

Protecting Your Computer From Malicious Code

Introduction

Since 2004 (and growing steadily since then) AusCERT has seen an increased level of threat in the use of Trojan horse malware to facilitate online identity theft. More than ever, it is critical that home users or SMEs (Small and Medium-sized Enterprise) without dedicated IT security support feel confident in the security of their computer before conducting any form of e-commerce or e-government transactions online. Examples of such transactions include accessing or updating your personal information on a government web site, filling in a web form to apply for personal documentation, conducting Internet banking or making online purchases.

Even if these transactions use SSL encryption (typically recognised by the presence of a golden padlock during the browser session), it is important for users to understand that it will not protect the leakage of personal information to an attacker, if their computer is already compromised with certain types of Trojan malware. Hence users should be aware that using e-commerce and e-government services involves a heightened risk that their personal identity information may be stolen, if they have not taken adequate precautions to secure the computer from which these services are accessed.

The results of the *2006 Australian Computer Crime and Security Survey* again show that malicious software (malware) continues to be one of the greatest threats to information systems in Australia. The most common form of attack reported by large and small organisations was infections by viruses, worms and Trojans.

Viruses and worms are well known forms of malicious code but Trojans, spyware and other types of attack tools and some mobile code also have the potential to harm the confidentiality, integrity or availability of your computer data or network, and can potentially cause more harm in terms of stealing your personal information.

Like other forms of computer network threats, malicious code continues to evolve and create new challenges for organisations seeking to protect themselves. But these challenges are not insurmountable and there are a number of practical and effective strategies to reduce the risk.

This paper outlines effective strategies that will assist in minimising the risk of harm to confidentiality, integrity and availability of your computer data and systems when connected to the internet. It provides practical advice for protecting personal computers from malicious code for home users and organisations without dedicated IT staff. Most of the information provided is generic however some specific recommendations are included for Microsoft Windows, Apple Mac OS X, and generic Linux platforms.

Before You Start

Once an unprotected computer has been connected to the internet, it is difficult to guarantee that it has not been compromised. Therefore, installation and configuration of security software is most effective when applied to a fresh installation of the operating system which has not been connected to the internet. Once the computer is connected to the internet, the first thing to do is download and install the latest patches. Re-installing the operating system may destroy data on your system and should not be attempted if you are not confident with this type of operation. Following these instructions on a system which has been previously connected to the internet, while not as ideal, is still recommended.

Minimum Security Requirements (For The Impatient)

The following is a summary of what AusCERT considers the minimum required to secure a computer system for use on the internet. Further details are provided in the sections that follow.

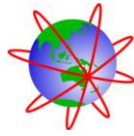
1. [Make sure you are running a supported Operating system.](#)
 - If using Windows 95, 98, ME or NT and connecting to the Internet, it is recommended you upgrade to Windows XP or Vista. Additionally if you are running Windows 2000, upgrading is advisable as some software (such as iTunes and QuickTime) is only updated for Windows XP and Vista. Microsoft has a [website](#) detailing various product life cycles.
 - If using a Mac, it is recommended you use Mac OS X 10.3 or later in order to be able to obtain the latest security updates (such as QuickTime).
 - If running Linux it is recommended to make sure you are running a currently supported distribution. For example Ubuntu lists support dates in the release notes (summarised on the [Ubuntu Wikipedia page](#)).
2. [Apply operating system patches, ideally via automatic updates.](#)
 - Windows systems should have Automatic Updates turned on in the Control Panel.
 - OS X systems should have Software Update (in System Preferences) set for automatic updates.
 - If your Linux distribution does not come with automatic updates, you should check for updates frequently.
3. [Perform day to day tasks under a user account with limited/reduced permissions.](#)
 - Windows guide for [adding users to Windows XP](#) and [to Windows Vista](#).
 - Apple has a guide for [adding a user](#), however both OS X and many Linux distributions require users to authenticate before allowing them to perform privileged tasks.
4. [Install and maintain security software: personal firewall, anti-virus and anti-spyware.](#)
 - Windows, OS X, and most Linux distributions come with an inbuilt firewall, however 3rd party firewalls are available which may provide extra functionality.
 - Windows Vista comes with Windows Defender, which is an anti-spyware tool.
 - A (non-exhaustive) [list](#) of firewall, anti-virus and anti-spyware tools is provided below.
5. [Install and configure anti-spam filtering software and/or consider using an ISP \(or email provider\) that performs spam filtering.](#)
 - Mail.app on OS X includes a [built in](#) spam/junk mail filter.
 - Outlook 97/98, 2000, 2002 (XP), 2003, and 2007 all come with a [built in](#) spam/junk email filter.

The [resources](#) section contains links to some popular tools which are free for non-commercial use.

Minimum Recommended Steps To Securing A Computer

1. **Make sure you are running a supported Operating system.**
 - **Microsoft Windows**

Microsoft no longer supports older versions of Windows. This means that they are no longer fixing security problems that may be found in the operating system. Many applications are also no longer supported under these operating systems and may not receive security fixes. Therefore anyone using Windows 98, ME, NT, or any prior version (such as Windows 95) should upgrade their operating system to one of the two fully supported ones: Windows XP (with service pack 2) or Windows Vista. These older operating systems from Microsoft also have features which make it easier for an attacker to steal stored secrets such as passwords or other data necessary to provide security for use in certain situations, such as when accessing e-government or e-commerce services. [\[1\]](#)



Windows 2000 is currently in an extended support period. This means that only security related updates are being released. This extended [support will end](#) on 13/07/2010. Before this date users should upgrade to Windows XP or Windows Vista. Further more, as many applications are starting to require Windows XP or Vista, upgrading sooner is recommended if you run any software that is no longer updated or supported for Windows 2000 (such as iTunes and QuickTime).

- **Apple Mac OS X**

Apple had two versions of their operating system: Classic and OS X. On their support website Apple still lists Mac OS 9, Mac OS X 10.2 and so on. Despite this Apple does not seem to be actively updating any classic OS versions (Classic or OS 9 and prior) and are [no longer supporting](#) it for emulation. Anyone running one of these versions (Classic and OS 9 or prior) should upgrade or disconnect from the internet.

Despite Apple listing Mac OS X 10.2 on the [support page](#), it does not appear to have any updates (including security updates) issued [for some time](#) - the last being in 2005 for the OS and 2006 for applications that run on it. Therefore anyone running OS X 10.2 should upgrade to 10.4 or 10.5 (if your hardware will support it).

The [support page](#) also lists 10.3, and the last security update for 10.3 was released quite recently. However over the coming months support for the 10.3 branch (or updates for applications that run on it) will probably be phased out. Therefore users should consider upgrading to 10.4 or 10.5 (if your hardware will support it).

- **Linux**

Most recent Linux distributions will provide some form of support schedule for the different releases. Ubuntu provides them in the release notes of each release (summarised in this [Wikipedia entry](#)). Fedora supported releases are listed on the [Fedora Releases](#) page.

2. **Keep software patches up to date for all applications and services in use on your network**

Some key applications (if used) are:

- Operating System and its Components
- Virus Scanner and Anti-Spyware Software (covered later)
- Web Browser
- Email Client
- Adobe ([Shockwave](#)) [Flash](#) Player
- Adobe [Reader](#)
- Sun [Java](#) Platform
- [iTunes/Quicktime](#)
- [Microsoft Office](#) or [Open Office](#)
- Other software that connects to the internet
- Other software you use to open files obtained from the internet or from an email

Not all email viruses use attachments in order to cause damage. Some email and web-based malicious code exploit vulnerabilities in host applications, which allow the code to execute (e.g. [Nimda](#) and Klez worms). Other malicious code exploits vulnerabilities in web browsers or attempts to trick users into installing the malicious software. This is often done by pretending to

be a security update or e-card. While most malicious code seems to target Windows, there is some that attacks Mac OS X and Linux, as well as many cross platform applications.

By applying relevant security patches for the operating systems, applications and services you have installed, you will mitigate the chances of being compromised by some form of malicious code or hackers seeking to remotely compromise your system. Information about the security vulnerabilities and patches affecting your systems can be found on the relevant vendors' web sites or from AusCERT. AusCERT also offers a free security bulletin service: the [AusCERT National Mailing List](#) as does [Microsoft](#).

The recommended strategy is to check for updates on an automated basis wherever possible. For example, Microsoft's Automatic Updates feature, when enabled on a machine, will automatically inform the user/administrator of the availability of new patches that should be installed. Mac OS X also has an automatic update feature that should be enabled (and is by default). Most popular distributions of Linux also come with an automatic updater.

Microsoft also provides (and it installs as part of automatic updates) a [Malicious Software Removal Tool](#). This software checks to see if prevalent malicious software is present on the computer and then removes the infection.

Both [Apple](#) and [Microsoft](#) provide a non-automated update web site. Linux distributions usually have some sort of [tool](#) for downloading and applying updates in a non-automated manner. Some of the common ones are: [Up2date](#), [Yum](#), [Synaptic](#), and [Aptitude](#).

3. Perform day to day tasks under a user account with limited/reduced permissions

When using your computer you should run applications you use with the least number or amount of permissions that it required. With this in mind, most (if not all) major operating systems provide limited or user (as opposed to privileged or super-user accounts). This then introduces the problem of running applications that require greater privileges, like installing programs. To solve this problem there are a few different [privilege authorisation features](#) built into most operating systems.

In Windows 2000 and later, operating with a limited user account (as opposed to an Administrator account) also limits the access available to malicious code, should a system be infected. This limited access may inhibit the ability of malicious code to operate effectively. Performing day to day tasks such as browsing the web, reading email, creating documents and playing games should be performed as a limited user. But installing software or manually updating Windows should be performed as an Administrator. Microsoft publishes information on using [limited user accounts](#) for Windows XP as well as the idea of [least privilege](#).

Windows Vista has a feature called [User Account Control](#). This allows a user with Administrator privileges to run as a limited user and only use the privileges when required. When this happens it is shown by a confirmation dialogue, or a password dialogue. This means that day to day tasks can be performed with a limited user account while still having easy access to run Administrator only tasks. Despite this it may still be beneficial for users to still run as a limited user.

All versions of Mac OS X have a feature similar to User Account Control called authorization services. This will prompt for the username and password of an administrator before running applications that require administrator privileges. This could be your current login details or those of a different user. Despite this we ([and Apple](#)) still recommend using a normal, or non-administrator account for common tasks.

Linux distributions often (but not always) have a very similar concept. Most major versions of Linux will prompt a user for an administrator password before allowing them to perform some tasks. If this is not the case with your distribution, then you should run as a limited (or normal) user and use [sudo](#) (or a graphical version like kdesudo or gksudo) to elevate your permissions.

4. Install a personal firewall and configure it to allow only essential connections

A firewall is [a bit like](#) a (hopefully) unclimbable fence with a guard at the only gate. You can tell this guard who (or what) to let in and out. This way if you leave a window open the guard (and fence) should stop anyone from being able to get into the house using the window, even when you are not there.

A firewall blocks access to services on your computer except for those you permit. Generally, computers being used for email and web browsing do not need to allow any incoming connections. However, Internet chat (e.g. ICQ or MSN Messenger), peer to peer (P2P) and online gaming systems may require incoming connections to function correctly. Blocking incoming connections will protect your computer from worms, such as [MSBlaster](#).

Some firewall products will also restrict outbound access from your computer to the Internet. The firewall will need to be configured (or trained) to allow the necessary outgoing connections, such as domain name service (DNS) look-ups, the sending and retrieving of email and web browsing. Also, some firewall products provide integrity checking to warn the user when programs are being replaced on your computer.

Windows XP and Vista both come with a firewall built-in to block incoming connections (though this was not enabled by default prior to XP Service Pack 2). Microsoft has information on [understanding](#) and [using](#) the Windows Firewall.

Mac OS X also has a [built in](#) firewall. It is enabled by default and most of the time is automatically configured according to the other settings you make in System Preferences.

Linux has many different firewalls available, some distributions enable them by default others do not. Some of the more common firewalls you will see in Linux are [Firestarter](#) and [Firewall Builder](#). Firewalls can also be configured from the command line.

If you are operating a small network for business or home use with a number of hosts, then you may need additional forms of firewall protection such as a gateway or border firewall. This will help to protect the network and the services offered on the network from users on the internet.

It is important to note that a computer should have **only one** personal firewall product installed.

5. Install anti-virus software, configure automatic updating, and perform weekly scans of your computer

Having anti-virus software that has expired or is not being updated at least daily will not protect against new viruses or Trojans that have been released into the wild since the last update. Viruses, Trojans and other malware (as of 2007) have around [372 new samples detected each day](#). This means that for every day (including weekends) that you do not update your virus scanner, around 400 new pieces of malicious code have been discovered that could infect your computer.

It is also possible you may already have a virus, Trojan or other type of malicious code on your system performing harmful activities without your knowledge. Even if you are running up to date anti-virus software there is always a delay between when a new Trojan, virus or worm is discovered in the wild, when vendors can develop a signature for it and when the client installs the new signature. For rapidly propagating worms and viruses this delay is often sufficient to cause widespread infection. By conducting regular scans you may be able to identify whether you have received a virus or other malware, by email or other source, which your anti-virus software did not detect and quarantine at the time of entry. For this reason it is a good idea to keep all expected email attachments and downloads for a week or so before using or installing them (if possible). This will increase the probability that a new virus definition has been created.

For individual files you may be worried about, websites like [VirusTotal](#) provide the results of over 30 different virus scanners. While this is not a substitute for a virus scanner on your computer, it can provide more information about a suspicious file.

For computers running a version of Microsoft Windows it is absolutely essential to have an up to date virus scanner installed. Most malicious software is written specifically for computers running some version of Windows.

Despite Mac OS X and Linux being targeted less, there are still many different forms of malicious software, applications, scripts, and web pages out there which target those systems and many of the applications they run. Therefore if you are running Mac OS X or a version of Linux, an up to date virus scanner is still highly recommended.

A computer should have **only one** anti-virus product installed.

6. Install spyware scanners, configure automatic updating, and conduct weekly scans of your computer

Spyware scanners do what anti-virus software often does not; they detect and protect against a variety of "legitimate" tools which can be installed on your system by attackers for malicious purposes. Much spyware collects profile information about your web browsing activities for the purposes of enhancing advertising but some spyware can install remote access software and keystroke loggers which can directly harm your systems or be used to compromise or harm other people's systems, and identify your computer or network as the source of the attack.

It is possible (even advisable) to install multiple anti-spyware products. This is recommended as different products have different sets of spyware they can detect.

7. Install and utilise spam filtering software for use with your email client

Spam is unsolicited bulk e-mail (junk email) that often advertises products or services. It can sometimes be explicit and offensive in nature and is increasingly used as a vector to spread malicious code. By reducing unwanted spam from entering your inbox, you reduce the risk of compromise by malware.

Spam filtering software uses pre-defined rules to determine what is and is not considered to be spam. By scanning incoming email looking for certain characteristics it determines whether the email is likely to be legitimate or not, and either blocks the email or allows it to pass accordingly.

While spam filtering software can be useful for helping to identify spam email, it will not successfully block all spam email. For this reason, do not assume that an email delivered to your inbox when using spam filtering software is legitimate, even if it appears to have originated from sources you know and trust.

Mail.app on OS X includes a [built in](#) spam/junk mail filter. Outlook 97/98, 2000, 2002 (XP), 2003, and 2007 all come with a [built in](#) spam/junk email filter. Some Internet Service Providers (ISPs) offer spam filtering services and most web based email services have some form of spam filtering.

Additional Steps To Secure A Computer

8. Don't open attachments or click on links in suspicious email or visit suspicious web sites.

Just as important as the technology counter-measures are good practice counter-measures, these are the things that users and system operators can do and are important. There will be times that when despite your best efforts to keep your anti-virus, anti-spyware and system patches up to date, vendors will not have developed the signatures or the specific patches required for protection.

Describing what is 'suspicious' is difficult, but this is where your instincts will help. Programs and people can forge email 'From' fields (ie change the 'From' field of the source of the email) so that tracking the source of the email is difficult and it helps to confuse the recipient. Viruses can send infected emails from legitimate email addresses of people you know by collecting addresses from infected systems. For this reason, the email 'From' field provides only limited clues as to its potential to contain a virus or links to malicious web sites.

Look also at the body and subject of the message. If the email is from somebody personally known to you or your organisation, is the message content and subject line consistent with what you would expect that person to email you about? If words are misspelt; if there are grammatical errors; or the expressions used are culturally inconsistent such as *"watchin' the game, having a bud"* or referring to imperial measurements when it is common to use metric measurements, then these are likely to be clues to regard the email with suspicion, in which case you should delete it without opening the attachment or clicking on any of the links it contains. If you don't personally know the person named in the 'From' field and the message was not expected then delete it. If you do know the person, then it would be a good idea to contact them and check they did in fact send the email before opening the attachment, clicking on the links it contains or replying to it.

Be particularly wary of social engineering plays, ie messages which are designed to increase your curiosity, concern or interest in opening the attachment or clicking links. For example, some of the random messages contained in the Fizzer worm were: *"the attachment is only for you to look at; you must not show this to anyone and if you don't like it, just delete it"*; others have claimed *"you are under police investigation, click here to learn more"*

9. Configure instant messaging software to allow only those on your contacts list to send you messages

Equally as important as blocking unwanted emails is blocking unwanted instant messages. Some malicious code uses instant messaging software such as Windows Live Messenger (previously MSN Messenger), AOL Instant Messenger, Yahoo! Messenger, ICQ or Skype to spread.

The following guides show how to configure your instant messaging software to block unsolicited instant messages for [Windows Live Messenger](#), [Yahoo! Messenger](#), [AIM](#), [Skype](#) and [ICQ](#).

10. Configure email clients to block potentially harmful content and attachments and possibly turn off the 'Preview pane'

In the past, some email clients have exhibited vulnerabilities which allow malicious code to execute automatically as they are previewed. Additionally, HTML email may download and execute potentially harmful mobile code such as Java, JavaScript, or display links to malicious web pages that can appear harmless to the user.

As a general rule don't open attachments with any of the file extensions .exe, .com, .pif, .scr, .vbs, .js, .ocx, .shs, .reg and .bat. While this is a good rule, file extensions and icons can often be hidden, changed or faked so it is good to be suspicious of all unexpected email attachments. Some email applications, such as newer versions of Microsoft Outlook, block certain types of potentially harmful email attachments, and for other types of attachments, require the user to save the attachment to disk before it can be opened. The latter allows the user to scan the file before opening it if your anti-virus software is not integrated with your email program. Microsoft provides [further information](#) about these features. Thunderbird by default will [not execute](#) any scripts that are contained in an email message.

Many webmail services (such as Hotmail, Gmail, and Yahoo! Mail) provide attachment virus scanning and stop users from clicking on potentially harmful content in email messages. However this does not mean that users should be any less diligent in checking that the email is legitimate.

11. Configure browser settings to be as secure as possible

Surfing the net can be as dangerous as reading your email - if you don't take precautions. ActiveX controls, Java, JavaScript, Flash and Shockwave are all forms of mobile code which are designed to enhance the web experience when you view a web page but all have the potential to harm your systems. Unlike worms, viruses and Trojans which are inherently malicious, mobile code for the most part performs a legitimate and harmless function. It is possible, however, for attackers to embed malicious mobile code within their web pages so that when unsuspecting users access a web site through their browser, the code is automatically executed on the client machine. Some anti-virus software can help protect against malicious mobile code.

While various browsers use different naming conventions, those that support scripting controls also provide mechanisms for disabling them. Firefox allows users to control [images, Java, and JavaScript](#) from the options window. If this is not enough control then there are Firefox extensions (like [NoScript](#)) that can block or allow specific sites' scripts. [Safari](#) and [Internet Explorer](#) both allow you to disable JavaScript (and other active content).

An *iframe* is an HTML tag which allows another document (possibly from a completely different web site) to be displayed in the current web page. While harmless on their own, they provide an easy way for malicious code to be added to a web page. Iframes can be hidden from the user while still loading a potentially malicious webpage and executing the scripts they contain. These scripts often attempt to download other malicious code onto the users' computer. The term [Drive-by Download](#) is often used to refer to situations when a web site attempts to download and execute files without the knowledge of the user.

12. Consider using a different web browser

During 2004 and the beginning of 2005 AusCERT saw a sharp increase in Trojan attacks with the sole purpose of capturing credentials for financial transaction sites (such as Internet banking). The vast majority of these attacks attempted to exploit vulnerabilities in Internet Explorer. For this reason using a different web browser was often a good idea.

More recently (2006 to 2008) many of these web pages have been written to determine what browser version is being used and use an exploit that the specific browser (or one of the plug-ins used by the browser) may be vulnerable to. So while using a different browser version may offer a little protection, it is far more important to run an up to date browser. It is also a good idea to enable or configure additional security precautions for the web browser you choose (things like NoScript and using Internet Explorer Security Zones). This will help to limit the mobile code (such as Java and JavaScript) which can be executed by this browser.

13. Consider using a modem/router device

There are now an abundance of affordably priced modem/router combinations available within Australia, particularly for broadband access (whether ADSL or Cable). By purchasing a dedicated device that handles the internet connection, your host computer is no longer directly connected to the Internet, thus providing some protection against many automated attacks.

Recovering From An Infection

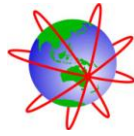
The old adage 'prevention is better than cure' is especially true for malicious code. Depending on the nature of the malicious code, the solutions to recover will vary. If you believe you may be infected, the key is to correctly identify the nature of the malicious code and apply the recommended recovery solution. For some types of malicious code, recovery may simply require a reboot or the use of a purpose-built removal tool. Anti-virus vendors' web sites may assist in providing specific advice. Microsoft has released a [malicious software removal tool](#), which can remove several variants of malicious code on Windows 2000, Windows XP, Windows 2003 and Windows Vista systems.

If the malicious code has installed a back-door, gained administrator level access or changed system files, then the integrity (not to mention confidentiality or availability) of your system has been fundamentally damaged. This means you can no longer trust the operating system, applications or data files. The best solution is to ensure you have a backup of your data and then format the hard drive, reinstall the operating system and applications from trusted media and data files from back-up media. If ever in doubt this is the one sure way to return a system to a known good state. Be careful though, if recovering from a backup, the backup *may also* be compromised. It is advisable to also scan the backup media before restoring the files.

For more information on recovering from a Trojan or virus infection, see '[Computer viruses: description, prevention, and recovery](#)' and AusCERT's [Windows Intrusion Detection Checklist](#) for Windows systems, and [Steps for Recovering from a UNIX or NT System Compromise](#) for Linux systems.

References

1. Howard, M and LeBlanc D (2003) *Writing Secure Code*, 2nd Edition, Microsoft Corporation, page 315
-



Resources

Most of the following links are to software that is free for non-commercial use. AusCERT provides these links as is and does not support these vendors in anyway. Questions or support inquiries regarding these products should be directed to the appropriate vendor, not AusCERT.

Anti-Virus

- [AntiVir](#)
- [Avast](#)
- [AVG](#)
- [Clam AntiVirus](#)
- [F-Secure](#)
- [Kaspersky Anti-Virus](#)
- [McAfee VirusScan](#)
- [Norton AntiVirus](#)
- [Sophos Anti-Virus](#)
- [Trend Micro Internet Security](#)
- See [Wikipedia](#) for a larger listing.

Anti-Spyware

- [Ad-Aware](#)
- [Windows Defender](#)
- [Spybot Search & Destroy](#)
- [Spyware Doctor](#)
- [HijackThis](#)
- [Spybot Search & Destroy](#)
- [SpywareBlaster](#)
- [MacScan](#)
- See [Wikipedia](#) for a larger listing.
- **Avoid [Fake Anti-Spyware](#) programs.**

Personal Firewalls

- [CA Personal Firewall](#)
- [CORE FORCE](#)
- [Kaspersky Internet Security](#)
- [Kerio WinRoute Firewall](#)
- [Windows Firewall](#)
- [Zone Alarm](#)
- [ipfirewall](#)
- [netfilter \(iptables\)](#)
- [PF \(packet filter\)](#)
- [IPFilter](#)
- [Comodo Firewall](#)
- See [Wikipedia](#) for a larger listing.

Web Browsers

- [Internet Explorer](#)
- [Firefox](#)
- [Netscape](#)
- [SeaMonkey](#)
- [Opera](#)
- [Safari](#)
- [Konqueror](#)
- [Epiphany](#)
- [Camino](#)
- [Maxthon](#)
- [K-Meleon](#)
- See [Wikipedia](#) for a larger listing.

Spam filtering software

- [SpamBayes](#)
- [SpamPal](#)
- [POPFile](#)
- [MailWasher](#)

Revision History

18 August 2003 Initial version

16 May 2005 Major structural modifications and updates of content.

1 February 2008 Apple Mac OS X and Generic Linux additions. Update of content.