Browsers and Security

There are three main browsers, three lesser known browsers and one browser that you should never use to browse the Internet, they are:

Three Main Browsers

- Mozilla Firefox
- Google Chrome
- Microsoft Edge



Three Lesser Known Browsers

- Apple Safari
- Opera
- Russian Yandex



The Browser you should never use to browse the Internet:

- Microsoft Internet Explorer 

Network Security

The first level of security is a boundary firewall. For a lot of people it is financially impractical to buy and install a quality boundary firewall. After a boundary firewall is desktop security followed by good backups that are not visible on your network. The final area of security you should be concerned with is browser and email security, which are additional services.

Which Browser is the best?

Yandex is <u>not recommended</u> for use in the US, it's a Russian based browser.

Mozilla Firefox is similar to Internet Explorer in operation and is probably the most used Browser in the US, is highly customizable and recommend by most security experts. In fact TOR uses it as their browser.

Google Chrome is installed on more systems than any except Internet Explorer, is a little more complicated than Firefox and is generally accepted to be just as secure as Firefox.

Microsoft Edge is technically the best, most secure, browser available, but it doesn't work with all web sites because of its "advanced" security.

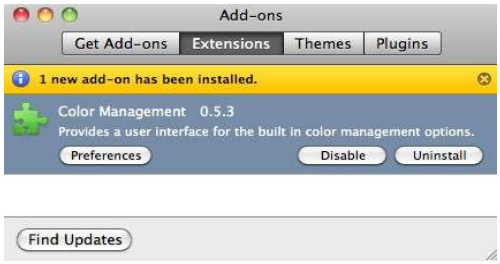
Apple Safari is the default browser for Apple products and within those products it does a good job. On any other platform you are better off with another browser.

Microsoft Internet Explorer

Microsoft has given up on Internet Explorer, what it is currently, is what it's going to be until it disappears. There will be no changes to it. The basic statement is that you should NEVER use Internet Explorer to Browse the Internet, only use it to do specific things on known safe sites. The issue is that Internet Explorer will do things that none of the other browsers can. With a little work, you can make Internet Explorer do what needs to be done and be safe. For this article we won't go into those areas, just know that it is capable.

Browser Add-in's

All browsers have Add-in's to allow them to do something that is not part of the basic browser. It is important that you consider at least uBlock Origin and don't go to sites that complain that it's on, they are not sites you should visit.



Browser Private Mode

When you go to a web site, a lot of information about you is provided to the site, including: your location, your PC type, where you go on the site, any preferences you set for the site, possibly your name and email, depending on what cookies are on your machine.

All Browsers have the ability to be put in "Private Mode", that is a mode where the browser won't store any cookies and won't reveal anything about you, your location, your machine or the other cookies that are on your computer. You should put your browser in "private mode" each time you visit social media sites, news sites or any other site that you think is questionable. It won't protect you from doing stupid things, but is a first step.

Remembering Passwords

Every browser has the capability to remember user names and passwords for the sites you visit. This capability in Microsoft Edge, Mozilla Firefox and Google's Chrome is secure and can be made more secure by turning on a master password. As long as you have a good user name and password for your PC that no one else knows, there is nothing wrong with taking advantage of this convenient service. But we recommend turning on the Master Password capability.

The passwords are stored in an encrypted format and when used do not show the password. A Master the Master Password is a password that allows the use of the stored passwords during a Browser session. You put the Master Password in once at the beginning of the session to use remembered passwords throughout the session.

Everyone and every business should use master passwords if you are allowing the browsers to remember passwords. Read that sentence out loud.

Add-Ons

All browsers support 3rd party add-on's that do a variety of things. Somewhere in each browser is a list of add-ons that have been tested and work with that specific browser. There are recommended add-ons: NoScript and uBlock Origin. NoScript only allows JavaScript and Flash to work from trusted domains while uBlock Origin is an ad-blocker.

Best Practices

It's tough to not recommend specific add-on's to enhance the abilities of each Browser. Keep in mind that what we recommend now, may not be relevant in 6 months. So keep getting our newsletters and check our new web site when it comes out to stay up to date.

Anyone can do a Google Search to find the "Best Browser Add-in's". The only add-in we recommend for everyone is uBlock Origin and NoScript, both work with Firefox and Chrome.

Antivirus

As you can imagine, Antivirus programs have to do a LOT. They have to check your hard drive for malicious software, they have to check memory for malicious programs running and they have to filter everything you are doing to try to prevent infections AND do it without effecting the perceived performance of your PC!

There is a trend to provide anti-threat protection based on what you are doing. There are now Internet Security packages that focus on just the Internet and work as a browser plug-in as well as a program running on the machine. They can limit where you go and prevent internet based threats. In addition, they do an ok job with the other aspects of protecting your machine from threats. They are Proxy Servers and are also called Secure Web Gateways (SWG). These are fairly new and there hasn't been a lot of testing done by independent sources.

All that said, for a machine that is mostly used to browse the Internet and doesn't have any other types of network security, we recommend considering one of these packages.