Internet Security

Key Terminology

Antivirus/Antispyware/Antimalware–program that scans your computer to find and remove viruses/spyware/malware

Cache-files stored by the browser to speed up web page loading

Cookies/browsing data–files placed on your computer by websites to track Internet usage. Cookies are similar to spyware, except cookies come from sites you visits, are easy to find and remove, allow you to opt out of using them (although the associated web site might not work if you do,) and their purpose is usually defined in the associated web site's terms of service.

Firewall–restricts access to and from your computer by programs you have installed and/or external sources.

Fishing Scams–usually emails but also web sites that try to trick you into providing personal information. They copy the look of legitimate companies, but secretly redirect the information elsewhere.

History–list of web sites and pages you have recently visited.

Malware–software intended to damage or gain control of your computer by an unauthorized party.

Operating System–Windows is the operating system. (Others include OSX for Apple computers, or Android for most mobile devices.) The operating system communicates with the hardware and allows other programs to run.

Pop-ups–browser windows or boxes that open automatically when you visit a web page.

Registry-database on your computer that stores information about the computer's settings and configuration.

Registry Cleaner–removes stray files that have been left behind in the registry by other programs.

Spyware–software that installs itself on your computer for the purpose of tracking your computer use and sending it to a third party. Spyware is similar to cookies, except that spyware is usually hidden and difficult to remove, may not be associated with any web site you've visited, do not allow you to opt out, and their purpose cannot be determined by the user of the infected computer.

System alert messages–boxes that open automatically from your operating system, intended to warn you of an unsafe condition or malfunction.

User accounts–Windows allows users to set up separate accounts for each person who regularly uses a computer. Each account can have its own separate desktop, preferences, settings, and installed programs. You can see these accounts from the " Welcome" screen when you first start your computer.

Virus–a computer program that is capable of making copies of itself

Web browser (or just browser, for short) –these are the programs that allow you to access the internet, such as Firefox, Chrome, or Internet Explorer.

Clear cache, cookies, browsing data, and history.

Websites that you visit can hide files here that run in the background. You may not see them in the task manager or startup window. Each browser on your computer has a different method of clearing these files.

Internet Explorer

Internet Explorer is the most widely used Web browser. That makes it the most vulnerable, because most viruses are written to target it. Its creator, Microsoft, also has very lax policies about how your information is shared with other companies. Also, Setting for Internet Explorer can be adjusted using "Internet Options."

- Click the gear button.
- Select "Internet Options."

The "General" tab allows you to delete your browsing history and adjust how often temporary files are deleted.

- Under the "Browsing History" section, check "Delete Browsing History on Exit."
- Clock the "Delete" button.
- Remove the check mark from the first option, "Preserve Favorites Website Data."
- Check each of the rest of the boxes.
- Then click the "Delete" button.
- Click the "Settings" button. This opens the "Website Data Settings."
- In the "Website Data Settings" window:
    - The "Temporary Internet Files" tab allows you to determine how often Internet Explorer saves information about the web pages you visit. The more often it stores copies of pages, the slower your browsing speed will be.
    - The "History" tab allows you to determine how long Internet Explorer keeps track of your browsing history. The history can be useful if you want to return to a website but you don't remember its name or address. The history allows you to review every website you visited on a specific day. But the longer the browser remembers your history, the more files are stored on your computer. This can use up system resources and pose a security risk. Also, anyone who uses your computer can view your history.
    - The "Caches and Databases" tab allows you to determine if you want the browser to store page information at all, and allows you to limit the amount of system resources that are used for storing page information. If resources are limited, the browse automatically deletes store page information.

The "Privacy" tab allows you to determine what types of cookies are blocked.

- Check the boxes next to "Never allow websites to request your physical location" and "Turn on pop-up blocker" if these aren't already checked.
- Additional pop-up settings can be adjusted by clicking the "Settings" button.

The "Content" tab allows you to adjust "Auto Complete" settings. Auto Complete pre-fills forms on websites using stored usernames, passwords, email addresses, street addresses, phone numbers and account numbers. Auto Complete doesn't really improve performance, but turning it off secures your private information.

- Click the "Settings" button.
- Remove all the check marks.

- Click the “Delete AutoComplete History” button.
- Remember your usernames, passwords, email addresses, etc.!

The “Programs” and “Advanced” tabs have more advanced settings that can improve speed and performance.
Once you’ve finished making all your changes in the Internet Options window:
Click “Apply”
Click “OK”

Mozilla Firefox

Firefox provides the best privacy options of any of the most commonly used browsers. It’s been developed by a non-profit organization with a focus on user control and internet security. It is not the speediest, but it is the most secure, with most security features selected by default. To clear cookies, history and cached information:

- In the menu across the top, select “Tools.”
- Then select “Options.”
- Select the “Advanced” icon.
- Then select the “Network” tab.
- Under “Cached Web Content,” click the “Clear Now” button.
- Select the “Privacy” icon.
- Choose your tracking preferences. Websites are not obligated to honor your wishes. If you choose not to tell websites anything about your preferences, they assume tracking you is OK.
- From the drop-down menu, choose “Never remember history.”
- Click the link that says “clear your recent history.”
- In the window that opens, select “Everything” from the drop-down menu.
- Put check marks in all the boxes.
- Then click “Clear now.”
- You can remove individual cookies by clicking “remove individual cookies,” and selecting from the list.
- From the drop-down menu under the “Location Bar” heading, select “Nothing.”
- Select the “Content” icon.
- Check “Block Pop-Up Windows.”
- Choose your image load preferences. Loading images automatically is faster, but choosing each image to load would significantly change your browsing experience.
- Choose your JavaScript preference. JavaScript is easily exploited by malware, but most online interactive content, such as games and chat programs, require it.
- Exceptions for individual sites can be made by clicking on the “Exceptions” buttons.
- Select the “Security” icon.
- Check the first three boxes, “Warn me when sites try to install add-ons,” “Block reported attack sites,” and “Block reported web forgeries.”
- Exceptions for specific sites can be made by clicking the “Exceptions” button.
- Remove the check marks from “Remember passwords for sites,” and “Use a master password.”
- Again, exceptions can be made by clicking the “Exceptions” button.
- When you’ve finished making all of your changes, click “OK.”

Chrome

Chrome is the web browser created by Google. Most of Google's products and services are free because their business depends entirely on selling your personal information and browsing habits. Although the Chrome browser is installed on your computer, any information Chrome tracks and saves about you is stores "in the cloud." That means it is saved on Google's servers and not on your computer. You can still adjust the settings and tell Google what they can and can't do with your information, but you must have a Google account to do so. We won't go into these settings here.

Virus removal and prevention

Dance the security tango:

The Security Tango was created by the co-host of Sound Bytes, which is a call-in radio show about computers that's been on the air for 25 years. It takes you through the virus removal process, step-by-step, and provides links to free, reputable, virus removal and prevention software.

- Enter "http://www.securitytango.com" in the address bar of your favorite browser.
- Hover over the "let's dance" menu at the top of the page, then select "the windows waltz."

We won't go through the whole process, but comments about the steps follow:

- The first couple of steps we've already completed above, deleting temporary internet files, emptying the recycle bin, and emptying temp folders.
- System Restore is kind of like an archive of computer back-ups. You're supposed to be able to reload an earlier back-up from before your computer became infected, or before you deleted or modified something important. However, viruses can hide here and re-infect your computer. So, System Restore can often do more harm than good.
- Downloading free software–all the recommended software is available for free through the Security Tango site. These are some of the best security tools available, as evaluated by securitytango.com. They should not harm your computer further.
- Safe Mode–as the website states, safe mode starts your computer with the absolute minimum software running. This prevents programs from inadvertently starting up hidden viruses. Safe Mode does not allow you to connect to the Internet, so it is very important to have all your virus removal programs downloaded before you try to run them in Safe Mode.
- Repeat the process–the security tango takes so long to complete the first time that I don't think I've ever repeated it immediately after completing it. But it probably is a good idea.
- Windows Update - If you automate updates, you shouldn't need to do this, or you won't find any available updates anyway. But again, it won't hurt.

Automate updates & virus scans–these are generally automated by default, and it probably shouldn't be changed.

- Click the Start button.
- Select "Control Panel."
- Select "System and Security."
- Under the heading "Windows Update," select "Turn automatic updating on or off."
- Make sure "Install Updates Automatically" is turned on.

Things to avoid:

Fishing emails–Don't click on links or open files in emails you don't trust.

- There can be a difference between what you see on the screen and the invisible code that creates the page.
- Hover over a link.
- Look at the bottom left corner of the screen. This will show where the link really points to.

Disreputable sites–stay away from

- Adult websites,
- Any site that offers something free,
- Free online games,
- Free online television shows or videos that you would normally have to pay for elsewhere.

Some pop-ups are designed to look like system messages.

- Even trying to close them can install a virus.
- It may be better to power off your computer by holding down the power button for five seconds.

Viruses can spread through USB drives. Scan them before opening files on them.

Don't run two antivirus or firewalls at once.

- They can counteract each other.
- When an antivirus program finds a virus, it puts it in "quarantine."
- The second antivirus program considers these safely quarantined viruses to be threats.
- When the second program tries to move these files to its own quarantine, it basically opens the virus.
- Hidden file extensions: make visible.
- Viruses exploit the default setting that hides file extensions.

Resources:

- http://lifehacker.com/5923017/how-can-i-prevent-my-isp-from-tracking-my-every-move
- http://www.usa.gov/topics/family/privacy-protection/online.shtml
- http://www.huffingtonpost.com/2014/07/21/facebook-terms-condition_n_5551965.html
- http://www.huffingtonpost.com/tedtalks/jennifer-golbeck-ted-facebook-likes_b_5515129.html
- https://www.privacyrights.org/online-privacy-using-internet-safely
- https://www.privacyrights.org/ar/alertstrongpasswords.htm
- http://www.419eater.com/html/419faq.htm
- https://support.google.com/mail/checklist/2986618?hl=en&ref_topic=3406179
- https://support.google.com/chrome/answer/114836?hl=en
- http://mzl.la/LFrKSH
- http://www.securitytango.com