Global Information Assurance Certification Paper

The Home Computer Security Primer

Ric Nepil
GIAC Version 1.4b

Introduction

For a family, the Internet is arguably one of the most exciting technical innovations since the television. The instant gratification of information searches, shopping, email, live video and file sharing are the major driving factors in the multi-billion dollar Internet and computer industry.

As hardware and software vendors grow their markets to include less technical customers, they in turn simplify the often complex installation of their products. While “Wizards” and “Plug-and-play” devices make installations quick and easy, it often compromises security.

This paper is intended to educate the causal internet user to possible risks, and in doing so assist in protecting them from personal scams, data corruption, and information and identity theft.

Basic Terms

Before we continue, you should understand some basic terms.

Networking Terms

Internet Service Provider (ISP) – An Internet Service Provider provides the equipment and interfaces to connect a customer to the internet. The interface might be a dialup access phone number or direct network access. Some examples of ISP's are America on Line (AOL), AT&T, CompuServe and NetZero.

Dialup Modem – A modem is a device that connects a user to an ISP via household phone lines. It converts requests from your computer to a digital signal that can be easily passed though the phone line. By today's standards, modems pass data very slowly – typically 500% slower that a direct network connection. However, dialup access only requires a phone line connection and is available almost anywhere.

Cable Modems, DSL Modems - When a customer connects to an ISP through a direct network connection, the ISP provides a connection directly to the customer's house through special wiring, a cable TV connection or a satellite dish. The ISP then uses this special type of modem to connect their wiring to the computer. Since the customer is connected directly, there is no need to dial an access number and their computer is always connected to the internet.

Network Interface Cards – The cable or DSL modem connects to the computer through a Network Interface Card (NIC)..

IP Address – Whether the customer connects to the internet through a dialup modem or directly, systems on the internet need to know where a request originated and where the response is going to, similar to the way a letter is delivered though the post office and back. The information traveling through the network is refered to as packets. Just as a letter requires a recipient and return address, network packets need to know who they have been sent to and where the information is to return. Every computer connecting to the internet requires its own unique IP address. Your IP will supply you one address for your dialup or direct connection.

Router – A router looks for address information in the network packets and determines how it should be routed. If you attempt to share information between two computers in your house, the router decides it does not need to pass that data through the internet and instead *routes* the data through the house to the other computer.

Network Address Translation (NAT) – OK. This isn't as tricky as it sounds. What do you do if you have three computers in your house and you want them all to access the internet? When you set up a router, it gets the IP address your ISP assigned you. Each computer in your house then gets an individual IP address. When a request is sent to the internet, the router uses NAT to convert the *from IP* address to the one assigned to you by the ISP and makes a note of which of your three computers requested information from that internet address. Then when the response is received, the router knows which of your

three computers should get the data back. To the ISP and internet it looks like the requests are coming from just one computer. Cool, huh?!

Hacking Terms

Trojan – A seemingly harmless program such as a free game or tool that installs or launches a backdoor, virus or worm. A Trojan is often propagated in the form of an email attachment.

Backdoor – A program that secretly runs on a computer and allows full access to that computer. Backdoors like SirCam, SubSeven and Back Orifice open network connections through your router to the internet that can be detected by hackers using port scanners. Once the hacker has connected to the backdoor, they can steal information, corrupt your data, or completely expose your computer.

Virus – A small program that attaches itself to legitimate applications on your system, such as Microsoft Word or Excel. When the application is launched, it first executes the virus program, which in turn can erase or corrupt files, erase your hard disk or simply replicates itself. A variant is the email virus which replicates itself by emailing copies of itself as an attachment to contacts found in your email application. The recipient then assumes that the attachment came from you and opens it, thus repeating the cycle.

Worm – A program that quickly spreads through a computer network using application vulnerabilities. An example is the recent SQL Slammer or Sapphire worm. As it began traveling through the Internet, the number of incidences doubled in size every 8.5 seconds. The worm infected over 75,000 hosts -- 90 percent of those hosts within 10 minutes. It and caused major network outages, canceled airline flights, interfered with elections and ATM failures before it was brought under control.

Hackers

When we talk about “hackers”, we might envision an extremely technical person with intimate knowledge of computer internals stealthfully downloading our credit card numbers and personal information and watching our online purchases while we are blissfully unaware. Statistics however show us that most attacks come from teens that have little knowledge beyond downloading files and executing programs. For these individual, hacking is more of a hobby then a career. For the majority of hackers the immediate goal is not to profit from stealing your credit cards and personal information as much as simply obtaining “bragging rights”.

The law currently does very little to protect individuals from hackers and hacker know this. To illustrate, imagine this analogy:

- A hacker goes through your neighborhood with a set of keys and tries the keys on every door of your house.
- Once the hacker finds a door he can unlock, he enters you house and goes through your drawers, cabinets, personal papers, etc.

- The hacker can then take your personal information and share it with others or destroy everything he finds in your house without incrimination.

Only if the hacker uses some of the personal information he finds for profit, do you have a chance to incriminate him, and only then if you can prove he took the information for profit.

Usually, the best you can do is report the hack to his ISP which may temporarily suspend his antics.

Two Types of Attacks

Attacks can be categorized in two types.

- Outside in – where a an attacker proactively finds a way to get to the data on your computer from your internet connection.
- Inside Out – where the attacker is able to access the data on your computer with the help of a program running on your computer.

Inside Out Attacks

Viruses, Worms, Backdoors and Trojans

Most typically these are hidden within programs or attached to emails. Interesting enough, with very few exceptions, these programs cannot be activated without human interaction; you must choose to run the infected program before it can cause damage. The problems they cause can range from annoying to catastrophic. The most benign will simple make copies of itself and continue spreading, while the most dangerous can randomly email confidential information, destroy all the data on your disk drive or even allow complete access to your computer through the internet.

Protection: Antivirus programs look at each file and compare the data inside the file to a list of patterns that are common in the viruses. Once this pattern is detected, the antivirus program will delete, repair or isolate the file to render it harmless. Since new viruses are constantly appearing, the antivirus program downloads a list of new virus patterns every time your computer connects to the internet. Without these updates the program would quickly become obsolete.

Before you begin using your computer you should install a good antivirus program. This will prevent viruses from infecting your computer through floppy disks and CD's. Once you are connected to the internet, download the latest updates (signatures) and allow the program to do a full scan of your system.

Two companies offering free antivirus scanners are:

GRISOFT Inc. - AVG 6.0 Free Edition (www.grisoft.com)

and

Trend Micro – HouseCall (housecall.trendmicro.com)

SPAM

Companies have found email a more cost effective means of advertising their products than postal distributions. From marketing companies, they can purchase lists of millions of email addresses for a fraction of what it would cost to physically send out a mailer.

The marketing companies collect the email lists from various internet sources including newsgroups, online purchases, registering software and memberships programs.

This unsolicited email is commonly referred to as SPAM. It is unclear who first coined the phrase, but some believe the computer group lab at the University of Southern California gave it the name because of the same characteristics as the lunchmeat:

- Nobody wants it or ever asks for it
- No one ever eats it; it is the first item to be pushed to the side when eating the entree
- Sometimes it is actually tasty, like 1% of junk mail that is actually useful to some people

Opting-out

Spam often has a link at the bottom of the email allowing you to "opt-out" of receiving future emails, but be aware that some companies use the link to confirm they have reached a real recipient. The best way to eliminate Spam is to filter it from your mailbox as it's coming in. There are a number of software programs what will do this for you. To name a few; SurfControl's Mailwasher (www.surfcontrol.com) and McAfee's Spam Killer (www.mcafee.com). Hotmail.com offers the ability to only accept mail from senders already in your address book.

Malicious Emails

Emails are a fast and easy way to convey a message to thousands of people. They do not require the material, printing and distribution costs of traditional mailings. The cost of an email anywhere in the world is the same as sending and email to someone across town. They can be virtually untraceable and easily distributed worldwide. Therefore, it is no surprise that emailing has become the media of choice by increasing numbers of scam "artists". Here are a few samples:

Nigerian Scam Email

"REQUEST FOR URGENT BUSINESS RELATIONSHIP

FIRST, I MUST SOLICIT YOUR STRICTEST CONFIDENCE IN THIS TRANSACTION. THIS IS BY VIRTUE OF ITS NATURE AS BEING UTTERLY CONFIDENTIAL AND 'TOP SECRET'. I AM SURE AND HAVE CONFIDENCE OF YOUR ABILITY AND RELIABILITY TO PROSECUTE A TRANSACTION OF THIS GREAT MAGNITUDE INVOLVING A PENDING TRANSACTION REQUIRING MAXIIMUM CONFIDENCE.

WE ARE TOP OFFICIAL OF THE FEDERAL GOVERNMENT CONTRACT REVIEW PANEL WHO ARE INTERESTED IN IMPORATION OF GOODS INTO OUR COUNTRY WITH FUNDS WHICH ARE PRESENTLY TRAPPED IN NIGERIA. IN ORDER TO COMMENCE THIS BUSINESS WE SOLICIT YOUR ASSISTANCE TO ENABLE US TRANSFER INTO YOUR ACCOUNT THE SAID TRAPPED FUNDS.

THE SOURCE OF THIS FUND IS AS FOLLOWS; DURING THE LAST MILITARY REGIME HERE IN NIGERIA, THE GOVERNMENT OFFICIALS SET UP COMPANIES AND AWARDED THEMSELVES CONTRACTS WHICH WERE GROSSLY OVER-INVOICED IN VARIOUS MINISTRIES. THE PRESENT CIVILIAN GOVERNMENT SET UP A CONTRACT REVIEW PANEL AND WE HAVE IDENTIFIED A LOT OF INFLATED CONTRACT FUNDS WHICH ARE PRESENTLY FLOATING IN THE CENTRAL BANK OF NIGERIA READY FOR PAYMENT.

HOWEVER, BY VIRTUE OF OUR POSITION AS CIVIL SERVANTS AND MEMBERS OF THIS PANEL, WE CANNOT ACQUIRE THIS MONEY IN OUR NAMES. I HAVE THEREFORE, BEEN DELEGATED AS A MATTER OF TRUST BY MY COLLEAGUES OF THE PANEL TO LOOK FOR AN OVERSEAS PARTNER INTO WHOSE ACCOUNT WE WOULD TRANSFER THE SUM OF US $21,320,000.00 (TWENTY ONE MILLION, THREE HUNDRED AND TWENTY THOUSAND U.S DOLLARS). HENCE WE ARE WRITING YOU THIS LETTER. WE HAVE AGREED TO SHARE THE MONEY THUS; 1. 20% FOR THE ACCOUNT OWNER 2. 70% FOR US (THE OFFICIALS) 3. 10% TO BE USED IN SETTLING TAXATION AND ALL LOCAL AND FOREIGN EXPENSES. IT IS FROM THE 70% THAT WE WISH TO COMMENCE THE IMPORTATION BUSINESS.

PLEASE,NOTE THAT THIS TRANSACTION IS 100% SAFE AND WE HOPE TO COMMENCE THE TRANSFER LATEST SEVEN (7) BANKING DAYS FROM THE DATE OF THE RECEIPT OF THE FOLLOWING INFORMATIOM BY TEL/FAX; 234-1-7740449, YOUR COMPANY'S SIGNED, AND STAMPED LETTERHEAD PAPER THE ABOVE INFORMATION WILL ENABLE US WRITE LETTERS OF CLAIM AND JOB DESCRIPTION RESPECTIVELY. THIS WAY WE WILL USE YOUR COMPANY'S NAME TO APPLY FOR PAYMENT AND RE-AWARD THE CONTRACT IN YOUR COMPANY'S NAME.

YOURS FAITHFULLY,

DR CLEMENT OKON

NOTE; PLEASE QUOTE THIS REFERENCE NUMBER (VE/S/09/99) IN ALL YOUR RESPONSES."

There are many versions of this email where, basically the sender distributes thousands of these emails randomly. While details may vary, essentially the sender solicits the recipient for assistance in reclaiming a large amount of lost funds. When the recipient contacts the senders, the details invariably request some sort of legal fees, cash for airline tickets, etc. The sender will continue to reply with assurances that the transactions are nearly completed with requests for more financial assistance. It may be an obvious scam to you, but remember the sender only needs a few trusting souls out of the thousands he has contacted to make a good deal of money.

Teddy Bear Virus Hoax

Dear All

A friend's Address Book has been infected by a virus and it was passed on to my computer. My Address Book in turn was infected. The virus (called jdbmgmr.exe) is not detected by Norton or McAfee anti-virus.

It sits quietly for 14 days before damaging the system. It is sent automatically by messenger and by the Address Book, whether or not you sent e-mails to your contacts.

It is quite easy to check for the virus and to get rid of it in a couple of minutes. I was given the following instructions:

1. Go to Start, Find or Search option.
2. In the Files/Folders option write the name jdbgmgr.exe
3. Be sure to search your C:drive and any other drives you may have.
4. Click "Find now".
5. The virus has a teddy bear icon and the name jdbgmgr.exe - DO NOT OPEN IT!
6. Go to Edit, choose "Select all" to highlight the file without opening it.
7. Now go to file and select "Delete". It will then go to the Recycle Bin.
8. Go to the Recycle Bin and delete it there as well.

IF YOU FIND THIS VIRUS, YOU MUST CONTACT ALL THE PEOPLE IN YOUR ADDRESS BOOK SO THAT THEY IN TURN MAY ERADICATE IT FROM THEIR OWN ADDRESS BOOKS.

APOLOGIES AS I'M SURE EVERYONE IN MY ADDRESS BOOK WILL HAVE IT.

To do this, open a new e-mail message.
Click the image of the address book next to "To".
Click every name and add it to BCC.
Copy this message... enter subject... paste to -email.... send

Or this is quicker as long as your server doesn't place a limit on the number of addresses you may use at once.

Go to Address Book, select "ALL" (Ctrl A), go to "Send Mail" which is in Tools of Action.

Thanks for your understanding and cooperation.

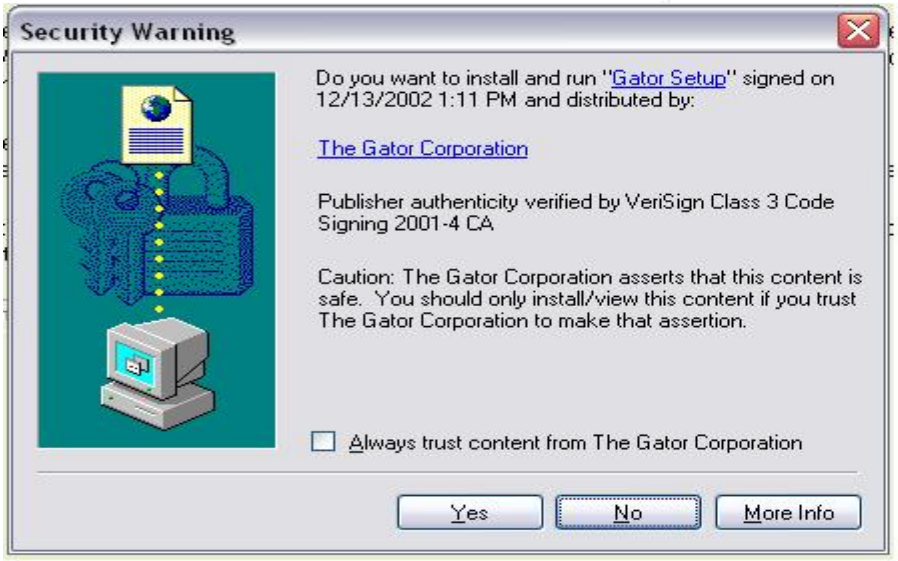
****

This scam tells you to manually delete a virus from your computer and then tell all your friends to do it too. The file it tells you to delete is a legitimate system file. It's hard to say what the goal of this hoax was since deleting this file would probably not affect you unless you were a programmer. Regardless, you should let your antivirus program detect and delete these files.

Web-based emails

When email systems were first created, emails were sent in plain text without any pictures links to web pages, etc. As email usage became more widely adopted by the general public, systems were created allowing web pages to be embedded in the email. This allowed pictures links and text formatting to be included in the email message and generally made it much easier for the recipient to interact with the sender.

The ability to format emails using HTML based commands also provides hackers with a means of hiding code within the email. Links placed with an email can now execute programs on a remote web server. Clicking on a link may now download and execute a program on your computer. Companies use the ability to install programs on your computer to monitor and report on your buying and internet surfing habits. The worst offender of this is probably the Gator Corporation. Gator controls a number of pop-up advertisements that actually look like Windows tools. These tools display messages like "Your system is not fully optimized. Click here to begin optimization." When you click on the message, you get a message like this:



When you see this dialog box, it is telling you a program is about to be installed on your computer. Unless you know exactly what that program will do, click on "No".

Two excellent free programs are available to detect and remove this "spyware":

LavaSoft - Ad-Aware (http://www.lavasoftusa.com)

and

PepiMK Software - Spybot - Search & Destroy 1.2 (http://security.kolla.de)

Neither program is automatic and you must periodically run the programs to detect and delete the Spyware.

Tricksy Little Hackers, we Hates Them!

Occasionally, you might receive an email like the one below.

Fake Mail Example

While this looks like Yahoo! has encountered a problem with your account, it is actually a web-based form that collects your Yahoo! username and password information and forwards it to a hacker. The hacker has copied the real Yahoo! login page to make it look official. NEVER put your password in an email.

We can look at this email closer to see if there are any clues as to its legitimacy.

Email programs have a option to turn on full headers – the detailed information of who sent the email and how it was routed. By doing this you can see information about the sender of the email that will help you determine if it is from a legitimate sender.

In the email above, notice that while the From: line says support@yahoo.com, the Received: line shows ommo.net (HELO ommo.net), and the To: is mikeyee2000@yahoo.com (not me). Without the full header information you would simply see:

To:	myname@yahoo.com
From:	support@yahoo.com

Outside In Attacks

Network Hacking

Network hacking is the easiest and safest way for a hacker to gain access to information on your computer. Using simple software tools readily available from the internet, a hacker can attempt to break in to your network from virtually anywhere in the world.

The typical network hacker will perform the following steps to gain access to your network:

- **Discovery**

  The first step a hacker will perform is discovery. Using a software tool called a "port scanner", he can scan thousands of network addresses in an attempt to locate computers with known vulnerabilities. As in the previous example, this would be the equivalent of checking the locks on the doors to see if he has a key that matches. The hacker has millions of doors to try, so the chances are good that he will find some that match. Recently published statistics show that computers are typically scanned within 15 minutes of connecting to the internet.

- **Vulnerability**

  Once a hacker detects what system you have and what you are running on it, he can research the vulnerabilities to that system. In other words, let's see if the door will unlock with the key I have. Many port scanners make this easy by conveniently referencing the vulnerabilities in the tool (sometimes called a vulnerability assessment tool).

  One of the simplest vulnerabilities to exploit is a network share. Windows provides the ability to make directories or entire drives available to the network. In fact, in many versions of Windows, your drives are happily shared by default.

  While a router normally blocks this access from the internet, misconfiguring or bypassing the router and connecting your computer directly to the internet exposes those shares to the port scanners. Furthermore, software programs like; instant messengers, personal web servers and databases can create vulnerabilities as they open internet connections by design.

- **Exploit**

  When a hacker detects a vulnerability, he will attempt to exploit it. Details of how to exploit various computer and program weaknesses are readily available on the internet. While most software vendors try and patch the vulnerabilities as soon as

they are detected, consumers rarely apply the patches in a timely manner, if ever.

- **Root Access**

  Now that the hacker can get into your computer, he will usually attempt to gain total access to your machine. This can be gained in a number of ways. One way is to steal passwords; another, often easier way is to infect the computer with Trojan or Backdoor program.

The Router

Your first line of defense against outside in attacks is a router.

A few years ago, dialup access through a telephone was the most common method of connecting to the internet. When a person wanted to connect to the internet, they would dial a phone number given to them by their ISP, who would connect them to the internet. Since people were unlikely to tie up their phone lines for long periods of time, most people dialed up, did their work and hung up, thus reducing their amount of expose to hackers.

Enter high speed internet. Always connected, always online.

When you sign up for high speed internet, your ISP gives you either a DSL or cable modem. The modem has a connection that allows you to connect you computer directly to the internet. Connecting your computer directly to the internet without a personal firewall instantly exposes all your shares and vulnerabilities to hackers scanning the internet.

Called a DSL/ Cable router or wireless router, they offer a number of functions, including:

- The ability to connect multiple computers to the DSL/cable modem
- The ability to restrict access to your computer from the internet, similar to a firewall
- The ability to connect computers within your house to each other
- In the case of a Wireless DSL/cable router, the ability to connect computers without wires

A router is a must if you are interested in allowing multiple computers to connect to each other and the internet, but when using a wireless router you should be aware there can be some serious security risks.

Wireless Networks and Wardrivers

Installing a wireless network in your home allows you to connect any computer or printer in your house in a matter of minutes without wires. You can work on your laptop computer virtually anywhere in or around your house up to about 300 feet. The cost is under $200 and you can be up and running in around 30 minutes.

The drawback to wireless networks is that without proper precautions, any computer with a wireless card can also access your network. Since the wireless access is on the inside of your network instead of the internet side of the network, the router does not block outside connections.

To “Wardrive”, a hacker will drive around with a wireless card and a laptop to locate and possibly exploit connections to wireless networks. Once they detect an open network, they will note the locations and whether the networks are open or secured. According to numbers posted by the Worldwide Wireless Wardrive in November 2002, over 72% of the nearly 25,000 wireless networks found by wardrivers around the world didn’t have any of the basic wireless security safeguards enabled. I blame this on the manufacturers focus on providing easy installation of security.

There are however some steps that can be taken to help protect your wireless network from Wardrivers.

1. To prevent your router from being reconfigured, change the default router password to a complex password. A complex password should contain at least 3 of the 4 following; uppercase characters, lowercase characters, numbers, special characters, for example ({}[],.<>;:’”?/|\‘~!@#$%^&*()_-+=), should be at least 8 characters long. A good password might contain the first letters and numbers of a phrase; mDjt12Yso! = my Daughter just turned 12 Years old!

2. Enable the Wired Equivalent Privacy (WEP). You must do this on both the router and the wireless cards. You must create a unique encryption key and assign it to both. Depending on the WEP encryption level this key may be between 10 and 26 characters. The method of doing this varies with vendors. Refer to the router and wireless card’s instructions to see how to do this.

3. Routers have a unique identifier called a SSID. This can be set to anything you want, but do not make this your surname, address, etc. since this can be seen by wardrivers even when encryption is enabled.

   The next two precautions are for advanced users, but will provide a significant increase in security.

4. Disable DHCP. DHCP is the mechanism that assigns addresses to computers connecting to the network. By assigning the addresses manually, WarDrivers will not be automatically added to the network should they be able to connect to the

router.

5. Filter on the network adapter's MAC address. Each network adapter has a unique address, like a serial number. You can configure your router to only accept the MAC addresses of the network adapter that you own.

Personal Firewalls

A firewall blocks access to your computer from the network much like the router does, but it can go a step further by actually examining what is connecting to your computer.

Personal firewalls limit access to your computer through the network by only allowing access you have approved. Some firewalls also integrate checks for trojans and backdoors or allow you to block inappropriate internet access for kids.

While there are a large number of personal firewall manufactures, most perform the same basic functions. Search for reviews on the internet or talk to your local computer store salesperson to decide which one is right for you. Don't want to spend the money right now? There are a number of companies that have free version of their firewalls, including:

ZoneLabs - ZoneAlarm (www.zonelabs.com)

and

Sygate - Personal Firewall (www.sygate.com)

Personal Firewalls and Antivirus software programs provides essential protection from viruses, hackers, and privacy threats.

Locking your computer

Laptop and work computers should be programmatically locked and physically secured when left alone. There are many cable based locking devices available that can be easily tossed in the computer bag.

A good habit is to lock your desktop when not in use and set your screensaver to automatically lock the desktop when it starts.

Password best practices

A good password should be hard to guess and easy to remember. It should be eight or more characters. It should be a combination of upper and lower case letters, numbers and symbols. Words should not be found in the dictionary.

Bad password examples

dodgers
d0dg3rs
fast!boy
big#fish

Good password examples

#t1mf%pw = # this 1s my favorite % pass word (phrase and substitute letters)
1lm$3ngc = 1 love my $ 3xpense new golf clubs (phrase and substitute letters)
gr8!d4agg = great ! day for a golf game (phonic, phrase and letter substitution)

Change your password at least every 45 days. Do not reuse your passwords.

Hack Thy Self

There are tools available that will simulate what a hacker would do to exploit your network. Using these tools on a regular basis will help you discover vulnerabilities that hacker may use to compromise your network.

A few examples are:

SyGate – Sygate Online Services (http://scan.sygatetech.com)
HackerWhacker – (http://www.hackerwhacker.com)
SmithMicro – CheckIt Firewall Scan (http://scan.checkit.com)

Summary

We have identified and examined various forms of ‘hacks’ that can occur with personal computer systems and in doing so hopefully have helped you reduce some of the associated risks. The simple precautions outlined are relatively inexpensive, easy to implement and can greatly reduce your chances of being compromised. Don’t wait to implement them!

We are constantly exposed to new technologies. When you trust those technologies with your confidential information, it’s important to have at least a basic understanding of how that technology works, whether it’s an online purchase or your computer system. Ask questions!

References

These references can help you keep up-to-date on the latest threats and scams:

U.S. government's central website for information about identity theft
http://www.consumer.gov/idtheft

Internet safety, help and education organization
http://www.wiredsafety.org

Cyber Angels – Internet safety by the Guardian Angels
http://www.cyberangels.org

FBI Publications - A Parent's Guide to Internet Safety
http://www.fbi.gov/publications/pguide/pguide.htm

I-SAFE America -Internet Safety Education Foundation
http://www.isafe.org

Sources

Thorsberg, Frank. "The World's Worst Viruses" August 23, 2002
URL: http://www.pcworld.com/howto/article/0,aid,103992,00.asp

CERT® Coordination Center. "Home Network Security" Febuary 15, 2003
URL: http://www.cert.org/tech_tips/home_networks.html#introduction

Makmur, Hanz. "Securing and Sharing Your Home Broadband Connection" March 20. 2001
URL: http://please.rutgers.edu/show/firewall/

Ellison, Craig. "Exploiting and Protecting 802.11b Wireless Networks" September 4, 2001
URL: http://www.extremetech.com/article2/0,3973,11388,00.asp

Hobbs, Scott. "Cyber Threats: Viruses, Worms, Trojans, and DoS Attacks" December 18, 2000
URL: http://www.sans.org/rr/malicious/threats.php

U.S Securities and Exchange Commission. "Internet Fraud: How to Avoid Internet Investment Scams" November 15, 2001
URL: http://www.sec.gov/investor/pubs/cyberfraud.htm

Gralla, Preston. "The complete idiot's guide to protecting yourself online" Indianapolis, IN :
Que, 1999.

Speed, Timothy / Ellis, Juanita / Korper, Steffano. "The personal Internet security guidebook : keeping hackers and crackers out of your home" San Diego :
Academic Press, 2002

Raymond, Ilene. "A parent's guide to the Internet" Los Angeles, Calif. :
Parent's Guide Press, 2001