

Software Protection for a Personal Internet Connected Computer over Public Network one alternative Virtual Private Network - VPN

Why mess with you?

- Tracking locations of children, you and your connects
- Tracking browsing habits for advertisers
- Reading / copying messages, files and photos
- Mischievous / blackmailers / threats
- Governments / political / law enforcement

Levels and Type of Protection:

- **YOU** – reasonability safe computing,
 - Other Infection methods:
 - USB infested
 - Email
 - Programs
 - Shard data
 - Wi-Fi
 - Blue tooth
 - Other devices
- Update - all programs often
- Firewalls – on computers as well as in router
- Antivirus / Malware – malwarebytes removes malware, ransomware and access to and from known malicious websites
- Encryption – Messaging/files/photos with PGP, Keybase or Signal

- Messenger – FaceBook’s WhatsApp is not open-source
- Virtual computing / Sandboxing - is a type of virtualization technology that separates a part of your hard drive and memory (and other resources allocated to a program to run) from the rest. Firefox’s “Browser in the Box” browser

- Private / Anonymous web browser – Opera, Firefox etc. ensures that your internet history and activity are removed as soon as you close all private windows. Note: https:// is TLS encryption, but the “Foremost data carving tool and Strings program” found things like traces of users, pages and sites visited

- TOR Browser - "traffic analysis." Onion layers as it bounces form hub to hub; e anonymous web browser with VPN. Need to defrag and clean disk often

- Virtual Private Network - VPN client, proxy server, enables users to send and receive data across shared or public networks by encrypting data (not header & not to/from).

Vedio:

The Importannce of Having a VPN

Presented by Joe Melfi:

Part 10 to 46 minutes

Youtube recording November 4, 2017

APCUG – www.apcug2.org – Fall 2017 vertual Technology Conference

APCUG - An International Association of Technology Computer User Group

What to look for in a VPN

- Affordability for as many devices as you can - 1 to 5 devices
- Should experience little sluggish performance: throttling, bandwidth limits, restricted services
- Multiple global exit nodes (other countries locations)
- No logs-no traffic records and no traces
- Kill switch-stop all traffic if not encrypted
- Flexibility and ease of use
- Optional: Add blocking (speed up browsing)Flexibility
- Payment methods should be private

Kasperksky VPN free for 200MB/day or \$29.99/yr – 5-devices 1-user

Avast VPN Service on windows free 7 days Android, iPhone/iPad, 1-device \$19.99/Yr: 5-divices \$79.99 PC, Mac 1-device \$59.99/Yr
You may want to check out more software, such as **Message Box Generator**, **Box for Outlook** or **Kiss-Box Editor**, which might be [similar](#) to Browser in the Box.

Notes about other threats:

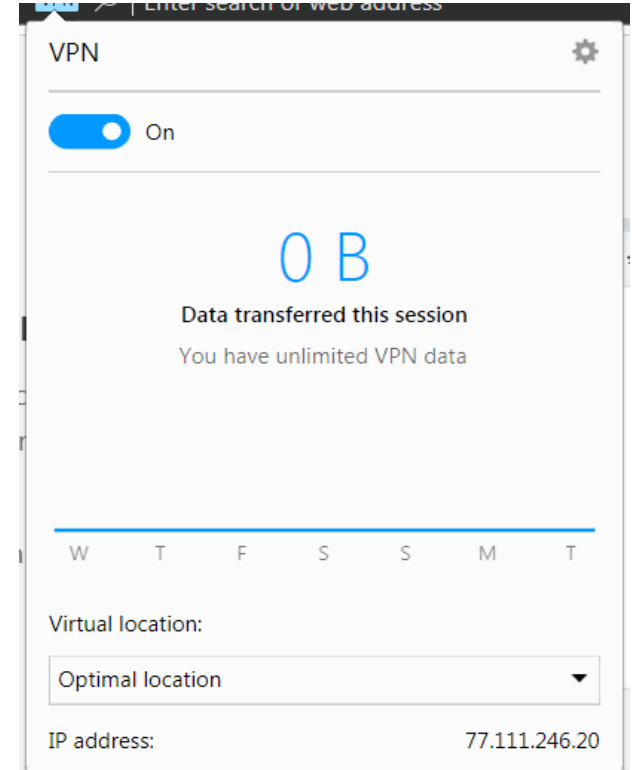
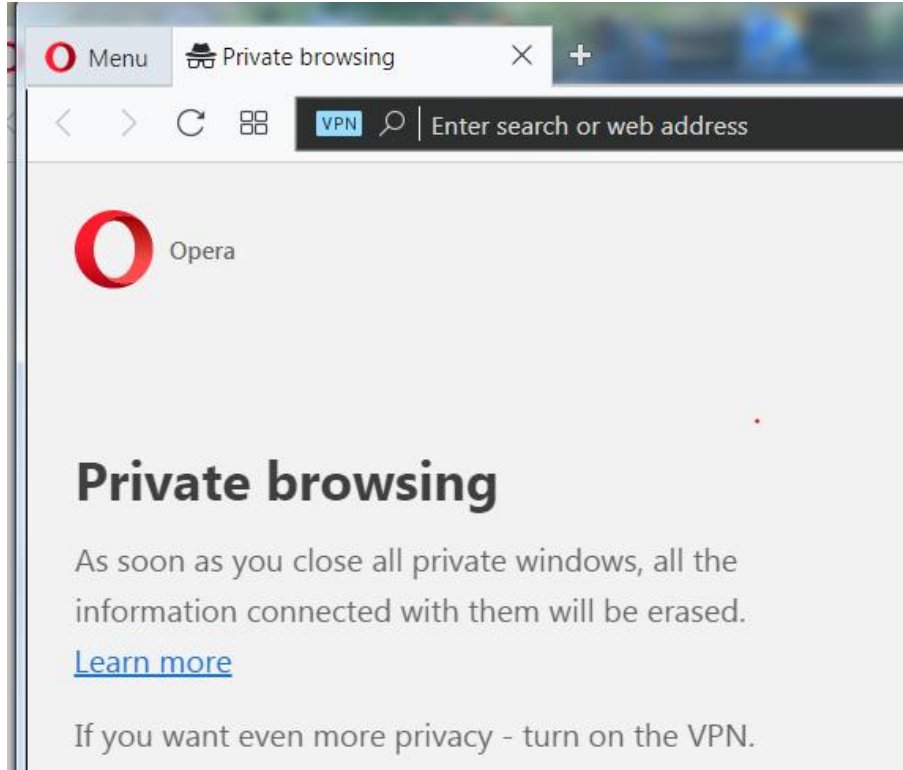
Keylogger

It's illegal for a malware author to spy on someone's webcam or microphone but it's ok for Google to do it just because they told the user to accept a long agreement. Now they can do whatever they want and it's legal for them to do it.

Linux has few hackers as compared to other operating systems

SIKURPhone claims "Hacker-proof" device \$700 to \$800

Example of free VPN you all can have free with just a download of Opera Browser.



Personal VPN Services for Android

- PIA (\$6.95/mo)
- Turbo VPN (free)
- Pure VPN (free)
- TunnelBear (free) o

Sandbox Tor Browser

Now, let us shift to another secure technology called Sandboxing. Basically, Sandboxing is a type of virtualization technology that separates a part of your hard drive and memory (and other resources allocated to a program to run) from the rest. Anything you do in that restricted environment (aptly named, Sandbox) does not impact rest of the system. In addition, when you are done with your work, you can just get rid of the Sandbox and everything is removed from your PC. This technology is already used by some of the browsers. Therefore, when you browse the web using those browsers, you are doing so in a restricted environment that cannot affect your system negatively. How cool is that?

This tutorial article explains **how to**. [I recently talked about Tor Browser](#) that provides an unprecedented level of anonymity.

<http://www.ilovefreesoftware.com/28/tutorial/sandbox-tor-browser.html>

Tor (product of Mozilla) protects you against a common form of Internet surveillance known as "traffic analysis." Traffic analysis can be used to infer who is talking to whom over a public network. Knowing the source and destination of your Internet traffic allows others to track your behavior and interests. if you're traveling abroad and you connect to your employer's computers to check or send mail, you can inadvertently reveal your national origin and professional affiliation to anyone observing the network, even if the connection is encrypted.


WikiHow teaches you how to change a Virtual Private Network's settings on a Windows or Mac computer, or on an iPhone or Android smartphone. In order to configure your VPN's settings, you must first [connect to a VPN](#). Most VPNs are not free and require a paid subscription before you can connect.


<https://www.wikihow.com/Configure-a-VPN>

Four Methods: [On Windows](#) [On Mac](#) [On iPhone](#) [On Android](#) [Community Q&A](#)

On Windows

Open Start  . Click the Windows logo in the bottom-left corner of the screen.

Open Settings  . Click the gear-shaped icon in the lower-left side of the Start window.

Click  Network & Internet. It's in the middle of the Settings window.

Click VPN. This tab is on the left side of the Network & Internet menu.

Select a VPN. Click the name of a VPN that you want to configure.

Click Advanced options. It's below the VPN that you selected. Doing so opens the VPN's page. you're adding a VPN for the first time, click + Add a VPN connection.

Click Edit. This option is near the middle of the page. The VPN's settings will open.

Configure your VPN's information. Change any of the following information:

Connection name - The name of the VPN on your computer.

Server name or address - Change the VPN's server address.

VPN type - Change the connection type.

Type of sign-in info - Select a new type of sign-in (e.g., Password)

User name (optional) - If necessary, change the username that you use to sign into the VPN.

Password (optional) - If necessary, change the password that you use to sign into the VPN.

Click Save. It's at the bottom of the page. Doing so will save your changes to the VPN and apply them
