

*Information and tools for users of technology*  
*Feel free to share this document with your friends and colleagues*  
Email us at [info@triella.com](mailto:info@triella.com) • Call us at 647.426.1004 • More articles [www.triella.com](http://www.triella.com)

## Best Practices for Protecting Against Malware

*Protecting your home and office computer from malware helps us all.*

Malware, short for malicious software, refers to any undesired software installed on a computer whose purpose is to infiltrate the computer and serendipitously compromise the security of that computer. It also covers spam. A few short years ago, the biggest worry relating to malware was whether a station was going to get a virus which could cause email broadcasts to your contacts or a piece of spyware that would cause numerous pop ups on the computer. In those days, it was obvious when the computer was infected. Nowadays, a computer can be infected and the user would not even know it.

In the office, we set up systems to protect our computers from malware. These systems can include:

1. An external email firewall to prescreen email before it enters the firm.
2. An internal firewall as a first defense against hacking and depending on model and capability, to shut down potential intrusions, scan for and eliminate malware in real time and block URL's known to contain infections, among many other things.
3. Sophisticated antivirus software on the servers, email system and desktops.
4. A set of backup strategies for recovering data should all of the above systems fail in protecting the infrastructure.

In addition to ensuring that all of the aforementioned items are in place, the following are also good practice:

1. A systematic sweep of all systems should be completed every 6 months to ensure that remote access programs such as GoToMyPC or Logmein.com, to name two examples, are not installed. These programs bypass the protections in place at the firm and go directly to the end user PC. Anyone who compromises the remote software has immediate access to the entire network - and without any of the usual monitoring that would normally take place within a network.
2. Circulate the Computer Use Policy (or equivalent) document to all users within the firm to remind them of their obligations relating to computer security.
3. Check the firewall logs to understand the top 10 web sites being visited and whether there have been ongoing attempts to compromise the system.
4. Apply patches for known vulnerabilities promptly.
5. Consider some level of locking down workstations to protect users from themselves.

At home, users often do not have any protection on their computers, or rely on a host of free products to provide protection. The users of home computers tend to be less sophisticated in their ability to deal with computer related issues and therefore are more likely to go to sites that could cause infections.

In fact, it is the home computer market that is driving the spam and malware market. Unprotected computers (or computers that lack adequate protection), are often co-opted into providing services for the spam and malware disseminators whose primary purpose has changed from personal recognition to profit.

And getting infected is simple. Visit an infected website, respond to a pop up and the computer is infected! Once infected, the malware can contact other web sites in stealth mode and download more sophisticated malware that can be controlled by external commands from a malware provider. Thus, if

such a provider needs to send out one million email messages, they can command the infected computers in their network, literally thousands of them, to send the messages for them. Similarly if an attacker wishes to prevent internet communications at a specific site, they can have the computers in their network overwhelm the target site with so many requests that the site essentially becomes unavailable.

As corporations we can help reduce the number of home computers that are infected by giving our home users the knowledge they need to secure their system. A secure home system would include:

1. A hardware based firewall.
2. A purchased “top 5” antivirus system. The top 5<sup>1</sup> products at the time of writing are:
  - a. BitDefender Antivirus
  - b. Kaspersky Antivirus
  - c. ESET Nod32
  - d. AVG Internet Security
  - e. F-Secure Antivirus
3. An alternate browser installed, such as Firefox, so that the user can get to a support web site for help should their machine become infected.

Protecting against malware is everyone’s concern for both businesses and home users. Taking these steps will help protect against infection. Should computers become infected, there are a couple of great free clean up tools available that will usually do a complete job in 30 minutes or less. They include:

1. Malware Bytes - available at [www.malwarebytes.org](http://www.malwarebytes.org)
2. Combofix - available at [www.bleepingcomputer.com/combofix/how-to-use-combofix](http://www.bleepingcomputer.com/combofix/how-to-use-combofix)

*Charles Bennett is the Principal Consultant of Triella, a technology consulting company specializing in providing technology audits, planning advice, project management and other CIO related services to small and medium sized firms. Triella is a BlackBerry Alliance Partner. Charles can be reached at [cbennett@triella.com](mailto:cbennett@triella.com) or 647.426.1004. For additional articles, go to <http://www.triella.com/publications.html>.*

© 2008, by Triella Corp. All rights reserved. Reproduction with credit is permitted.

---

<sup>1</sup> Based on TopTenREVIEWS.com, October 28, 2008.