June 2017

TechTidbit.com

brought to you by Tech Experts

Rules Of Thumb To Avoid An Infection

Anthony Glover is a Senior Network Engineer and Service Manager at Tech Experts.

A virus can be an upsetting, expensive endeavor to deal with. A virus can wreak havoc on your personal files (like important spreadsheets or family photos) or the system files that keep your computer functioning.

These files can become corrupted, encrypted, or deleted, which makes recovery difficult or sometimes impossible.

Some less obvious viruses — the ones that might slow down your system instead of destroying it — can still affect you by stealing data and what you type on your keyboard, gaining access to your stored credit card information or important sites you use, like your bank.

First things first: if you email or get email frequently, the best practice to avoid a virus is to only open emails from senders that you are familiar with.

This will mitigate the risk of receiving a malicious message that could lead to you self-inflicting a virus by mistake. If the email does come from a friend but the email subject sounds suspicious, take precaution and contact them on an alternate method to confirm they did send it.

Some infections, once in an email account, will send out spam emails to infect others and, while you personally may not be infected yet, a friend might be.

Second, be careful what you download and where you download from. Malicious software is everywhere and recklessly browsing the Internet can lead to getting a virus.

To avoid this, always check for a secure website, one that starts with "HTTPS://" — this means that the connection is secure and it's safe to visit due to the encryption on the webpage.

Fortunately, most websites that people visit daily have the option for a secure "https://" URL, so try adding an "s" to the "http://" portion of your address bar when browsing your favorite websites (if it doesn't already have it).

Third, install anti-virus software and make sure to keep it up to date. Legitimate anti-virus software aims to keep your device protected, however it's a method of prevention and can't keep out everything depending on your actions.

Even with anti-virus, you should browse responsibly and update the software as soon as possible, whenever possible to cover yourself.

New threats are being created and distributed daily and updating the software gives your anti-virus the means to combat malicious files.

The best tool to prevent this issue is managed anti-virus, such as the one provided by Tech Experts.

We provide a solution that is managed and monitored so we can catch viruses as they happen rather than after they happen. This reduces (or eliminates) downtime and keeps your computer clean and running smoothly throughout the year.

Remember, a computer is only as safe as you make it, however with the proper precautions, you will be able to enjoy your personal computer without the dangers of viruses, spyware, adware, or ransomware.

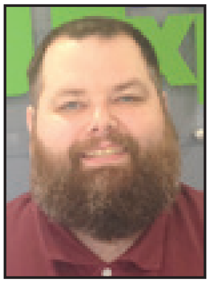
Evaluate everything before you open it or navigate to it, don't download anything that seems even slightly suspicious, and always err on the site of caution.

Taking a chance on something could mean losing all of your data and facing an unexpected cost from a repair bill.

Some less obvious viruses — the ones that might slow down your system instead of destroying it — can still affect you by stealing data and what you type on your keyboard, gaining access to your stored credit card information or important sites you use, like your bank.

Anti-Virus: It's Worth Protecting Yourself

> *"Often, users say, 'I have such and such subscription,' or 'I don't click on anything I don't know,' but the people spending countless hours causing havoc on computer users will always find new and sneaky ways to infect computers."*



Ron Cochran is a Field Service Engineer at Tech Experts.

You can have any machine — from the latest and greatest, to the old dinosaur in the corner — but if you don't have virus protection, your latest and greatest machine might soon run like that dinosaur in the corner.

All of your sensitive images, documents, billing information, and passwords are subject to infection. No matter how careful you are, there is always something that slips through the cracks.

Often, users say, "I have such and such subscription," or "I don't click on anything I don't know," but the people spending countless hours causing havoc on computer users will always find new and sneaky ways to infect computers.

Viruses can be attached to images or links on websites. They can also be renamed to look like something that you should install. Once inside your computer, they are hard to track down even by a seasoned computer technician.

Viruses very rarely remove anything from your computer. Instead, they have a tendency to add things that can record your activities on your computer. A person could install a silent program that will start recording your keystrokes triggered by keywords; it can also take a screenshot or record email addresses and passwords. Most of the time, they don't need to even gain access back to your computer to report the data.

They can have an email sent from your computer and Internet connection without you knowing it. That email, secretly sent from you to them, would contain your information (keystrokes, clicks, etc.).

By now, you have heard of the "crypto virus" and all of its variants. There are many solutions out there, but select few offer "zero-hour" infection reversal, however it's something that businesses can especially benefit from. Let's say you accidentally encrypt your machine; it would then be inaccessible until you pay the ransom to unlock your files.

Protection that offers infection reversal can revert your system back to its state right before you were infected and it would be like you never infected by the virus at all. This feature is part of Webroot Secure Anywhere, which is something we can provide.

Viruses not only help people steal your data, but they can also delete or corrupt files, degrade system performance, and make your computer run slower.

Viruses can also prevent programs from working and they can use your email to send out copies of itself to your contacts and other users. Sometimes, they can disable your computer from starting up by corrupting your BIOS firmware.

A couple of the main things that you'll notice once you're infected is that your system could run slower and you'll receive all kinds of fake pop-ups, ads, warnings from "Microsoft," etc. These type of files are referred to as "scareware" and the makers feed on the fear that you might lose your data, so you'll pay them to "unlock" your system or "remove" the virus.

Again, we go back to protection. If you had virus protection, then it's likely that would stop it before it even established itself inside your computer.

There are a few things you should do, if you haven't already: get some sort of whole computer protection (such as Webroot), have restore points saved on your operating system, have a backup of your operating system install saved on some sort of external media, and save your documents, pictures, and videos to an external source.

When you find yourself in a predicament where you have to wipe an entire computer to remove an infection, you'll be glad you took the time to prepare for the worst.

Easy And Common Steps To Resolve Internet Issues

Luke Gruden is a Help Desk Specialist at Tech Experts.

The Internet is key in almost all that we do on computers. A computer without Internet would have limited use — not only because of the browser, but because many programs require the connection to function.

That's why when we are right in middle of working and we lose Internet, we can get very frustrated very quickly. Luckily, there are a few things you can try to potentially restore your Internet with minimal time and effort.

Calling your Internet service provider or your IT techs can result in an issue taking longer to resolve as someone may have to drive out to your business or you have to wait for the next available phone representative. Why wait when, most likely, you can fix your own Internet in about 15 minutes or less with minimal experience?

However, before we talk about how to bring back the Internet, we must talk about terminology and devices.

The first device that handles your Internet from the outside of your building is the Internet modem. Your modem usually has your Internet provider's logo on it and is plugged in by a cord going outside (usually through a wall). You also need to know what a router is. A router plugs into all the computers with either wired or wireless connections. Sometimes, the modem is also a router when it's a two-in-one device.

Finally, you should know what a firewall device is. Firewalls are usually a box that is plugged in between the router and modem, protecting your network. That said, not every business has a firewall.

Now that you have the basic terminology, we can potentially fix the Internet. First of all, if you lose your connection to the Internet, try a reboot of your workstation.

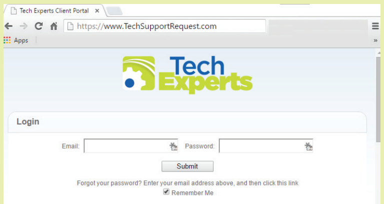
If the reboot does not work, see if anyone else has Internet. If it is just you that's lost connection, try to see if you can push your Internet wire (Ethernet cable) into your computer. Sometimes, the connection can become loose and that's all there is to the problem.

If you are using a wireless connection, turn off your Wi-Fi with a button on your computer and turn it back on. If your Internet is not back, you might have to contact your IT. If no one has Internet, take a look at the modem. The modem usually has lights showing the status of the Internet connection. If it shows that there is no Internet, try to unplug the power from it and wait 15 seconds and plug it back in.

The modem will take time, potentially 10 or 15 minutes, but you will see if the Internet connection comes back. If the modem does have Internet, try to unplug the firewall (if you have one), then plug it back in after 15 seconds. If the Internet still is out after 15 minutes, try to do the same thing with the router by unplugging and plugging the power back in. If the Internet is still out for everyone, you probably have to call your Internet service provider as there could be an outage in the area. Most of the time when the Internet goes out, following these steps can likely bring back the Internet connection. This is especially true if you are at home.

Hopefully, following these steps can resolve your lost Internet connection. Sometimes, your equipment essentially needs a restart to get things back into working order. Should you need further help, we at Tech Experts have you covered!

> *"Calling your Internet service provider or your IT techs can result in an issue taking longer to resolve as someone may have to drive out to your business or you have to wait for the next available phone representative. Why wait when, most likely, you can fix your own Internet in about 15 minutes or less with minimal experience?"*


Tech Experts Client Portal
https://www.TechSupportRequest.com
Apps
Tech Experts
Login
Email:
Password:
Submit
Remember Me

Forgot your password? Enter your email address above, and then click this link

Create new service requests, check ticket status, and review invoices in our client portal:

http://TechSupportRequest.com

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

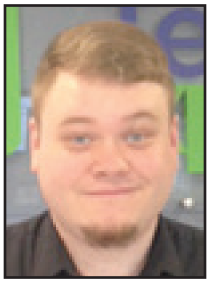
Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of
our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Built-In Windows 10 Tools You May Not Know About



Jared Stemeye is a help desk specialist at Tech Experts.

As we approach the second anniversary of Windows 10 this July, users have continued to steadily adopt Microsoft's flagship OS and move away from the limited support of Windows 7 and clunky interface of Windows 8.

With this, many new users are currently unaware of the simple, yet powerful features that are now built right into Windows 10.

Some were present in previous iterations of Windows, but have been improved upon within 10.

Built-in Screenshot Utility

Those of us without fancy third-party screenshot software had to resort to the old tried-and-true Control + Print Screen function to copy and paste the screenshot into Paint to save. However, there's now an easier way.

The Snipping Tool application built into Windows since Vista has a ton of intuitive features for taking screenshots.

You can easily find this handy tool by typing "snip" into your start menu search. Windows 10 has added time delayed screenshots as an additional feature to take screenshots that were not previously possible.

Sticky Notes

Built-in since Windows 7, Sticky Notes allows small text boxes to be attached to your desktop. They are great for reminders or quick notetaking. You can create multiple notes and change the background and text colors for better visual organization.

These notes are also smart, using "insights" to provide contextual information to your notes automatically. If you add an email, address, or phone number, your note will recognize it as such to make the note easier to interact with.

Action Center

Brand new to Windows 10, the Action Center can be accessed next to your clock at the bottom right of the screen. By clicking the text box icon, you can access alters from your operating system and applications.

This menu also allows quick access to tablet mode, Connect (Bluetooth device pairing), VPN settings, and other tools. My favorite Action Center tool is night light mode, which dims your screen and provides a warmer tone that's easier on the eyes in low light.

Display Calibration

In my opinion, the Display Calibration tool is by far the best and most underused tool built into Windows 10. Out of the box, your PC monitor is usually too bright and the colors are typically oversaturated. That may not be an issue if all you do is spreadsheet work, but if you're editing photos or video, you'll want to fine-tune the colors for accuracy.

Sure, you could spend $60 or more for color-calibration software and hardware and that might be money well spent if you're a graphics professional or a movie buff who's finicky about faithful color reproduction. However, the color-calibration tool built into Windows can give you most of what you without additional software.

Type "calibrate" into the start menu search, and select Settings. You want to pick Calibrate Display Color, which is usually the top option.

The color calibrator's welcome screen includes a link to a help-center tutorial. All you really need to do, however, is walk through the steps and read the explanatory text.

The first time you do this, don't skip any of the steps. The steps are, in order: gamma settings, brightness adjustment, contrast adjustment, and color balance. Your monitor's color will look better than ever once you complete the tuning.

For even more information on the new tools that are in the works for Windows 10, visit *microsoft.com/windows/upcoming-features*

Create new service requests, check ticket status, and review invoices in our client portal: *http://www.TechSupportRequest.com*