You can improve the Security Settings in Windows' Internet Explorer Browser

(A paraphrase of a Windows Secrets Newsletter Article)

presented by Gary Patrick
March 2, 2016

Lexington Computer & Technology Group
Lexington, MA

This subject is applicable to users of
Microsoft Windows 7, 8, 8.1, and 10.

Table of Contents:

(slide numbers appear lower right)

Windows Secrets Newsletter recommends tightening some security settings in I.E.11 to improve its defenses against malware and hackers.

- Microsoft's default security settings are more to ensure backward compatibility than to optimize security.
- Even if you don't use Internet Explorer online in favor of another browser (Chrome or Firefox, for example) I.E.'s vulnerabilities could affect your system's overall security and performance, because -
- Components of I.E. can be automatically used in Windows processes such as Windows Update.
- We will look at nine changes recommended for the "Advanced Settings" page of "Internet Options" for I.E.11.

Do you have Internet Explorer 11?

- Important because Microsoft support **ended** for all previous versions of I.E. as of Jan. 12th! (except in Vista – see below right)
- To confirm 11, open the browser from the Desktop or System Tray icon. (for Windows 10 there's help in the next slide).

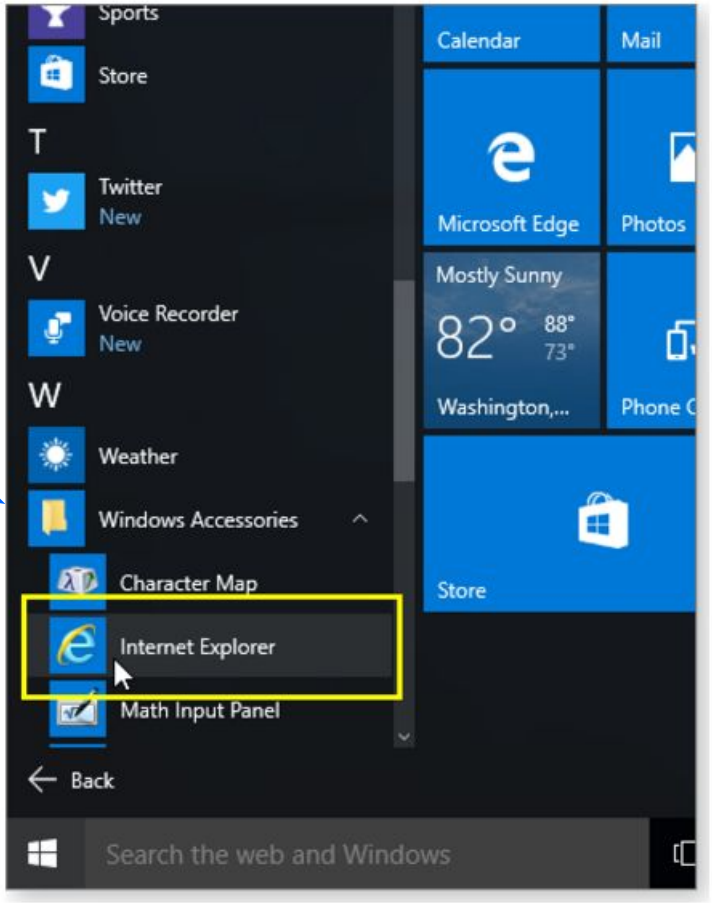
  (On a Win 8.1 system open the desktop version rather than the tiled version, for simplicity sake).
- Next, click on the “gear” icon in the upper right corner, and
- Select “About Internet Explorer”.
- You should see the display as shown here above right:

Figure 1. Click *About Internet Explorer* in IE's settings menu to check your installed version. (Shown: IE 11 on Win7.)

A footnote for Vista only: I.E. 9 will have Microsoft support until April 11, 2017.

Windows 10 comes with I.E.11 installed but may need to be coaxed out of hiding (its default state)

- Click Start and select "All apps."
- Scroll down to the Windows Accessories folder.
- Click it, to open down,
- Then click "Internet Explorer" to launch it.
- Click on the "gear" icon and select "About Internet Explorer."
- For the future, Internet Explorer can be made easier to open, by creating one or more shortcuts (refer to the next slide).



I.E. 11 co-exists with the Edge Browser in Windows 10 – you can use either one!

In Windows 10, Internet Explorer can be made easier to find for starting it:

- If I.E.11 is running, you can right-click on the I.E. icon in the Taskbar to pin it to the Taskbar;

  - or -

- Alternatively, pin it to either the Start Menu or the Taskbar by

  a) clicking the Start button,

  b) select "All Apps," then scroll down to "Windows Accessories,"

  c) Right-click the "Internet Explorer" line and select "Pin to Start" or "Pin to Taskbar."

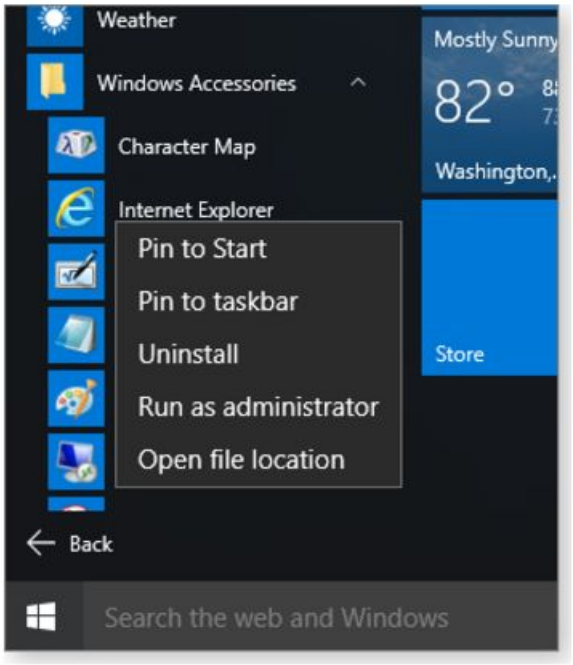


Figure 3. For easier access to IE 11, right-click and select *Pin to Start* or *Pin to taskbar.*

If you don't yet have I.E. 11, here's how to get it:

- Go to the Microsoft Download page: http://windows.microsoft.com/en-US/internet-explorer/download-ie
- This site should automatically offer the correct release of the browser for your specific system.
- If you have trouble with this automated page, go to the following manual download pages:
- Windows 7, both 32 and 64 bit: https://www.microsoft.com/en-us/download/Internet-Explorer-11-for-Windows-7-details.aspx
- Windows 8.1 32-bit: http://www.microsoft.com/en-us/download/details.aspx?id=40852

  Windows 8.1 64-bit: https://www.microsoft.com/en-us/download/details.aspx?id=40854
- If you have trouble installing I.E.11, refer to Microsoft Support Article: https://support.microsoft.com/en-us/kb/2847882, to be sure you have all the necessary prior updates and other prerequisites.

Next, let's look at the changes Windows Secrets Recommends.

With I.E.11 running, click on the Tools "gear" icon.

Select "Internet options" from the pull-down menu;

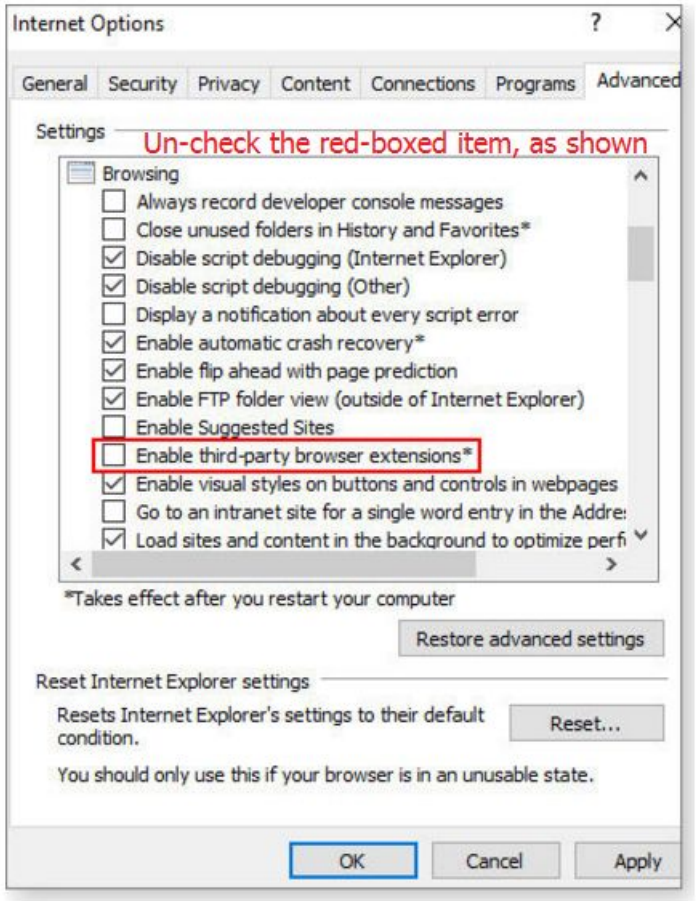
In the Dialog Box that comes up,
Click the "Advanced" tab (upper right);

Scroll down slightly to display the "Browsing" settings, where change #1 will be done. Refer to the graphic view on the left side of the next slide. Discussion is on the slide after next.

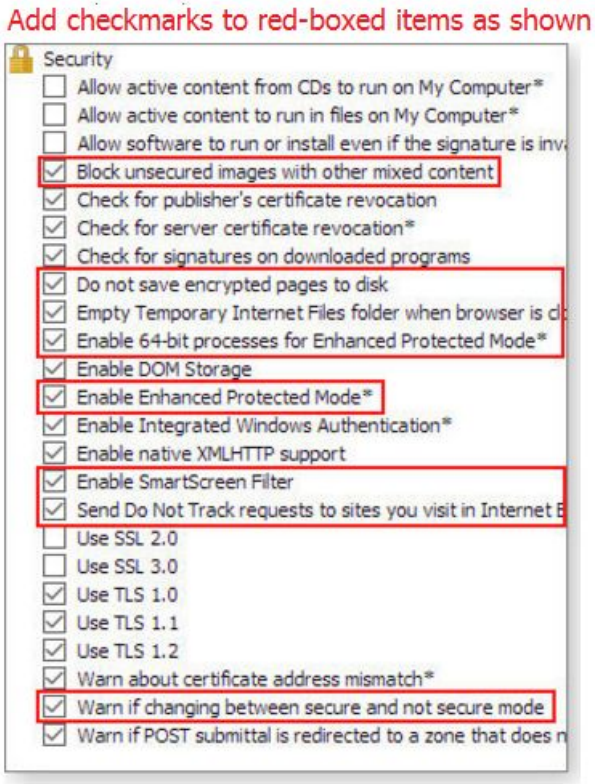
Following that, it will be necessary to scroll down in the "Advanced Settings" dialog box, to the "Security" heading – refer to the graphic view on the right side of the next slide.

Here are views of the applicable portions of the "Advanced Settings" pane, with the changes highlighted.

The "Browsing" settings:



The "Security" settings, by scrolling down further:



Note: The specific line items and the list order in which they appear on your p.c. may vary slightly from what's shown here. (You may possibly have an extra feature, or one of those illustrated may be missing, depending upon 32-bit vs. 64-bit versions of I.E. 11).

Note: after making these changes, you will need to click "Apply" and then "OK," to exit the Advanced Settings box. Some of the changes will not take effect until you "Restart" Windows (or Shut Down and later Restart Windows).

Change #1): In the "Browser" list, click to remove the default check-mark on "Enable third-party browser extensions."

Effect: This change will block nonstandard toolbars, search redirectors, popups, add-ons, etc. from altering IE 11.

- these are common vectors for spyware, malware, and browser hijackers, that might
- change your home page, alter your search-engine choices, redirect your links to locations you don't want, deliver popup ads, install unwanted toolbars, alter your Favorites, etc.

The flip-side to disabling third party extensions:

If you depend on specific third-party add-ons, toolbars, or other extensions, you might prefer to leave this option enabled (checked) — accepting somewhat reduced online security.

For the remaining changes, stay on the Advanced Settings window, and scroll down until you reach the “Security” settings.

Change #2): Place a check-mark on “Block unsecured images with other mixed content.”

Explanation of Change #2):

Some websites, such as online banking pages:

- draw most of their content from secure servers,
- but also mix in content with images from unsecured graphics or ad servers.
- that could leave a gaping hole in your browser security.

Potential drawback:

- some websites might not display normally;
- some images and/or graphic links could be broken.

Change #3): Place a check-mark on
"Do not save encrypted pages to disk."

Explanation: although secure-website pages are SSL/TLS-encrypted for your safety,

- Internet Explorer can store fully decrypted, plain-text versions of these pages in the Temporary Internet File area on your PC;
- makes these pages potentially vulnerable to snooping.

Downside:

- future access to SSL/TLS-encrypted sites could be slightly slower;
- the page(s) will have to be fully downloaded again, not simply recalled from Temporary Internet File area on your p.c.

Change #4): Place a check-mark on
"Empty Temporary Internet Files folder when browser is closed."

Explanation: no copies of webpages or page elements will be retained after you close your browser.

- A potential snoop won't have an easy way to pull up copies of the sites and pages you've visited.
- also reduces the clutter and digital debris that IE tends to accumulate over time.

Potential drawback:

- revisiting any given webpage might be fractionally slower because the pages will have to be fully downloaded again.

Change #5): Place a check-mark on
"Enable 64-bit processes for Enhanced Protected mode."

- (This setting is available only on 64-bit PCs) The 64-bit instance of IE 11 has two main classes of internal processes:
  Manager processes involve the browser's main operations; 64-bit throughout.
  Content processes involve creating and displaying the separate tabs you open, which may invoke 32-bit processes, even on 64-bit PCs.
- this setting elevates Content/tab processes to full, Protected Mode, 64-bit operation when possible.
- provides better security — might also give better performance.

Potential drawbacks, change #5:

- Some websites and add-on components might not work properly, if they’re based on elements that are 32-bit only.
- If you must visit sites or use add-ons that are not 64-bit compatible, temporarily disable the “Enable 64-bit processes for Enhanced Protected mode” option.

Change #6): Place a check-mark on
"Enable Enhanced Protected Mode."

Helps prevent Web-based malware and attackers from installing unwanted software, or modifying your system settings. Enhancements are:

- extra safeguards against memory-based malware exploits,
- better isolation for individual browser tabs,
- helps block several types of data-mining (such as remotely accessing documents on your PC)
- but, for reasons of backwards compatibility. Microsoft made the I.E.11 default "not enabled."

Contra-indications for Change #6:

You may encounter issues with websites you regularly visit or tools you use, in which case, disable the "Enhanced Protected Mode."

Example: Qualys Browsercheck needs a helper plug-in within I.E. that is thwarted by "Enhanced Protected Mode; I had to turn the latter off on my 1st p.c.

(Curiously, on my second p.c., starting Internet Explorer 11 gives an error message banner across the bottom that "the Qualys Browser Helper isn't compatible with Internet Explorer Enhanced security features and has been disabled," but if I invoke Browsercheck it seems to run normally, maybe because it was already installed when I made the Advanced Settings changes).

Change #7: Place a check-mark on "Enable SmartScreen Filter."

Explanation: warns you when visiting a site known to host hidden malware or that's been reported for phishing.

- Checks the underlying HTML and other code of each page, looking for signs of malicious intent.
- Also checks any software you download against a list of known-malicious programs.

Potential negative:

- Some people view SmartScreen Filter as too intrusive, because IE has to communicate with Microsoft servers (to check the list of sites that host malware, for example).

Change #8): Place a check-mark on
"Send Do Not Track requests to sites you visit in Internet Explorer."

Explanation: requests this small measure of extra privacy from websites you visit;

- some sites will respect your wishes;
- some will ignore it.

Potential downside to this setting – none known.

Change #9): Place a check-mark on
"Warn if changing between secure and not secure mode."

Enabling this setting can safeguard you against websites that redirect, divert, or otherwise deliver you from a secure (e.g., HTTPS) page or area to one that isn't secure (e.g., plain HTTP).

Potential downside: in some environments — especially mixed intra-/inter-networks — this setting might generate an annoying number of alerts. If so, disable it.

Lastly, after making these changes, remember to click "Apply" and then "OK," before exiting. Some of them will not take effect until you "Restart" Windows (or Shut Down and later Restart Windows).

Note: After making these “Advanced Settings” changes you can always undo them individually, or revert the “Advanced Settings” section to Microsoft's default settings, by clicking the “Restore Advanced Settings” button.

Users' Feedback

A check of the Readers' Forum section of the Windows Secrets website turned up one comment on having to back off on these Advanced Settings:

David Salahi posted a message February 9th that images in Outlook email were blocked after he implemented the nine changes. He had to undo Change #3, “Do not save encrypted pages to disk,” (uncheck it) to see images.

For further reading:

- Security and Privacy Settings for Internet Explorer:
  http://windows.microsoft.com/en-us/internet-explorer/ie-security-privacy-settings#ie=ie-11
- Change Internet Explorer Security Settings:
  http://windows.microsoft.com/en-us/windows/change-internet-explorer-security-settings#1TC=windows-7
- Internet Explorer Browser Settings:
  http://windows.microsoft.com/en-us/windows-vista/internet-explorer-browser-settings

Acknowledgments:

- Fred Langa. “Improve Internet Explorer 11’s security settings.” Windows Secrets Newsletter, February 4, 2016, Issue #520, (a division of Penton Publications).