**SOP – Internet Security Overview **

4/2/18

**The Best Internet Security Suites Software of 2018:**

[Antivirus software](https://en.wikipedia.org/wiki/Antivirus_software) and Internet security programs can protect a programmable device from attack by detecting and eliminating viruses.

|  |  |  |
| --- | --- | --- |
| **Ranking** | **Best Internet Security Suites** | **Price** |
| 1 | Bitdefender | $39.99 |
| 2 | Norton Security | $44.99 |
| 3 | Kaspersky Labs | $39.99 |
| 4 | Trend Micro | $39.95 |

**McAfee** doesn't perform as well as most other **antivirus** software tested.

Comcast offers **Norton Security Suite** for free to subscribers! Security Suites contain a suite of firewalls, anti-virus, anti-spyware and more. **YOU MUST HAVE A SECURITY SUITE ON YOUR COMPUTER!**

**Best Practices:**

Trinity College Video (end 3:30): <https://www.youtube.com/watch?v=pfnFqOItSIg>

When surfing use HTTP**S** and SSL whenever possible:

Regular web site connections over HTTP exchange lots of plain text over the wireless network you're connected to, and someone with the right skills and bad intent can sniff out that traffic very easily. It's not that big of a deal when the text is some search terms you entered at Lifehacker, but it is a big deal when it's the password to your email account. [Using HTTPS](http://lifehacker.com/5745086/why-should-i-care-about-https-on-facebook-or-other-web-sites) (for visiting web sites) or enabling SSL (when using applications that access the internet, such as an email client) encrypts the data passed back and forth between your computer and that web server and keep it away from prying eyes.

Note that if the sensitive browsing can wait—especially if it's something very sensitive like banking or credit card info—**you should just wait to do that sensitive browsing at home**.

Coffee shops:

“Wherever there is an unsecured public Wi-Fi network, there is the threat of attack.” Coffee shops are seen as the most dangerous public Wi-Fi venue of all.

**Long Realty Office Network:**

**Firewalls** impose restrictions on incoming and outgoing [Network packets](https://en.wikipedia.org/wiki/Network_packet) to and from private networks. Incoming or outgoing traffic must pass through the firewall; only authorized traffic is allowed to pass through it. Firewalls create checkpoints between an internal private network and the public Internet, also known as [*choke points*](https://en.wikipedia.org/wiki/Choke_points) (borrowed from the identical military term of a combat limiting geographical feature). Firewalls can create choke points based on IP source and TCP port number.

Most OS’s come with at least a basic firewall nowadays, and it's a [simple step](http://lifehacker.com/5805326/how-to-turn-your-computers-firewall-on-and-off) to keeping unwanted local users from poking at your computer. You may already be using a firewall, but just in case, go into your security settings (in Windows under Control Panel > System and Security > Windows Firewall; and on a Mac under System Preferences > Security & Privacy > Firewall) and make sure your firewall is turned on. You can also edit which applications are allowed access by clicking on "allow a program or feature" in Windows and "advanced" in OS X. Your firewall [is not an end-all, be-all protector](http://lifehacker.com/5560567/nine-common-myths-and-misconceptions-about-viruses-examined-and-debunked), but it's always a good idea to make sure it's turned on.

Microsoft Windows and MAC OS protect access somewhat after the firewall. But be careful if you have shared any files or access with anyone. They will have access until you revoke it!

**Internet Security Definitions**

From Wikipedia

**Internet security** is a branch of [computer security](https://en.wikipedia.org/wiki/Computer_security) specifically related to the [Internet](https://en.wikipedia.org/wiki/Internet), often involving [browser security](https://en.wikipedia.org/wiki/Browser_security) but also [network security](https://en.wikipedia.org/wiki/Network_security) on a more general level, as it applies to other applications or [operating systems](https://en.wikipedia.org/wiki/Operating_systems) as a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of [intrusion](https://en.wikipedia.org/wiki/Hacker_%28computer_security%29) or fraud, such as [phishing](https://en.wikipedia.org/wiki/Phishing), online [viruses](https://en.wikipedia.org/wiki/Computer_virus), [trojans](https://en.wikipedia.org/wiki/Trojan_horse_%28computing%29), [worms](https://en.wikipedia.org/wiki/Computer_worm) and more.

**Malicious software** - an internet user can be tricked or forced into downloading software onto a computer that is of malicious intent.

[Malware](https://en.wikipedia.org/wiki/Malware), short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term badware is sometimes used, and applied to both true (malicious) malware and unintentionally harmful software.

A [botnet](https://en.wikipedia.org/wiki/Botnet) is a network of [zombie computers](https://en.wikipedia.org/wiki/Zombie_computer) that have been taken over by a robot or bot that performs large-scale malicious acts for the creator of the botnet.

[Computer Viruses](https://en.wikipedia.org/wiki/Computer_Viruses) are programs that can replicate their structures or effects by infecting other files or structures on a computer. The common use of a virus is to take over a computer to steal data.

[Computer worms](https://en.wikipedia.org/wiki/Computer_worms) are programs that can replicate themselves throughout a computer network, performing malicious tasks throughout.

[Ransomware](https://en.wikipedia.org/wiki/Ransomware_%28malware%29) is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.

[Scareware](https://en.wikipedia.org/wiki/Scareware) is scam software with malicious payloads, usually of limited or no benefit, that are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety, or the perception of a threat, generally directed at an unsuspecting user.

[Spyware](https://en.wikipedia.org/wiki/Spyware) refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user's consent.

A [Trojan horse](https://en.wikipedia.org/wiki/Trojan_horse_%28computing%29), commonly known as a *Trojan*, is a general term for malicious software that pretends to be harmless, so that a user willingly allows it to be downloaded onto the computer.

[KeyLogger](https://en.wikipedia.org/wiki/Keystroke_logging), Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a [keyboard](https://en.wikipedia.org/wiki/Keyboard_%28computing%29).

Phishing is an attack which targets online users for extraction of their sensitive information such as username, password and credit card information.[[5]](https://en.wikipedia.org/wiki/Internet_security#cite_note-5) Phishing occurs when the attacker pretends to be a trustworthy entity, either via email or web page. Victims are directed to fake web pages, which are dressed to look legitimate, via spoof emails, instant messenger/social media or other avenues. Often tactics such as [email spoofing](https://en.wikipedia.org/wiki/Email_spoofing)are used to make emails appear to be from legitimate senders, or long complex [subdomains](https://en.wikipedia.org/wiki/Subdomain) hide the real website host.

**Remedies:**

**Network layer security -** [TCP/IP](https://en.wikipedia.org/wiki/TCP/IP) protocols may be secured with cryptographic methods and [security protocols](https://en.wikipedia.org/wiki/Cryptographic_protocol). These protocols include [Secure Sockets Layer](https://en.wikipedia.org/wiki/Secure_Sockets_Layer) (SSL), succeeded by [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS) for [web traffic](https://en.wikipedia.org/wiki/Web_traffic), [Pretty Good Privacy](https://en.wikipedia.org/wiki/Pretty_Good_Privacy) (PGP) for email, and IPsec for the network layer security.

**Internet Protocol Security (IPsec) -** [IPsec](https://en.wikipedia.org/wiki/IPsec) is designed to protect TCP/IP communication in a secure manner.

**Multi-factor authentication** - Multi-factor authentication (MFA) is a method of computer access control in which a [user](https://en.wikipedia.org/wiki/User_%28computing%29) is granted access only after successfully presenting several separate pieces of evidence to an [authentication](https://en.wikipedia.org/wiki/Authentication) mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are). Internet resources, such as websites and email, may be secured using multi-factor authentication.

**Security token -** Some online sites offer customers the ability to use a six-digit code which randomly changes every 30–60 seconds on a [security token](https://en.wikipedia.org/wiki/Security_token). The keys on the security token have built in mathematical computations and manipulate numbers based on the current time built into the device. This means that every thirty seconds there is only a certain array of numbers possible which would be correct to validate access to the online account. The website that the user is logging into would be made aware of that device's serial number and would know the computation and correct time built into the device to verify that the number given is indeed one of the handful of six-digit numbers that works in that given 30-60 second cycle. After 30–60 seconds the device will present a new random six-digit number which can log into the website.