The Ways to Protect Yourself in the Internet

Tracking cookies and LSO (flash) cookies are small pieces of code that websites attach to your computer to store information about your online activities. Information about you can then be sold to companies around the world without your consent.If you are concerned about what information about you is collected and how it is used, you should block or remove unwanted cookies on your browsers on a regular basis or use the anonymous browsing or get better privacy plugin.

Use Strong Passwords

Device fingerprinting is a fairly new technology that is useful in fraud prevention and safeguarding any information from one's computer. Device fingerprinting uses data from the device and browser sessions to determine the risk of conducting business with the person using the device. Use privacy focused search engines/browsers like DuckDuckGo, MetaGer, etc.

Use Anonymizer

An Anonymizer such as I2P – The Anonymous Network can be used for accessing web services without them knowing one's IP address and without one's ISP knowing what the services are that one accesses. Additional software has been developed that may provide more secure and anonymous alternatives to other applications. For example, Bitmessage can be used as an alternative for email and Cryptocat as an alternative for online chat. On the other hand, in addition to End-to-End encryption software, there are web services such as Qlink which provide privacy through a novel security protocol which does not require installing any software.

Be Careful What You Share On Social Networking Sites

Use web proxy. A proxy server (sometimes called an "open proxy" or just "proxies") can be use to re-route your browser (Chrome, Firefox, Safari, Internet Explorer, or Edge) around company or school content filters. There are risks involved in using masking your IP address with a proxy: Many will slow down your internet connection, some are run on compromised machines, and may not be legal in some countries. Websites know only the IP address, not mac. So hiding IP is enough. You can use web proxy. If you are not worried about time consuming process, you can use VMware which is the latest trend in it. But for every session you have to delete the VMware Windows installation. - Use encryptions and decryption programs like PGPPretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

Use Firewall Rules

Firewall rules allows computer to send traffic to, or receive traffic from, programs, system services, computers, or users. Rules can be created for either inbound traffic or outbound traffic. The rule can be configured to specify the computers or users, program, service, or port and protocol. You can specify which type of network adapter the rule will be applied to: local area network (LAN), wireless, remote access, such as a virtual private network (VPN) connection, or all types. You can also configure the rule to be applied when any profile is being used or only when a specified profile is being used.