

## ***Recovering from Viruses, Worms, and Trojan Horses***

Unfortunately, many users are victims of viruses, worms, or Trojan horses. If your computer gets infected with malicious code, there are steps you can take to recover.

### **How do you know your computer is infected?**

Unfortunately, there is no easy way to identify that your computer has been infected with malicious code. Some infections may completely destroy files and shut down your computer, while others may only subtly affect your computer's normal operations. Be aware of any unusual or unexpected behaviors. If you are running anti-virus software, it may alert you that it has found malicious code on your computer. The anti-virus software may be able to clean the malicious code automatically, but if it can't, you will need to take additional steps.

### **What can you do if you are infected?**

1. **Minimize the damage** – disconnect your computer from the network and contact InfoGuard immediately . The sooner we can investigate and clean your computer, the less damage to your computer and other computers on the network. If you are on your a laptop, disconnect your computer from the internet. By removing the internet connection, you prevent an attacker or virus from being able to access your computer and perform tasks such as locating personal data, manipulating or deleting files, or using your computer to attack other computers.
2. **Remove the malicious code** - If you have anti-virus software installed on your computer, update the virus definitions (if possible), and perform a manual scan of your entire system. If the software can't locate and remove the infection, you may need to reinstall your operating system, usually with a system restore disk that is often supplied with a new computer. Before taking this step you should let InfoGuard attempt to resolve the issue because reinstalling or restoring the operating system typically erases all of your files and any additional software that you have installed on your computer.

### **How can you reduce the risk of another infection?**

Dealing with the presence of malicious code on your computer can be a frustrating experience that can cost you time, money, and data. The following recommendations will build your defense against future infections:

- **use and maintain anti-virus software** - Anti-virus software recognizes and protects your computer against most known viruses. However, attackers are continually writing new viruses, so it is important to keep your anti-virus software current.
- **change your passwords** - Your original passwords may have been compromised during the infection, so you should change them. This includes passwords for web sites that may have been cached in your browser. Make the passwords difficult for attackers to guess
- **keep software up to date** - Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.
- **install or enable a firewall** - Firewalls may be able to prevent some types of infection by blocking malicious traffic before it can enter your computer. Some operating systems actually include a firewall, but you need to make sure it is enabled.

- **use anti-spyware tools** - Spyware is a common source of viruses, but you can minimize the number of infections by using a legitimate program that identifies and removes spyware.
- **follow good security practices** - Take appropriate precautions when using email and web browsers so that you reduce the risk that your actions will trigger an infection.
- **have a tested backup and recover plan**- As a precaution, maintain backups of your files on CDs or DVDs so that you have saved copies if you do get infected again.
- **contact InfoGuard to provide a free Risk Assessment.** InfoGuard can easily find the most common vulnerabilities and provide advice on how to run a safer more reliable computer system