Internet Troubleshooting Tips

Can't Connect to the Internet?

If you are unable to connect to the internet, there are a few troubleshooting techniques you can try that may get you back up and working without a visit from a technician.

The number one thing to do when your internet goes out is try a simple **reboot**.

Quick Reboot Guide

1) Turn off your computer by selecting log off and then shut down or restart

2) If you have any routers or other transport devices connected to our equipment, unplug them

3) Unplug your modem or antenna

4) Wait at least 1 Minute

5) Plug your modem or antenna back in and wait for it to fully initialize- this will take about 2 minutes

6) Plug your router or other transport device back in and wait for it to fully initialize- this will take about 2 minutes

7) Turn your computer back on and try connecting again- make sure your Modem or Antenna is powered on as well as your Router or Other Transport Device

If you still cannot connect to the internet after rebooting your devices, you can try to ping a website to see if your internet connection is down or if your internet browser is not functioning properly. For instructions on how to ping a website, see information below.

Pinging a Website

Ping is a command that sends a message to another computer or device and waits for a response. It is used to verify connectivity between devices, such as a customer’s computer to a webpage or our console to a customer’s antenna.

1) Click on START
2) Click on RUN (in newer versions of windows type CMD in the search box on start menu and skip step 3)
3) In the box that pops up, type the letters cmd (small case, no spaces); depending on the version of windows the computer is running you may need to type the full word, command (this usually pertains to machines running windows 98 or lower)
4) A dos prompt will open
5) In the dos prompt type the word (ping), then a (space), and then a (URL) or (IP address)
   For example: (ping unicom-alaska.com or ping 209.165.134.28)

Internet Troubleshooting Tips

6) The dos prompt will show the results of the ping test:
   a) If the ping was successful: There will be a total of 4 signals sent. If there are 4 Reply from lines then you have a good connection with the device you are connecting to
   b) If one or more of the reply from lines says request timed out: This means one or more of the signals did not get a reply, try pinging again. If you consistently see request timed out on your list, you are not receiving a good signal from the device you are pinging
   c) If you do not get any reply from lines and the prompt just says request timed out: This means that the device or URL you are trying to connect to is offline, and not able to send and receive signals

If you can successfully ping a website but when you try connecting to the internet your connection times out or you get a "page cannot be displayed" message, you have a problem with your internet browser. These problems can be caused by Virus/Spyware infections or corrupt program files in the internet browser program. Reinstalling or doing a repair install on your browser program (if possible) can fix the problem by removing the Virus/Spyware infections from your computer and keeping it safe in the future.

If you can not successfully ping a website, in general you are not getting a connection to the internet. If you have a router, hub, or other transport device, try bypassing it. Disconnect the transport device and plug your Ethernet cable directly into your computer from your modem. If you can connect to the internet after disconnecting the transport device, then most likely your transport device is not configured properly. If you do not have a transportation device, or bypassing it did not work, Please contact our customer service office.

If your computer seems to be running slowly, taking a long time to connect to web pages, has random errors and kicks you out of programs you are using, or just doesn't seem to be running as smoothly as it used to, you could have a virus/spyware infection. It is very important to maintain the health of your computer in order to keep it running properly.

Computer Health

In order to keep your computer running smoothly and save a lot of time and troubleshooting, it is important to keep your computer free of Malware. When your computer becomes infected with viruses, spyware, grayware, and other forms of Malware, it begins to run slower, you can loose data, experience random errors, and even infect other computers using the same ISP (Internet Service Provider) as you.

What is Malware/Viruses/Spyware? Click on the link below to read about what these things are and how they can affect you and everyone on your network.

MALWARE-VIRUSES & SPYWARE

How do I Detect a Computer Virus?

You can keep your computer safe and detect possible threats and infections using Virus & Spyware scanners. These scanners can be set to run on your computer at certain times every day or as little as weekly, they find and remove infections from your computer and warn you about possible security threats. It is important to have a scanner that looks for both spyware and viruses, most scanners on the market today search for both. It is even a good idea to have two programs because some programs find things that others miss.

Aside from just having a Virus & Spyware scanner you need to be proactive to make sure that it works for you. The number one thing that you should do is make sure you download the updates at least once a week; most programs can be set to auto update, just make sure that you have administrative privileges to auto download the updates to your computer, otherwise your updates will fail.

Can I Prevent My Computer From Getting A Virus?

Aside from routinely running Anti Virus and Spyware scans on your computer, there are things you can do to avoid getting infections. The most common viruses are attached to emails. Never open email attachments from someone you don't know, even if it is an email claiming to be from a bank, credit card company, ISP Administrator, PayPal, etc. There is a lot of junk email out there claiming to be from someone they are not.

Downloading things onto your computer is another common way to get infected. Only download things from trusted sites.

It is very common to have a small amount of spyware on your computer and sometimes even if you are careful you can still pick up some form of malware. Keeping up to date antivirus and spyware programs with the latest definitions, and running them regularly, is your best defense against Malware.

Antivirus & Spyware Programs

The following are only some of the available programs on the market. It is always best to do your research and decide what program is best for you.

- **Microsoft Security Essentials**
- **Spybot Search & Destory**
- **Trend Micro**
- **Mcafee**
- **Norton**

Windows Updates

Windows Customers should search for and download Windows Updates regularly. Microsoft is constantly fixing bugs in their software and making it more secure; keeping up on the latest windows updates will keep your system running smoothly and your software working properly.

Internet Troubleshooting Tips

Windows Updates can be set to run automatically and new patches, upgrades and fixes will be automatically downloaded and installed on your computer, or you can manually download and install the updates when you choose. Copy and paste the link below to visit the Windows Updates webpage.

Windows Updates
http://www.update.microsoft.com/windowsupdate/v6/thanks.aspx?ln=en&&thankspage=5

To use this site, you must be running Microsoft Internet Explorer 5 or later.

To upgrade to the latest version of the browser, go to the Internet Explorer Downloads website.

If you prefer to use a different web browser, you can obtain updates from the Microsoft Download Center or you can stay up to date with the latest critical and security updates by using Automatic Updates. To turn on Automatic Updates:

1. Click **Start**, and then click **Control Panel**
2. Depending on which Control Panel view you use, Classic or Category, do one of the following:
   - Click **System**, and then click the **Automatic Updates** tab
   - Click **Performance and Maintenance**, click **System**, and then click the **Automatic Updates** tab
3. Click the option that you want - Make sure Automatic Updates is not turned off

What is Malware?

Malware is an extension of the original threat to computer security from viruses. The term Malware is short for ***malicious software,*** which is software designed specifically to damage or disrupt your computer system. The term encompasses not only viruses, but new threats such as Spyware, Trojan horses, and worms.

What is a Virus?

In computer security, a "virus" is a self-replicating computer program that spreads by inserting copies of itself into other executable code or documents. A computer virus behaves in a way similar to a biological virus, which spreads by attaching itself to cells. Keeping with the analogy, the "attachment" of a virus into the program is termed as an "infection", and the infected file, or executable code, that is not part of a file, is called a "host". Viruses are one of the several types of malware.

While viruses can be intentionally destructive, most other viruses are fairly benevolent or merely annoying. Some viruses have a delayed payload, which is sometimes referred to as a "bomb". For example, a virus might display a message on a specific day or wait until it has infected a certain number of hosts. A "time bomb" occurs during a particular date or time, and a "logic bomb" occurs when the user of a computer takes an action that triggers the bomb. The predominant negative effect of viruses is their uncontrolled self-reproduction, which wastes or overwhelms computer resources.

Today, viruses are somewhat less common than network-borne worms, due to the popularity of the Internet. Anti-virus software, originally designed to protect computers from viruses, has in turn expanded to cover worms and other threats such as spyware, identity theft and adware.

What are Trojan Horses?

A Trojan horse is just a computer program. The program pretends to do one thing (like claim to be a picture) but actually does damage when one starts. Trojan horses cannot replicate automatically like viruses but have proven to be much harder to remove from an infected system.

What is a Worm?

Worms copy themselves and infect files much like a virus. However, a worm is a piece of software that uses computer networks and security flaws to create copies of it self. A copy of the worm will scan the network for any other machine that has a specific security flaw. It replicates itself to the new machine using the security flaw, and then begins scanning and replicating anew. This can affect not only computers on the same local area network (LAN) but can also affect computers on the Wide Area Network (WAN) which is the network your ISP uses to provide you with internet service.

Email Viruses - The most common virus!

Email viruses work in the same way as a regular virus. However, an e-mail virus will use an e-mail message as a mode of transport, and usually will copy itself by automatically mailing itself to hundreds of people in the victim's address book. Most email viruses can only infect files once opened. Usually the virus will originate from an email attachment, making it ever important to only open attachments from trusted sources.

A computer virus will pass from one computer to another like a real life biological virus passes from person to person. For example, it is estimated by experts that the Mydoom worm infected a quarter-million computers in a single day in January of 2004. In March of 1999, the Melissa virus spread so rapidly that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be dealt with. Another example is the ILOVEYOU virus which occurred in 2000 and had a similarly disastrous effect.

Also, if you receive an e-mail requesting you to update OR provide sensitive account information or confirm your username/password, **do not reply** to the e-mail as it is most likely a scam (also known online as a “phishing scam”). Please note that these 3rd parties often send messages that appear to come from legitimate email addresses but they are not.

In addition, you should not click on web links sent to you in emails and then provide personal or account information on those sites. These links may take you to pages that look similar to your financial institution or other familiar sites but are in fact imitation sites set up to acquire your personal information with malicious intent.

Internet Troubleshooting Tips

Passwords

It’s hard to remember all those different passwords! Here are some tips to create unique passwords that are easy for you to remember, but hard for others to guess.

Unique passwords made easy—but not easy to guess

Chances are, you use dozens of sites that require you to log in with a user name and password—your bank, your email, your favorite online stores. We’ve heard that we should use a different password for each site, but so many of us don’t. It’s hard to remember all those different passwords! Here are some tips to create unique passwords that are easy for you to remember, but hard for others to guess.

The key to remembering a bunch of different passwords is to make sure they each have consistent elements without being identical. That can be tricky, with more and more sites requiring long and complicated passwords. So let’s look at what makes up a good, strong password.

A strong password typically contains:

- Lots of characters. The longer the password, the more secure it’ll be. Aim for 15 characters
- At least one letter—preferably multiple letters with at least one capitalized
- At least one number
- At least one special character (like a punctuation mark or symbol)

The string of characters you use for your password should also seem random. Dictionary words, names, and predictable patterns (such as QWERTY or 987654) are too easy to hack.

By creating a “base” or “master” password with all of these elements, we won’t have to change up the formula for sites that have tougher password guidelines than others. Once the base of your password has been established, you can add to it to create a custom password for each site you use.

To start, pick a phrase that you can easily remember—perhaps lyrics to your favorite song or a funny or inspirational quote. Let’s start with this: See you later, alligator! Now shorten it by using the same tricks you’d use when getting a custom license plate: CUL8rAllig8r

You can also try using the first letter of each word of a longer phrase, making sure to include at least one number. Whichever method you choose, be sure to use more than a single word, which is relatively easy for password cracking applications to guess, even with character substitutions.

This password is relatively easy to remember, and it meets our criteria because it has:

- Multiple characters
- Capital letters and lowercase letters
- Numbers

Password Don’ts

- Do NOT put your username as the password
- Do NOT use "password"
- Do NOT use your first or last name
- Do NOT use repeating or sequential numbers such as 1234567890, 22222222
- Do NOT use dictionary words
- Do NOT use single "hacker phrases" as passwords e.g. "M1cr0$0ft" or "P@ssw0rd"
- Do NOT write down the password on a post-it and stick it on the monitor

Experiencing Slow Internet Speeds?

Your plan speed is the maximum speed expected to be achievable for that plan. Several factors will affect the actual speed you experience. These factors include, but are not limited to: the capability of the device you're using to access the Internet; the application and/or server/web site you are accessing; limitations of Wi-Fi and other equipment you may be using; other active users and/or devices on your home network at the same time; routers on the public Internet being over-loaded by high demand – particularly during peak hours of the day.

Due to the fact that UUI’s broadband speeds meet the capability of many home networks and devices, running speed tests from a single device is no longer an effective measure of service quality. If you feel there may be issues impairing your service, please contact UUI Customer Service as they have the tools to identify any issues that may exist.

Wireless Networks

When you set up a wireless network in your home or business it is important to secure the connection. A Secured Network allows only authorized people to use your internet connection and access information on your network. A Unsecured Network allows anyone near your home who has a wireless device to be able to use your internet connection to connect to the internet as well as access information on your network.

If you have an unsecured wireless network in your home, anyone in close proximity can monitor your online activities. Depending on how your home network is configured, someone could even gain full access to your computer’s hard drive over an unsecured wireless network.

Aside from the risk of people being able to gain access to your computer through an unsecured wireless network, your neighbors could sponge off of your Internet connection. This would not only deprive you of bandwidth that you are paying for, but if your neighbor conducted some illegal activity while online, it could be traced back to your network.

What is Encryption

By far the most important thing that you can do to secure your wireless network is to use encryption. Almost every wireless access point has some type of encryption mechanism built in. Most older access points offer WEP encryption, and newer access points offer a choice between WEP and WPA.

***WEP** (Wired Equivalent Privacy) - a security protocol for wireless local area networks*:
WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. Basically you are adding a password to your internet access so someone has to know the password to access your wireless network. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model (Open System Interconnection Model) - the data link and physical layers; it therefore does not offer end-to-end security. Most new devices offer WPA which was invented to take the place of WEP due to its obvious security flaws.

***WPA** (WiFi Protected Access) - a more secure form of encryption than its predecessor WEP*:
WPA operates using more layers of the OSI model making it true end-to-end security. Protecting everything from Data Sent and Data Received to Information processed on and stored within your personal network. If the option is available always choose WPA encryption over WEP to create a more secured network.

Ethernet Connection

Routers

This set up uses an Ethernet router and cable physically connected between each computer and the router. This set up is inexpensive, and works best if all of the computers, the router and the cable modem are all located in a close area.

To set this up, you will require:

- A router
- A network interface card (NIC) in each computer
- and Ethernet cable (Commonly called Cat 5 cable)

Routers are recommended over hubs for several reasons.

1. Routers will provide you increased security.
2. A router is a piece of hard ware with a built in fire wall.
3. Routers are easy to set up and provide you greater flexibility if you decide to set up a network.
4. The prices of routers have decreased significantly and are no longer prohibitive for most people.

Hub

An Ethernet hub can be used instead of the router shown above, but does expose your computers to a greater risk on the Internet. *If using a hub: A critical note is - File and Print Sharing should be turned off on all computers you hook up this way*. By turning off *File and Print Sharing* you decrease the risk of other Internet users gaining access to your computers.

As with all forms of “always on” Internet connections UUI recommends use of a Firewall application for increased protection.

Other Resources

There are many excellent sites on the Internet on how to set up a network. We have provided a few below. Any system you set up must be able to pass data traffic using TCP/IP protocol, the data language of the Internet.

- http://www.linksys.com/
- http://www.bricklin.com/homenetwork.htm
- http://www.apple.com/support/airport