

Whether you've just picked your computer up after a virus cleaning, or you just want to avoid catching an infection entirely, the best way to keep infections away from your computer is to be proactive and follow a few simple steps.

Why Do People Make Infections?

Today, infections are all about making money. In the worst cases, these rogue programs can monitor your online activity to target you for advertising or to trick you into giving them your credit card numbers, bank account numbers, or other personal information. Think of it this way: if one million people get an infection that asks for money and only 1% of victims pay for it, that gives the virus creators \$800,000 for very little work! On top of that, you have just handed a stranger your credit card number and all relevant information for them to commit credit card fraud or identity theft.

Keep Your Anti-Virus / Anti-Malware program Up to Date and use them

Keeping your anti-Virus & Anti-Malware program up to date is critical. Any program is only as good as its latest update from the manufacturer. At this time, we recommend "[Microsoft Security Essentials](#)", "*Windows Defender (built into Windows 8 & 10)*" or "[Avast](#)" for Free Anti-Virus Programs and "[MalwareBytes](#)" for spyware detection & removal. You can also buy [Malwarebytes Pro](#) for automated protection (\$29.95). If you're having your computer serviced with us, we may have already installed one or more of these programs for you. (All are free programs at this time but keep in mind; we are not able to guarantee that you will not get a virus while using these programs). It is **not** necessary to run a daily scan. Important note: You can only have one Anti-Virus on your PC at a time. If you would like to purchase an Anti-Virus program, we like [Eset Nod32](#).

Be Very Careful When Clicking on Links

You want to be particularly careful about emails sent to you from Facebook, Twitter, Etc. They trick you by making it look like someone you know is sending you a message to "Watch this funny video!" When you click the link, it takes you to a website that asks you to download something, (Like a video player) but what you're downloading is actually an infection. Another example: Emails from UPS saying they have a tracking number for you.

Also, when searching using Google, Yahoo, or any other search website, don't assume that the top results in any search engine are safe. Many companies pay top dollar to be on top of search results, they're hoping you call them for help...they login to your computer, plant a virus and then ask for money to remove it. In other words... don't use the search bar looking for "Microsoft" It is best to go to the manufacturer's website directly using your address bar: Example: www.microsoft.com. Also remember that not all websites are designed to infect you intentionally; sometimes, websites are hacked without their knowledge and used to spread the hacker's infection.

Stay Away from:

Adult Web Sites: Many adult-oriented websites will download infections onto your computer. They usually package these as video players or free software offers. File Sharing Programs: Programs like BitTorrent, uTorrent & FrostWire are designed to allow you to get free movies and music. You are almost guaranteed to get a virus from this type of program.

Be cautious when:

Installing ANY program. Don't just click next, next, next to get the program to install quickly...In most cases you just installed other programs and/or toolbars that may bring in viruses later. Look for the "custom" option and go through each page slowly.

What browser is best?

At this time we prefer Google Chrome. We have found that this is the safest browser to use; our second choice would be Mozilla Firefox. Both of these browsers are a better choice than using Internet Explorer...Especially for Windows XP users. We also recommend the use of [AdBlock Plus](#). This will prevent many of the advertisement you see while browsing the web. www.adblockplus.org

Don't Click on Pop-Ups

If something pops up while you're browsing the internet that tells you it will "scan your computer for free" for possible threats, do not click on it. Even clicking the 'No' option will download the program onto your computer. Sometimes, even clicking on the 'X' up in the right corner of the window brings the infections in. Try the windows command 'Alt' + 'F4' to manually kill the window. If that doesn't work, try to shut down or restart your computer, it is very likely that the virus is just sitting in Memory and a restart may prevent it from actually installing. Never, ever pay for anything that pops up and tells you that it will fix all your problems for \$69.95. Below are some examples of possible pop-up messages:

Don't Panic!

The most important thing to remember is to not panic when something pops up on your computer. The virus creators are counting on your knee-jerk reaction to give them your credit card number because "Your personal information is being stolen!" or "Your hard drive is failing! Your data is gone!" Don't let them trick you into something you wouldn't do if you had taken time to think about it. If something unknown pops up on your computer, take a moment, sit back, and read the entire thing that popped up. Look for things like spelling or grammar errors, or blatantly suspicious attempts to get you to run a scan on your computer that you didn't prompt. If it seems suspicious at all, it probably is!

More

What is Ransomware?

A ransomware is a type of malware that locks your files, data or the PC itself and extorts money from you in order to provide access. This is a new way for malware writers to 'collect funds' for their illegitimate activities on the web. It was found that the United States was on the top of ransomware attacks; followed by Italy and Canada.

How does ransomware get on your computer?

Ransomware looks like an innocent program or a plugin or an email with 'clean' looking attachment that gets installed without the user's knowledge. As soon as it gets its access to the user's system, it starts spreading across the system. Finally, at one point of time, the ransomware locks the system or particular files and restricts the user from accessing it. Sometimes, these files are encrypted. A ransomware writer demands a certain amount of money to provide the access or decrypt the files. However, during the ransomware attacks, there is no guarantee that the users will get back their files even after paying the ransom. Hence, it is better to prevent the ransomware attacks than trying to get back your data from some way or other.

How to identify ransomware attacks

The ransomware generally attacks the personal data, such as user's pictures, documents, files, and data. It is easy to identify the ransomware. If you see a ransomware note demanding money to give access to your files, or encrypted files, renamed files, locked browser or a locked screen of your PC, you can say that ransomware has got a grip on your system. However, the symptoms of ransomware attacks can change as per the types of ransomware.

Types of ransomware attacks

Ransomware attack in two ways. It either locks the computer screen or encrypts certain files with a password. Based on these two types, the ransomware is divided into two types:

Lock screen ransomware: locks your system and demands ransom for letting you access it once again

Encryption ransomware: changes the files in your system and demands money to decrypt them again.

Who can be affected by the ransomware attacks?

It doesn't matter where you are and what device you are using. Ransomware can attack anybody, anytime and anywhere. The ransomware attacks can take place on any mobile device, PC or laptop when you are using the internet for surfing, emailing, working, or shopping online. Once it finds a way to your mobile device or the PC, it will employ its encryption and monetization strategies into that PC and mobile device.

When can ransomware get a chance to attack?

So what are the possible events when a ransomware can strike? If you are browsing untrusted websites. Downloading or opening file attachments received from unknown email senders (spam emails). Installing pirated software, outdated software programs or operating systems.

Precautions against ransomware attacks

The only reason a ransomware is created, is because the malware writers see it as an easy way to make money. Vulnerabilities such as unpatched software, outdated operating systems or people's ignorance is beneficial for such people with malicious and criminal intentions. Hence, **awareness** is the best way to avoid any attacks by the ransomware.

Here are a few steps you can take to tackle or deal with ransomware attacks:

~Windows users advised to keep their Windows Operating System up-to-date. If you upgrade to Windows 10, you will reduce the events of the ransomware attack to the maximum extent.

~Always back-up your important data in an external hard-drive.

~Enable file history or system protection.

~Beware of phishing emails, spam, and check the email before clicking the malicious attachment.

~Use two-factor authentication.

~Use a safe and password-protected internet connection.

~Avoid websites that are often the breeding grounds for malware such as illegal download sites, porn sites and gambling sites.

~Install, use, and regularly update an antivirus solution

It is advisable that you take the problem of ransomware attacks seriously. It not only endangers your data, but it can also breach your privacy to such extent that it can harm your reputation also.

The number of enterprise victims being targeted by ransomware is increasing. The sensitive files are encrypted, and large amounts of money are demanded to restore the files. Due to the encryption of the files, it can be practically impossible to reverse-engineer the encryption or "crack" the files without the original encryption key – which only the attackers will have access to. The best advice for prevention is to ensure confidential, sensitive, or important files are securely backed up in a remote, unconnected backup or storage facility.

Original link to article courtesy of www.thewindowsclub.com

[Ransomware Attacks, Definition, Examples, Protection, Removal, FAQ](#)

ONE MORE THING! The latest trend is heavily accented technicians calling you saying they are from Microsoft. The claim you have a virus and want to log into your computer to check it for free...they plant a virus and ask for \$300 to clean it. It's just a scam...hang up!