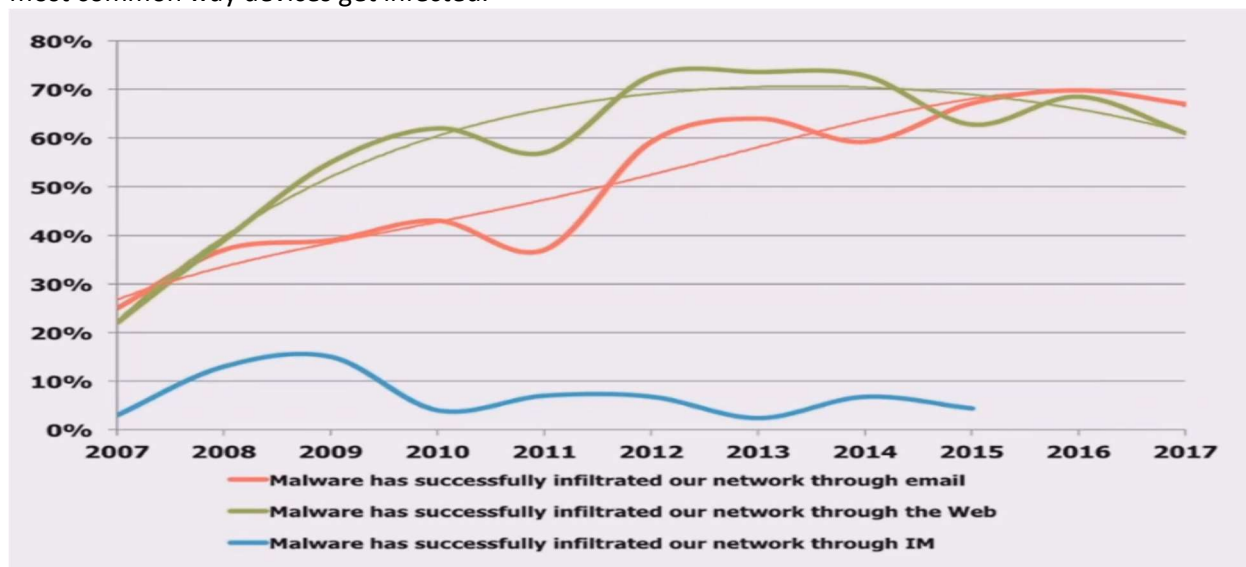


Securing your Browsers

The United States Computer Emergency Readiness Team (US-CERT) is a taxpayer funded US agency that works with the US Cyber Command and other government Cyber related agencies to secure US networks, both government and civilian. US-CERT recently released guidelines for securing your Internet browsers. This article is a condensed version of their recommendations with our slant on it. If you'd like to see the entire US-CERT article, the web address is:

<https://www.us-cert.gov/publications/securing-your-web-browser>

There is no doubt that you should protect all aspects of your digital world, it is more important now than ever. There is an undeclared digital war going on. The problem is anyone can be a casualty without knowing who the attacker is. Email recently became the primary way devices become compromised, browsers are now the 2nd most common way devices get infected.



The main reason for this change is that desktop security has gotten better, but email security hasn't. Plus, there are a lot more businesses and individuals using quality boundary firewalls. Securing email is another tech tip you will see in the future.






This may seem obvious, but the only way to browse websites is through use of a browser. You use several browsers whether you realize it or not. Browsers are on computers, phones, tablets and Smart TV's, but they are also on your gaming consoles, cars and many HDMI devices. Each type of browser has unique ways to be made more secure and it can seem to be a daunting task to secure them all. Some programs use browsers to complete tasks, so you need to understand the different programs you use at work and at home. It could take days to ensure all your browsers are secure, or you could make the decision to browse the Internet from certain devices.

NO ONE should ever use the original Microsoft Internet Explorer (IE) to access the Internet. IE is no longer supported by Microsoft and is not safe for use browsing the Internet for any reason. It should only be used to access network devices that are older and when you need to access such a device, you should consider if it should be replaced with a newer, more secure device.

The main Internet Browsers are, in order of popularity: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari and the open web browser Opera. Opera is used by many set-top boxes because it is Linux based, plus it has features that other browsers don't have. Most of those browsers have built-in tracking capabilities, to reveal your location, especially Google Chrome and Microsoft Edge. Most web sites add cookies to your devices through the browser to provide specific tracking information. If you'd like to read more about it, here

are two excellent articles: <https://www.howtogeek.com/180175/warning-your-browser-extensions-are-spying-on-you/> and <https://tiptopsecurity.com/what-is-the-most-secure-web-browser/>

Browser Comparison Chart (with no add-ons)

| Browser | Security | Privacy |
|---|-----------|----------------|
|  Chrome | Very good | Serious doubts |
|  Firefox | Good | Very good |
|  Edge | Good | Good |
|  Opera | Good | Probably okay |
|  Safari (Mac only) | Good | Maybe okay |

You can make any browser safer. Plus, there are secure browsers, some are free but difficult to use and some cost and are still difficult to use. They are: TOR (The Onion Router), SRWare Iron, Epic (MAC Only) and Comodo Dragon.

About now you are wondering if we will get to the point of securing Browsers. Now is the time!

All browsers have “add-ons” that provide special characteristics so the Browser can work in different environments. Some of these add-ins prevent advertisements from popping up, some prevent specific scripts from running, others stop specific kinds of cookies from being accepted, still others add limited filtering. Investigating what is available as add-ins for each browser is not hard to do on your own by just poking around, but there is a web page to help you: <https://fieldguide.gizmodo.com/8-extensions-that-should-make-your-browser-a-little-mor-1793325559>

Here is the list:

- LastPass (Chrome & Firefox)
- uBlock Origin (Chrome & Firefox) Ad Block & Privacy HIGHLY recommended
- Privacy Badger (Chrome & Firefox) tracking protection
- ScriptBlock (Chrome & Firefox) HIGHLY recommended
- uMatrix (Chrome & Firefox) adds another layer of firewall
- Disconnect (Chrome & Firefox) Blocks tracking cookies
- HTTPS Everywhere (Chrome & Firefox) HIGHLY recommended

How do you get and install these Add-On's???

<https://www.lifewire.com/installing-and-managing-browser-add-ons-and-extensions-4115522>

We hope this inspires you to poke around and make easy changes to your browsers to increase their security.