User Vulnerabilities on the Internet; How to Mitigate Your Risk.

Thomas Erickson, CISSP
Master CNE, CDE, CLE, LPIC-1, MCSE, and CCNA

Capella University
M.S. Information Technology, Information Security Specialization
Instructor: Kerry Green
ThomasCISSP at gmail.com
TS5508: Enterprise System Security
June 2005
Table of Contents

Abstract:.................................................................................................................................................. 3
Introduction:........................................................................................................................................ 3
General security best practices:.............................................................................................................. 3
Summary of Internet User Threats/Vulnerabilities:............................................................................... 4
Internet Security Myths:....................................................................................................................... 7
Why has Internet exploits proliferated in recent years?....................................................................... 8
Examples of Internet vulnerabilities/history:....................................................................................... 8
Assessing your system for vulnerabilities:............................................................................................ 9
Counter measures for Internet risk:.................................................................................................... 11
  Kids' Rules for Online Safety................................................................................................................. 11
  Kids' Pledge........................................................................................................................................ 12
  Parents' Pledge.................................................................................................................................. 12
  Can the software I use or chose not to use affect my risk?............................................................ 13
  Basic system lock-down/hardening:.................................................................................................. 13
General rules and guidelines for Internet safety (safeguarding against pornography):...................... 19
  What do I do if I get unwanted porn pop-ups?.................................................................................. 19
Minimum Technical counter measures for Internet Users:............................................................... 20
Conclusion:........................................................................................................................................... 22
Appendix A – Additional Online Materials for families..................................................................... 28
Abstract
This document outlines the risks and vulnerabilities an Internet user may be subjected to in a hostile network (The Internet). We will investigate the impact of these risks and how to mitigate risk for the typical Internet user.

The audience for this paper is users that have been using the Internet and computers for a while and would be considered intermediate computer users. Otherwise this paper would never end and I would have to explain and re-explain basic computer concepts.

Introduction

Vulnerabilities: “...weakness that may provide an attacker the open door...”
Threat: “...any potential danger... a specific vulnerability and use it against the company or individual.”
Risk: “is the likelihood of a threat agent taking advantage of a vulnerability.”
Exposure: “...exposed to losses from a threat agent.”
Countermeasures: “...or safeguard, mitigates the potential risk (Harris, p. 56).”

General Security Best Practices:
1. Disable the service(s) if you are not using them or do not need them. Also keeping services disabled unless or until they are needed, then enable them temperately.
2. Least privilege – “no more privileges than necessary to be able to fulfill its functions (Harris, p. 209).”
3. Baseline configuration that is audited (verified) via routine checkups.
4. Defense-in-depth, Security in layers – Layer 1, Layer 2, Layer 3. Multiple countermeasures and controls to mitigate risk. One application of this principle is filtering the ports and disabling the ports.
5. Education! From the common worker to the IT professional (of course different awareness training)
6. Continuous vigilance (process and methods and routines). Do NOT rely on technology, which is ONLY one piece/layer of security.
7. Availability, Integrity, and Confidentiality (CIA).

7.1) Availability – Is the service available? Denial of Service (DOS, DDOS). Capacity, reliability, timely?

7.2) Integrity – errors and omissions – accurate? reliability of the system, unauthorized modification, and mistakes.
7.3) Confidentiality – secrecy/unauthorized disclosure, (Harris p. 54)

8. “Security is always a balance between risk and function (Maslowski-Yerges).”

Summary of Internet User Threats/Vulnerabilities:

- Social engineering: “tricking another person into sharing confidential information by posing as someone authorized to have that information (Harris, p. 55)”
- Lack of understanding/computer skills. What is abnormal/normal? Should I be concerned/alerted?
- Phising: “In computing, phishing is the fraudulent acquisition, through deception, of sensitive personal information such as passwords and credit card details, by masquerading as someone trustworthy with a real need for such information. It is a form of social engineering attack (http://en.wikipedia.org/wiki/Phising).”

Example of phising:

Dear client of the Regions Bank,

Technical services of the Regions Bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data:

https://online.regions.com/libregions/cmoserv/users/default/confirm.cfm

We present our apologies and thank you for co-operating.
Please do not answer to this email – follow the instruction given above. This instruction has been sent to all bank customers and is obligatory to follow.

© 2003 Regions and Union Planters

What is wrong with this email?
1) Organizations are NOT going to send an email asking you to confirm your information.
2) Urgency – Whenever you feel the email is urgent, this should be a red flag.
3) Displayed URL is different from the real URL (see red box).
4) This is a nice blend of technology and social engineering. Someone with very little skill could pull this off in under 30 minutes and mass mail it to millions of people. By the way. I used to be a customer of theirs. The target, may or may not be a customer.
Impact of this phishing email:

As you can see there is no pad-lock (non-ssl) and it is to an IP address. If I fill this out I lose my identity (my most valuable earthly possession). Get in the practice of NEVER clicking on email links. Search Google.com for it and go to it another way.

- Scams: Very diverse and creative scams. For a partial list see: http://isaaf.com/scams.shtml
- Spam: Unwanted email.
- Inappropriate content: pornography, drugs, bomb making, etc. (I will address this further below)
- Google hacks – is your credit card, social security number or child's name and school Online? You would be concerned with what information can be 'found' online. For more details see: http://johnny.ihackstuff.com/ on Google hacks.
- Buffer overflows: “In computer programming, a buffer overflow is an anomalous condition where a program somehow writes data beyond the allocated end of a buffer in memory. Buffer overflows usually arise as a consequence of a bug and the use of languages such as C or C++ that are not "memory-safe". One consequence of the overflow is that valid data can be overwritten as a result. Buffer overflows are also a commonly exploited computer security risk—since program control data often sits in the memory areas adjacent to data buffers, by means of a buffer overflow condition, the computer can be made to execute arbitrary (and potentially malicious) code that is fed to the buggy program as data (http://en.wikipedia.org/wiki/Buffer_overflow).”
- Identity Theft: Stealing your name, social security number, and/or credit card number
and using your name and good credit to commit fraud and other illegal activity. It is nearly impossible to regain a good credit score after being a victim of identity theft.

- Predators: Those searching out and hunting victims (Youth (boys and girls), and even adults).
- Personal information leak: Cookies, windows shares, what you have searched for, bought, downloaded, viewed, and email (unencrypted, offensive email), DNS digs.
- Copyright infringement. (music/MP3, movies etc)
- Peer-to-peer (P2P) file sharing vulnerabilities. If you have P2P on your machine you are opening the door for others to access your computer.
- Instant messaging vulnerabilities. Particular buffer overflows, but this can also include sniffing/logging who and what you chat. I recommend GAIM and GAIM encrypt for a chat client. GAIM can use the following chat protocols: MSN, YAHOO, AOL IM (AIM), GroupWise, ICQ, Gadu-gadu, IRC, Jabber and Napster chat. GAIM runs on Windows and Linux. In order to encrypt chat, the other person you are chatting with must have GAIM and GAIM encrypt.
- Remote control/execute – Yes, your PC can be remote controlled or can have programs launched/started remotely.
- Malware (malicious software): Viruses, trojans, worms, spyware, adware, zombie, key loggers (logs all keyboard input, including Passwords etc).
- ActiveX
- Scripting
- Java and Javascripting
- Cross site scripting
- Macros: Object Linking and Embedding (OLE) and other software launching
- Wireless Access points (covert traffic from your connection? sniff user names and passwords.
- DOS (Denial of service) and DDOS (Distributed Denial of Service).
- Data lose due to various things. Hard drive failure, little Jonny's friend that thinks he can fix your computer, virus, flood damage. Consider burning your data to a CDROM or DVD from time to time and sending it off site to a friend or relative. I use ifolder for my critical data (http://ifolderdemo.novell.com/iFolder/), which is automatically synchronized every five seconds and only changes are synchronized. The communication is encrypted and the data on the server is encrypted.

Internet Security Myths:
- Cracker vs. hacker: Think of a Cracker as a criminal (C for criminal) and Hacker as someone that is able to hack through or figure out things that others are not able to.
- To be a cracker one must be skilled or have special/extra knowledge. This is not true, criminals often do not posses extra ordinary skills. Of course there are always exceptions but as a general rule it does not require extra skills to exploit people and or systems.
- “My firewall (FW) and anti-virus (AV) program will protect me.” Not so, many exploits/risk are not blocked by your AV or FW. However, you must do due diligence and a AV and FW is part of that. Your best defense is inbetween your ears (your
Many people feel their information/data is secure seeing the lock on their browser. This too is false, because this communication is encrypted (so the transmission is usually secure). However, the data being stored on the destination system may not be secure.

Why has Internet exploits proliferated in recent years?
- Large number targets running the same OS (Windows) and same applications (Internet Explorer, Outlook and MS Office). Malware writers want the biggest impact, so they write to the largest audience.
- Haphazard software development, rush to market – feature focused and Convenience/ease vs security.
- Crackers getting more malicious as society slips on the slippery slope.
- Criminals have not changed in 1000 years. Their tools have changed. Weapons, communication and money will always be the critical elements of crime.
- Distributed computing models. In the early days of computing organizations had strict control on the system, but in recent years the system is distributed, and many people understand the inner-workings of systems.

Examples of Internet vulnerabilities/history:

In this section I highlight a sampling of security related issues.

- One out of five IT managers admitted that a hacker had gained unauthorized access to their company network (britestream.com).
- Disgruntled employee used his knowledge of the sewage system to crack into the system and release sewage (http://mailman.anu.edu.au/pipermail/link/2004-April/056025.html).”
- It is projected that 70% of all email messages in 2007 will be spam (http://cobb.com/spam/numbers.html).
- Youngster inflicted a denial of service attack, but the authorities could do little to punish or stop the penetrator until $5,000 worth of damage had been done. “Both FBI guys said similar things: They explained that until $5,000 of damage had been done, no crime had even been committed. That's the law... (http://grc.com/dos/grcdos.htm).”
- “The global economic damage from all types of digital risk including overt and covert digital attacks, malware incidence, phishing scams, DDoS and spam lies between USD 470 billion and USD 578 billion for 2004, more than double the damage calculated for 2003 by the mi2g Intelligence Unit. [Breakdown damages are available.] At an estimated 1.2 billion computer units worldwide, the damage per machine lies between USD 390 and USD 480 per machine. As of 2004, the damage caused by digital risk manifestations per machine is running equivalent to the average price of a new computer unit (http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/010305.php).”
● Studies shows that a typical virus outbreak at normal sized organizations cost $100,000 (http://securitymanagement.com/library/ICSA_Virus0604.pdf).”

● “British authorities stymied a massive bank heist that reportedly was dependent on a keylogger, the same kind of spyware that has jumped three-fold in the last year and puts consumers at risk from hackers and phishers”

Keyloggers, a type of spyware, are used by hackers and increasingly, by phishers, to snatch users account information--such as log-in names and passwords--and grab other lucrative data, including credit card numbers (http://www.techweb.com/wire/security/159901593).”

● “Spyware/Peer-to-Peer

Only six percent of employees who access the Internet at work said they have ever visited any Web sites that contain spyware; however, 92 percent of IT managers estimate that their organization has been infected by spyware at some point (http://websense.com/company/news/research/webatwork2004.pdf).”

Assessing your system for vulnerabilities:

You should test your Internet connection. One easy way to do this is by going to https://www.grc.com/x/ne.dll?bh0bkyd2 and click proceed.

Also, another service offered by grc is a check of your services/ports. http://www.grc.com/default.htm Click on shields up – It will scan your connection for problems. (Do all services/ports.)

Here is an example of my system being scanned (Configuration: My windows XP box is behind a Broadband router, which does not have a firewall, but is protecting the private network via NAT. However, my PC does have a client firewall).
Your computer at IP: 24.2

Is being carefully examined:

The port number of any location on the grid above may be determined by floating your mouse over the square. Most web browsers will display a pop-up window to identify the port. Otherwise, view the URL display at the bottom of your browser.

Text Summary

Open  Closed  Stealth
Total elapsed testing time: 27.538 seconds

Shields UP!!

Port Authority Edition - Internet Vulnerability Profiling
by The Shareware Company

Shields UP!! is checking YOUR computer's Internet connection security... currently located at IP: 24.2

Please Stand By...

Attempting connection to your computer...
Shields UP!! is now attempting to contact the Hidden Internet Server within your PC. It is likely that no one has told you that your own personal computer may now be functioning as an Internet Server with neither your knowledge nor your permission. And that it may be serving up all or many of your personal files for reading, writing, modification and even deletion by anyone, anywhere, on the Internet!

Your Internet port 139 does not appear to exist
One or more ports on this system are operating in FULL STEALTH MODE! Standard Internet behavior requires port connection attempts to be answered with a success or refusal response. Therefore, only an attempt to connect to a nonexistent computer results in no response of either kind. But YOUR computer has DELIBERATELY CHOSEN NOT TO RESPOND! (that's very cool!) which represents advanced computer and port stealth capabilities. A machine configured in this fashion is well hardened to Internet NetBIOS attacks and intrusions.

Unable to connect with NetBIOS to your computer.
All attempts to get any information from your computer have FAILED. (This is very uncommon for a Windows networking-based PC.) Relative to vulnerabilities from Windows networking, this computer appears to be VERY SECURE since it is NOT exposing ANY of its internal NetBIOS networking protocol over the Internet.
Counter measures for Internet risk:

Internet use policy (expectations, agreements and clear enforcement).

Here is an example of a policy/agreement for kids:

**'Kids' Rules for Online Safety**

1. I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.

2. I will tell my parents right away if I come across any information that makes me feel uncomfortable.

3. I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.

4. I will never send a person my picture or anything else without first checking with my parents.

5. I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the service provider.

6. I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.

7. I will not give out my Internet password to anyone (even my best friends) other than my parents.

8. I will be a good online citizen and not do anything that hurts other people or is against the law ([http://www.safekids.com/kidsrules.htm](http://www.safekids.com/kidsrules.htm)).”

“Family Contract for Online Safety
**Kids’ Pledge**

1. I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.

2. I will tell my parents right away if I come across any information that makes me feel uncomfortable.

3. I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.

4. I will never send a person my picture or anything else without first checking with my parents.

5. I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the service provider.

6. I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.

7. I will not give out my Internet password to anyone (even my best friends) other than my parents.

8. I will be a good online citizen and not do anything that hurts other people or is against the law ([http://www.safekids.com/contract_kid.htm](http://www.safekids.com/contract_kid.htm)).

**“Parents' Pledge**

1. I will get to know the services and Web sites my child uses. If I don't know how to use them, I'll get my child to show me how.

2. I will set reasonable rules and guidelines for computer use by my children and will discuss these rules and post them near the computer as a reminder. I'll remember to monitor their compliance with these rules, especially when it comes to the amount of time they spend on the computer.

3. I will not overreact if my child tells me about a problem he or she is having on the Internet. Instead, we'll work together to try to solve the problem and prevent it from happening again.
4. I promise not to use a PC or the Internet as an electronic babysitter.

5. I will help make the Internet a family activity and ask my child to help plan family events using the Internet.

6. I will try to get to know my child's "online friends" just as I try get to know his or her other friends (http://www.safekids.com/contract_parent.htm).

Can the software I use or choose not to use affect my risk?
Yes, by knowing the top targeted and top vulnerable software you can reduce your risk.

“In the update released on Monday, the vulnerable software packages identified by SANS as being highly targeted and highly vulnerable -- if unpatched -- include the following:

1. Microsoft Internet Explorer.
7. Antivirus Products from Symantec, F-Secure, TrendMicro and McAfee.

Do I have a choice on what Internet browser to use?
Yes, of course you have a choice (Microsoft does not own the world...yet). One of the better choices is Mozilla's Firefox browser. I have been happily using firebird/firefox instead of Internet Explorer for several years. After using Firefox as my primary browser my anti-spyware tools stopped finding/alerting me to spyware/adware. As of June 15, 2005, Firefox web browser has been downloaded 64,303,778 times (spreadfirefox.com).

Basic system lock-down/hardening:
You should disable all file shares. To do this, Start | settings | control panel | administrative tools | computer management | shared folders | shares | Now make a note of any non-default shares you should browse to and unshare them (right click the directory that is shared and go to sharing and disable it). Even better, uninstall or disable file and print sharing.

Default shares shown:
You should also disable unneeded services to 'harden' your PC. Search google for good articles for which services to disable (this is beyond the scope of this document).

For example: Do NOT install/configure file sharing or peer-to-peer (P2P) software like Bearshare, Napster, IRC, Nutella, etc.

For example, here is a screenshot of the services my PC is running and I can configure them to not auto start/run by selecting MANUAL.
Also, you should consider uninstalling unneeded software or old software you no longer use.
NEVER, NEVER delete or remove something you do NOT understand as this may adversely affect your system. Search the Internet (my favorite search engine is google.com) for the file/application before removing or deleting it.

What is in your system startup?
Start | run | msconfig
Also, for more advanced users you can check (disable) services in your RUN key in the registry. Start | run | regedit | HKLM\Software\Microsoft\Windows\CurrentVersion\Run
General rules and guidelines for Internet safety (safeguarding against pornography).

What do I do if I get unwanted porn pop-ups?
It is not uncommon for predatory porn pushers to hi-jack your browser with endless pop-ups that you are not able to close without many others opening.
You should be ready to react quickly. This the counter measure I suggest:
1) Simply turn off your monitor.
2) Once your monitor is off, you can press the Windows key (between the left CTR and left ALT keys) and then M (which minimizes all windows). Then you can click start | shutdown. Or, you can simply power off your computer (but it may cause your system harm, better your system than yourself).
3) Afterwards you'll want to run anti-spyware tools to clean your system (many porn pushers will put hooks into your browser to auto-launch other unwanted sites).

Preventive Measure: Use Firefox that has a native pop-up blocker. And a porn filter (discussed below).

“Pornography and Internet Safety

Parents can do many things to safeguard their homes from the harmful influences found on the Internet. While there is no foolproof system, some simple steps can help reduce the risk of family members seeing pornographic materials on the Internet.

1. Place computers in high-traffic areas of the home. Kitchens, family rooms, and studies usually have the most traffic. Because these rooms usually don’t have doors, they are typically less secluded than bedrooms. Position computer monitors so the screen faces out for public view.
2. Install a filtering program, and learn its features and how to use it. Good filtering programs allow you to view a history of which sites (including chat rooms) have been visited and when, as well as a record of incoming and outgoing e-mails. Information on filtering programs can be found on Internet sites such as www.internetfilterreview.com.
3. Teach family members about the dangers of Internet pornography, including how to escape if an inappropriate site is accidentally accessed. This usually involves shutting down the entire system.
4. Teach family members to tell parents if they encounter any form of pornography while on the computer. This will help reduce the fear or shame of accidental exposure. It also serves to open discussion about the dangers of pornography.
5. Teach family members to use the Internet for a specific purpose only. Aimless surfing makes it easier to wander onto inappropriate sites.
6. Instant messaging is a cost-effective, easy way to communicate with family
and close friends. However, teach family members to avoid public chat rooms, bulletin boards, or unfamiliar areas on the Internet. Such places present an unnecessary risk for children and adults.

7. Teach children not to share any personal information online without parental knowledge and permission. Many predators pose as children to gain access and information that may put children at risk.

8. Educate yourself about your computer and how the Internet works.

9. Be aware of what your children’s school and public library policies are regarding Internet use and accessibility.

10. Teach family members to never open e-mail from someone they don’t know.

The Internet is a wonderful tool and resource for families, but caution must be exercised in order to protect families and individuals from the potential dangers that are present online (http://www.providentliving.org/content/display/0,11666,5302-1-2769-1,00.html).

"We must give our Nation's children every opportunity to grow in knowledge while protecting them. Parents have the first responsibility for protecting children online, by paying attention to their children when they are on the Internet, and by preventing children from giving out personal information online."

President George W. Bush
U.S. President
(http://www.comptia.org/pressroom/election_2004.aspx)

Minimum Technical counter measures for Internet Users:

Many security professionals will tell you that technology is the answer to your security risks. Technology is only PART of the solution. Your best defense is your human brain by being suspicious, careful, and be continuously vigilant.

In this section I will talk about the minimal tools you need running on your system as a minimum.

1) Anti-Virus: With the broad base (proliferation) of Windows, virus writers largely target Windows systems (they are easy targets too). Many people recommend different Anti-Virus vendors. The main three are: Symantec, Mcafee, and Trend Micro. However, these can be expensive for the home user on a budget. I often recommend a free Anti-virus solution called AVG. You can find the free version at: free.grisoft.com
Another free tool to neutralize viruses (not preventative) is Stinger. Stinger can be downloaded from (you will always want to download the latest one as it is updated often): http://vil.nai.com/vil/stinger/

Please note you will of course need to configure your Anti-virus solution to auto-update as new viruses come out every day, and all (most) anti-virus vendors have a weekly anti-virus database pattern update. If you do not update your anti-virus program weekly you are at risk.

2) Anti-Spyware/Malware. There are commercial solutions, which are great for corporations, but home users often will not use anti-spyware unless it is free or low cost. Please note that almost all anti-spyware is really Spyware. The ONLY two free anti-virus solutions you should use is Adware (www.lavasoft.com) and Spybot - Search & Destroy (http://www.safer-networking.org/en/download/). Many recommend running both programs. Anti-spyware tools must be continuously updated too.

Once you have run adware and Spybot to clean your system you may still have spyware or hooks into your system.

What do you do if you still have spyware after running spybot and adware?
2.1) Reinstall the OS (usually beyond most home users capabilities – and you must be careful or you may lose your data). 2.2) Visit http://spywarewarrior.com/swww-help.htm and follow their instructions. Before posting your report of 'hijack this' scrub your log for personal information.

Configuring your anti-spyware tool:
I configure spybot to auto-scan my machine three minutes after I boot and to auto-update its 'pattern' (database of what spyware/adware looks like). By using firefox and being a savvy Internet user, I rarely ever have any spyware.

3) Firewall: A firewall blocks ports/services. What is a port? Think of a port as a door or window to your home. So, an IP address is similar to your street address and a port is similar to a door or window. You will want to 'lock' your doors and windows that you do not use, or only allow certain people to pass through your doors/ports.

You guessed it, firewalls must be auto-updated too.
After Windows XP SP2 Microsoft implemented a 'lite' firewall for users, most people will be happy with XP SP2 firewall (FW).

Popular 'client' firewalls.
3.1) zonelabs.com (Browse their website until you find the free personal one)
3.2) www.blackice.com/PCProtection-Firewall.htm for about $40
3.3) I use the Novell Client Firewall, which is free to those that own Novell BorderManager (an enterprise perimeter firewall).
3.4) XP SP2 default firewall.

In addition to a client firewall you should have a border or perimeter firewall. An example of a perimeter firewall would be a Broadband Router (used to share one Internet connection). Even if your broadband router is only doing Network Address Translation (NAT) (NAT translates your internal/private IP address to the public/routeable IP address) you are shielding your PC (external devices see you as your broadband router's IP address and your PC is not directly plugged into the Internet). NAT is a good start, but you also need a packet filtering Broadband router.

A word about firewalls, THEY MUST BE CONFIRUGED CORRECTLY!!!

4) Stop using Internet Explorer!!!
Use firefox for all your browsing and your spyware/security issues will decrease significantly. Sure, there may be a site or two that firefox will not work on. Then you must use Internet Explorer (IE) for those few sites. Use firefox for most of your browsing and your spyware/security issues will decrease. Download the awesome/free Firefox at: mozilla.org/products/firefox/
Sure, firefox is not perfect and has security issues, but it is significantly better.

5) Use another OS other than Windows. I recommend Linux. Many choose MACs (Macintosh). Most Linux distributions have a native firewall and currently there is very little virus risk on Linux.

6) Update your OS (Windows operating system) and your applications regularly. Many applications can be configured to auto-update, which is key because if they are not configured to auto-update home users rarely will manually update.

Conclusion:
Knowledge is power. Our best defense is knowing our risk and mitigating it. There is no fully secure system and no foolproof process to guarantee safety. However, being more secure than others offers protection as predators move onto easier targets (the slowest deer gets eaten by the lion). In this document I have outlined basic guidelines on how to be a faster/smarter prey. I hope you will now take on a new outlook Online life/perspective. Be very, very suspicious and have a 'mode of operation' that if you follow will prevent/mitigate your risk of using the hostile Internet. The Internet is a wonderful place if you know the rules and abide by them.
**Annotated Bibliography**

britestream.com (n.d) Research Reveals False Sense of Security Among Network IT Managers


“an unexpected 1 in 5 admitted that a hacker had gained unauthorized access to their company’s network”


“[Boden], an engineer, had been employed by Hunter Watertech as its site supervisor on the project [to install Maroochy Shire Council’s sewerage control system] for about two years. [He didn't get a job with the Council, so he used his knowledge of the system to crack into it]”

cobb.com (n.d) Spam by the numbers


70%... “Percentage of all email messages that will be spam by 2007”

grc.com (2005) The Strange Tale of the Attacks Against GRC.COM


“Both FBI guys said similar things: They explained that until $5,000 of damage had been done, no crime had even been committed. That's the law...”


I plan to quote and or paraphrase security principles from this book. I read and re-read this book when I studied to challenge the CISSP exam. Now, after passing the exam I find myself going back to it as a reference book. This book covers well the 10 common body of knowledge (CBK). The 10 CBK's are: Security

Retrieved May 24, 2005 from  
http://www.novell.com/coolsolutions/appnote/1651.html

I will quote general computer security principles from this source.

mi2g.com (2005) The end of computing culture as we know it?  
Retrieved May 25, 2005 from  
http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http% 3A//www.mi2g.com/cgi/mi2g/press/010305.php

“...The global economic damage from all types of digital risk including overt and covert digital attacks, malware incidence, phishing scams, DDoS and spam lies between USD 470 billion and USD 578 billion for 2004, more than double the damage calculated for 2003 by the mi2g Intelligence Unit. [Breakdown damages are available.] At an estimated 1.2 billion computer units worldwide, the damage per machine lies between USD 390 and USD 480 per machine. As of 2004, the damage caused by digital risk manifestations per machine is running equivalent to the average price of a new computer unit.”

providentliving.org (n.d) Pornography and Internet Safety  
Retrieved May 24, 2005  
http://www.providentliving.org/content/display/0,11666,5302-1-2769-1,00.html

I plan to quote and use the information from this site.

securitymanagement.com (n.d) Computer Virus Prevalence Survey (Executive Summary)  
Retrieved May 25, 2005 from  

Cost of Virus outbreak disaster = $100,000

techweb.com (March 2005) Keyloggers Foiled In Attempted $423 Million Bank Heist  
“British authorities stymied a massive bank heist that reportedly was dependent on a keylogger, the same kind of spyware that has jumped three-fold in the last year and puts consumers at risk from hackers and phishers”

“Keyloggers, a type of spyware, are used by hackers and increasingly, by phishers, to snatch users account information--such as log-in names and passwords--and grab other lucrative data, including credit card numbers.”

websense.com (2004) Web@Work Survey Results 2004

“Spyware/Peer-to-Peer
Only six percent of employees who access the Internet at work said they have ever visited any Web sites that contain spyware; however, 92 percent of IT managers estimate that their organization has been infected by spyware at some point.”

wikipedia.org, (n.d) Web-based, free-content encyclopedia that is written collaboratively by volunteers
I plan to use wikipedia.org to define many technical terms including phising.

isaaf.com (n.d) Scams
This resource lists the reported scams. If something sounds too good to be true, you ought to check it out here.

ihackstuff.com (n.d) Google hacks resources. What information you can find out, simply by using google's advanced searches.
This is a eye opener, proving someone does not need a lot of technical knowledge to exploit people and systems.

spreadfirefox.com (2005) Site dedicated to the spreading of firefox.
I will use the download counter of Firefox to show its common use. Now over 64 million downloads.

grisoft.com (n.d.) A Anti-Virus Vendor who also offers a free AV for personal use.

Retrieved June 15, 2005 from free.grisoft.com

nai.com (n.d.) A one time virus neutralize.


A free tool to 'sting' or kill a virus on your system. It does not guard against future viruses though.

lavasoft.com (n.d.) A free Anti-Spyware tool.


safer-networking.org (n.d.) Spybot search and destroy mirror.


A good place to download the free anti-spyware, Spybot search and destroy.

spywarewarrior.com (n.d.) A great resource to clean your machine from spyware.


Collaborative help on manually removing spyware from your machine. If you have lost hope of cleaning your machine, get the help of these guys. They are great!

zonelabs.com (n.d.) A good place to download zonelarm, a free personal firewall.

Retrieved June 15, 2005 from zonelabs.com


I will reference this site as a recommended personal firewall.
Appendix A – Additional Online Materials for families.

“ADDITIONAL ONLINE MATERIALS

"NetSmartz Workshop www.netsmartz.org, 2004. The NetSmartz Workshop is an interactive, educational safety resource that teaches kids and teens how to stay safer online. (Note: This site is not affiliated with nor endorsed by the Church.)

Kid Smart Web Site www.kidsmart.org.uk, 2004. This site focuses on five safety tips for children to remember when using the Internet. (Note: This site is not affiliated with nor endorsed by the Church.)

ContentWatch Web Site www.contentwatch.com, 2004. This site lists family-safe sites, online safety tips, and other helpful information. (Note: This site is not affiliated with nor endorsed by the Church.)

Web Wise Kids Web Site www.webwisekids.com, 2004. This nonprofit organization is dedicated to teaching adults and children how to avoid online predators. (Note: This site is not affiliated with nor endorsed by the Church.)

Pornography and Internet Safety www.providentliving.org, 2004. Parents can do many things to safeguard their homes from the harmful influences found on the Internet. This page includes some helpful safety tips (http://lds.org/topics/1.8170,1569-1-118,00.html).”