

Remove Infection

A. Possible threats from infection

- Use of your computer to allow spamming or to assist with Denial Of Service (DOS) attacks
- Data theft (accessing your personal data to see your passwords, credit card information and contact lists)
- Installing software, including 3rd party malware
- Downloading or uploading of files on the user's computer, including installation of computer virus
- Modification or deletion of files
- Keystroke logging
- Watching the user's screen
- Turning on the user's built-in web camera
- Crashing the computer

B. Symptoms of infection

- You find yourself thinking that your computer is EXTREMELY slow
- Your computer seems to be "doing something" even when you are not
- Pop-up ads keep showing up
- Notices that you are infected appear and demand that you install software to remove it. DO NOT INSTALL ANY SOFTWARE in this manner.

C. If you suspect you are infected

- You should run a quick detection scan to determine the type of infection. McAfee offers an excellent scanning tool: <http://vil.nai.com/vil/stinger/> However, keep in mind that this is just a quick scan for the latest threats and not an everyday option for protection.

D. You may need to run more than one type of scanner to clean your system.

Not all virus and malware software is equal. Keep in mind that some virus scanners may not detect other malware intrusions, like adware or spyware.

- If you discover you are infected, installing specific scanners to clean your system may be your best option. AdAware is specifically designed for adware infections, SpyBot works great for spyware and you may need a "virus-specific" removal tool which can be found at any of the scanner sites listed on the back of this brochure.
- MalwareBytes often detects non-viral threats that are not found with normal virus scanners: <http://www.malwarebytes.org/>

E. You might need professional assistance. Call your help desk or IT professional.

References

- ⇒ **What is the Government doing about malware threats? Did you know there is an entire team of specialists that work on "cyber-related" threats?**
 - The Cyber-Incident Response Capability (formerly CIAC) is found under the Department of Energy: <http://www.doecirc.energy.gov/>
- ⇒ **Definitions and descriptions can be found at:** <http://www.wikipedia.org/>
- ⇒ **Information regarding hoaxes can be found at:** <http://www.snopes.com/>
- ⇒ **Scanner sites are provided for information only. No warranty is expressed or implied. There are many more good scanners. Do a little research before using one not mentioned. The scanner that is best for you is one that works specifically with the type of operating system and software you own. Look for FREE versions at the sites listed (find downloads).**
 - AdAware: <http://www.lavasoft.com/>
 - Avast: <http://www.avast.com/>
 - AVG-Free: <http://www.avg-free.us/>
 - Computer Associates: <http://shop.ca.com/>
 - MalWareBytes: <http://www.malwarebytes.org/>
 - McAfee: <http://www.mcafee.com/>
 - SpyBot Search & Destroy: <http://www.safer-networking.org/>
 - Symantec: <http://www.symantec.com/>



Tier3Backup.com

Tier3 Hosting & Consulting

558 Castle Pines Pkwy B4302
Castle Rock, CO 80108

Phone/Fax: 800-762-4912
E-mail: support@tier3backup.com

Malware— Do you know?

- ⇒ Malware is "malicious software" designed to access computer information without the owner's consent?
- ⇒ How to prevent or remove malware infections?
- ⇒ Scams, SPAM, Hoaxes, and ScareMail are not malware?
- ⇒ References you can use to find out more and clean your system?

A "Do It Yourself" Resource

Types of Malware

- A. A virus is a computer program that can copy itself when an application it is attached to is opened or shared.**
- A virus is spread from one computer to another via internet, email or when copied to CD/DVD or USB drives and shared. A benign virus copies itself and does no real harm, however a malicious virus will cause noticeable symptoms and can damage data.
- B. Worms are self replicating programs that do not need another application to spread**
- A worm is often used to open a “back door” to a computer/server allowing others to send email from this machine. The machine is then referred to as a Zombie or BotNet and begins SPAMMING the world or initiating a Denial Of Service (DOS) attack.
- C. AdWare is typically software that downloads advertisements and “pop-ups” to your computer.**
- Adware is usually benign advertisements used to generate income for the author but can be used to mask other more obtrusive malware.
- D. SpyWare is software designed to capture personal information about you or your computer habits. (what you do & what web-sites you visit)**
- E. Trojan Horse is software that often looks legitimate but performs functions without the users knowledge or consent. Users are often “tricked” into installing a Trojan horse.**
- Trojan Horse spreads like a virus, however, vulnerabilities in software (i.e. browsers or chat tools) can often lead to infection. It can also be acquired by visiting malicious websites that intentionally put code in a link you would click.
REMEMBER: Trojan Horse often look legitimate!
- F. Rootkits are software installed to gain access to the computer as a “privileged user”**
- Rootkits give backdoor access to your system (often the entire network) allowing the offender to obtain information that is typically secure, even allows them to fraudulently act as an authorized user. Often a “hacker” is able to obtain or guess a user password and work up from there. **RETHINK YOUR PASSWORDS!**

Prevent Infection

- A. Install, update and continue to run virus and malware software**
- There are many good FREE scanners. However, you may feel more comfortable with the features of a paid subscription. Many free options are not automated, requiring the user to REMEMBER to run the updates and the scans. **See back for more details.**
 - You may need to install and run more than one type of scanner
- B. Do NOT open email attachments**
- If you were not expecting an attachment from someone you know, delete it immediately.
- C. Apply software updates**
- Allow your operating system to update and apply updates to your browser frequently.
- D. Create STRONG passwords**
- Your password is your first line of defense.
 - Do not use the same password on every site.
 - Use a password manager to create and manage your passwords.
 - NEVER share your passwords!
 - Change your password frequently.
- E. Backup your data frequently**
- It might be possible to restore your system back to a point prior to infection (be careful, your backups might be corrupt or infected too!)
 - Malware can cause hardware failure. Backups can enable you to restore on a new system.
 - For more information regarding secure online backups, please visit: <http://www.tier3backup.com/>
- F. Adjust the settings of your scanner to your needs**
- SpyBot has advanced settings that allow you to lock certain browsers so that changes cannot be made without administrator user permissions. This is nice if you have multiple children accounts, or a computer in the reception area of your office.
 - Adjust your browser settings to “always ask” about cookies and NEVER accept 3rd party cookies.
- G. Make sure your ISP (or email service) is scanning your email for virus protection.**

Scams, SPAM, Hoaxes & ScareMail

- A. You might receive email that contains fraudulent information, however, this is not malware**
- SPAM is Unsolicited Commercial Email (UCE) to an indiscriminate set of recipients that does not follow proper subscription processes (it also has many other names). It is an electronic version of the kind of “junk mail” that comes to your home mailbox. SPAM is often sent via Zombie/BotNet computers that have been hijacked by malware, and is almost impossible to track. The best course of action is to delete. NEVER “click here” to unsubscribe... that just tells them you are a valid email address. NOTE: Unsubscribing from a valid distribution list is fine.
 - The same common sense rules apply to SPAM as they do for “junk mail.”
 - * If it sounds too good to be true, it's probably a hoax.
 - * Never send money.
 - * Never give out personal information.
 - * Foreign lotteries are hoaxes because as a US Citizen, you are ineligible to win a foreign lottery.
 - * Emails about lost or dying children are usually hoaxes. They might have been true a number of years ago.
 - * No CEO is going to pay you for forwarding an email.
- B. ALWAYS CHECK TO SEE IF IT'S A HOAX before forwarding:**
<http://www.snopes.com/>

Tier3 Hosting & Consulting

558 Castle Pines Pkwy B4302
Castle Rock, CO 80108

Phone/Fax: 800-762-4912

E-mail: support@tier3backup.com