Ways to use the Internet more securely

Ways to use the Internet more securely

There are a number of options to use to increase security when using the internet.

1. Private browsing

All browsers have the ability to browse the internet in a more private manner. Private browsing is found in Microsoft Edge, Microsoft Internet Explorer and Mozilla Firefox, Incognito browsing found in Google Chrome. They are accessed via the browsers settings menu. The browsing sessions accept cookies (small programmes to track you) and add the site to your history but will delete all cookies and history when you end that internet session

Epic Privacy Browser (www.epicbrowser.com) is a browser that is especially built for online anonymity. It permanently runs incognito mode.

A more private search engine is StartPage (www.startpage.com). This uses Google search but does not transmit any information to Google. DuckDuckGo is another private search engine (dudckduckgo.com).

2. Browser Extensions

A browser extension is a plug-in that extends the functionality of a web browser. All browsers have the option to add extensions. There are a large number of them but three worth noting here are Adblock Plus, Ghostery and HTTPS Everywhere. Adblock Plus simply blocks external ads on webpages. It does not block ads that are incorporated into the webpage. Plus, some sites recognise the use of Adblock and demand you disable on their site if you want to access. Ghostery strips out tracking objects on the pages you visit. Tracking cookies, online analytics and more are prevented from running. HTTPS Everywhere forces webpages to use the more secure HTTPS rather than the usual HTTP if that site has the option to run HTTPS.

Note, however, that browser extensions are running within your browser but are not part of the browser so they bypass the browsers security features giving them the potential to snoop on your activity. Assuming you stick with extensions from well-known developers and well-reviewed extensions with lots of users the risks are fairly minimal. You shouldn't overload your browser with extensions. Each extension another piece of code running on your computer and can slow your browsing experiencer.

3. Block third party cookies

These come from objects embedded in the webpage rather than from the provider of the webpage. They have the ability to download their cookies and monitor your activity. All browsers have, in their settings, the option to block third party cookies.

4. Adobe Flash Player

This programme allows video to be played in the webpage. The programme itself is fine but hackers have been known to embedded malware into the videos to infect your computer. Make sure you are using the latest version of Adobe Flash. Windows updates regularly downloads the latest version of Adobe Flash. Microsoft Edge does not allow Adobe Flash to automatically run within the browser. If you click on a vide that uses the programme Edge will ask if you will allow it. Google Chrome will also be blocking the automatic running of Adobe Flash in a later version. Adobe has stated that it will discontinue Adobe Flash in 2020. Websites are moving to the more secure HTML5 format.

5. Virtual Private Networks (VPN)

The most secure method of using the internet. You first need to subscribe to a VPN service. There are paid and free subscriptions available. The website request between you and the VPN provider is encrypted so anyone monitoring your internet activity can only see the link of the VPN provider. They cannot see your data, though your VPN provider can see your activity. You can select a service from basically anywhere in the world so you need not use a server based in Australia. VPNs are particularly useful when using free wifi services as you don't know who the provider of that service is. Hackers can set up free wifi in these situations. Also, useful if you don't want your internet provider seeing what your activity is for whatever reason.

There are many VPN providers and you will need do research to pick the one best suited to you. If your needs are modest and you only need a VPN for particular activities then a free service should suffice. The downside of free services is that your download limit may be small. The free service I use is Tunnelbear (www.tunnelbear.com). Because data is fully encrypted the internet speed will be slightly reduced.

Peter Day