



# So – What is Anti-Virus?

(and maybe VPNs and Firewalls Too)

---

ANTI-VIRUS IS LIKE TAKING  
VITAMIN C OR ZINC FOR A  
COLD - IT'S BETTER TO HAVE  
SOME THAN NONE AT ALL

# There are MANY, MANY, MANY Anti-Virus (AV) Programs - - - Some are FREE while others will cost you

---

- What does anti-virus do?
- How do you get a virus?
- How do you know you have a virus?
- How do you protect yourself?
- Which is best for me (Free or Paid)?

It protects your device from viruses (malware).

By exposing yourself (websites, email, portable storage)

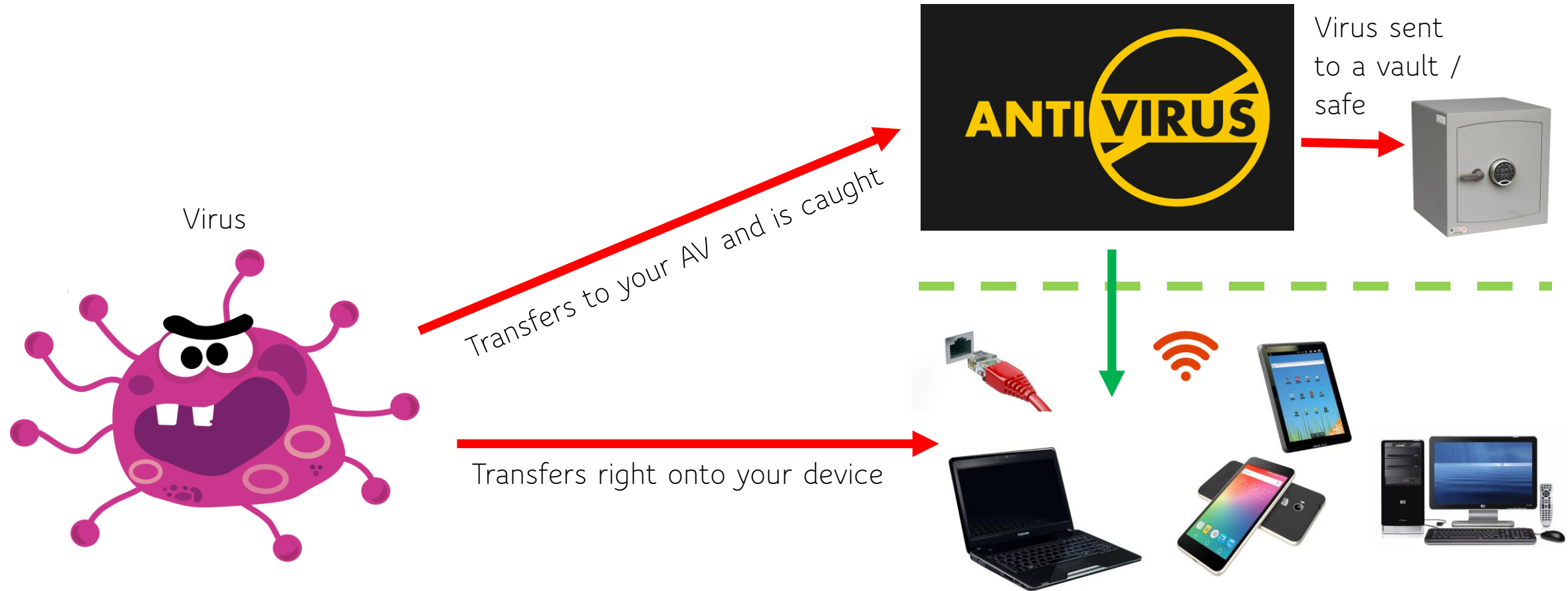
Your device starts to operate strangely

Install anti-virus software, (maybe firewall, vpn)

To start with – just get one.

# How Does Anti-Virus Protect My Device ?

---

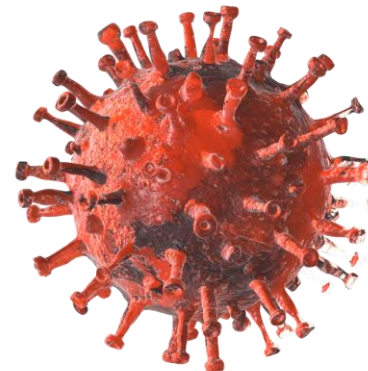
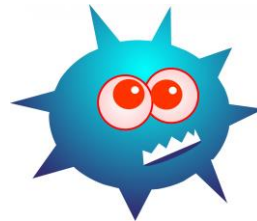
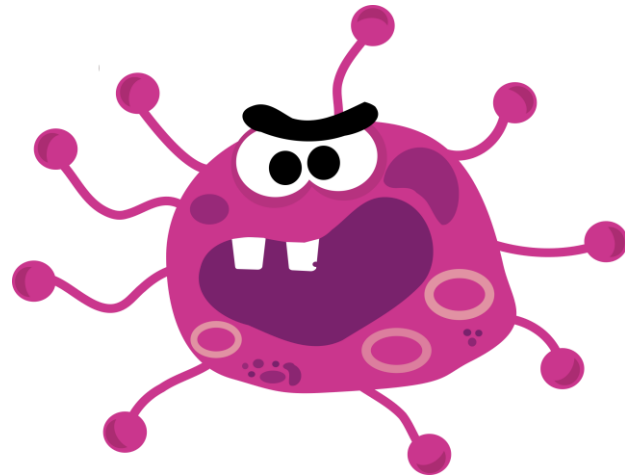


# How Do You Get A Virus ?

---

## Viruses sit on the Internet

- you may have it sent to you accidentally -or- on purpose
- sitting on a website grab it there (link, picture, etc)
- attached to a download (email, link)



There are **more than 1 billion** malware programs out there on the internet.

**1,000,000,000**

## DataProt.NET

“Even with built-in antivirus software protecting the newest operating systems, there's more malware online than ever before.”

Nov 2, 2022

# How Do You Know You May Have A Virus ?

---

**Your device may begin to operate strangely (laptop / pc / ipad / tablet / smartphone)**

- **unexpected pop-up windows**
- **random sounds**
- **unexplained file or folder changes**
- **slow startup, extremely slow response, seems to hang**
- **random connections to unknown websites / default website changes**
- **unexpected images**
- **inability to download anti-virus programs or updates**
- **spam sent from your email address to social media**

# How Do You Know You May Have A Virus ?

---

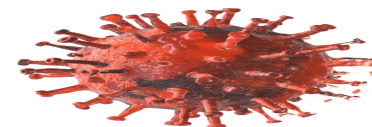
## **Other possibilities .....**

- suspicious hard drive activity**
- lack of storage space**
- missing files**
- crashes and error messages**
- high network activity**
- your email is hijacked**
- security attacks**

# How Do You Protect Yourself ?

---

1. Install and run an anti-virus software program to remove malware. (viruses).
2. Then set the software to automatically scan your system on a regular basis.
3. Keep it up-to-date to protect against the most recent threats.



Then ....

Ensure your computer firewall is turned on to block malware attacks via the internet.

# Which Is Best For Me; Free or Cost ?

---

**1<sup>st</sup> Off – It's Much Better to have an up-to-date anti-virus software than nothing at all !!!!!**

**2<sup>nd</sup> Free is a good place to start. There are many very effective Free AVs. It's Quick & Simple to install . It gives you a chance to try one out before deciding to purchase one.**

**Best Free Antivirus software for the US.**

**<https://us.cybernews.com/lp/free-antivirus-software-us/>**





















**Best Paid Antivirus software for the US.**

**<https://us.cybernews.com/lp/best-antivirus-software-us/>**



# Which Is Best For Me; Free or Paid ?

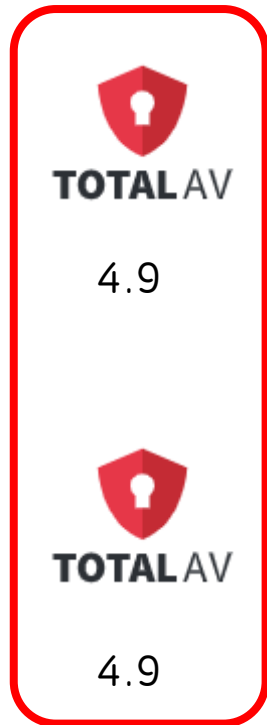
## FREE

 <b>TOTAL AV</b> 4.9	 <b>NordVPN</b> Threat protection 4.6	 <b>Surfshark Antivirus</b> 4.4	 <b>Bitdefender</b> 4.2	 <b>norton</b> 4.0	 <b>eset</b> 4.0	 <b>McAfee</b> 3.9	 <b>Avira</b> 3.9	 <b>TREND MICRO</b> 3.8	 <b>PCPROTECT</b> 3.7
<h2>PAID FOR</h2>									
 <b>TOTAL AV</b> 4.9	 <b>norton</b> 4.6	 <b>NordVPN</b> Threat protection 4.4	 <b>Surfshark Antivirus</b> 4.2	 <b>Bitdefender</b> 4.0	 <b>ĀURA</b> 4.0	 <b>eset</b> 3.9	 <b>McAfee</b> 3.9	 <b>Avira</b> 3.8	 <b>TREND MICRO</b> 3.7

Rating System: out of 5

# Which Is Best For Me; Free or Paid ?

---



<https://www.totalav.com/free-download>

1. Install and run an anti-virus software program to remove malware. (viruses)
2. Then set the software to automatically scan your system on a regular basis.
3. Keep it up-to-date to protect against the most recent threats.

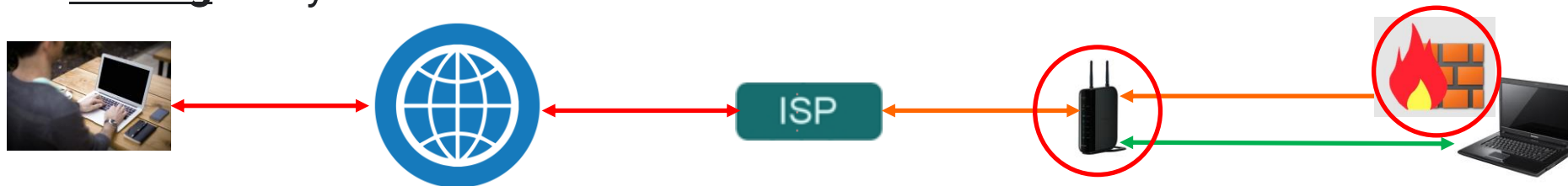
# Firewalls



## What is a firewall and how does it work?

Firewalls are **network security systems that prevent unauthorized access to a network**. It can be a hardware or software unit that filters the incoming and outgoing traffic within a private network, according to a set of rules to spot and prevent cyberattacks. Firewalls are used in enterprise and personal settings

Firewalls will help protect you from various threats, such as **malware and cyber-attacks**, from **coming** into your network.



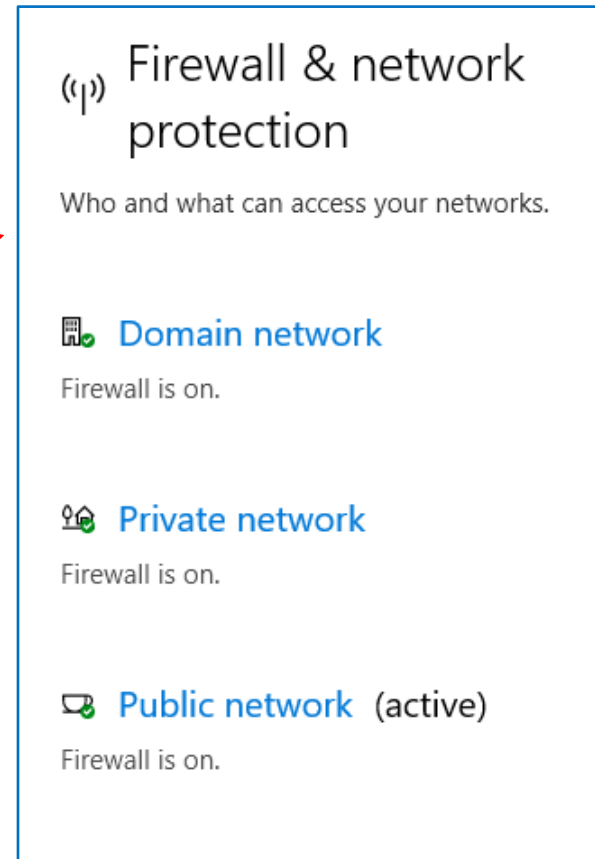
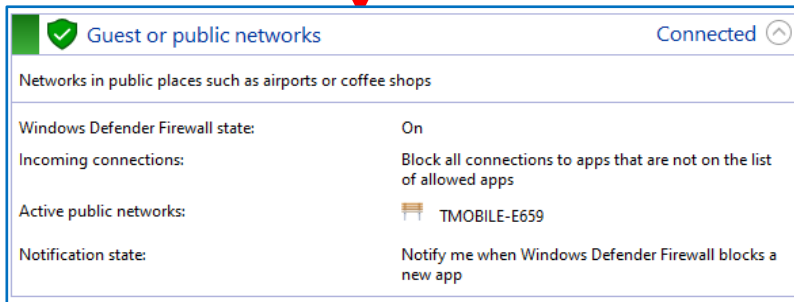
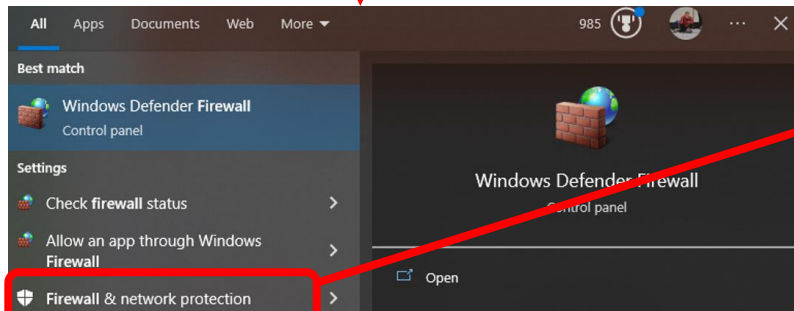
*Your Antivirus will protect you from **bringing** a threat into your device.*

# Firewalls

Windows: Bottom left task bar; click on it



Key in **firewall** <return>



# Firewalls

---

## **IOS:**

Does an iPad have a firewall?

iPad's security systems make it so that iPad does not need a separate firewall. you don't need an extra firewall 1st of all, iPhones and iPads are 99.9% immune to viruses. A dedicated firewall App for iOS/iPadOS doesn't exist per-se

## **Android:**

How do I turn on my Android firewall?

In the Firewall window, click Configure. The Firewall window opens. Select the Firewall mode: To allow all inbound and outbound connections, move the slider to Allow all.

Google App Store:

NetGuard

Droid Firewall

VPN Safe Firewall

AFWall

Mobiwol

# VPNs

---

## What is a VPN used for?

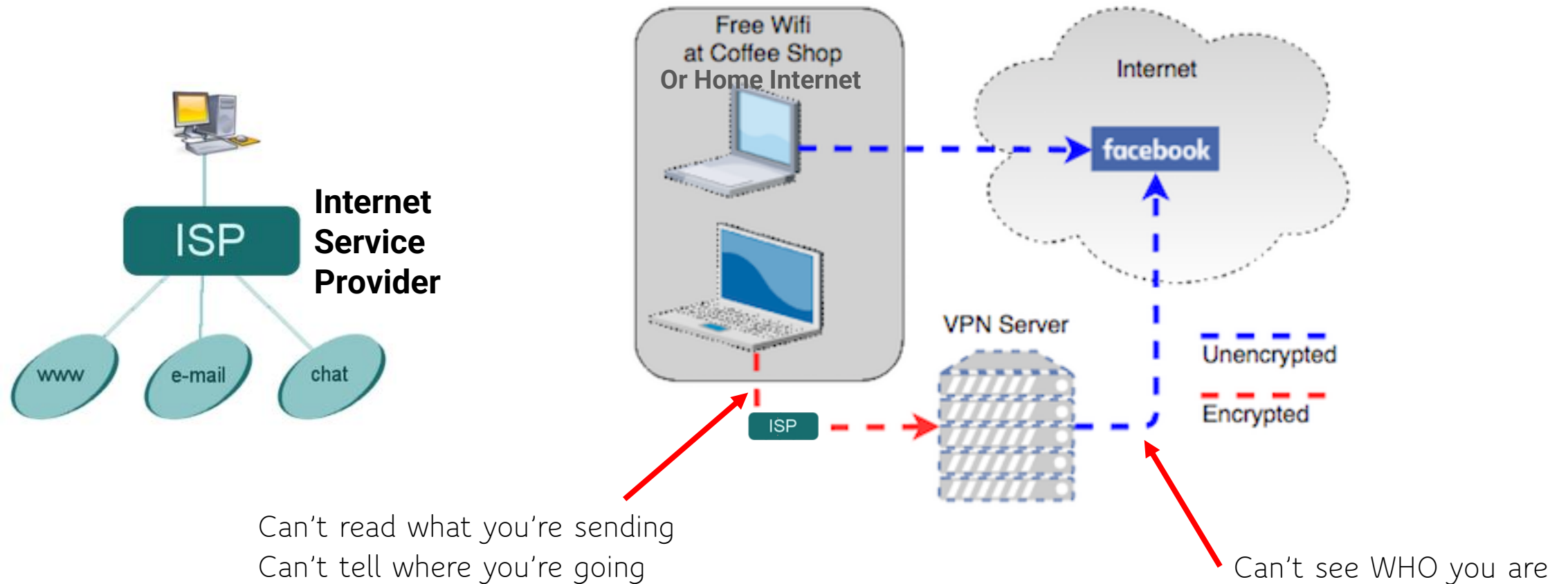
VPN stands for "virtual private network" – a service that **helps you stay private online**. A VPN establishes a secure, encrypted connection between your computer and the internet, providing a private tunnel for your data and communications while you use public networks

## Do I really need a VPN at home?

**Without a VPN, everything you do online can be monitored and tracked by intrusive snoopers like your ISP and other third parties.** Your sensitive information could then be sold to third parties like advertisers, the authorities, and government agencies or even used to initiate malicious actions against you

Keeping your VPN on all the time is not only perfectly safe but actually recommended. It can keep your online identity anonymous, protect you from attacks associated with unsecured public Wi-Fi networks and help you bypass various artificial restrictions.

# VPNs



# Reference Sites Used:

**Ten Sure Fire Signs Your Computer Has A Virus (with detailed explanations)**

---

<https://www.saga.co.uk/magazine/technology/computing/security/10-signs-your-computer-has-a-virus>

## Related Articles

- [Beware bogus calls from computer hackers](#)
- [Keep your computer in top condition](#)
- [7 password mistakes to avoid](#)
- [5 signs your email has been hacked](#)
- [6 things to do if your emails are hacked](#)
- [How to protect your valuable data](#)
- [What are cookies?](#)
- [WiFi explained: what it is and how it works](#)
- [7 password mistakes to avoid](#)
- [6 tips for staying safe on social media](#)

**Android Firewalls** <https://www.techamerica.org/best-firewall-apps-for-android-phone>

**Free VPNs for PCs** <https://us.cybernews.com/lp/free-vpn/pc/>