



How to Avoid Computer Viruses

Mankato Computer Technology

Adapted from:

<https://www.autodesk.com/redshift/10-tips-on-how-to-prevent-malware-from-infecting-your-computer/>

tips to avoid getting a virus on your devices from the internet

- Whether it's a virus, worm, trojan, malware, ransomware, or anything in-between, one thing is clear: It's not something you want on your PC or Mac.
- If you browse the internet, it's a good idea to think about antivirus protection.
- Viruses can infect your devices with malware which can then steal your personal information, delete your files, and slow down your computer or cause it to stop working altogether.
- If you follow these tips, you'll have a better idea of how to spot a virus on the internet.

Tips on How to Prevent Malware From Infecting Your Computer


- **Most of us have had to deal with a computer virus or some sort of malware by now.**
- **It wasn't fun;**
- **it was annoying,**
- **time consuming,**
- **and very frustrating.**

Tips on How to Prevent Malware From Infecting Your Computer


- When our computers start slowing down or behaving in an unusual way, we are often quick to suspect that we have a virus.
- It might not be a virus, but it is likely that you have some sort of malware.
- Some are malicious, and others are just annoying.
- The worst culprits are the hijackers—malware programs that take over your browser, or worse yet, your computer.
- I have had to remove these types of evil programs from personal computers and work computers in the past, and I'm sure you have, too.
- Here are 10 tips on how to prevent malware from infecting your computer, keeping your hardware safe.

Know the Signs of Infection

- Despite your best efforts, computer viruses can still happen.
- Do you know how to identify a virus on your computer? Here are a few things to watch for:
- Repeated error messages
- Unexpected shutdowns
- Computer suddenly slows down
- Takes too long to shut down or restart
- New toolbars you didn't install
- Changes to your homepage
- Rapidly draining battery
- Any of these signs could mean your computer is infected. If you see more than one of these signs, you almost surely have a virus.
- Make sure all your software is updated and then perform a scan. You can also search online forums for users who have similar issues and see how they were able to solve them.



Install Anti-Virus/Malware Software.

- This tip may go without saying
 - However, I have seen many computers—especially home computers—that don't have anti-virus/malware protection.
 - This protection is a must-have first step in keeping your computer virus free.
- 

Install antivirus software

If you want to avoid getting a virus on your devices from the internet, installing and running antivirus software is important.

Cyberthreats have evolved, and everyday activities like online banking, shopping, and browsing can make you vulnerable to cyberthreats.

Viruses are a major cyberthreat, which is why it's smart to keep your devices protected against them.


Reputable security software can help protect against phishing and other online threats as you bank, shop, and browse online.

Use Antivirus Software

- Next up on our list of how to prevent computer viruses is—no surprise here—antivirus software.
- Antivirus software acts as a “vaccine” against virtual viruses. It can identify and eliminate the threat before you were even aware of it.
- Microsoft Security Essentials and Avast are both free antivirus programs you can install. There’s also a host of paid options, although [experts debate](#) whether the extra cost is really worth it.

Run Regularly Scheduled Scans with Your Anti-Virus Software

- This too may seem like a no-brainer, but many of us forget to do this.
- Set up your software of choice to run at regular intervals.
- Once a week is preferred, but do not wait much longer between scans.
- It's difficult to work on your computer while your anti-virus software is running.
- One solution is to run the software at night when you aren't using your computer.
- However, we often turn off our computers at night, and so the scan never runs.
- Set your anti-virus software to run on a specific night, and always leave your computer running on that day.
- Make sure it doesn't shut off automatically or go into hibernation mode.



Keep Your Anti-Virus Software Up to Date.

- Having protection software is the first step;
- maintaining it is the second.
- Free anti-virus software is better than nothing, but keep in mind that it's not the best solution.
- Many users aren't aware of this program, but it's actually decent protection.

Keep Everything up to Date

Another basic step to take is to make sure you have the latest versions of all software installed on your devices.

Why is this so important? Because software updates include features designed to withstand the latest security threats. Microsoft, Oracle, and other makers regularly update their software to eliminate “bugs” that hackers could exploit.

If you’re operating a system from 3 years ago, it’s defenseless against any viruses or malware developed in the interim. Make it a habit to install all new software updates as soon as they become available.

Patch your operating system and applications

- Tech companies routinely put out software updates to make their devices or software safer to use.
- Without these updates, cybercriminals can abuse security flaws and force a device to download a virus.
- This cyberthreat is called a software vulnerability.
- You might be careful to avoid viruses on the internet, but a software vulnerability may lurk in the background of your computer.
- The only way to ensure you've covered this risk? Regularly update your software whenever a patch is available. Or you can adjust your computer settings to accept updates automatically.


Keep Your Operating System Current.

- Whether you are running Windows, Mac OS X, Linux, or any other OS, keep it up to date.
- OS developers are always issuing security patches that fix and plug security leaks.
- These patches will help to keep your system secure.
- Similarly, keep your anti-virus software up to date.
- Viruses and malware are created all the time.
- Your scanning software is only as good as its database.
- It too must be as up to date as possible.

Use a Firewall

- Using antivirus programs doesn't automatically mean you have a firewall.
- Macs and PCs both come with pre-installed firewall software. Make sure it's enabled to provide an extra layer of protection from viruses and malware.





Secure Your Network.

- Many of our computers connect to our files, printers, or the Internet via a Wi-Fi connection.
- Make sure it requires a password to access it and that the password is strong.
- Never broadcast an open Wi-Fi connection.
- Use WPA or WPA2 encryption.
- WEP is no longer strong enough as it can be bypassed in minutes by experts.
- It's also a great idea to not broadcast your SSID (the name of your Wi-Fi network).
- You can still access it with your device, you will just have to manually type in the SSID and the password.
- If you frequently have guests who use your Internet, provide a guest SSID that uses a different password, just in case your friends are evil hackers.

Install a Popup Blocker

Many attacks happen through browsers, as you're going about your daily online routine. Hackers can gain access to your computer from one innocent click on the wrong ad or link.

An ad or popup blocker is essential to protecting your computer's data. It will prevent any unwanted pages from opening automatically.

Never click on, open, or download anything unless you know exactly who it's from. This is especially important with emails, which is our next topic.

Be careful with email attachments

- Email services like Gmail and Outlook ask for your permission before downloading an attachment. There's a reason for that. Downloading an attachment can be dangerous.
- While email services often have virus protection built into their software, emails with viruses as attachments can still reach your inbox.
- Cybercriminals often try to spread a virus with spamming emails. They send the emails with malicious attachments to a multitude of people.
- Once opened and executed, the virus can install in the background and begin its work.
- If you don't know the person who sent you an email attachment — or if the email looks like it could be a phishing attempt — then ignoring it might be your best option.
- Only click on attachments or download files from your email if you trust the source.
- It's also smart to disable image previews within your email software.
- This feature can be found in the Options or Settings of the program.
- Some viruses can attach to images and install themselves as soon as the email is opened.
- You can configure your settings to only show images from trusted sources.
- This can help prevent an infected image from turning into a virus on your computer.

Beware of Email Phishing Scams

- [32% of reported security breaches](#) begin with a phishing scam.
- These appear in email form under the guise of a legitimate company. The goal is to get you to either enter personal information or click on an infected link that allows access to your computer.
- Any legitimate company will have its own domain name for emails. If an email address claims to be from PayPal or Netflix but ends with @gmail.com, it's a scam.
- Other signs include misspellings, poor grammar, and suspicious attachments, buttons, or links. A legitimate company will *never* invite you via email to log in and provide personal or billing information
- Here's a good rule to live by—if in doubt, don't click on it!

Avoid questionable websites

It is believed that there are over 1.7 billion websites in the world, and not all of them have the best intentions.

The bad ones that pose a cyberthreat will use a variety of tools to download a virus to your computer, like drive-by downloads, hosting malicious advertisements, and getting you to click on misleading links.

Avoid clicking on links to websites with suspicious names, such as mixtures of letters and numbers that don't resemble words.

Also be on the lookout for websites that share names of trusted brands, but have a variation within the URL.

If there are extra symbols in the URL, it's likely a fake website.

Think Before You Click.

- Avoid websites that provide pirated material.
- Do not open an email attachment from somebody or a company that you do not know.
- Do not click on a link in an unsolicited email.
- Always hover over a link (especially one with a [URL shortener](#)) before you click to see where the link is really taking you.
- If you have to download a file from the Internet, an email, an FTP site, a file-sharing service, etc., scan it before you run it.
- A good anti-virus software will do that automatically, but make sure it is being done.

Avoid pirated software

It might be tempting to get a free copy of a game, movie, or application that everyone else has to pay for.

But if you download a cracked or illegal version of software, your computer or mobile device could be at risk.

Pirated software often comes from difficult-to-find websites or peer-to-peer sharing, both of which contain users who may simply be looking for their favorite movie, or those who are looking to spread a virus.

With no virus protection built into what's being downloaded, it's easy for a cybercriminal to slip a virus into a free application.

Sometimes there won't even be any free software — just a virus.

Be cautious when downloading anything for free.

If you download pirated files — which is not recommended — make sure you're using antivirus software.

Keep Your Personal Information Safe.

- This is likely the most difficult thing to do on the Internet.
- Many hackers will access your files not by brute force, but through social engineering.
- They will get enough of your information to gain access to your online accounts and will glean more of your personal data.
- They will continue from account to account until they have enough of your info that they can access your banking data or just steal your identity altogether.
- Be cautious on message boards and social media.
- Lock down all of your privacy settings, and avoid using your real name or identity on discussion boards.

Don't Use Open Wi-Fi.



WHEN YOU ARE AT THE LOCAL COFFEE SHOP, LIBRARY, AND ESPECIALLY THE AIRPORT, DON'T USE THE "FREE" OPEN (NON-PASSWORD, NON-ENCRYPTED) WI-FI.



THINK ABOUT IT. IF YOU CAN ACCESS IT WITH NO ISSUES, WHAT CAN A TRAINED MALICIOUS INDIVIDUAL DO?



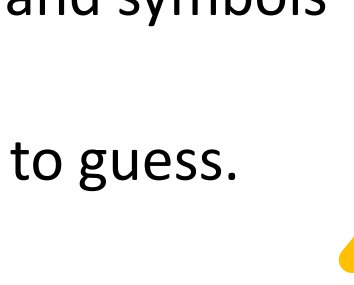
Back Up Your Files.

- The best thing you can do is back up your files—*all of them*.
- Ideally you will have your files (your data) in at least three places:
 - the place where you work on them,
 - on a separate storage device,
 - and off-site.
- Keep your files on your computer, back them up to an external hard drive, then back them up in a different location.
- You can use a backup service or simply get two external hard drives and keep one at work, at a friend's house, at a family member's house, or in a safe deposit box.

Backup your computer

- This tip may not help you avoid getting a virus on your devices from the internet, but it will help you sidestep some of the damage and stress that comes with it if you do.
- By regularly using a cloud backup, you can keep copies of all your important files and records in a location that won't be contaminated by the virus.
- Then, should you become a victim of a computer virus that's difficult to get rid of without damaging your files, you can simply wipe your device and restore it to the most recent point before it was infected.

Use Multiple Strong Passwords.

- Never use the same password, especially on your bank account.
 - Typically, we use the same email address or username for all of our accounts.
 - Those are easy to see and steal.
 - If you use the same password for everything, or on many things, and it is discovered, then it takes only seconds to hack your account.
 - Use a strong password.
 - Use lower case, upper case, numbers, and symbols in your password.
 - Keep it easy to remember but difficult to guess.
 - Do not use dates or pet names.
- 

Use Strong Passwords

- The most commonly used passwords in the cyber world are also the worst. As of 2018, the [top 3 passwords](#) in use were:
 - 123456
 - password
 - 123456789
- And people wonder why we have security breaches everywhere?
- Keep your data safe by creating unique, complex passwords. The best passwords include a mix of numbers, letters, and symbols and are at least 8 characters long.
- While we're on the topic, avoid using the same username and password combination across multiple sites. If a hacker can access just one site, you've left the door wide open to the rest of your data.

Educate Your Family

- Most cyber-attacks happen through an innocent action by an uninformed person.
- This could be a member of your family, a child, or an employee who isn't aware of smart internet practices.
- If you have any doubts about anyone who uses your computer, take a few moments to teach them the basics. Review a few points from this post, such as not opening emails or clicking on links from unknown sources.
- A few moments of education could mean the difference between cyberattack success or failure.

How to Prevent Computer Viruses: Now You Know

- So, how can you protect your computer from viruses?
- Much of the defense starts with you. Use antivirus software and keep your programs and software up to date. You should also be proactive with firewalls, popup blockers, and strong passwords.
- Of course, the more you use your computer, the more you have to lose.