If you don't use it already, I suggest downloading and using Firefox as your web browser. There are some very good security add-ons available for it.

Firefox: http://www.firefox.com/

NoScript add-on - probably the most important add-on you should consider. NS blocks all scripts and active content from running (a very common source of infection) and gives YOU control over which scripts YOU want to allow.

https://addons.mozilla.org/en-US/firefox/addon/noscript/

Adblock Plus add-on - blocks ads and pop-ups - another common source of infection.

https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/

Web of Trust add-on - helps warn you against malicious web sites.

https://addons.mozilla.org/en-US/firefox/addon/wot-safe-browsing-tool/

Spybot: http://www.safer-networking.org/

Many downloaded programs include software that you may not want. Be careful to choose “custom install” (instead of “recommended or typical install) when installing software.

This type of software is known as “Trojan software” or “Trojan virus”.

The Trojan Horse is a tale from the Trojan War about the subterfuge that the Greeks used to enter the city of Troy and win the conflict. In the canonical version, after a fruitless 10-year siege, the Greeks constructed a huge wooden horse, and hid a select force of men inside. The Greeks pretended to sail away, and the Trojans pulled the horse into their city as a victory trophy. That night the Greek force crept out of the horse and opened the gates for the rest of the Greek army, which had sailed back under cover of night. The Greeks entered and destroyed the city of Troy, decisively ending the war.

Be Careful when using hotspots (Starbucks) or stealing neighbor’s wifi!

**Banking on one browser/one tab**

Don't have several tabs or several browsers open when doing online banking

Beware: Don’t download music, movies, coupons, pc cleaner, optimizer, registry cleaner from sites that offer free downloads. Torrenting, P2P file sharing, downloading random free games and programs, and opening email attachments from people you don't know are all great ways to get infected.

**Layout in email program...change to No Preview.**

If your email program is set to preview emails, it is essentially opening each email, which is a safety risk.

Tips for Wireless Network Management

Wireless networks can provide an unintended open door to your business network. Unless a valid business reason exists for wireless network use, it is recommended that all wireless networks be disabled. If a wireless network is to be used for legitimate business purposes, it is recommended that wireless networks be secured as follows:

Change the wireless network hardware (router /access point) administrative password from the factory default to a complex password. Save the password in a secure location as it will be needed to make future changes to the device.

Disable remote administration of the wireless network hardware (router / access point).

If possible, disable broadcasting the network SSID.

If your device offers WPA encryption, secure your wireless network by enabling WPA encryption of the wireless network. If your device does not support WPA encryption, enable WEP encryption.

If only known computers will access the wireless network, consider enabling MAC filtering on the network hardware. Every computer network card is assigned a unique MAC address. MAC filtering will only allow computers with permitted MAC addresses access to the wireless network.

**Norton AV:**

Highlights from the 2014 Internet Security Threat Report:

91% increase in targeted attacks campaigns in 2013

62% increase in the number of breaches in 2013

Over 552M identities were exposed via breaches in 2013

23 zero-day vulnerabilities discovered

38% of mobile users have experienced mobile cybercrime in past 12 months

Spam volume dropped to 66% of all email traffic

1 in 392 emails contain a phishing attacks

Web-based attacks are up 23%

1 in 8 legitimate websites have a critical vulnerability

Religious websites might now actually be more of a threat to believers than pornographic pages.

Well, at least for their computers.

Internet surfers viewing websites with religious content are more likely to receive a virus from a religious page than they would from looking at a site with pornographic material, according to a recent study by U.S.-based anti-virus vendor Symantec.

The company reported that hackers perform "drive-by attacks" on religious websites where they booby-trap them with malicious code.

These faith-based sites were found to have triple the average number of "threats" than those with pornographic content, according to Symantec's data.

"It is interesting to note that websites hosting adult/pornographic content are not in the top five, but ranked tenth," said the company the report.

"We hypothesize that this is because pornographic website owners already make money from the Internet and, as a result, have a vested interest in keeping their sites malware-free; it's not good for repeat business," Symantec added.

The report was based on data collected last year by the Symantec Global Intelligence Network, which monitors the activity of hackers in over 200 countries worldwide.

The company stated that it blocked 5.5 billion cyber attacks in 2011. This showed an 81 percent increase from the previous year.

Symantec also reported that the attacks on other internet ready devices such as smartphones and tablet computers have increased. The company also has seen a surge in attacks towards companies and government agencies

**7 Practices for Computer Security**

1 Protect your personal information. It’s valuable.

2 Know who you’re dealing with.

3 Use security software that updates automatically.

4 Keep your operating system and Web browser up-to-date, and learn about their security features.

5 Keep your passwords safe, secure, and strong.

6 Back up important files.

7 Learn what to do in an e-mergency.

**1. Protect your personal information. It’s valuable.**

To an identity thief, your personal information can provide instant access to your financial accounts, your credit record, and other assets. If you think no one would be interested in YOUR personal information, think again. ANYONE can be a victim of identity theft. In fact, according to the Federal Trade Commission, millions of people become victims every year. Visit ftc.gov/idtheft to learn what to do if your identity is stolen or your personal or financial information has been compromised – online or in the “real” world.

How do criminals get your personal information online? One way is by lying about who they are, to convince you to share your account numbers, passwords, and other information so they can get your money or buy things in your name. The scam is called “phishing”: criminals send email, text, or pop-up messages that appear to come from your bank, a government agency, an online seller or another organization with which you do business. The message asks you to click to a website or call a phone number to update your account information or claim a prize or benefit. It might suggest something bad will happen if you don’t respond quickly with your personal information. In reality, legitimate businesses should never use email, pop-ups, or text messages to ask for your personal information.

To avoid phishing scams:

Don’t reply to an email, text, or pop-up message that asks for personal or financial information, and don’t click on links in the message. If you want to go to a bank or business’s website, type the web address into your browser yourself.

Don’t respond if you get a message – by email, text, pop-up or phone – that asks you to call a phone number to update your account or give your personal information to access a refund. If you need to reach an organization with which you do business, call the number on your financial statement, or use a telephone directory

Some identity thieves have stolen personal information from many people at once, by hacking into large databases managed by businesses or government agencies. While you can’t enjoy the benefits of the internet without sharing some personal information, you can take steps to share only with organizations you know and trust. Don’t give out your personal information unless you first find out how it’s going to be used and how it will be protected.

If you are shopping online, don’t provide your personal or financial information through a company’s website until you have checked for indicators that the site is secure, like a lock icon on the browser’s status bar or a website URL that begins “https:” (the “s” stands for “secure”). Unfortunately, no indicator is foolproof; some scammers have forged security icons. And some hackers have managed to breach sites that took appropriate security precautions.

Read website privacy policies. They should explain what personal information the website collects, how the information is used, and whether it is provided to third parties. The privacy policy also should tell you whether you have the right to see what information the website has about you and what security Measures the company takes to protect your information. If you don’t see a privacy policy — or if you can’t understand it — consider doing business elsewhere.

**2. Know who you’re dealing with.**

And what you’re getting into. There are dishonest people in the bricks and mortar world and on the internet. But online, you can’t judge an operator’s trustworthiness with a gut-affirming look in the eye. It’s remarkably simple for online scammers to impersonate a legitimate business, so you need to know who you’re dealing with. If you’re thinking about shopping on a site with which you’re not familiar, do some independent research before you buy.

If it’s your first time on an unfamiliar site, call the seller’s phone number, so you know you can reach them if you need to. If you can’t find a working phone number, take your business elsewhere.

Type the site’s name into a search engine: If you find unfavorable reviews posted, you may be better off doing business with a different seller.

Consider using a software toolbar that rates websites and warns you if a site has gotten unfavorable reports from experts and other internet users. Some reputable companies provide free tools that may alert you if a website is a known phishing site or is used to distribute spyware.

File-Sharing: Worth the hidden costs?

Every day, millions of computer users share files online. File-sharing can give people access to a wealth of information, including music, games, and software. How does it work? You download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. Often, the software is free and easy to access.

But file-sharing can have a number of risks. If you don’t check the proper settings, you could allow access not only to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents. In addition, you may unwittingly download malware or pornography labeled as something else. Or you may download material that is protected by the copyright laws, which would mean you could be breaking the law.

If you decide to use file-sharing software, be sure to read the End User Licensing Agreement to be sure you understand and are willing to tolerate the potential risks of free downloads.

**3. Use security software that updates automatically.**

Keep your security software active and current: at a minimum, your computer should have anti-virus and anti-spyware software, and a firewall. You can buy stand-alone programs for each element or a security suite that includes these programs from a variety of sources, including commercial vendors or from your Internet Service Provider. Security software that comes pre-installed on a computer generally works for a short time unless you pay a subscription fee to keep it in effect. In any case, security software protects against the newest threats only if it is up-to-date. That’s why it is critical to set your security software to update automatically.

Some scam artists distribute malware disguised as anti-spyware software. Resist buying software in response to unexpected pop-up messages or emails, especially ads that claim to have scanned your computer and detected malware. That’s a tactic scammers have used to spread malware. OnGuardOnline.gov can connect you to a list of security tools from legitimate security vendors selected by GetNetWise, a project of the Internet Education Foundation.

Once you confirm that your security software is up-to-date, run it to scan your computer for viruses and spyware. If the program identifies a file as a problem, delete it.

AntiVirus Software

Antivirus software protects your computer from viruses that can destroy your data, slow your computer’s performance, cause a crash, or even allow spammers to send email through your account. It works by scanning your computer and your incoming email for viruses, and then deleting them.

Anti-Spyware Software

Installed on your computer without your consent, spyware software monitors or controls your computer use. It may be used to send you pop-up ads, redirect your computer to websites, monitor your internet surfing, or record your keystrokes, which, in turn, could lead to the theft of your personal information.

A computer may be infected with spyware if it:

Slows down, malfunctions, or displays repeated error messages

Won’t shut down or restart

Serves up a lot of pop-up ads, or displays them when you’re not surfing the web

Displays web pages or programs you didn’t intend to use, or sends emails you didn’t write.

Firewalls

A firewall helps keep hackers from using your computer to send out your personal information without your permission. While anti-virus software scans incoming email and files, a firewall is like a guard, watching for outside attempts to access your system and blocking communications to and from sources you don’t permit.

Don’t Let Your Computer Become Part of a “BotNet”

Some spammers search the internet for unprotected computers they can control and use anonymously to send spam, turning them into a robot network, known as a “botnet.” Also known as a “zombie army,” a botnet is made up of many thousands of home computers sending emails by the millions. Most spam is sent remotely this way; millions of home computers are part of botnets.

Spammers scan the internet to find computers that aren’t protected by security software, and then install bad software – known as “malware” – through those “open doors.” That’s one reason why up-to-date security software is critical.

Malware may be hidden in free software applications. It can be appealing to download free software like games, file-sharing programs, customized toolbars, and the like. But sometimes just visiting a website or downloading files may cause a “drive-by download,” which could turn your computer into a “bot.”

Another way spammers take over your computer is by sending you an email with attachments, links or images which, if you click on or open them, install hidden software. Be cautious about opening any attachments or downloading files from emails you receive. Don’t open an email attachment — even if it looks like it’s from a friend or coworker — unless you are expecting it or know what it contains. If you send an email with an attached file, include a text message explaining what it is.

**4. Keep your operating system and Web browser up-to-date, and learn about their security features.**

Hackers also take advantage of Web browsers (like Firefox or Internet Explorer) and operating system software (like Windows or Mac’s OS) that don’t have the latest security updates. Operating system companies issue security patches for flaws that they find in their systems, so it’s important to set your operating system and Web browser software to download and install security patches automatically.

In addition, you can increase your online security by changing the built-in security and privacy settings in your operating system or browser. Check the “Tools” or “Options” menus to learn how to upgrade from the default settings. Use your “Help” function for more information about your choices.

If you’re not using your computer for an extended period, disconnect it from the internet. When it’s disconnected, the computer doesn’t send or receive information from the internet and isn’t vulnerable to hackers.

**5. Protect your passwords.**

Keep your passwords in a secure place, and out of plain sight. Don’t share them on the internet, over email, or on the phone. Your Internet Service Provider (ISP) should never ask for your password.

In addition, hackers may try to figure out your passwords to gain access to your computer. To make it tougher for them:

Use passwords that have at least eight characters and include numbers or symbols. The longer the password, the tougher it is to crack. A 12-character password is stronger than one with eight characters.

Avoid common words: some hackers use programs that can try every word in the dictionary.

Don’t use your personal information, your login name, or adjacent keys on the keyboard as passwords.

Change your passwords regularly (at a minimum, every 90 days).

Don’t use the same password for each online account you access.

**6. Back up important files.**

If you follow these tips, you’re more likely to be free of interference from hackers, viruses, and spammers. But no system is completely secure. If you have important files stored on your computer, copy them onto a removable disk or an external hard drive, and store it in a safe place.

**7. Learn what to do in an e-mergency.**

If you suspect malware is lurking on your computer, stop shopping, banking, and other online activities that involve user names, passwords, or other sensitive information. Malware could be sending your personal information to identity thieves.

Confirm that your security software is up-to-date, then use it to scan your computer. Delete everything the program identifies as a problem. You may have to restart your computer for the changes to take effect.

If the problem persists after you exhaust your ability to diagnose and treat it, you might want to call for professional help. If your computer is covered by a warranty that offers free tech support, contact the manufacturer. Before you call, write down the model and serial number of your computer, the name of any software you’ve installed, and a short description of the problem. Your notes will help you give an accurate description to the technician.

If you need professional help, if your machine isn’t covered by a warranty, or if your security software isn’t doing the job properly, you may need to pay for technical support. Many companies — including some affiliated with retail stores — offer tech support via the phone, online, at their store, or in your home. Telephone or online help generally are the least expensive ways to access support services — especially if there’s a toll-free helpline — but you may have to do some of the work yourself. Taking your computer to a store usually is less expensive than hiring a technician or repair person to come into your home.

Once your computer is back up and running, think about how malware could have been downloaded to your machine, and what you could do to avoid it in the future.

Also, talk about safe computing with anyone else who uses the computer. Tell them that some online activity can put a computer at risk, and share the seven practices for safer computing.

**Tips for Parents**

Parents sometimes can feel outpaced by their technologically savvy kids. Technology aside, there are lessons that parents can teach to help kids stay safer as they socialize online. Most ISPs provide parental controls, or you can buy separate software. But no software can substitute for parental supervision. Talk to your kids about safe computing practices, as well as the things they’re seeing and doing online. Read more about chatting with kids about being online.

**Myths and Misconceptions:**

1. If your computer starts popping up errors, you’ve got a virus!

There are a lot of working components to make your computer operate. And any one of these can get corrupted in a number of ways without the help of a virus. As a matter of fact, it’s even possible that your antivirus itself may be causing the conflict that’s causing the error. However, don’t take it lightly. If you’re not really savvy in the ways of geek-ery, trust your local IT guy to have a look.

2. I don’t have to worry about viruses. I have a Mac.

This one just makes my head hurt to even type. Macs have gotten the reputation for being virus-proof, but nothing could be further from the truth. Due to their relatively low install base, it’s true that they are safer than PCs – but that will change as Macs become more popular, making them more of a target base. More and more Mac users are falling victim to malware, and Apple has humbly recanted their boast of the virus-proof computer. Of course, nothing is user-proof… Many a Mac has been infected by illegal downloads.

3. You won’t get infected if you keep Antivirus on your computer.

Unfortunately, we have to admit that not only is it untrue, your anti-virus itself may be infecting your computer! First of all, you have to understand how antivirus works. Antivirus uses signature files of known viruses to be able to identify one coming in. When it sees one it can identify, it puts it into quarantine until you can check it out. And it has to do regular updates to keep up-to-date on the latest viruses to guard against.

Of course, an antivirus can guard against potential unknown viruses, too, by watching for typical “virus” behavior, like things targeting EXE files. However, a virus that’s not quite so typically aggressive can go unnoticed, and just like that, your computer’s infected.

And of course, there are also those lovely viruses that disable your antivirus without your knowledge.

Then, there’s the Antivirus Virus. As you’re surfing along on the Internet, admiring all the cute kittie videos, a warning box comes up of a virus of your computer and asks if you want to remove it. You choose to kill said threat (as any good web citizen would)…. Congratulations. Your computer is now infected. And that “anti-virus” that’s on your computer is actually the virus itself.

4. I don’t have antivirus on my computer, and I’ve never had a virus.

I wouldn’t wager money on that, my friend. Most viruses are actually made to go undetected for quite a long time. Ransomware often does nothing to damage your computer – it’s only purpose is to take important personal files with the intention of requiring you to pay money to get them back. Spyware, on the other hand, sits quietly in the background while you surf the Internet – inserting advertisements that actually shouldn’t be there, or worse … gathering those usernames, passwords, and credit card numbers you use.

And then you have the really fun viruses that lay low until they’re set to detonate.

5. Porn sites are the most likely place to get a virus.

The world is full of cruel irony, and this would be no exception. Last year, when Symantec did it’s annual Internet Security Threat Report , they caused quite a stir. After doing their year’s worth of research on trends in Internet threats, they released their 10 Most Dangerous Website Categories. And Pornography was at the bottom of the list at number 10!

Truth of the matter is, you’re actually more likely to get a virus from an average church website than a pornography website, and the reason is simple. Money.

The adult-themed industry has the financial backing to take the proper security measures when it comes to their websites – website updates, brute force counters in place, etc.

However, a religious, ideological, non-profit, or personal website may not have the funds or the know-how to keep up such practices – leaving them far more likely to pass malware to their visitors.

**So, lesson is:**

1. Get a good, solid antivirus from a respectable source. (Good rule of thumb – check a friendly geek’s computer to see what’s on his! Hey – I’ll even let you see what’s on mine…)

2. Keep that antivirus running updates constantly so it can trap the new stuff that’s going around.

3. If you’re on the Internet, you’re at risk. Period. No matter what brand you use, what site you’re on, or even if you already have AV.

**Myth 1: Firewalls Protect You From Viruses**

It's surprising how many people don't realize this, but your firewall is not going to protect you from a virus, trojan, or spyware—in fact, the only type of malware that you'll definitely be helping prevent is a worm, because they travel over the network. And sure, theoretically an outbound firewall will alert you when a malware application is sending data back, but that's a false sense of security, since once you are infected, a clever virus can simply disable the firewall.

Don't misunderstand, we aren't recommending that you go and disable your firewall—in fact you should keep it enabled at all times, especially when you're on an insecure network like a coffee shop. If you aren't sure what firewall to choose, we recommend you don't pay for Windows security and use the built-in one, but you can also check out our list of the best Windows firewalls.

When it comes to keeping your Windows PC secure, all of the scare tactics and overblown virus…

**Myth 2: Viruses Can Physically Damage Your Hardware**

Sure, a virus like CIH can infect your firmware or BIOS, but the hardware itself is unaffected. Rumors of viruses causing your PC to go crazy and explode are unfounded and a little ridiculous. If your computer ends up infected by one of these more dangerous BIOS-level viruses, you'll probably have to take the computer to somebody that can wipe the BIOS manually, or replace it, but software viruses aren't going to murder your hardware.

**Myth 3: My Computer Is Throwing a Lot of Errors, So It Must Have a Virus**

Files can get corrupted on their own, without the involvement of any viruses—whether it's through a bug in the software, a bad sector on your hard drive, faulty memory, or ironically, a conflict with your antivirus software. So the next time you get a warning about being unable to open a file, scan it with your antivirus software before you accuse your computer of having a virus.

**Myth 4: I Can Just Reinstall Windows and Copy Everything Back**

I can't count the number of times I've seen somebody reinstall Windows on their PC after a virus infection, only to copy their files from a backup drive and then re-infect themselves all over again. You need to make sure that your documents and data have been scanned for and are free from viruses, especially after an infection.

To help prevent these problems in the first place, make sure that you've got an antivirus package installed and real-time protection enabled. If you aren't sure which one to choose, we recommend the free Microsoft Security Essentials, but if you want to shop around, take a look at one of these five popular antivirus applications.

Computer viruses are increasingly sophisticated and pervasive. If you can't afford to run your

**Myth 5: I Can Always Trust My Antivirus Application to Steer Me in the Right Direction**

More often than you'd think, your antivirus software is just plain wrong, and especially when you're using a scanner that employs heuristic scanning to check if a file might have a virus. Do you remember the recent McAfee fiasco? Be sure to check out our guide to understanding if your download really has a virus.

McAfee corporate customers across the globe using Windows XP experienced massive shutdowns today as …

How Do You Know If Your Download Really Has a Virus?How Do You Know If Your Download Really Has a Virus?Antivirus and anti-malware apps fill an important need on our computers, but they're not…

**Myth 6: The Blue Screen of Death Means I've Got a Virus, Right?**

While some viruses can certainly cause an appearance by the feared blue screen of death, the majority of the time a BSOD is caused by bad drivers or faulty hardware. It's very rarely a virus, and assuming that it is will increase your troubleshooting time.

Your best bet when dealing with the blue screen of death is to disable the automatic reboot so you have time to write down the error message. Once you've done so, chances are good that Google will help you out with an answer to what it could be. If your system is stable enough to actually use, you can also use the free, portable system utility BlueScreenView to help troubleshoot previous BSOD errors.

Windows only: Free, portable system utility BlueScreenView displays your last Blue Screen of Death, …

**Myth 7: Windows Is the Only Platform with Malware**

While it's true that almost all viruses are targeted at Windows, it doesn't mean that Windows is the only platform with malware issues. There's been a recent increase in trojans targeting Macs, usually through pirated software cracks (same as Windows), and the trend will probably continue as Macs become more popular. And since trojans exploit human error rather than a security hole, all platforms are susceptible to them.

If you're using a Linux or Mac computer, you can protect yourself by following many of the same rules that you would for Windows: Don't install software from places you don't know, be wary anytime a piece of software asks you for your password, and avoid installing "codecs" from porn sites. Some simple common sense will keep you from being the victim of a malware attack.

**Myth 8: This Damn Virus Went Browsing for Porn—It Wasn't Me!**

I always get a good laugh when somebody brings a PC over to me and tells me that it's infected with viruses—and then they proceed to tell me that those darn viruses opened up all these sleazy porn sites, and they have no idea how it happened. If you've spent any time in the tech help world, you've probably heard the same thing before.

Sure, you might accidentally see a porn ad popup if you don't have a popup blocker in your browser and you're already browsing sleazy sites, but viruses don't browse through porn sites, people do. It's usually at this stage that I point out that just like the people on the screen, anything downloaded from a porn site is much more likely to contain a virus.

**Myth 9: Viruses Can Infect Humans, or Alien Spacecrafts**

Yeah, so this one is a little ridiculous, but there are just too many movies and TV shows that have a plot dependent on the idea of humans infecting an alien spacecraft with a virus that spreads from one ship to another, until it finally infects the mothership and kills them all. I mean, really? Is that the best plot they can come up with? We can barely even share files between Macs and PCs without problems, much less infect a human being or an alien spacecraft with a virus. To quote Southpark's Chef: "That doesn't make any goddamned sense!"