# Global Information Assurance Certification Paper

# INFORMATION SECURITY FOR THE BROADBAND HOME USER

GSEC Option 1, Version 1.4b

by

Chris J. Domeisen

A practical submitted in partial fulfillment of the requirements for the

GIAC Security Essentials Certification

http://www.giac.org

March 16, 2004

## ABSTRACT

This paper will focus on the recent boom of broadband connections and its implications with regards to security. Most new users of broadband Internet access are not security conscious beyond the daily rage about SPAM and other undesired intruders. Even though stories of what is really happening in the net are widely known and every virus/worm outbreak affects millions of users, the average broadband user is not taking action.

Based on a real life example, I have decided to write my GSEC practical about this topic and also show a few simple solutions that will not make you absolutely safe but provide a good "Security for Money" return on investment. The people involved are real as are the issues and solutions.

## INTRODUCTION

This paper is written for the average, non-technical Internet user - in terms understandable for all. More detailed information and technical explanations would not fit into this paper and a selection of reference links and further reading is attached below for the interested user.

As most home computers nowadays run a Microsoft operating system, I will focus on the Windows family to be of best use to all and show a few simple steps that can make the life of the average PC user easier and safer.

By January 2004, an estimated fifty million home users worldwide connected to the Internet via broadband access – this is an amazing 38% of all home Internet users.[1] While many of these home users are experienced users, most are not and have – at best – only a vague understanding of what they are doing from a security point of view.

So what exactly are these fifty million people doing?

First of all they enjoy a fast Internet connection – but not only that…they also potentially share their PCs with the rest of the world!

While that may sound like lots of fun (file sharing, free data exchange, etc), it can also have serious implications[2]. If a mere 10% of these fifty million broadband users leave their PCs running and connected to the Internet at all times, then we have five million broadband connections that are constantly online.

[1] Nielsen Netrating on Broadband Internet Usage

[2] Chis Jenkins in News.com.au on broadband and Viruses

"Why should hackers be interested in my PC? And how would they know that I even exist? Security is fine but I am not in danger" says my best friend's father, a 56 years old major of a small town close to Zurich/Switzerland. He could not be more wrong like an article on http://www.surferbeware.com shows.[3] Hackers are only marginally interested in your secrets – they care much more about (ab-)using your PC or your identity for their sinister purposes…

## Ruedi – a case study in IT Security

Ruedi is 56 years old, major of a small, idyllic town in central Switzerland. Two years ago, the local government had a special offer for all its employees – they could purchase a PC and a broadband Internet connection at a very interesting price. Of course Ruedi signed up immediately – even though he never really felt at ease with things that have blinking lights and cables sticking out of them. But Internet (and a PC) at home was a must.

It all started out perfectly well in the beginning – an email account was set up (so that private mail did not have to be sent to his work address anymore) and Internet was THE thing in Ruedi's house.

But soon enough trouble came – first in the form of emails he never wanted: SPAM. Ruedi started receiving all kinds of messages about penis enlargements and other – to him – useless things. The second thing he remembers still were the pop-up windows that just started appearing all of a sudden. Being happily married, Ruedi did not particularly care for "cheap sex with local girls" (and similar things) and so he clicked them all away with angel-like patience.

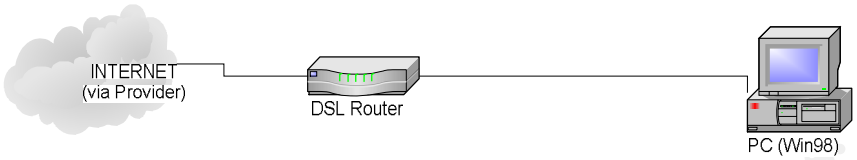
One day his PC absolutely refused to work and Ruedi was devastated – how should he access his emails now? What about his calendar and the work-related things that he was doing from home?

When I went to have a look at the PC I discovered the following…

[3] Surferbeware.com on Security Concerns – Why would a hacker invade my PC ?

## 1. PC SETUP

The PC and the broadband connection that I encountered looked like this:

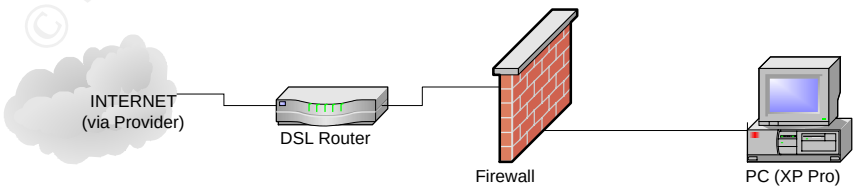



The first thing I noticed was that the PC was running on Windows 98. Not a very good choice for a PC that is continuously connected to the Internet[4].

Then I noticed that there was no firewall (neither hardware nor software on the PC) – basically Ruedi trusted the ISP with the data on his PC. His reply – the ISP is a professional – they don't care about my data is typical for many non-technical broadband users. Problem is that Internet has to be cheap – firewalls and security cost money and time to maintain.

After explaining him possible consequences, Ruedi needed little convincing that action needed to be taken. First of all we replaced Windows 98 with Windows XP. The solution was perfect because Microsoft will not support Win98 anymore as from this summer (i.e. no more security updates) and we managed to find a cheap (equivalent US$ 70) license for XP Professional in English, which suited Ruedi who always wanted to practice his rusty skills.

Then a DSL Router with built-in firewall[5] (equivalent to US$80) ensured that all incoming packets that were not requested from Ruedi's PC were filtered out - we could now start to look at the other issues that remained…




[4] Channelzone/Ziff Davis on Win98

[5] Linksys Router/Firewall – Product Description

## 2. SOFTWARE INSTALLATIONS

Besides having an operating system that is very insecure, Ruedi's son also used the home PC as a surfing and download station. When I checked out the PC, there were three different file-sharing tools installed – and that was just the beginning.

### File Sharing Tools[6]

Even if we forget about the legal aspects of freely sharing copyrighted material amongst many users without paying for it, file-sharing stays at best problematic from a security point of view.
Many actual P2P (peer to peer) tools are available – the current flavor being Kazaa[7] - with different configuration options. Common to all of the ones that I tested (Kazaa, BearShare, Filetopia, Gnutella, iMesh, LimeWire, Morpheus and XoloX) is that a folder (or several) is being shared with anonymous people that may download files or copy files to my PC. The ideal way to import Viruses, Worms, Trojans and other security relevant code as well as having commercial pop-ups annoy you all the time. Even if one has a firewall, the file-sharing tool opens the door (port) from within and lets all kinds of traffic enter…

### Malware

Many sites – especially pornographic and "freeware" sites – prompt the surfer to accept some kind of "license agreement", "age confirmation" or – more honestly – download a viewer tool for their site. When clicked (regardless whether Yes, No or Cancel) oftentimes a program is installed that then reconfigures the PC in some way. Most often the only thing that changes are the dial-up settings – instead of the regular ISP, an expensive ISP is set up as default connection. That may cost the unsuspecting user several hundred dollars a month…if he uses the telephone to connect to Internet. Ruedi did not have this problem – as broadband user he does not connect via telephone to the Internet.

Besides the described dialer, there are many other types of Malware widely distributed. The impact ranges from "do not notice anything" to "where do these commercials always come from" and "why is my default Internet site always changing". In short: it affects us in different ways.

In Ruedi's case the file sharing tools that were constantly running had "imported" commercial pop-ups, which annoyed Ruedi very much (remember that someone has to pay for free software) and had also installed some viruses and Trojans. His son downloaded several virus infected files, Internet Explorer was configured in a way that Ruedi accessed all Websites via a third website, he had a program installed that told him the weather in Hawaii even though he had never been there

[6] Internet Safety Group on Filesharing

[7] Kazaa P2P File Sharing

and when looking through the list of installed programs I found many more items that I could remove without impacting his work at all in a negative way.

Spyware

I could not find any type of Spyware on Ruedi's PC but that may well be attributed to the cleansing program he downloaded and installed just days before.

"Spyware can track your surfing habits, abuse your Internet connection by sending this data to a third party, profile your shopping preferences, hijack your browser start page or pages, alter important system files, and can do this without your knowledge or permission."[8]

It is rather clear that we do not want anyone snooping around in our PC – so we have to remove the Spyware. There are several tools available on the market – for Ruedi we used Lavasoft's AdAware.

Remedy

Be it File Sharing tools, which share our most intimate data with the world, or be it other non-desired programs: They have no place on a PC where the owner values security and privacy.

Each threat has its countermeasure and staying up to date is not easy for the professional and near to impossible for the non-technical Internet user.

Several well-priced packages are commercially available (remember that cracked downloads often contain some undesired add-ons…) and will keep your PC out of the worst trouble.

In Ruedi's case it was his son that used his fathers PC for his adolescent Internet adventures. The result was a frustrated father, a shameful son (when we found all the "things" he downloaded from the net) and a good topic for my GSEC practical.

[8] Lavasoft.de – on Spyware

## 3. INTERNET BEHAVIOR

Can I then not surf the net anymore without being scared of catching something I don't want?

Yes you can. A few very simple rules make sure that all the defense layers that we have built (PC operating system, firewall, virus scanner, awareness of installed programs, good passwords, mail program hardened, removal of private documents) are not fruitless.

One of the bigger threats is still the user himself. While Netiquette regulates the way that one treats others in mails, chats and other communications forums, it is also of importance how one behaves while generally surfing.

- Whenever you are surfing the net – remember that your every move can be tracked – a bit of paranoia often helps.
- You are not anonymous in the Internet – you can be traced back to your PC.
- Do not leave your real name or address on any site that you do not trust.
- Register a free email account in order to receive product updates and to register legally purchased products. Be aware that any email address that you publish on the web (home page, forum, registration, etc) will receive unsolicited SPAM emails
- Configure your Internet Explorer Browser so that you surf in a safe way[9]
- Do not "click away" messages because you think you do not understand them anyway – when in doubt say no.
- Do not trust everyone – in fact only trust site certificates from known companies (see below) when prompted.


[9] Windows Help.Net on Internet Explorer configuration

## 4. GOOD PRACTICES/LESSON LEARNED

### Mail

The easiest approach to avoid many issues is not to use Microsoft Outlook as mail reading program. Other programs are freely available that offer similar or equal functionality without the associated security issues. Downsides are the knowledge that is often needed to setup and keep the program running plus compatibility issues when migrating to another program.
If Outlook /Outlook Express are a must, then these steps help to avoid the most common issues[10]:

- First of all, turn off the Preview Pane function in Outlook[11]- it opens the mail that it displays and may run a virus this way.
- Turn Off Java Script – there is no reason to have it activated in Outlook.
- Make sure the virus scanner of your choice is always up to date and scans all incoming mails.
- Always apply the latest security patches from Microsoft (Outlook E-Mail Security Update)
- Never open a mail from an unknown sender.
- Never open unsolicited attachments – even from known senders.

### Installation of programs

Be very careful which programs you install onto your PC. Generally only install software that you have purchased or downloaded from a trusted site in Internet. Do not trust free versions of otherwise commercial software as they may contain much more than just the regular code…

As a rule you need a good quality virus scanner (with regular updates) and a software firewall[12] if you do not have a hardware firewall. All other software is bonus but be aware – too many different ("cracked versions free from internet") tools may have a negative impact as they may interfere with each other…

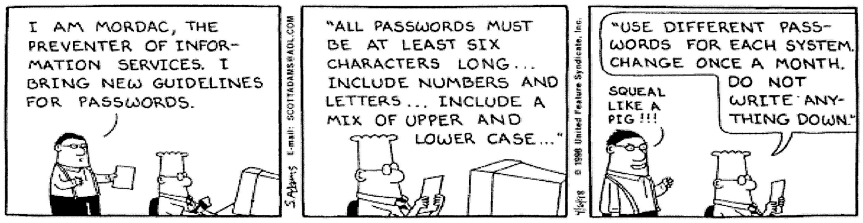
[10] Securityfocus.com on Securing email clients

[11] Securityfocus.com on Securing Outlook

[12] Zone Alarm – Software firewall

Passwords

Passwords are the easiest way to make unauthorized entry more difficult and also one of the easiest ways to allow unauthorized entry… How is that possible? Simple – the quality of the passwords.




A good quality password contains upper/lower case characters, numbers, and special characters and is at least 8 characters long. An easy way to remember a good password is to make sentences (e.g. WorkA11N8!, Print2File?) – that way it is easy to remember when you change it every half year.

Sharing of personal information

Remember that most intruders are looking for a place to hide behind (hijack your PC to do things for them) or look for information on who you are to make use of your identity.

In the State of Georgia/USA what happened with stolen identities looked like that[13]:

- Credit Card Fraud
- Phone / Utilities Fraud
- Bank Fraud
- Employment Related Fraud
- Others

So we want to make sure those easy targets like Curriculum Vitae, a reference letter or other private information is kept private. Best practice here is to store these documents on a rewritable CD, a ZIP or floppy disk and then delete them from the hard disk itself.

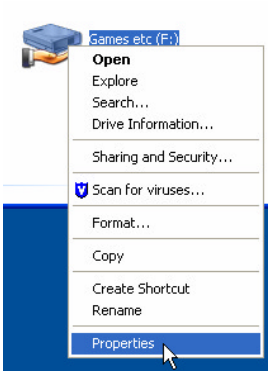
Even after you have removed all personal documents to a safe place, it is not a bad idea to ensure that you are not sharing your disk with others. Sharing is usually only necessary in a network – with only one PC there is no reason to share drives.

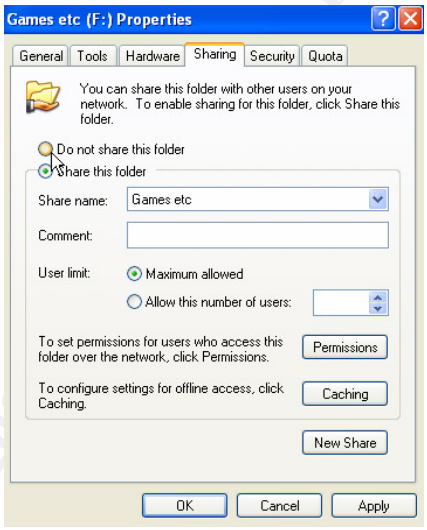
[13] Gaetc.org on What hackers want from my PC and Identity Theft

Under Windows XP (the operating system used with Ruedi) you can find out whether you are sharing by:

- double click “My Computer”
- look at the icons – the ones with a hand below are shared


- to remove a sharing, right-click the drive in question (here Games etc.), select “Properties” and then select “Do not share this folder” in the “Sharing” tab. Click “Apply” then OK. The sharing will now be removed.



## CLOSING

Security is always relative – any system can be broken into if the attacker is pursuant enough and well funded. The average home user does not usually store extremely valuable (in monetary terms) information on his home PC as companies do and he does not have the possibility to rely on expensive professionals. He is on his own.

A more secure operating system and the trusted computing initiative[14] [15] may remove or mitigate many of the current security and privacy issues but only at the price of losing control over your PC. The end user will have to decide whether he is willing to sacrifice control (and privacy?) for the sake of security[16]. Currently the debate is raging but the TCPA members are rolling out their products. Game on…

The average home user is being increasingly flooded with good advice, trendy tools and gadgets, hysterical or well-founded information and all kinds of marketing approaches – as a consequence people like Ruedi switch off completely and avoid using anything.

Most supermarkets nowadays sell PCs and accessories but what they lack is the consulting and training that small, specialized PC vendors (resellers) offer with great success to those that do not mind paying a bit more for much more value. The result is that many people have access to ever more powerful machines and better connections without having a minimal idea on how to behave in that environment.

I strongly believe that this trend will prove to be one of the big threats in the future – using a large number of unprotected, powerful machines on fast connections is an invitation for a really big DDoS attack and other activities…

[14] Trusted Computing FAQ by Ross Anderson

[15] Home Page of TCPA (Trusted Computing Platform Alliance)

[16] CNet's News.com on Digital Rights

# GLOSSARY[17]

(all terms are explained in further detail following the link in the title of each section
the text following the title is taken from the linked source)

Broadband (Internet Access)
In general, broadband refers to telecommunication in which a wide band of frequencies is available to transmit information. Because a wide band of frequencies is a vailable, information can be multiplexed and sent on many different frequencies or channels within the band concurrently, allowing more information to be transmitted in a gi ven amount of time (much as more lanes on a highway allow more cars to travel on it at the same time).

Browser
A browser is an application program that provides a way to look at and i nteract with all the information on the World Wide Web. Th e word "browser" seems to have originated prior to the Web as a generic term for user interfaces that let you browse (navigate through and read) text files online. By the tim e the first Web browser with a graphical user interface was generally available (Mosaic, in 1993), the term seemed to apply to Web content, too.

DSL
DSL (Digital Subscriber Line) is a technology for bringing high -bandwidth information to homes and small busine sses over ordinary copper telephone lines.

E-mail
E-mail (electronic mail) is the e xchange of computer-stored messages by telecommunication. (Some publications spell it *email*; we prefer the currently more established spelling of *e-mail*.) E-mail messages are usually encoded in ASCII text. However, you can also send non -text files, such as graphic images and sound files, as attachments sent in binary streams. E-mail was one of the first uses of the Internet and is still the most popular use.

File Sharing
File sharing is the public or private sh aring of computer data or space in a network with various levels of access privilege. While files can easily be shared outside a network (for example, s imply by handing or mailing someone your file on a diskette), the term *file sharing* almost always means sharing files in a network, even if in a sm all local area network. File sharing allows a number of people to use the same file or fi le by some combination of being able to read or view it, write to or modify it, copy it, or print it.

Firewall
A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from ot her networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own pri vate data resource s and for controlling what outside resources its own users have access to.

Freeware
Freeware (not to be confused with free software) is programming that is offered at no cost and is a common class of small applicat ions available for downloading and use in most operating systems. Because it may be copyrighted, you may or may not be able to reuse it in programming you are developing.

Hacker
Hacker is a term used b y some to mean "a clever programmer" and by others, especially journalist s or their editors, to mean "someone who tries to break into computer systems."

[17] Whatis.com – IT-specific encyclopedia

Eric Raymond, compiler of *The New Hacker's Dictionary*, defines a hacker as a clever programmer. A "good hack" is a clever solution to a programming problem and "hacking" is the act of doing it. Raymond lists five possible characteristics that qualify one as a hacker, which we paraphrase here:

- A person who enjoys learning details of a programming language or system
- A person who enjoys actually doing the programming rather than just theorizing about it
- A person capable of appreciating someone else's hacking
- A person who picks up programming quickly
- A person who is an expert at a particular programming language or system, as in "Unix hacker"

Hardened (PC)
A PC that has been configured in such a was as to permit least possible weaknesses. Generally all non-essential services have been disabled to ensure that as little problem points as possible are available. (definition by Author due to lack of proper definition)

Hardware
Hardware is the physical aspect of computers, telecommunications, and other information technology devices. The term arose as a way to distinguish the "box" and the electronic circuitry and components of a computer from the program you put in it to make it do things. The program came to be known as the software.

Internet
The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers).

Internet Explorer
Internet Explorer (IE) -- sometimes referred to as Microsoft Internet Explorer (MSIE) -- is the most widely used World Wide Web browser. It comes with the Microsoft Windows operating system and can also be downloaded from Microsoft's Web site. The IE browser competes with an earlier browser, Netscape, now owned by AOL. Three other browsers are Mosaic (the browser on which Netscape's browser was originally based), Lynx, and Opera.

ISP
An ISP (Internet service provider) is a company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic area served. The larger ISPs have their own high-speed leased lines so that they are less dependent on the telecommunication providers and can provide better service to their customers.

Java
Java is a programming language expressly designed for use in the distributed environment of the Internet.

Mail
See E-mail

Malware
Malware (for "malicious software") is programming or files that are developed for the purpose of doing harm. Thus, Malware includes computer viruses, worms, and Trojan horses.

Netiquette
Netiquette is etiquette on the Internet. Since the Internet ch anges rapidly, its netiquette does too, but it's still usually based on the Golden Rule. The need for a sense of n etiquette arises mostly when sending or distributing e-mail, posting on Usenet groups, or chatting. To some extent, the practice of netiquette depends on understanding how e -mail, the Usenet, chatting, or other aspects of the Internet actually work or are practiced.

Online
Online is the condition of being connected to a network of computers or other devices. The term is frequently used to describe someone who is currently connected to the Internet.

P2P
On the Internet, peer-to-peer (referred to as P2P) is a t ype of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives. Napster and Gnutella are examples of this kind of peer-to-peer software. Major producers of c ontent, including record companies, have shown their concern about what they consider illegal sharing of copyrighted content by suing some P2P users.

Password
A password is an unspaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user. Typically, users o f a multiuser or securely protected single-user system claim a unique name (often called a *user ID*) that can be generally known. In order to verify that someone entering that user ID really is that person, a second identification, the password, known only to that person and to the system itself, is entered by the user. A password is typically somewhere between four and 16 characters, depending on how the computer system is set up. When a password is entered, the computer system is careful not to display the characters on the display screen, in case others might see it.

Pop-Up Windows
A pop-up is a graphical user interface (GUI) display area, usually a small window, that suddenly appears ("pops up") in the foreground of the visual interface. Pop -ups can be initiated by a single or double mouse click or rollover (sometimes called a mouseover), and also possibly by voice command or can simply be timed to occur. A pop -up window must be smaller than the background window or interface; otherwise, it's a replac ement interface.

On the World Wide Web, JavaScript are used to create interactive effects including pop -up and full overlay windows

Router
In packet-switched networks such as the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router i s connected to at least two networks and decides which way to send each information packet (…)

Software
Software is a general term for the various kinds of programs used to operate computers and related devices. (The term hardware describes the physical aspects of computers and related devices.)

SPAM
Spam is unsolicited e-mail on the Internet. From the sender's point-of-view, it's a form of bulk mail, often to a list obtained from a spambot or to a list obtained by companies that specialize in creating e-mail distribution lists. To the receiver, it usually seems like junk e-mail. It's roughly equivalent to unsolicited telephone marketing calls except that the user pays for part of the message since everyone shares the cost of maintaining the Internet. Spammers typically send a piece of e-mail to a distribution list in the millions, expecting that only a tiny number of readers will respond to their offer. Spam has become a major problem for all Internet users.

Trojans
In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk.

Virus
A virus is a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. A virus is often designed so that it is automatically spread to other computer users. Viruses can be transmitted as attachments to an e-mail note, as downloads, or be present on a diskette or CD. The source of the e-mail note, downloaded file, or diskette you've received is often unaware of the virus. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer. Some viruses are playful in intent and effect ("Happy Birthday, Ludwig!") and some can be quite harmful, erasing data or causing your hard disk to require reformatting.

Worm
In a computer, a worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

ZIP disk
A Zip drive is a small, portable disk drive used primarily for backing up and archiving personal computer files. The trademarked Zip drive was developed and is sold by Iomega Corporation. Zip drives and disks come in two sizes. The 100 megabyte size actually holds 100,431,872 bytes of data or the equivalent of 70 floppy diskettes. There is also a 250 megabyte drive and disk. The Iomega Zip drive comes with a software utility that lets you copy the entire contents of your hard drive to one or more Zip disks.

# REFERENCES


**MyCERT** "Home User PC Security" MyCERT Web Site

URL: http://www.mycert.org.my/homepcsecurity.html (15th February 2004)

**Magid, Larry** "Worms, Viruses, Spam & Hack Attacks. Oh My." PCAnswer.com

URL: http://www.pcanswer.com/articles/synd_wormsohmy.htm , September 4, 2003

**Pilgrim, Mark** "Seven ways to protect your home windows PC for free" diveintomark.org

URL: http://diveintomark.org/archives/2001/09/04/ , September 4, 2001

**Villano, Matt** "Report: Most Broadband Users Lack Basic Security" Internetnews.com

URL: http://www.internetnews.com/infra/article.php/2217421 , June 4, 2003

**Tanase, Matthew** "Always On, Always Vulnerable: Securing Broadband Connections" , Securityfocus.com

URL: http://www.securityfocus.com/infocus/1560 , March 26, 2002

**Getnetwise** "About Broadband Security" getnetwise.com web site

URL: http://security.getnetwise.org/broadband , March 8, 2004

**Thorsberg, Frank** "Half of U.S. Broadband Users Unprotected" , PCWorld.com web site

URL: http://www.pcworld.com/news/article/0,aid,55154,00.asp , July 16, 2001

**Spychecker** - General Information Portal on Spyware and countermeasures, Spyware.com Web Site

URL: http://www.spychecker.com

**Rebeyro, Jaeson** "Broadband Security Concerns For Home and Remote Users" , GIAC Web Site

URL: http://www.giac.org/practical/Jaeson_Rebeyro_GSEC.doc , January 29. 2002

**Lai, Wayne** "Managing Peer to Peer Applications in dormitory Networks" , GIAC Web Site

URL: http://www.giac.org/practical/GSEC/Wayne_Lai_GSEC.pdf

**Gattine, Kara,** "Security Awareness for End Users", TechTarget.com web Site, February 20, 2003

URL: http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci890972,00.html

**Intel Corp., "**Enterprise Security and the PC Infrastructure", Intel Web Site, May 2003

URL: http://www.intel.com/business/bss/infrastructure/security/pc_infrastructure.pdf

**Captain, Timothy, "**Build your own Spy-Proof PC", from the October 2003 issue of PC Upgrade

URL: http://www.techworthy.com/PCUpgrade/October2003/Build-Your-Own-Spy-Proof-PC.htm?Page=7

**Green, Natalie M.** "Securing your Internet Explorer Browsing Experience at Home", GIAC Website, Jan 19, 2004

URL: http://www.giac.org/practical/GSEC/Natalie_Green_GSEC.pdf

## Appendix A: Why Win9x/ME is a bad choice for Internet

Windows 9x/ME has never been designed for security and cannot be secured due to its architecture.

A few simple examples are:

- Uses FAT File System which has no access control built in like NTFS
- Initial logon can be circumvented by pressing “Cancel” at logon
- No meaningful security logs can be recorded
- With a boot disk from another operating system all security measures can be circumvented
- Other smaller ones

Windows 9x/ME was never intended for networked office usage either – the professional operating system for that usage was Windows NT and nowadays Windows 2000/XP.

For further, Win9x specific security information, please check cert’s info page.

## Appendix B: Step-by-Step guide for a safer Internet PC

### Step 1: Virus Scanner

- Install a good virus scanner that can be updated regularly
  - Recommended free scanner: http://www.free-av.de/
    - detects over 70'000 viruses and provides for easy updates
    - includes user-guide on the web
    - available in English and German
  - Commercial scanners:
    - McAffee Virusscan http://us.mcafee.com/default.asp
      - Combined Internet Security Suite also available
      - Easy to understand guide
    - Symantec Antivirus http://www.norton.com/
      - Difficult to understand user guide

### Step 2: Firewall

- Install a software firewall if you do not have a hardware one
  - Recommended free firewall: Zone Alarm
    - Setup guide easily available[18]
  - Recommended commercial products
    - Norton Internet Security http://www.norton.com/
      - Very widely used
      - Technical documentation
    - McAffee Personal Firewall http://us.mcafee.com/default.asp
      - Available in an Internet Security suite package
      - Easy to understand guide
      - Rather complicated handling once installed
      - Easy update function

### Step 3: Internet Browser Security

- Ensure that you are using an up-to-date browser with the actual security patches
- As 83% of all Internet users make use of Internet Explorer[19], please refer to the excellent work by Nathalie Green on securing Internet Explorer[20]

---

[18] Zone Alarm Setup Guide

[19] Trojaner-Info-de on Information Security Steps

[20] GSEC Practical by Natalie M. Green on securing the Internet Explorer

Step 4: Securing your e-mail client

- E-mail is the killer application of internet, most internet users use internet
- E-mail is also one of the most troublesome applications – Malware, SPAM and other undesired side effects result directly from e-mail usage or are closely related to it
- Securing the email client is key
- As with the Operating System, always have the actual patches installed
- Follow the guide from Security Focus[21] to further secure your Outlook (the most frequently used e-mail client)

Step 5: Internet Behavior

As mentioned above, Internet behavior can be key to staying safe or risking unwanted visitors:

- Whenever you are surfing the net – remember that your every move can be tracked – a bit of paranoia often helps.
- You are not anonymous in the Internet – you can be traced back to your PC.
- Do not leave your real name or address on any site that you do not trust.
- Register a free email account in order to receive product updates and to register legally purchased products. Be aware that any email address that you publish on the web (home page, forum, registration, etc) will receive unsolicited SPAM emails
- Configure your Internet Explorer Browser so that you surf in a safe way[22]
- Do not "click away" messages because you think you do not understand them anyway – when in doubt say no.

[21] Guide to Securing Outlook by securityfocus.com

[22] Windows Help.Net on Internet Explorer configuration