SECURING PERSONAL COMPUTERS

[A Proactive Approach]

Author: Aman Hardikar M, amanhardikar@yahoo.com

Date: April 30th 2010
Version: 2.3

Abstract

This paper is part of a community effort to help home users and students secure their personal computers. Due to lack of security awareness, a large number of users face multiple risks including virus infection, hacking, phishing, social engineering, identity theft and various other attacks. Well known security software (ones that are commonly advertised) that can protect the computers usually require some financial investment (before use and mostly have yearly recurring license cost) and certain amount of technical proficiency to use the software for protecting the system. Many users either aren't aware or may not be able to afford (students) investing in various security products. This makes them an easy target for cyber criminals and usually ends up as victims of identity theft and fraud. This paper tries to make the user aware about why and how he/she needs to protect the system they are using. It discusses methods to protect the system using freely available software and create a minimum security baseline. A brief introduction about the basic technologies involved is discussed followed by the construction of a secure network using the technologies discussed. It is concluded by giving some of the best practices that a user having personal computer(s) can follow to stay safe online and be a responsible computer user.

1. Introduction

1.1. Purpose of this paper

The paper tries to explain the home users and students about what, why and how of securing the system. By these it tries to increase the awareness of the user about the various security issues that are required to protect their system from various threats. It talks about the basic set of tools or software that are required to secure their computers to a moderate level from viruses, hacking, identity theft and other threats. These tools mitigate majority of the threats that are faced by home users. Multiple other tools / software also exist that mitigate only a particular granular threat and advanced users might be interested in researching about them.

All the tools or software discussed in the paper are “FREE FOR PERSONAL USE”. So, home users need not invest to procure and use the software mentioned. It is hoped that this paper would encourage the home users to secure their systems, in turn reducing the spread of viruses among peers and help avoid identity theft.

Most home users systems are infected by new viruses that are released every day. The average rate of new viruses or variants being released is currently at 1 every 1.5 seconds as reported by Trend Micro in the E-Crime Congress, UK 2010. The infected systems in turn are used for most of the malicious purposes on the internet, without their owner’s knowledge. Though the majority of the home users have an antivirus software to protect their systems from these malware, they still end up getting infected. This is because the antivirus software is most often outdated or is an expired 3-month free / OEM version or has an invalid license. This affects the efficiency of the antivirus software in detecting malware and as a result, it most often does not function as expected or advertised.

The majority of the present attacks are through connection to the internet and are sophisticated enough to evade most of the traditional security tools. As there is no control on the information posted on the internet, any user visiting a web page with malicious scripts can get infected without their knowledge as the scripts are executed in the background by the browser performing evil activities.

Viruses and hacking nowadays have become so complex that simple antivirus software cannot protect the system from all these blended threats. We need to look at certain other tools or software to handle these threats and stay protected.

1.2. Attacks/Risks for Home Computers

The various attacks that are faced by home users are grouped into three categories, namely, **Malware, Hacking and Identity Theft**.

Malware: There are many types of malware, but for the sake of simplicity we will be referring to them as viruses. The numbers of new viruses being created are increasing exponentially. The risks from virus infection include corruption of files, slowing down of the system, annoying popup and theft of personal information (leading to identity theft). The biggest threat faced by infection of viruses is the exposure of the system to botnets (large network of compromised computers) that use them for malicious purposes like doing mass scale attacks on targets which include companies and governments, generating spam and storing illegal materials like pirated software and music, pornographic (including pedophilic) material that are available over the Internet without the owner’s permission or knowledge.

Hacking: This attack mainly involves actively stealing credentials and taking control of accounts on websites, taking control of systems and either destroying or denying access to the original owner. This is now increasingly performed by using highly sophisticated scripts that are automatically executed when a web page is opened.

Identity Theft: Theft of any personal information that can be used to spoof the identity of the victim is known as Identity Theft. Social Engineering is a type of attack where the attacker convinces the victim to perform a particular action whose impact is not known to the victim. Examples include disclosure or theft of sensitive information by clicking a link or by talking. Phishing is a very popular attack mainly targeting e-banking customers. It involves luring customers into giving their credentials on an identical site. This most commonly involves an email sent to the customers asking for some action (like verification or updating of their account information) with a link to the imposter bank site.

2. The Basics

Before going into how we can protect our home computers, let us first look at some of the basic technology that is used to secure our home computers.

2.1. Antivirus

An ANTIVIRUS is a piece of software that detects and prevents any malicious program (virus or hacking tools) from infecting other files on the system. It helps the user in verifying whether a program or file is safe to be run on the system. It detects these malicious program using both the signature based and heuristics technologies. Heuristics is a technology that can identify a malicious program by its behavior and is a technology that is currently basic and is actively being developed at present.

Every malicious program can be identified uniquely by using a signature. This signature is generated by using part of a code in the program that distinguishes itself from others. If any program has this code present in it, it is identified as infected by the respective virus. Due to this reason, antivirus updates that contain all the signatures for the latest viruses are very important. If the signature of a virus is not present with the antivirus software, it might not be able to detect the malicious software. If there is no internet connectivity, manual update of signatures must be performed. All the vendors provide downloadable signature update files for performing manual update. The main reason why an update is required even when the system is not connected to internet is that viruses can also spread via the use of removable media such as USB flash drives, disks (CDs and DVDs) and hard disks. Most of the viruses create an autorun.inf file in the USB device that runs automatically when it is connected to a system. Through this they get executed on all the systems on which the USB is used. If the USB is used for document transfer to or from Internet (cyber cafes), there is a high probability that a new virus might have copied itself to the USB as the systems in the cyber cafes are generally fully exposed to the public and access is not controlled.

Most of the hardware vendors ship their systems with a pre-installed OS that also has a trial version of Antivirus software. Once the trial period is over, the software still works; but, it will not be allowed to get updates without paying for the license. While some folks try and make do with pirated (illegal) antivirus software, they are usually still unsafe as most of the time the antivirus vendor blacklists (blocks) the pirated license keys. So, when the antivirus software contacts the vendor site for updates, the pirated key is detected and the license is withdrawn. This blocks all the necessary program and signature updates.

There are few antivirus vendors who offer their software free for personal or home use. They are the same as the commercial products but without the bundled features. Some of the software that are available for free is listed in the below table along with the URL from where they can be download.

PRODUCT	REMARKS, DOWNLOAD URL
MICROSOFT WINDOWS (2000, XP, VISTA, 7)	
Comodo Internet Security	http://www.comodo.com/home/internet-security/free-internet-security.php
Avira Antivir	http://www.free-av.com/en/download/index.html
AVG	http://free.avg.com
Avast	http://www.avast.com/eng/avast_4_home.html
LINUX & UNIX	
BitDefender	http://www.bitdefender.com/PRODUCT-80-en--BitDefender-Antivirus-Scanner-for-Unices.html
Avast	http://www.avast.com/eng/avast-for-linux-workstation.html
AVG	http://free.avg.com/ww-en/download?prd=afl
F-prot	http://www.f-prot.com/products/home_use/
APPLE MAC OSX	
ClamAV	http://www.clamxav.com/
iAntiVirus	http://www.iantivirus.com/

Table 1: Antivirus Software that are "Free for Personal Use"

Comodo Internet Security is the only free security suite that is available for both 32bit and 64bit MS Windows home users. **BitDefender** is the only free Linux based antivirus software with an inbuilt GUI mode. The antivirus (anti-malware) that is now included in the latest version of Mac OS X is limited in functionality at present. So, it is recommended to install third party antivurus software for better security.

If a file is downloaded from a site that is not trusted, it can be scanned using multiple antivirus engines. Even if the antivirus installed on the system does not identify, the virus (if present) might still be detected by other antivirus software through this procedure. The following table gives few of the popular sites / services that can be used for free. However, installation of multiple antivirus software is not recommended as it affects the stability of the system.

SERVICE	URL	SERVICE	URL
VirScan	http://www.virscan.org	**Filterbit**	http://www.filterbit.com
VirusTotal	http://www.virustotal.com	**VirusScan**	http://virusscan.jotti.org
VirusChief	http://www.viruschief.com	**Virus.org**	http://scanner.virus.org
Novirusthanks	http://scanner.novirusthanks.org		

Table 2: Free online multiple antivirus file scanning services (9-39 AV scanners)

2.2. Firewall

In the real world, a firewall is a barrier used to contain and prevent fire from spreading to adjacent areas. Similarly in the IT world, a FIREWALL is a device or software that prevents the spread of malicious traffic to adjacent networks. If the access is explicitly permitted / allowed, only then can traffic from the other side pass through the wall. This is achieved by the use of firewall rules. A rule is similar to a command issued to the firewall so that if the traffic meets the criteria of allowed traffic, only then it is permitted. So, a firewall is only as good as the rules that are set on it. An inbuilt firewall is present in most of the present day operating system. Microsoft ships its OS (MS Windows XP SP2 and higher) with a built-in firewall. But, the default settings reduce the security purpose of the firewall. Linux (most of the flavors) is shipped with IPTables, which is a strong firewall. But, configuration of these inbuilt firewalls is complex and requires advanced system level knowledge. For these reasons, additional firewall software installation is recommended. Gufw, Firewall Builder and system-config-firewall (redhat based) are few of the graphical firewall configuration utilities for configuring IPTables easily.

It is recommended to have a firewall on the system even though the network is protected by a network based firewall (mostly on the router). Both (network level and system/host based) firewalls complement each other and make the entire network secure. The following table gives few of the popular and efficient tools that are free for personal or home use.

PRODUCT	REMARKS , DOWNLOAD URL
MICROSOFT WINDOWS (2000, XP, VISTA, 7)	
ZoneAlarm	http://www.zonealarm.com/security/en-us/anti-virus-spyware-free-

Basic	download.htm
Outpost	http://free.agnitum.com/
Online Armor	http://www.tallemu.com/products-online-armor-free-overview.php
LINUX & UNIX (IPTables GUI Interface)	
Gufw	http://gufw.tuxfamily.org/index.html
Firewall Builder	http://www.fwbuilder.org/
APPLE MAC OSX	
(Inbuilt)	Has an inbuilt firewall with Graphical Interface

Table 3: Firewall Software that are "Free for Personal Use"

2.3. Sandbox / Virtualization

A SANDBOX is a technology / software that create an isolated area on the system for the programs / process to run. Any program running inside the sandbox can only access resources that are available inside the sandbox. This helps in controlling the access of web browsers and restricting them to a predefined set of resources. So, when a virus infection or a hacking attempt happens, it is controlled inside the sandbox. When such an event is identified, the sandbox can be destroyed erasing all the traces of the malicious program that have entered the sandbox. A new sandbox can be created and used as normal.

VIRTUALIZATION is a technology / software that create a simulated environment like simulated computer or network. Any program running in the simulated environment behaves the same way if were run on an actual environment (actual computer). The simulation is controlled by the software installed on the main operating system of the host computer and is not visible to any programs that are running in the simulated environment. So, when a virus infection or a hacking attempt happens, it is controlled inside the simulated computer and is prevented in most of the cases from spreading to other areas on the system. The virtual stores that host virtual computers or accounts can be destroyed, if they get infected. New virtual stores can be created and used as normal.

The following tables lists products that help home users in reducing/mitigating the risk from a majority of the web based attacks, both the old known ones and the new unknown ones using the technologies discussed above.

PRODUCT	REMARKS, DOWNLOAD URL
MICROSOFT WINDOWS (2000, XP, VISTA, 7)	
SafeSpace	User friendly; .Net Framework 2.0 required
	http://www.artificialdynamics.com/content/products/register-personal.aspx
Sandboxie	Supports only 32-bit; User friendly; Simplest of all
	http://www.sandboxie.com/index.php?DownloadSandboxie
RVS2010 Home	Very technical
	http://www.returnilvirtualsystem.com/rvs-home-free
LINUX & UNIX	
Plash	http://plash.beasts.org
Sandbox	Available in Fedora 12 (command line) – Uses SELinux
APPLE MAC OSX	
(Inbuilt)	Has an inbuilt GUI application called "Sandbox"

Table 4: Sandbox Software that are "Free for Personal Use"

PRODUCT	REMARKS, DOWNLOAD URL
MICROSOFT WINDOWS (2000, XP, VISTA, 7)	
VMWare	http://www.vmware.com/products/player/
VirtualBox	http://www.virtualbox.org/
LINUX & UNIX	
Xen	http://www.xen.org/
VMWare	http://www.vmware.com/products/player/
VirtualBox	http://www.virtualbox.org/
APPLE MAC OSX	
VirtualBox	http://www.virtualbox.org/

Table 5: Virtualization Software that are "Free for Personal Use"

2.4. Software Version Checker

SOFTWARE VERSION CHECKER tools are software that identify the applications/programs that is installed on a computer and lists all the software that is outdated or unpatched along with the link to the updated newer version of the software. They do this by creating the list of software and their version and comparing this list against the available list of software. If an earlier version is found, this tool adds it to the report along with the link to the updated or patched version of that software. Few software tools go beyond giving just links and give information regarding the level of threat, step-by-step procedures for installation.

Most of the malware and hacking attacks are performed by exploiting outdated and unpatched software. Due to this reason if the software is not updated, it can be exploited. Once the software running on the system get exploited, the virus or hacker gains control (by getting the permission level of the user logged in, which is usually administrator level) of the system and can then install other malicious code.

The main or critical part of any home computer is the Operating System or OS. Most of the operating systems come installed with their own OS update tools and these updates are very important for an OS from a security and functionality point of view. The OS must be patched immediately if any high security patches are released. In Microsoft Windows, "Windows Update" is one such tool. Linux update tools vary according to the flavour of the Linux distribution. Mac OS X can be updated using the Software Update tool in the operating system. Linux update tools also install the updates available for other non-system software programs/applications that are installed.

Below is a list of few tools that help in version checking of the installed software.

PRODUCT	REMARKS , DOWNLOAD URL
MICROSOFT WINDOWS (2000, XP, VISTA, 7)	
FileHippo Update Checker	Very simple to use; .Net Framework 2.0 required
	http://www.filehippo.com/updatechecker/
Secunia PSI	Very technical and detailed
	http://secunia.com/vulnerability_scanning/personal/
TechTracker	http://www.cnet.com/techtracker/
LINUX & UNIX	
(Inbuilt)	APT (Ubuntu, Debian) YUM (Red Hat, Fedora, SuSE)
APPLE MAC OSX	
(Inbuilt)	Uses "Software Update" for updating software

Table 6: Software Version Checkers that are "Free for Personal Use"

2.5. Secure Browser (Add-ons & Toolbars)

Some of the browsers have built-in feature for private browsing that do not store any browsing related information for the session they are enabled. It is called InPrivate in Internet Explorer, Private Browsing in Firefox and Incognito in Chrome. When private browsing is enabled, no information related to the site browsed (like history, cookies) are stored making it safe for sites with sensitive information like e-banking and e-trading.

Plugins in Firefox make it more secure than most of the other browsers. But, some of the plugins can also be malicious. So, it is recommended to only install plugins from a trusted site like Mozilla.org. Use of older plugins is also not recommended as bugs/vulnerabilities found in them can be exploited. Internet (Web) has become a major medium for distribution of malware. Browsing an infected web site is enough to lose sensitive information and also get infected. Most of the infection through web browsing happens through running active content (javascript, java and flash). “NoScript” plugin available at http://noscript.net/ blocks all the active content (javascripts, java, flash and other plugins) in a website unless they are permitted by the user. “Flashblock” is another plugin similar to NoScript that can block all flash based content unless permitted.

There is another class of software (addons/plugins/toolbars) that helps a user in identifying malicious websites and browse the web safely. They achieve this by marking sites as safe or unsafe and are displayed to the user when the user tries to visit the site. The sites are marked accordingly by the vendors who test them periodically for any malicious content.

SOFTWARE	URL
McAfee SiteAdviser	http://www.siteadvisor.com/
Web Of Trust	http://www.mywot.com/
Finjan SecureBrowsing	http://securebrowsing.finjan.com/
Browser Defender Toolbar	http://www.browserdefender.com/download/

Table 7: Freeware Add-ons/Plugins/Toolbars for safe browsing

2.6. Other Miscellaneous Tools / Software

2.6.1 Secure Data Store

One of the most important security feature required is a place to store all confidential data, similar to bank lockers in real life. This can be achieved by using a software called “TrueCrypt” that is available for Windows, Linux and Mac operating systems. It creates an encrypted volume from either a file or a partition or a device like USB drive / hard disk that can be used to store all sensitive data. It is very easy to use and has a simple GUI. It is available at http://www.truecrypt.org/

2.6.2 Secure Browser Password Management

The common problem faced by many users today is the password compromise. This partly happens as the users stores his/her credentials on the browser using the save password feature of the browser. With a login in a number of web sites, it is difficult to remember all the passwords on each of those sites. Due to this reason, most of the users save the passwords on the browser. This can increase the risk of password compromise through the use of scripts. To help reduce the risks from saving the passwords, a plugin called "Secure Login" is created. It is a Firefox plugin that integrates with password management feature on the browser and can mitigate some of the attacks by using whilelisting of sites for which scripts are allowed. It is available at https://addons.mozilla.org/en-US/firefox/addon/4429.

2.6.3 Anti-Keylogger Techniques

If trough an unfortunate event the system gets compromised, a key logger is installed in most of the cases. It is a software to capture all the activities on the system. Few of the malware are specifically designed to install a key logger that only monitors activity related to a particular event (like when the user does any ebanking on the system). The activity stored is then sent to the attacker. This software is one of the main tools used for password compromise. To mitigate this risk, a software called "KeyScrambler Personal" can be used. This software randomizes the characters in the sensitive areas during input, so that the keyloggers will only be able to capture the garbage. It is available at http://www.qfxsoftware.com/Download.htm. It is only available for Windows OS.

2.6.4 Parental Control

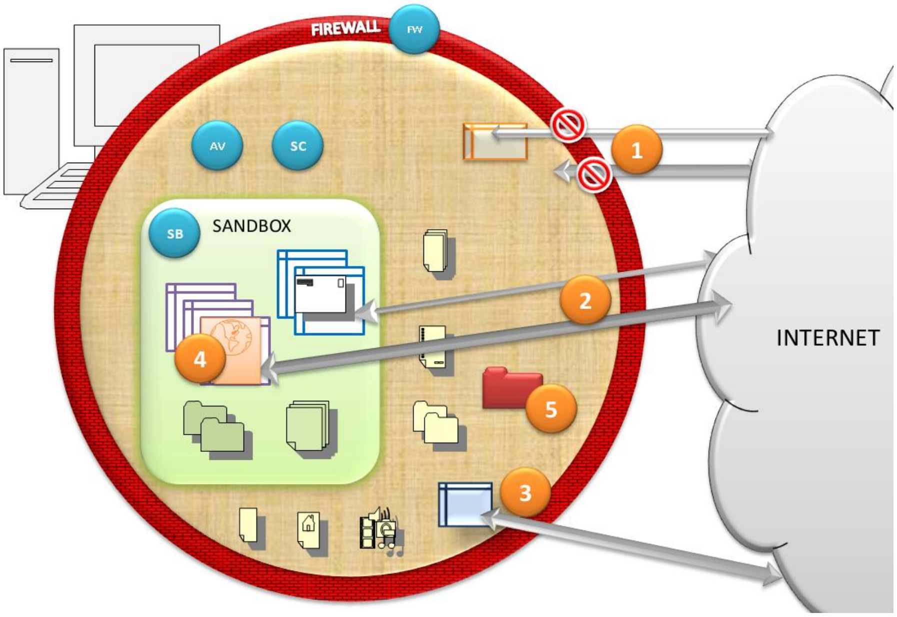
Parental control is a major concern due to the amount of unrestricted adult oriented content on the Internet. The following table (Table 8) lists some of the free software that are available to help parents control the access of content available to their children. Firefox plugins like Glubble (http://www.glubble.com) and Procon (http://procon.mozdev.org/) also help in parental control. Sites like Family Online Safety Institute (http://www.fosi.org), Cybersmart (http://cybersmart.gov.au) and software like Kidrocket (http://kidrocket.org) hosts lot of resources that help in good cyber parenting.

SOFTWARE	URL
Parental Control Bar	http://www.parentalcontrolbar.org/
K9 Web Protection	http://www1.k9webprotection.com/
SafeFamilies	http://www.safefamilies.org/

Table 8: Free Software/Add-ons/Plugins/Toolbars for parental control

3. The Setup

As discussed in the above section, we will be securing the home computer using the above mentioned software tools, namely, antivirus, firewall, sandbox, software version checker and by securing the browser and sensitive information.



1 Any traffic or connections from the internet that are not explicitly allowed are blocked by the firewall.

2 Applications like browsers (Firefox, Internet Explorer) started from the sandbox are allowed access to the internet; But they are kept inside the sandbox.

3 Applications like windows update are allowed access to the internet.

4 Secure browser for accessing the Internet.

5 Secure (encrypted) folder to store all sensitive personal information.

AV **ANTIVIRUS -** Scans the OS and alerts (and prevents), if a malware or malicious tools are found.

FW **FIREWALL** – Blocks any attacks that arrive through network by blocking inbound and Outbound connections.

SB **SANDBOX** - All access is controlled and is limited to the sandbox. The applications can interact with other applications or resources inside the sandbox.

SC **SOFTWARE CHECKER / SOFTWARE VERSION CHECKER -** Checks for any outdated software and provides information to download the patch or the updated software version.

The following table gives an example selection from the list of previously discussed security software.

ANTIVIRUS	FIREWALL	SANDBOX / VIRTUALIZATION	SOFTWARE CHECKER
MICROSOFT WINDOWS (2000, XP, VISTA, 7)			
Avira Antivir	Online Armor	SafeSpace	Secunia PSI
LINUX & UNIX			
Bitdefender	IPTables/Gufw	Plash	(Inbuilt)
APPLE MAC OSX			
iAntiVirus	(Inbuilt)	(Inbuilt)	(Inbuilt)

Table 9: Combination of products – Example Selection

Vendor sites and other community sites like Youtube can help in understanding the installation and usage of the selected software. Few of the software in the above list are easy to use, but present less information. They are good for home users who are not tech savvy and who cannot understand most of the information displayed. Few of the software in the list are very technical and need a medium knowledge of computers to understand the information displayed. They are complex and are not intended for home users with basic computer skills. The respective table in "The Basics" section (section 2, tables 1 to 7) above gives information/remarks about few of the software listed.

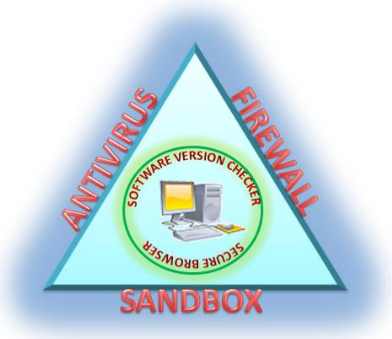
The following table summarizes the various attacks that can happen and the way various security tools discussed protect the system from these attacks.

ATTACK SOURCE	ATTACK	PROTECTION	EXPLANATION
USB Devices, MP3 Players and other USB based devices	Malware (Virus) Infection	Antivirus	Repairing, deleting or blocking access to malware or infected files
CDs, DVDs and other personally created media	Malware (Virus) Infection	Antivirus	Repairing, deleting or blocking access to malware or infected files
Hard disks (external or internal)	Malware (Virus) Infection	Antivirus	Repairing, deleting or blocking access to malware or infected files
Network (LAN)	Malware (Virus) Infection	Antivirus	Prevents infected remote files or processes from executing or running on the system
		Firewall	Reduces infection from worms (kind of malware) by blocking their traffic coming from the network
		Software Checker	Reduces infection from worms that infect computers by exploiting vulnerable software running on the system.
	Hacking	Antivirus	Identifies and prevents the execution of hacking tools
		Firewall	Prevents most of the attacks by blocking the ports
		Software Checker	Reduces the risk of getting hacked by reducing the number of vulnerable software running on the system.
	Stealing personal information	Antivirus	Identifies and prevents malicious software from execution
		Firewall	Prevents any software from sending information or connecting to non-permitted servers
Web Browsing	Malware (Virus) Infection	Antivirus	Identifies and prevents execution of some of the malicious scripts
		Sandbox	Reduces the infection to the scope/area of the sandbox
	Hacking	Sandbox	Reduces the availability of system resources that can be exploited
	Stealing personal information	Sandbox	Reduces the access of information available to applications inside the sandbox

Table 10: Various attacks and the protection mechanisms

4. Conclusion

This paper gives the minimum set of tools required to secure your computer. There are many other specific tools to protect against other threats such as infection from malicious sites, detection of malware (like rootkits and bots). But, most of the threats arising due to a network (internet) connection can be mitigated using the software/tools discussed. These tools increase the number of layers of protection making it hard to break into the system.



Staysafeonline (http://www.staysafeonline.info) and thinkuknow (http://www.thinkuknow.co.uk) are few of the web sites that help general computer users in using their computers efficiently, securely and responsibly.

The home users who are able to understand and implement these to protect their systems should help other home users in securing their system and make them security aware. This helps us all to enjoy a safe and peaceful use of computers and the related information technology.

BEST PRACTICES FOR SECURING HOME COMPUTERS

1. Install the above discussed security tools (antivirus, firewall, sandbox and software version checker).
2. Update Antivirus signatures regularly. Update manually if there is no internet connectivity to the system.
3. Update all the software installed on the system with relevant updates and patches. Use OS update tool (For example, Windows Update for Windows) to update the OS. Run software checker and update any outdated installed software.
4. Backup required documents from the sandbox to a folder on the system regularly.
5. Use different browsers for general internet browsing and sensitive internet browsing (like e-banking, online shopping, e-trading...). It is recommended to always use sandboxed application for general internet browsing.

“*There is no security on this earth. There is only opportunity*.”

– Douglas MacArthur

So, it all depends on who grabs the opportunity – You (to protect your system and the information it holds) or the attacker (to grab your information).

5. Acknowledgements

The author is very grateful to Anand Nair, Steve Milner and Arun Jose for the review, feedback and corrections. Thanks to Rajesh Seetharaman, Satish Dwibhashi, Adi Seshu and other friends for their feedback.

6. References

DISCLAIMER: The products discussed are free for home or personal use only. This paper does not promote any of the products for any kind of gain. The author will not be responsible for any issues due to misconfiguring or improper use of the products. Please read the associated help before installing. There are other products that are also free; but, they are not included here for the sake of simplicity. Only the popular products are referred here.