

# FACTSHEET

## Preventing Viruses, Worms & Trojans



### What is Malware?

The term malware encompasses 3 main types of unsolicited, unwanted computer intrusions:

- Viruses - self-replicate to spread, use a host program
- Worms - self-replicate to spread, do not need a host, and spread via networks
- Trojans – do not replicate, often contain hidden intent

### Viruses

A virus is a computer program or code that attaches itself to a "host" program on another computer. It then makes copies of itself and tries to spread to other computers. To qualify as a true virus, a program must be able to self-replicate. When the host program is shared with another computers and the host program code is run, the virus is executed. Not all viruses are destructive to computer programs or data.

Common modes of transmission include:

- Email attachments – most popular
- Social engineering (tricks that rely on human nature)
- Shared disks (floppy, flash drives, external hard drives, CD's)
- Macros and Visual Basic scripts
- File sharing applications
- P2P (peer-to-peer) such as BearShare, Gnutella, KaZaA, Limewire, Morpheus, etc.

Other modes of transmission that are less common, but on the rise include:

- IM (Instant Messaging)
- Cell phone viruses

### Worms

A worm is a stand-alone program that does not need a host program to replicate and spread. It typically modifies the operating system to become part of the boot process and it can also write changes to the registry. Unlike most viruses, worms can travel and spread via networks.

Common modes of transmission

- Social engineering (tricks that rely on human nature)
- Email attachments
- Over networks/Internet
- Exploits of security vulnerabilities and bugs found in applications



## Trojan (Trojan horse)

A Trojan, in the world of computers, describes a harmful program disguised as a helpful one. A Trojan is sometimes defined as any program with hidden intent. They may be attached to and hiding behind a legitimate program or be a program whose intent is misrepresented. Trojans do not self-replicate, but can be used to spread, activate, or hide other viruses.

Common modes of transmission include:

- Social engineering
- E-mail attachments
- Seemingly harmless links on web sites or pop-up windows

A **RAT** is a type of Trojan that gives a hacker full access to your computer whenever you are online. Once installed, RATs:

- Can delete, add, or transfer files and programs
- Can control mouse and keyboard
- Often include key-loggers

Keyloggers track, record, and reply back to the hacker with the text of everything you type, including passwords and bank account numbers and credit card information.

One of the most dangerous and difficult types of Trojans to detect and remove is the **Backdoor Root Kit**. These contain hacker tools that create a backdoor into your system, giving the hacker "root" (administrative) access to your computer. The tools then cover their tracks, making the hack very difficult to detect and remove.

---

## Protecting Your Computer and Identity

Fortunately, protecting your computer from unwanted intrusions is simpler than you may think. With a few simple steps and adjustments to how you think about surfing and downloading from the Internet, you can increase your computing safety dramatically. Listed below some common-sense steps and tips you can take increase you computing safety.

### **Antivirus Software- Install it and keep it up-to-date!**

Most antivirus software can be set to automatically update the virus definition files and you should use this feature. If you're using Trend Micro Worry Free products, definition files are automatically updated from the UITSC server.

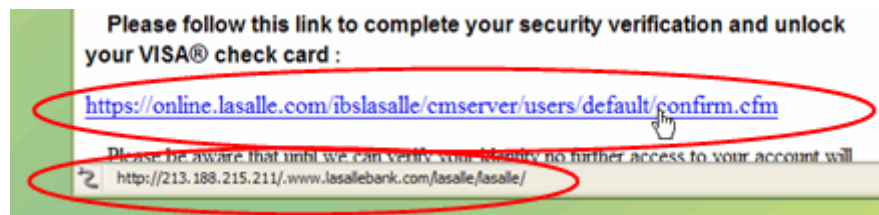
### **Keep software, such as Microsoft XP Microsoft Office, Internet Explorer, Mac OSX.x, and Firefox patched and up-to-date.**

### **Use a complex passwords**

### **Install and use a firewall.**

### Be a suspicious user.

- Email attachments - Don't open attachments directly from your e-mail. Instead, save them to a location on the hard drive where your virus scanner will have the opportunity to examine it before you open it.
- Be cautious when clicking on links in emails. To preview the true link path, hover your mouse cursor above the link and looking at the bottom of your email window. If the URL appears to be garbage text or includes a long string of numbers before the actual link, it's probably not legitimate.



- Never “unsubscribe” to junk by clicking a “remove me” link in an email. “A 2002 study performed by the FTC demonstrated that in 63% of the cases where a spam offered a “remove me” option, responding either did nothing or resulted in more email”. - <http://www.webroot.com/resources/spywareinfo/glossary.html>
- Consider a “trash” email account to use for web registrations.

### Be a cautious Internet surfer.

- Do not click “Yes” or “No” or “Cancel” on pop-up windows. Clicking can cause a drive-by download, where software is dropped onto your computer, without your knowledge, no matter which of the three responses you choose. Instead, find the page on the Taskbar, right-click on it and select **Close**.
- Use the built-in popup blockers that come with most current Internet browsers.

### Be a conservative and informed downloader.

- If it's free (and the site doesn't end in .org), be suspicious.
- Do your homework.
- Do a search on the product/service name.
- Look to user forums for the true story.
- Take the time to read the license agreement – be suspicious of extremely long ones.
- Take your time installing applications and look for tricks that ask you to sign up for email notifications or install other applications (browser toolbars, desktop weather info, etc.).



## Recognising the Signs

How can you tell if your PC has been compromised by an intrusion, virus, worm, or excessive amount of adware and spyware? The most common signs are:

- Your browser home page has changed and reverts to the new one after reboot, even if you manually change it.
- Mistyping a URL redirects you to an odd (sometimes pornographic) web site.
- You have new toolbars, favourites and/or icons on your desktop without any action by you.
- Some sites, such as Microsoft Updates or reputable antivirus and spyware removal sites no longer connect/function. Clicking their links leads you to what appear to be junk sites.
- Tons of pop-up ads – may even pop up when you aren't actively on the web.
- You're PC slows to a crawl and takes forever to boot.
- If your intrusion includes viruses, your antivirus software may also be disabled or unable to update.

If you suspect the worst has happened, contact us immediately. We have the tools to analyse your PC and can prescribe the best next step.