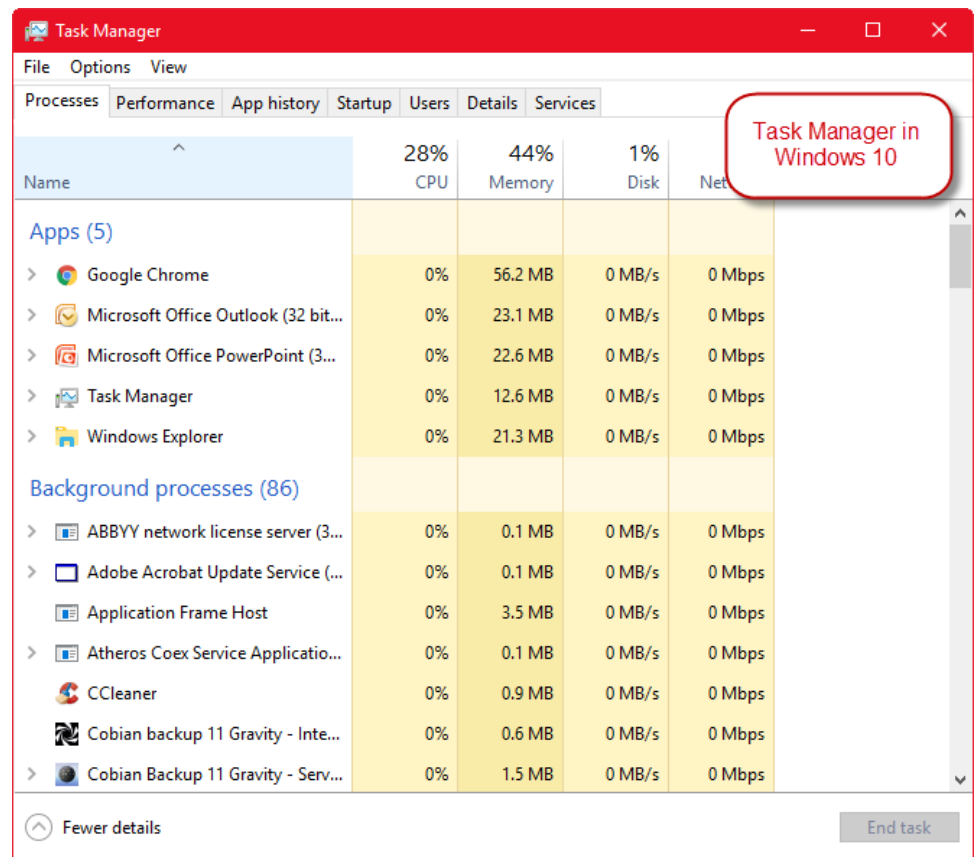
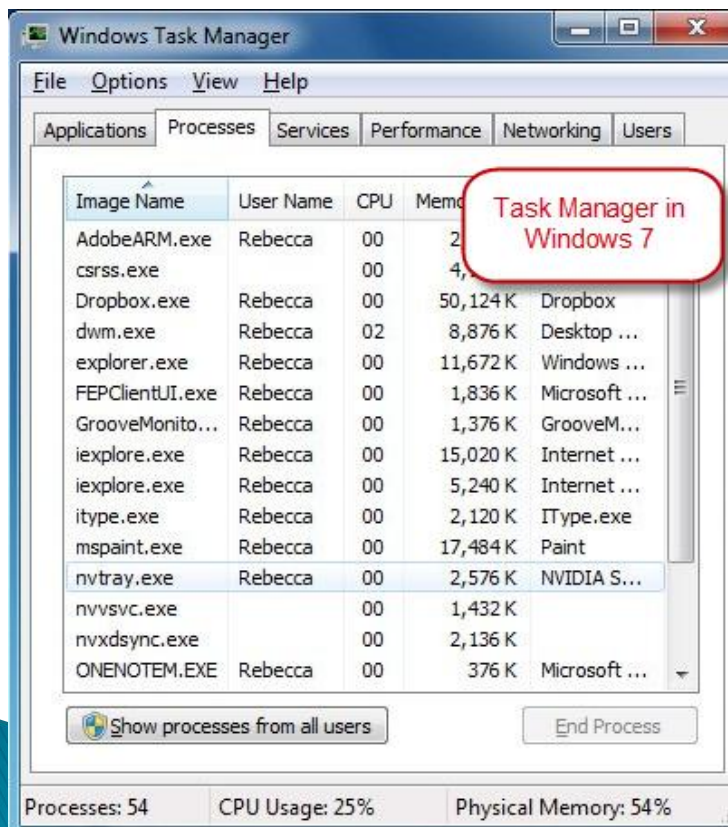
Using Ctrl-Alt-Del

Sometimes when we are browsing the internet, a pop-up occurs that we seemingly can't get out of. The first thing to try is the old "three finger salute", i.e. pressing the Ctrl, the Alt, and the Del keys together which will give us the opportunity to invoke the Task Manager.



Using Ctrl-Alt-Del

Once Task Manager appears, you need to End Process (in Win7) or End task (in Win10) to stop the offending pop-up. But most times you can't just stop just one thing, you may need to quit the entire browser. Click on the browser name, iexplore.exe, Firefox or Google Chrome, then click End Process/End task



>> *The End* <<

To create this presentation, I used:



-A copy of this presentation can be found at the links below in either PowerPoint or Adobe Reader format:

<http://guistino.com/Training/Common Browser Mistakes.ppsx>

<http://guistino.com/Training/Common Browser Mistakes.pdf>