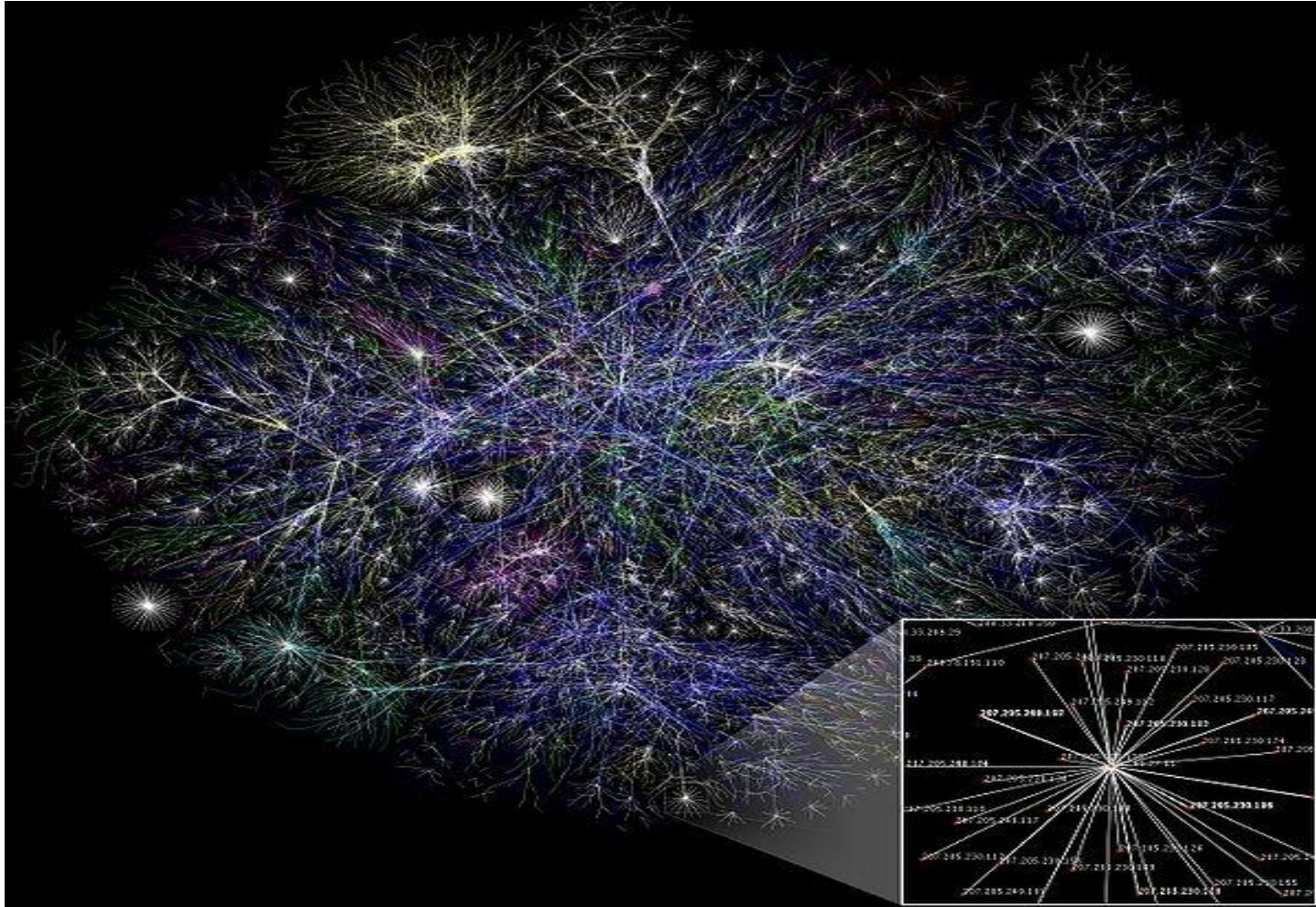


On the Internet What You Don't Know Can Hurt You!

Rick Spillane

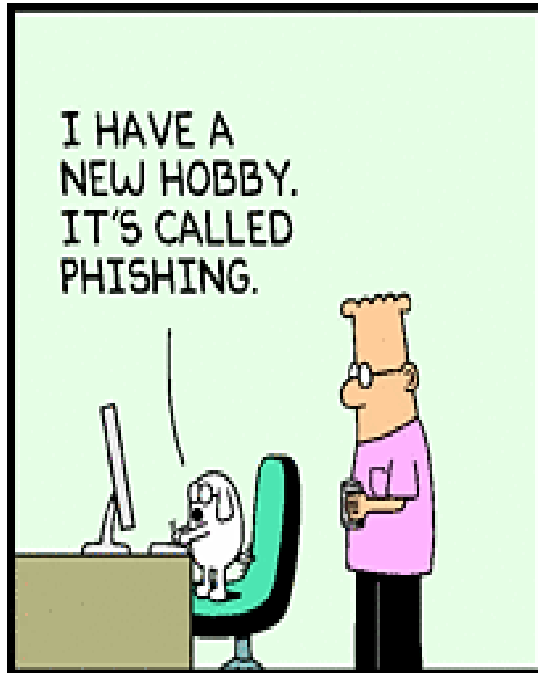
- **Phishing**
- Phishing is a common trick scammers use to "fish" your information using fake emails and websites. The sites ask consumers to enter financial or personal information.
- **SMiShing**
- This is the text messaging (also known as SMS messaging) equivalent to phishing, using text messages to deliver fake website links to your phone.
- **Slamming and Cramming**
- Scammers call and misrepresent themselves and then start asking for account information. They will take that to make unauthorized changes to your phone service.
- **International Area Code Scam**
- In this scam, a message tells you to call a phone number with an 809, 284 or 876 area code. The area code is actually for a number outside the United States, often in Canada or the Caribbean, which charges the customer for placing the call.
- **Email Viruses, Worms and Malware**
- Viruses, worms and malware are computer programs that can be destructive to computers. Bad guys can hide these things in email attachments or web links, activating as soon as the customer opens the file.

Internet

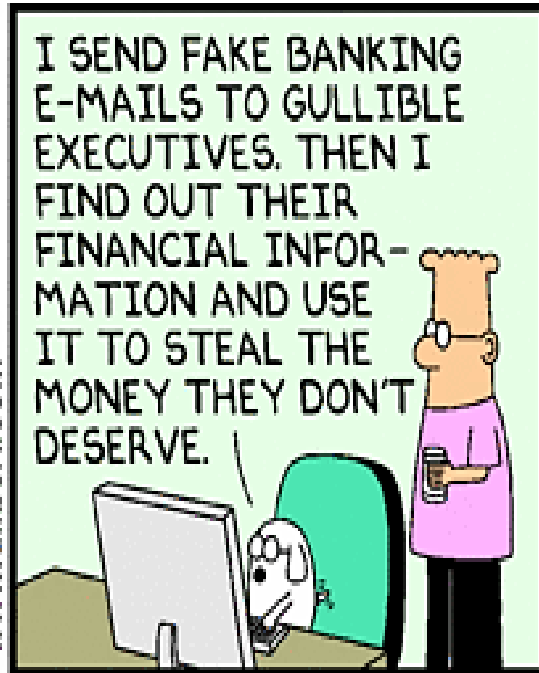


Some things you should know

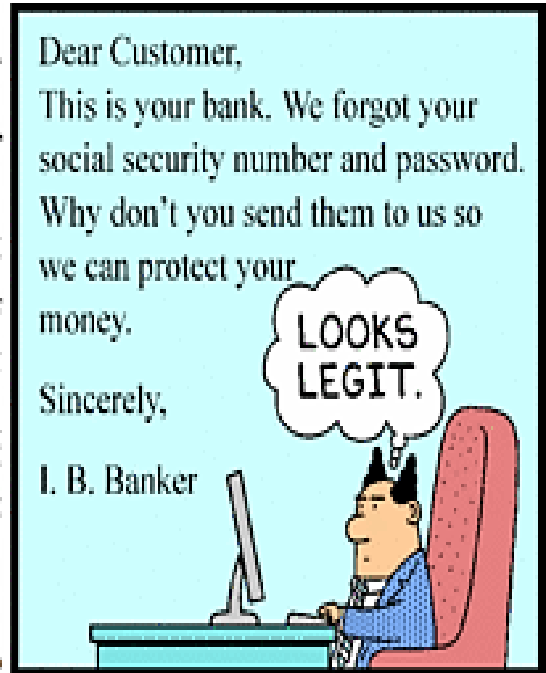
- Who is your internet provider?
 - Is your email and browser from your provider?
 - Consider using Firefox (browser) and Thunderbird (email) from Mozilla as free, more secure alternatives. (addons Adblock, Better Privacy & WOT)
- SPAM is the use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately.
- **Spyware** is a type of malware that is installed on computers and collects little bits of information at a time about users without their knowledge.
- The presence of spyware is typically hidden from the user, and can be difficult to detect. Typically, spyware is secretly installed on the user's personal computer. Sometimes, however, spywares such as **keyloggers** are installed by the owner of a shared, corporate, or public computer on purpose in order to secretly monitor other users.



www.dilbert.com scottadams@aol.com



8-12-05 © 2005 Scott Adams, Inc./Dist. by UFS, Inc.



More things you should know



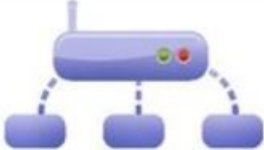



- A **computer virus** is a computer program that can copy itself and infect a computer.
- **Phishing** is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
 - Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.
 - Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
- Zip files – Do not open unless you are sure you know who sent it and why

Router

Nighthawk X6 R8000

BASIC **ADVANCED**

- Home
- Internet
- Wireless
- Attached Devices
- Dynamic QoS
- Parental Controls
- ReadySHARE
- Guest Network
- NETGEAR Downloader

 Internet STATUS: GOOD	 Wireless Name (SSID): StatenIsland Key/Password: SItO NY2LA	 Attached Devices Number of devices : 14 Dynamic QoS : Off
 Parental Controls STATUS: NOT ENABLED	 ReadySHARE STATUS: No USB drive	 Guest Network STATUS: NOT ENABLED

Security Options

Nighthawk X6 R8000

BASIC **ADVANCED**

Home ▶
Internet ▶
Wireless ▶
Attached Devices ▶
Dynamic QoS ▶
Parental Controls ▶
ReadySHARE ▶
Guest Network ▶
NETGEAR Downloader ▶

Wireless Setup

Apply ▶ X Cancel

Region Selection
Region:
North America ▼

Wireless Network (2.4GHz b/g/n)
 Enable SSID Broadcast
Name (SSID): StatenIsland ⓘ
Channel: Auto ▼
Mode: Up to 600 Mbps ▼

Security Options
 None
 WPA2-PSK [AES]
 WPA-PSK [TKIP] + WPA2-PSK [AES]
 WPA/WPA2 Enterprise

TOP SEVEN CYBER-SAFETY ACTIONS



1. Install OS/Software Updates



2. Run Anti-virus Software



3. Prevent Identity Theft



4. Turn on Personal Firewalls



5. Avoid Spyware/Adware



6. Protect Passwords



7. Back up Important Files

What is a VPN?

- All you need in order to do this is a VPN app on your device and an affordable subscription. The best VPNs work across laptops, desktops, smartphones and tablets – even a Smart TV, with the aid of an Ethernet cable or a Chromecast dongle.
- When you want to mask your real location, simply launch the VPN app, select the country from which you want to connect then off you go! After that, simply use your browser and any apps as you would normally do.
- The use of VPNs can be very useful when accessing public Wi-Fi hotspots in hotels, coffee shops or airports to connect to the Internet. All of the data being transferred to and from a laptop, tablet or smartphone (over the Internet) will be encrypted, ensuring high levels of security as well as privacy.

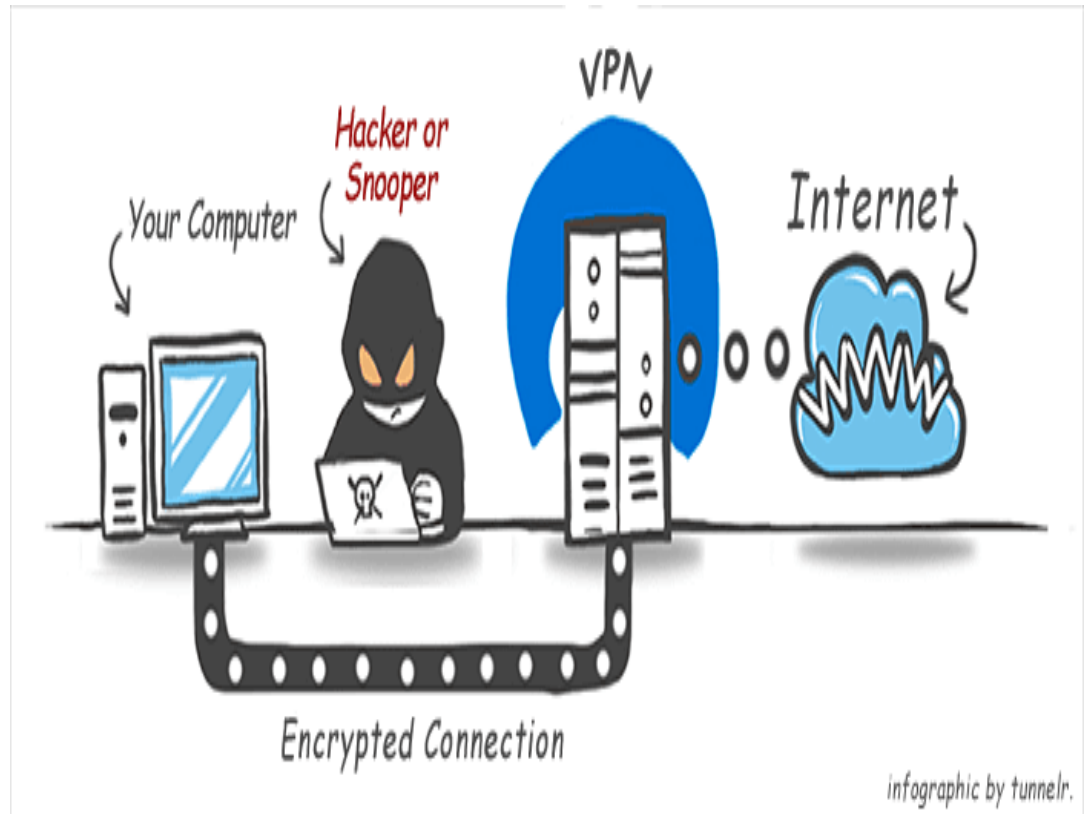
How a VPN Works

Your computer will encrypt all data (requests, upload data) and send to the VPN server through a secure connection.

The VPN server will decrypt the data and send to the Internet.

The VPN server will grab the returned data from the Internet, encrypt all of them and send it back to your computer

Your computer will decrypt the data and display on your browser or whatever program you are using.



VyprDNS™ FAQ

What is VyprDNS

- [VyprDNS](#) is Golden Frog's 100% owned and operated service available exclusively for VyprVPN users. Golden Frog developed their [zero-logging VyprDNS service](#) to increase user privacy and defeat censorship across the world. VyprDNS requires VyprVPN.
- **How does VyprDNS protect from man-in-the-middle attacks?**
- DNS man-in-the-middle attacks can occur when a government or 3rd party redirects you to a different online destination than you were trying to reach. For example, when you try to reach www.facebook.com governments in China, Iran and Turkey could intercept your DNS request and redirect you to an error page. Using VyprVPN with VyprDNS, your data and DNS requests pass through an encrypted tunnel that defeats "man-in-the-middle" DNS attacks and prevents DNS filtering so you can experience an open internet.
- **How does VyprDNS protect from DNS Filtering?**
- Coffee shops, airports and other public WiFi hotspots frequently configure their DNS servers to deny access to specific types of websites. Golden Frog strongly believes in a [free and open internet](#) and their VyprDNS service does not restrict access to websites or hosts.
- **How do I enable VyprDNS?**
- Open settings from within the VyprVPN application, scroll down and select the DNS menu item. You can select VyprDNS or configure a third party DNS from the DNS settings screen.
- **How can I use VyprDNS?**
- When you connect to VyprVPN using a manual connection or through our Android, Mac, or Windows applications with VyprDNS enabled in the settings , your connection will utilize VyprDNS.

How do I connect to a VPN?

- Most of the time, this means using a VPN client (software) that you install on the device(s) you want to connect to the VPN with. The VPN client then will give the option to connect to a range of servers located around the world. The number of locations available will depend on the VPN provider you choose to connect with. By using a VPN, you are in fact setting up a secure connection between your device – a desktop, laptop, tablet or smartphone – and the server, network or other digital device you need to connect to.
- Also worth knowing is that a VPN uses what are called networking protocols. This is the language the VPN uses to encrypt the information you are sending or receiving over the VPN (consult the dedicated protocols answer for more information).
- The type of VPN you use will depend on how you want to connect to the Internet, and how secure you want that connection to be.
- In most cases, you will be able to set up your VPN by downloading the setup software after signing up to a provider and installing it on your device. Most VPNs offer software for all major operating systems.

What are the benefits of using a VPN?

- There are a number of instances where using a VPN would be a major advantage. Companies such as IP Vanish and Hide My Ass offer a range of paid VPN services that offer a number of core benefits including:
 - **1. Access All Websites**
 - A VPN offers universal access to websites and apps that might otherwise be blocked, often due to geo-restrictions. No matter where you are located, a VPN will give you access to a number of servers located around the world, allowing you to access your favorite music and video streaming websites from anywhere in the world.
 - **2. Enhanced Security**
 - A very good reason for using a VPN is the added security that it brings. If you need to send or receive any sensitive information over the Internet, a VPN is vital. Match the level of security you need to the VPN protocol to ensure you're always safe and secure online.
 - **3. Privacy and Anonymity**
 - When total privacy is needed, a VPN is the ideal solution. Unlike proxy services or applications that hide your device's IP address, a VPN offers a greater level of privacy since a secure connection is made between your device and the server or network you are connecting to.

What are the benefits of using a VPN?

- **4. Remote Access**
- One of the major reasons why businesses use VPNs is because it allows their employees secure remote access to their networks and servers. With business often conducted on the move, being able to connect to the office server with a secure line is critical. A VPN delivers that secure connection.
- **5. Reduced Costs**
- Once a VPN is set up the maintenance of the connection is very low. Businesses with large roaming sales personnel for instance, see massive cost savings when a VPN is implemented.
- Moving away from a standard Internet connection with its security issues and fragmented performance is why VPNs are becoming more and more popular.

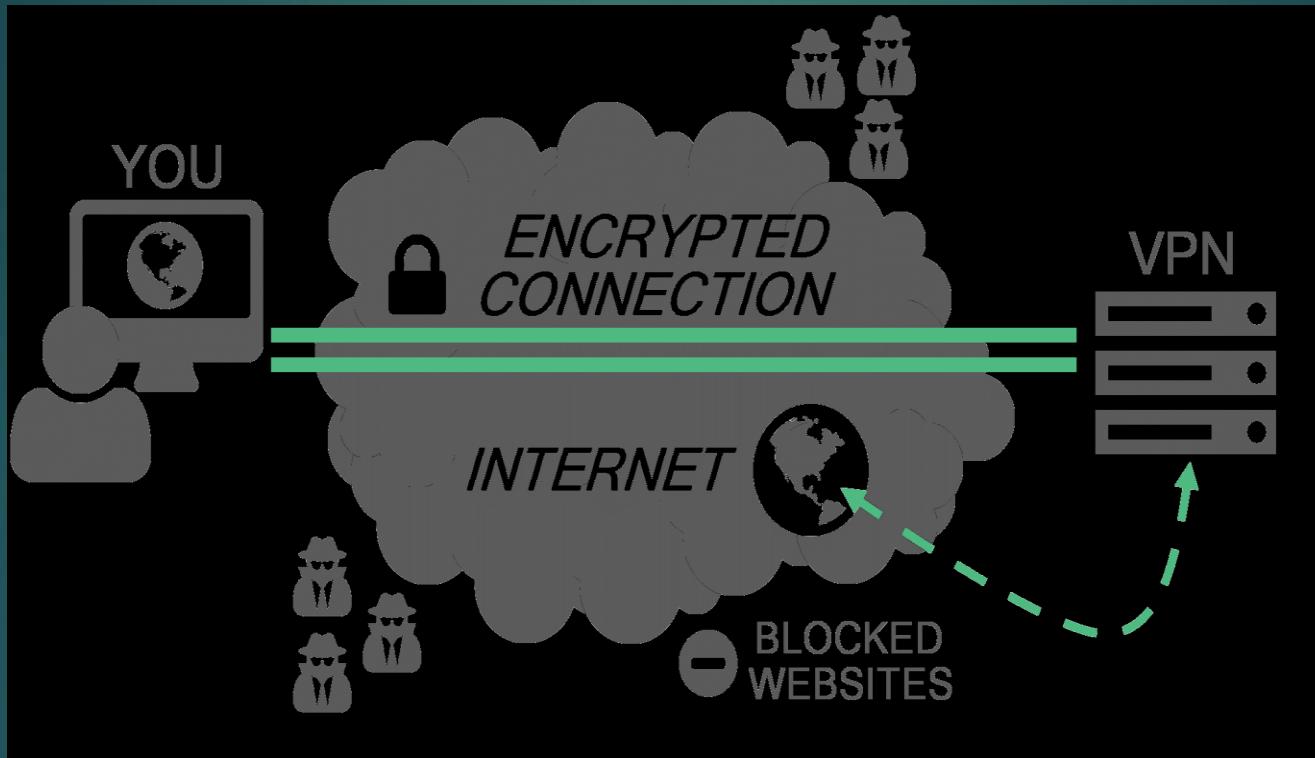
Can I use a VPN on any device or operating system?

- Generally speaking, most VPNs are available on more or less every device you are planning to use but please check that the VPN you are planning to subscribe to covers your operating system. For example, SaferVPN and CyberGhost support all of the leading operating systems.
- The level of security you need will also mean choosing the right VPN protocol. You will see that VPN vendors will have different protocols available for specific operating systems. This is why you should take your time to assess the VPN protocol you want to use and then identify which VPN vendors offer this for the operating system you use.

Benefits of Using a VPN Service

- ▶ A VPN or “virtual private network” is a service that allows Internet users to enjoy increased levels of privacy and security while they go about their business online. These types of connections are very attractive to both home and business users. Business users can access work networks from outside their offices, for example, without needing to worry about information being sent and received over the network getting intercepted. Personal users don't have to worry about private data that could potentially identify information like an address getting into the hands of rogue system administrators while they browse the Web. Virtual private network services have a large number of clear benefits that shouldn't be ignored.











VPN



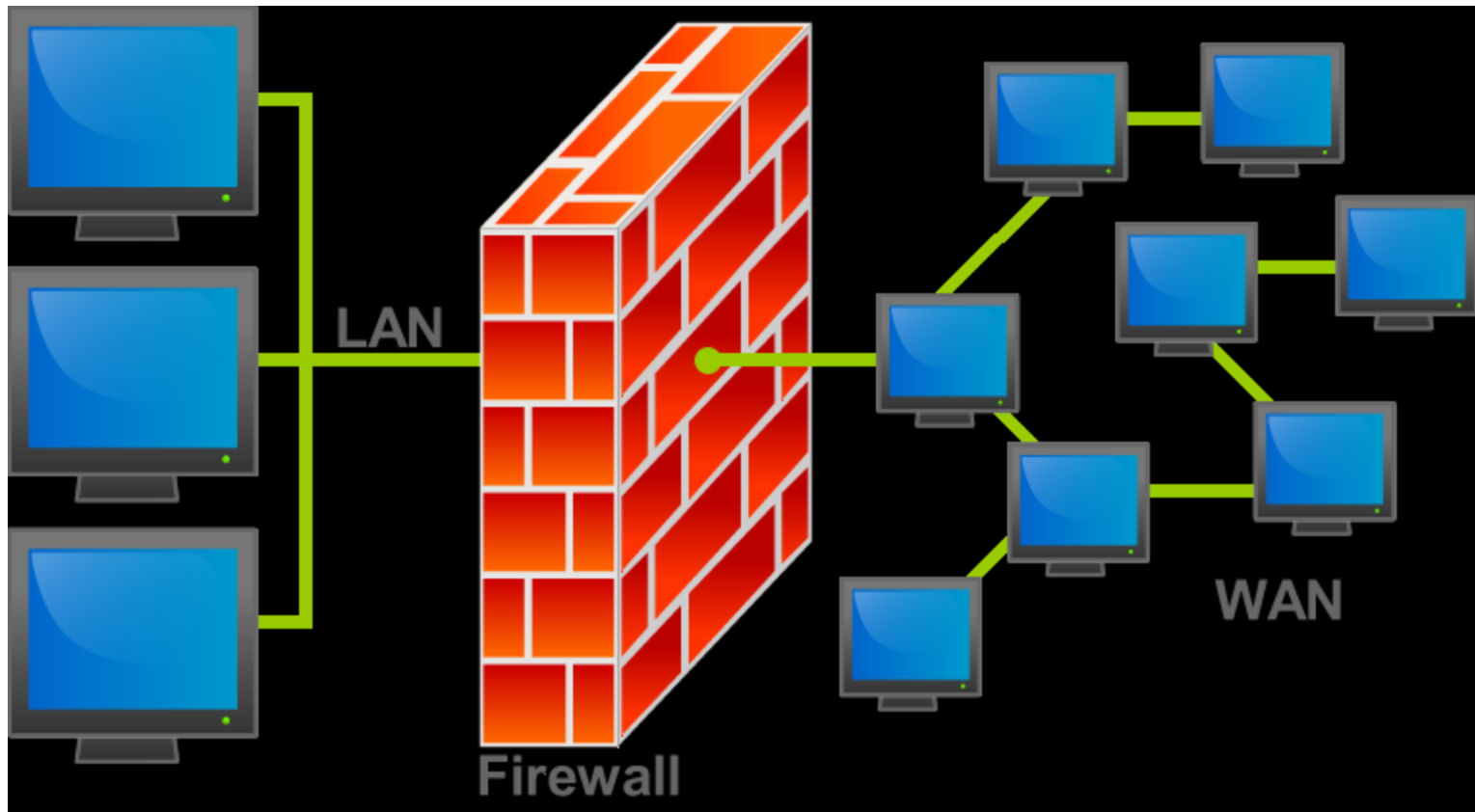
Paid vs Free VPNs

- Paid services therefore have a number of advantages over their free counterparts:
- More robust security
- Multiple VPN protocols to choose from
- Access to a larger pool of servers (and locations)
- Higher bandwidth for fast and efficient connections
- Professional Customer and IT support services, often available 24/7

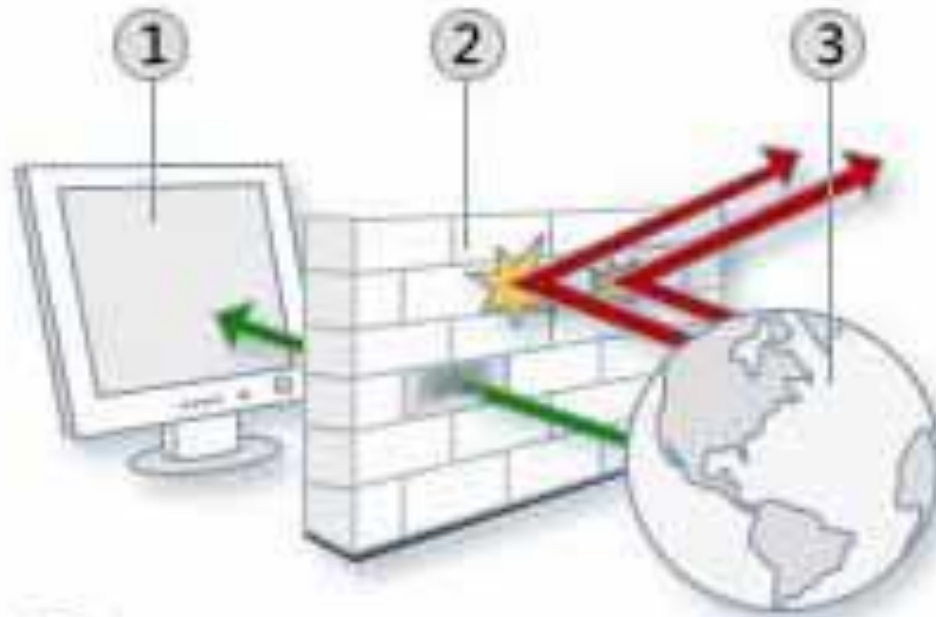
Best VPNs 2017

Name	IPVanish VPN	NordVPN	PureVPN	Private Internet Access VPN	KeepSolid VPN Unlimited	TunnelBear VPN	TorGuard VPN	Golden Frog VyprVPN	AnchorFree Hotspot Shield Elite	Hide My Ass VPN
										
Lowest Price	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT
Editors' Rating	●●●●○	●●●●● EC	●●●●○ EC	●●●●● EC	●●●●● EC	●●●●○	●●●●○	●●●●○	●●●●○	●●●●○
Best For	General Users	General Users	Speed Demons	Power Users	Frequent Travelers	First-Time Users	BitTorrent Users	General Users	Nervous Shoppers	Security Novices
Supported Client Software	Android, ChromeOS, iOS, Linux, macOS, Windows	Android, iOS, macOS, Windows	Android, Chrome, iOS, Linux, macOS, Windows	Android, Chrome, iOS, Linux, macOS, Windows	Android, Chrome, Firefox, iOS, Linux, macOS, Windows	Android, Chrome, iOS, macOS, Opera, Windows	Android, iOS, Linux, macOS, Windows	Android, iOS, macOS, Windows	Android, Chrome, Firefox, iOS, macOS, Windows	Android, iOS, macOS, Windows
Allows 5+ Simultaneous Connections	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
500+ Servers	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Geographically Diverse Servers	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓
P2P or BitTorrent	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
Advanced Features	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Ad-Blocking	✗	✓	✗	✓	✓	✓	✓	✗	✓	✗
Free Version Available	✗	✓	✗	✗	✗	✓	✗	✓	✓	✗
Read Review	IPVanish VPN Review	NordVPN Review	PureVPN Review	Private Internet Access VPN Review	KeepSolid VPN Unlimited Review	TunnelBear VPN Review	TorGuard VPN Review	Golden Frog VyprVPN Review	AnchorFree Hotspot Shield Elite Review	Hide My Ass VPN Review

Protect your system



Firewall



- ① Your computer
- ② Your firewall
- ③ The Internet

2017's Best Antivirus, Malware & Internet Security Software

Ric
2/

Name	McAfee Total Protection (2017)	McAfee LiveSafe (2017)	Symantec Norton Security Premium (2017)	Bitdefender Total Security	Webroot SecureAnywhere Internet Security Complete	Kaspersky Internet Security	Bitdefender Internet Security	Kaspersky Total Security	Symantec Norton Security Deluxe (2017)	Trend Micro Internet Security (2017)
Lowest Price	\$44.99 McAfee	\$44.99 McAfee	\$49.49 Norton - 1 year plan	\$58.49 Bitdefender	\$29.99 Webroot	\$39.99 Kaspersky Lab	\$51.99 Bitdefender	\$49.99 Kaspersky Lab	\$39.99 Norton - 1 year plan	\$49.95 Trend Micro
	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT
Editors' Rating	●●●●○	●●●●○ EC	●●●●○ EC	●●●●○ EC	●●●●○	●●●●○ EC	●●●●○ EC	●●●●○	●●●●○	●●●●○
Firewall	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
Antispam	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
Parental Control	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓
Backup	✓	✗	✓	✗	✓	✗	✗	✓	✗	✗
Tune-Up	✓	✗	✓	✓	✓	✗	✗	✓	✓	✓
Read Review	McAfee Total Protection (2017) Review	McAfee LiveSafe (2017) Review	Symantec Norton Security Premium (2017) Review	Bitdefender Total Security Review	Webroot SecureAnywhere Internet Security Complete Review	Kaspersky Internet Security Review	Bitdefender Internet Security Review	Kaspersky Total Security Review	Symantec Norton Security Deluxe (2017) Review	Trend Micro Internet Security (2017) Review

Firewall

- Is a dedicated appliance, or software running on a computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules/criteria.
- It is normally placed between a protected network and an unprotected network and acts like a gate to protect assets to ensure that nothing private goes out and nothing malicious comes in.
- **Can be software or hardware**
- Wireless modems should have a password enabled setup

What is HTTPS?

- Hyper Text Transfer Protocol Secure (HTTPS) is a secure version of the Hyper Text Transfer Protocol (http). HTTPS allows secure ecommerce transactions, such as online banking.
- Web browsers such as EDGE and Firefox display a padlock icon to indicate that the website is secure, as it also displays https:// in the address bar.



- When a user connects to a website via HTTPS, the website encrypts the session with a digital certificate. A user can tell if they are connected to a secure website if the website URL begins with https:// instead of http://.

<http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx>

- Phishing

Hello!

As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Links in email

Note: If you dont fill the application your account will be permanently blocked.

Threats

Regards,

Facebook Copyrights Department.

Popular company

Ransomware



Ransomware

- Encryption is now used as a weapon,
- holding companies' and individuals'
- critical data hostage

What to Do

Isolate the infected computer.



Do this before the ransomware can attack accessible network drives.

Submit the malware to Security Response.



If you can identify the malicious email or executable, submit it to Symantec Security Response:

[Symantec.com/security_response](https://www.symantec.com/security_response)



Don't pay the ransom.

If you pay the ransom:

- There's no guarantee that the attacker will supply a method to unlock your computer or decrypt your files.
- The attacker will likely use your ransom money to fund attacks against other users.



Restore damaged files from a known good backup.

As with other security products, Symantec Endpoint Protection cannot decrypt the files that ransomlockers have sabotaged.

Free Software

- **Free anti-malware programs**
- These are mostly downloads from such names as Avira and AVG. But there's also a Microsoft Security Essentials anti-malware program that's available as a free download for XP, Vista, and Windows 7 computers.
- **Free security suites**
- These offer not only malware protection but add a firewall and in some cases, other extras such as a child filter.
- But none of the free suites include some other features that are often found on pay suites such as anti-spam protection, built-in backup software, and a browser toolbar that will alert you when you're visiting sites that host malware.

Malware Protection

- **These programs are worth running several times a month.**
- **Ad-Aware** [Lavasoft](#) - 93MB (Non-Commercial Freeware)
 - Ad-Aware gives you comprehensive malware protection. With real-time monitoring, threat alerts, and automatic updates you can rest easy knowing that you are protected.
 - **Shop, bank, and make travel arrangements online** - We keep you safe from password stealers, keyloggers, spyware, trojans, online fraudsters, identity thieves and other potential cyber criminals.
 - **Control your privacy** - Erase tracks left behind while surfing the Web - on browsers such as Internet Explorer, Opera, and Firefox - in one easy click.
- **Spybot Search & Destroy** [PepiMK Software](#) - 16MB (Freeware)
 - Spybot - Search & Destroy detects and removes spyware, a relatively new kind of threat not yet covered by common anti-virus applications. Spyware silently tracks your surfing behaviour to create a marketing profile for you that is transmitted without your knowledge to the compilers and sold to advertising companies.

Free protective software

- **Windows Defender** Microsoft Windows Defender 4.9 is awfully convenient. It's already installed on your Windows 8 or Windows 10 system; all you do is make sure it's turned on. Sometimes, though, you get what you pay for. Microsoft's scores with independent antivirus testing labs are improving, but they're still not tip-top. And in my own hands-on tests it proved mediocre at best.
- We've identified three Editors' Choice products for free antivirus, Avast Free Antivirus, AVG AntiVirus Free, and Panda Free Antivirus. Best of all, since they're free you can try all three and decide which one suits you best.
- **FileHippo** is an internet download website. It offers freeware as well as shareware programs, but does not accept user uploaded files.
- It also offers the FileHippo Update Checker, a small program that scans your computer for installed software from the FileHippo site and suggests available updates for it. According to Quantcast, it receives more than three million US visitors each month and as of March 2010, Alexa lists filehippo in the top 1000 most visited websites.
- Free at Filehippo.com <http://www.filehippo.com/>

Pay security suites

- Such suites, from brands that include Kaspersky, Symantec and McAfee, promise comprehensive protection in one package.
 - They offer not only malware protection but also a firewall, an anti-spam filter, and other extras. The latter usually include a child filter, often include a browser toolbar that will alert you when you're visiting sites that host malware, and sometimes include a file shredder and file backup software.
- You typically buy the program online, either by downloading it or upgrading from a free trial version carried on your PC.
 - You can use a suite on as many as three computers in the same household. Prices typically range from \$40 to \$80, and include a first year of service. After that, you'll typically pay another \$40 to \$80 per year to renew service.

Additional Software

- **Spam filters**
- These offer supplemental protection that you may want because your e-mail program isn't adequately filtering out unwanted messages. Often built into pay suites, free options include SPAMfighter at spamfighter.com.
- **Anti-phishing toolbars**
- Free security toolbars available for all major browsers provide extra protection against phishing sites, especially if you're using an older browser version or just want extra protection.
- **File shredders**
- Deleting a file from your hard drive does not remove all electronic traces of it--which can allow someone who accesses or inherits your computer to recover some or all of the file's data. To eliminate that possibility, you need file-shredding software.

7 Online Blunders

1. Assuming your security software is protecting you
 1. Security software is fully effective only when activated and frequently updated.
2. Accessing an account through an e-mail link
 1. If an e-mail message asks you to update your password, account number, or other information, don't take the bait.
 2. Access an online account only by using your existing browser bookmark or typing in the institution's Web address.
 3. If you suspect that an e-mail is a phishing attempt, forward it to *spam@uce.gov* and *reportphishing@antiphishing.org*.
3. Using a single password for all online accounts
 1. Nine percent of home Internet users who responded to Consumer Reports' State of the Net survey said they used a single password for all their accounts.
4. Downloading free software

(6) Clicking on a pop-up ad that says your PC is insecure



(7) Shopping Online the Same Way You Do In Stores

- Online shopping requires special precautions because the risks are different than in a walk-in store:
 - You can't always be sure who you're doing business with.
 - You must disclose more personal information, such as your address, to the online retailer.
 - Thieves can sneak in undetected between you and the retail site.