A Guide to Internet Safety

Presented by

David Demland

Overview

This guide was developed to show some of the risks when using the Internet. Parts of this guide will be important for anyone using the Internet, other parts will be more use to parents in understanding the risks their children face when they use the Internet, and other parts will be more use to children to help them learn, and understand, the risks they face when using the Internet. The hope is to help improve the Internet experience for everyone who uses the Internet, or wants to start using the Internet.

This guide has been setup so that it may be a quick reference of information. In no way will the information in this guide be a complete view of any single issue. It is to be an overview of the presented information and used as a starting point of the basic knowledge. There are many references that may be used to gain farther knowledge in any specific area.

Internet and Children

Before diving into the detail issues of Internet Safety, there needs to be a baseline of information that has to be established. The following statistics are being presented to established this baseline as to what the risks are for children on the Internet today.

- Forty-five percent of children in the United States use the Internet.[1]

28 PC World (February 2005) Scott Spanbauer and Steve Bass The New Web Challengers.

29 http://www.usatoday.com/tech/news/2004-07-01-cyber-threat_x.htm

30 Ibid.

31 http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=41867

32 http://www.webopedia.com/TERM/r/router.html

33 http://www.webopedia.com/TERM/f/firewall.html

34 http://www.cybersitter.com

35 http://www.netnanny.com

36 http://www.afafilter.com

37 http://www.webuser.co.uk/news/news.php?id=41614

38 http://www.webopedia.com/TERM/c/cyber_crime.html

39 U.S. Department of Justice OVC Bulletin December 2001

13 Ibid.

14 Ibid.

15 Ibid.

16 Ibid.

17 http://www.webopedia.com/TERM/M/malware.html

18 http://www.webopedia.com/TERM/v/virus.html

19 http://www.webopedia.com/TERM/w/worm.html

20 http://www.webopedia.com/TERM/T/Trojan_horse.html

21 http://www.webopedia.com/TERM/p/phishing.html

22 http://helpdesk.its.uiowa.edu/security/phishing.htm

23 http://www.webopedia.com/TERM/p/pharming.html

24 http://www.webopedia.com/TERM/s/spyware.html

25 http://www.webopedia.com/TERM/a/adware.html

26 http://www.networkmagazineindia.com/200503/newsanalysis01.shtml

27 http://www.theage.com.au/articles/2004/10/26/1098667733033.html?oneclick=true

- 81% of parents of online teens say that teens aren't careful enough when giving out information about themselves online and 79% of online teens agree with this.[2]
- 65% of all parents and 64% of all teens say that teens do things online that they wouldn't want their parents to know about.[3]
- One in 5 youth received a sexual approach or solicitation over the Internet in the past year.[4]
- One in 33 youth received an aggressive sexual solicitation in the past year. This means a predator asked a young person to meet somewhere, called a young person on the phone, and/or sent the young person correspondence, money, or gifts through the U.S. Postal Service.[5]
- One in 4 youth had an unwanted exposure in the past year to pictures of naked people or people having sex.[6]
- Only 17 percent of youth and 11 percent of parents could name a specific authority, such as the Federal Bureau of Investigation (FBI), CyberTipline, or an Internet Service Provider (ISP), to which they could report an Internet crime, although more indicated they were vaguely aware of such authorities.[7]
- Number of porn sites grew from 14 million to 260 million from 1998 – 2003.[8]
- Cybersex industry is expected to grow to 5 –7 billion dollars by 2007.[9]
- More than 20,000 images of child pornography are posted on the Internet every week.[10]
- One in five children who use the computer chat rooms have been approached over the Internet by a pedophile.[11]

- 89% of sexual solicitations were made in either chat rooms or Instant Messages.[12]
- Only 25% of youth who received sexual solicitation told a parent.[13]
- 26 popular children's characters, such as Pokemon, My Little Pony, and Action Man, reveled thousands of links to porn sites. 30% were hardcore.[14]
- 43% of children said they do not have rules about Internet use in their home.[15]
- The majority of teenagers' online use occurs at home, right after school, when working parents are not at home.[16]

These facts are not being shown just to start a panic, they are being shown so that the risks that children face may become more real. The fact is that children today are being introduced to technology at such a young age, that technology has become part of their world. The world that they see as safe from the "bad things" that are happening in the news.

In some ways nothing could be farther from the truth. Children are just as unsafe with technology as they were without it. All technology has done is to allow predators to use different means to do their evil work and make it harder for them to be found.

Today the FBI employs teenagers to help teach FBI agents to "talk like kids" on the Internet to help find these predators. A story that has been circling around the Internet to show how law enforcement is using these type of "kid talk" tools can be found at *http://www.wiredsafety.org/*

References

1 The Pew Internet & American Life Project, 2001

2 3/17/2005 - Pew Internet & American Life Project report; http://www.pewinternet.org/PPF/r/152/report_display.asp

3 Ibid.

4 Finkelhor, David, Kimberly J. Mitchell, and Janis Wolak, 2000, Online Victimization: A Report on the Nation's Youth, National Center for Missing & Exploited Children: Arlington, VA.

5 Ibid.

6 Ibid.

7 Ibid.

8 http://www.protectkids.com/dangers/stats.htm

9 Ibid.

10 Ibid.

11 Ibid.

12 Ibid.

Yahoo! Messenger:
msg.edit.yahoo.com/*
Yahoo! Messenger:
messenger.yahoo.com/*
http.pager.yahoo.com/*

askparry/special_reports/spr1/qa19.html. This is a great story that every child, and parent, should read. The best part of this story is that it shows how personal information can be given out without identifying that it is personal information being given out.

General Computer Information

Before looking at the direct risks of the Internet, there needs to be an understanding that some of these risks involve the heart of the computer. Many times evil work occurs because of a flaw with the operation of the local computer system. In short to reduce the risks of problems from the Internet, the diligent work must start at the local computer system that is being used to access the Internet.

Operating System

The Operating System, OS, is the heart of the computer. This is what allows the computer to do its work. The OS allows programmers to create programs for different tasks. Most of the time these programs are for legitimate use. Examples of these legitimate type of programs are: Word Processors, Spreadsheet, and Point of Sale Systems. Other types of programs that can be written are not for legitimate use. These illegitimate type of programs are: keystroke capturing programs, Website tracking programs, and Website redirection programs.

OS Updates

Since the OS is the heart of the computer, it can be a very good target for hackers. A weakness in the OS can leave the computer at the mercy of a hacker. Ways to reduce the risk of the hacker being able to take control includes updating the OS. An OS update, or patch, is new software that is added to the OS to fix a software defect. There are many different types of patches applied to an OS.

Some of these patches are to fix security problems that have been discovered. These patches are often referred to as a critical, or security, update. These updates need to be applied as soon as possible to a system. This is due to the risk of a hacker using a vulnerability to “take over” a system. Another type of patch is an application patch. An application patch fixes defects in an application that do not present a security risk. Many of these patches do not need to be applied unless there is a problem running the current software, or there is a new feature that has been added that may be needed. If an application patch is installed, it may be hard to see a difference, unless there was a known problem running the application that the patch fixed. The good news is that almost all platforms have some sort of automatic update. Automatic update is where the system can be configured to get all the security patches automatically. This way the system will always be up to date with its security patches. The downside is that the system needs to be turned on and running at the time the update is scheduled, or the update will not occur.

Appendix 1

Applications	Port Numbers	Type	Comments
IRC	194	TCP	
ICQ	5190	TCP	NOTE: ICQ by default will use this port to connect, and any available port above 1024 to listen for new connections. This is kind of insecure, so go to the ICQ site and read their firewall configuration information
AOL messenger	5190, 4099	TCP	Also will self configure to available ports.
MSN messenger	6891-6900	TCP	For file transfer
MSN messenger	6901	TCP/ UDP for voice	Otherwise self configures messaging.
Kazaa	1214	TCP	Can be reconfigured within Kazaa.

Block Internet Messengers by URL:

AOL Instant Messenger:
- login.oscar.aol.com
- toc.oscar.aol.com
- login.icq.com

MSN Messenger:
- gateway.messenger.hotmail.com

ICQ:
- login.icq.com
- http.proxy.icq.com

Contact Resources

National Center for Missing & Exploited Children
699 Prince Street
Alexandria, Virginia 22314-3175
Hotline:1-800-THE-LOST (1-800-843-5678)
On the Web: www.missingkids.com

www.cybertipline.com

www.warningsigns.info/chat_rooms_warning_signs.htm

www.netsmartz.org

www.fbi.gov/publications/pguide/pguidee.htm

kids.getnetwise.org

yahooligans.yahoo.com/parents

http://www.sdcda.org/protecting/children_parents.php

http://www.google.com/Top/Computers/Internet/Child_Safety/

http://www.protectkids.com

http://www.sdcda.org/protecting/children_parents.php

Malware

Malware, as defined by webopedia.com, is short for *mal*icious soft*ware*, software designed specifically to damage or disrupt a system.[17] The more common terms that malware is referred to is virus, worm, or Trojan Horse. This section is intended to give an overview of each of these different types of malware as well as what they do. Understanding the risks of this malware can only be understood in the light of what type of malware that is being used.

A virus, as defined by webopedia.com, is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.[18] This is one of the most common forms of malware. These types of malware can capture every keystroke and log it, allowing a hacker to find out login IDs and passwords. It can also be code that will attack another system to block it from legitimate users. This type of attack is called a Denial of Service, DOS, attack. Many times this malware is delivered to a system through an E-Mail.

A worm, as defined by webopedia.com, is a program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.[19] This malware is usually a virus that has extra code to replicate itself to other systems. One of the most common ways this is done, is by using an E-Mail client. The worm is

delivered in an E-Mail, and when executed, it uses the address book to replicate itself to other systems. A worm can be used to launch a DOS from many different systems. This type of attack is called a Distributed Denial of Service, DDOS, attack.

A Trojan Horse, as defined by webopedia.com, is a destructive program that masquerades as a benign application.[20] A great example of this is software that is used to block pop-ups, but in turn, does its own pop-ups on the system. A Trojan Horse are also called an *illicit server.* This is because most Trojan Horses will open what is called a "back door" to the system. This back door can be used to take over the system and use the system, or worse, take data from the system.

The way to reduce the risks of malware on a system is to use *Anti-Virus Software*, or *Virus Software* for short. Virus software is software that has been developed to find and clean different types of malware. Today most of the major virus software will not only identify malware, but it will also identify the malware type. This is a good feature to the software because it allows the ability to identify if there is any more risk due to the malware. For example, if the malware found is a Trojan Horse, the system can be inspected closer to see if there are risks associated with the malware even if the malware has been removed.

The best way to keep the virus software working at its peak, is to ensure the signature files are up to date. The signature files are the files that contain the data needed for the virus

- yahooligans.yahoo.com/parents
- http://www.sdcda.org/protecting/children_parents.php
- http://www.google.com/Top/Computers/Internet/Child_Safety/
- http://www.protectkids.com

There are many places to get an Internet Usage Contract on the Internet. The San Diego District Attorney's office has one at their Website *http://www.sdcda.org/protecting/children_parents.php*.

National Center for Missing & Exploited
Children
699 Prince Street
Alexandria, Virginia 22314-3175
Hotline:1-800-THE-LOST (1-800-843-5678)
On the Web: www.missingkids.com

If the report is being filed through the Website please select the CyberTipline line on the left side of the page. The CyberTipline may be reached directly by going to **www.cybertipline.com**.

Remember there is a simple rule for the Internet: **Do not reveal personal information over the Internet to anyone, unless the source requesting the information has been validated as a trusted source**.

Resources

The good news is that there are many resources on the Internet that can be used to find more information about some of the risks that have been explored in this guide. The following is a list of some resources that can be used for information. Many of these resources include various statistics to help clarify risks. They all contain information, in some form, to help identify possible problems or how to avoid problems when using the Internet.

- www.warningsigns.info/chat_rooms_warning_signs.htm
- www.netsmartz.org
- www.fbi.gov/publications/pguide/pguidee.htm
- kids.getnetwise.org

software to find the different malware in a file. This file contains the virus signature and the process needed to remove the virus from the system. If this file is not up to date, then new virus' can be missed and not cleaned.

Most virus software will have a feature that is called a "real time scan". This feature allows the virus software to scan files when the files are accessed. The issue now becomes complacency. Most users will assume that the real time scanner will catch all the virus problems. The real time scan does not replace the regular disk scan, it supplements the disk scan. A disk scan needs to be done on a regular basis to ensure that nothing is missed. The good news is that the disk scan does not have to be done as often, and can be done automatically when the system is not in use; so long as the system is on and running.

Hacker's Tools

For a hacker to be successful, they must first gather valuable information from the victim. There are many tools available to the hacker in their tool kit. Many of these tools will allow the hacker to get the necessary information without tipping off the victim. In fact many times the victim will be more than willing to give this information to the hacker. Unfortunately, the victim will never know that it is the hacker that has been given this information in most cases.

Phishing

Phishing, as defined by webopedia.com, is the act of sending an E-Mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.[21] Although E-Mail is the most common tool used in phishing, some hackers will also use the phone to make their phishing attempts. In general do not give out personal information unless you established the original contact with another party. Here are some rules of thumb to help reduce the risk of successful phishing scams:[22]

- Always be suspicious of E-Mails asking for sensitive information.
- Never respond to an email request for personal information.
- Never follow the links in an email you suspect might be phishing.
- Consider installing a toolbar that blocks scam sites.
- Always make sure your operating system, anti-virus software, and browser are up to date.

One of the best ways to avoid phishing attempts is to use the Internet to help decipher if an attempt has been received. Sites such as **www.antiphishing.org** is a great place to check to see some of the more common phishing scams that are currently being used.

Since phishing attempts may come by phone, it is important not to forget that the phone can be a tool of a hacker. If a phone call is received, it is important to know the source of

Ways to reduce these risks, listed at the same site, are:

- Place your computer in a common area of the house.
- Educate yourself about computers and the Internet.
- Spend time with your children online.
- Make reasonable rules and set time and use limits. Enforce them.
- Educate yourself and your child about the dangers of the Internet.
- Do not allow your child to go into private chat rooms, especially when you are not present.
- Reinforce the guiding rule, “Don't talk to strangers.”
- Put accounts in your name and know your child's passwords.
- Never allow your children to arrange a face-to-face meeting with someone they met online without your permission.
- Do not let your child give out any personal information of any kind on the Internet.
- Do not let your child download or upload pictures without your permission.
- Utilize your Internet Service Provider's parental controls and commercial blocking and filtering software tools.
- Be sensitive to changes in your children's behaviors that may indicate they are being victimized.
- Be alert to a teenager or adult who is paying an unusual amount of attention to your children or giving them gifts.
- Be aware of other computers your children could be using.
- Be aware of your child using another person's screen name.
- Develop a “contract” with your children about their Internet use.
- Review the use histories or logs of your computer to see where your children have been.

If there is a reason to believe that a child is involved with a predator on the Internet, then report the incident right away. The way recommend by the FBI to report this type of issue is by contacting the Center for Missing and Exploited Children. They can be reached at:

their business without all the risks of personal contact. With the use of technology these predators can avoid public places such as schoolyards, playgrounds, and shopping malls and instead use the privacy of the victims home to carry out much of their work.[39] It is now up to parents to look for signs at home that there might be a problem.

There are ways that these risks can be reduced. The best rule to follow for children on the Internet, is that they have no privacy rights. Leaving children alone on the Internet will only increase the risk of a child falling into many of the statistics mentioned in this guide. Parents need to ensure that children are following rules that have been established for Internet usage. This will mean that parents will need to look at E-Mail, monitor Websites visited by children, and lockout Websites, or pages, that a child should not be at.

Most of the time there will be warning signs that there are possible problems. Parents need to understand these signs and take proper steps if these signs start showing up. The following list is a great starting point that has been created by the San Diego District Attorney's Office. They are found at *http://www.sdcda.org/protecting/children_parents.php*:

- Unsupervised time in chat rooms
- Downloaded photos of strangers
- Downloaded pornographic pictures
- Phone calls, gifts or letters from strangers
- Using an online account that belongs to someone else
- Changes in behavior and being secretive about online activity
- Quickly turning off the computer or changing the screen monitor when someone else enters the room

the phone call for trustworthiness. Ways to help find out the source of the phone call can include caller ID. If a call is received that says it is from a business, then the caller ID should reflect that business. If the caller ID does not reflect the business name, or is withheld, then be suspicious of the call until it can be proven, beyond a reasonable doubt, that the call is from the business that it is professing to be from.

If there is no caller ID, or the ID is blocked, then try to get a call back number that can be used some other time. Call this callback number during the next business day to confirm that the business is who they said they were. This is a good process for verifying the business. Remember not to give out any personal information until the business has been confirmed.

Pharming

Pharming, as defined by webopedia.com, seeks to obtain personal or private (usually financial related) information through domain spoofing.[23] In this type of scam, a different approach is used to get information from a user - an approach, that will most often hide, the fact that the user is not where they think they are. There are two ways that pharming can be done.

The first is to compromise a server on the Internet and redirect traffic from one Website to another Website. This is hard to do because the hacker must attack an Internet server and change its data, but it is definitely not undoable.

The second way is to insert code onto the victim's computer and let it wait until the user goes to a particular Website. At that moment the dormant code wakes ups, intercepts the request, redirects the request to another Website, then changes the URL display to show the victims's intended site and goes back to sleep. The risk with this code is that it may redirect a user from multiple sites, it does not have to redirect only a single site. For this type of pharming to be successful it requires software to be installed on the victim's computer. This is where anti-virus software can be useful in removing the threat.

From a legal view, Website redirection is a real problem if the redirected site is located outside the U.S. Websites that are hosted on servers outside the U.S. are very hard to prosecute under U.S. law.

Spyware / Adware

Spyware, as defined by webopedia.com, is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes.[24] Adware, as defined by webopedia.com, is a form of spyware that collects information about the user in order to display advertisements in the Web browser based on the information it collects from the user's browsing patterns.[25] Since both definitions are close to the same it is not uncommon to hear the term spyware used for both spyware

re-enable them when they are done. This will leave the children of the house in a position that they can bypass the parental controls that have been put into place, thus the children are not protected like parents think they are. The key point here is that if the children, in the house, are the Internet experts, then there has to be a change to make the parents just as much of an expert or more so.

There is a great Website that can be used to show how content filter, and other issues of the Internet, work. Please refer to **http://www-personal.umich.edu/~csev/hng/book/11content/11content.htm**.

Cyber Crime and Risk Reduction

Webopedia.com defines cyber crime as:

> Cyber crime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet.[38]

As this definition shows there are many different types of cyber crime, and many of these are traditional types of crime. As stated before, the major problem with cyber crime is that it is, in many cases, harder to detect and it may be time consuming to find the perpetrator.

One of the concerns with the Internet is that it has made the predator's job a little safer. A predator can now conduct

information. The down side is that the information must be known first. So how are children protected if the information is not known before hand? The answer comes in the form of what is called *content filtering*. Content filtering is a form of security that look at the text on the web page. If the text falls into certain requirements, then the page is not allowed to be displayed.

There are many ways that content filtering can be achieved. In many businesses this is done with very sophisticated software that takes higher level expertise to configure and maintain. This approach is called a *proxy server.* In this approach, a server is setup that all web pages pass through. This is done so that no one on the internal network can bypass the proxy server. This is a very high level of security and it can protect the business from many legal issues. The problem is that this type of approach is not necessarily reasonable for home use.

This does not mean that there is no way to do content filtering at home. There is software available to do this content filtering that runs on the local computer. Software like *CYBERsitter*[34], *Net Nanny*[35] and *American Family Association*[36] are just a few of the many different content filters that can be used on local computer systems. Most of these will provide very good security for home use. There is one fact that needs to be kept in mind about these software packages. In most homes children feel that they are the main Internet experts.[37] If this is the case, in a home, then there is a good chance that the children can disable these tools and

and adware. For that reason spyware will be used to mean both.

Spyware can be downloaded and installed without the user's knowledge. It is for this reason that user's need to be aware of what Websites they go to and software they allow to be installed from a Website. On some occasions, spyware that is download will show a signature for a trust source, remember that this signature can be spoofed. This means that a signature can be displayed from a site that is not the real creator of the software. The rule: *Beware of what software is allowed to be installed on a system*.

Spyware has become one of the major focuses in IT today. A recent survey showed that the IT industry considers spyware as one of the Top Network Security threats in 2005.[26] This threat does not exist not only in the business environment, but at home as well. A survey of 329 dial-up and broadband adult computer users by the US National Cyber Security Alliance and America Online has found that 80 percent of home computers were infected with spyware or adware of some kind.[27] As these numbers show, most home users do not understand the risks that spyware brings to the home environment.

Spyware can be used to record all the keystrokes entered at a computer and send this information back to a hacker. With this information a hacker can obtain user names and passwords for virtually every Website the user will go to. Also, it is possible for this spyware to find user accounts and passwords on computer systems. Spyware can also

track what Websites are visited, and thus be used to track a user's surfing habits. All of these uses are considered by some to be an invasion of privacy. The privacy issue is by far one of the hottest topics when it comes to spyware. Another hot topic, in regards to spyware, is loss of productivity. Since spyware enhances the number of pop-ups on a computer, it can slow down the computer to the point that users can not get their work done.

To remove spyware, spyware removal software needs to be installed and used. Spyware removal software is similar to anti-virus software, but it has some of it's own characteristics when it comes to running and updating the signature files. User's should run the spyware removal software on a regular basis to ensure that all spyware threats are addressed.

Internet Browsers

The hacker's tool box not only contains software that they install on a computer, it contains software that comes with the OS that has security holes. One of the most common tools used today on the Internet is an *Internet Browser*, or *Browser*. A browser is software that is used to look at information on the Internet. There are many different browsers. Internet Explorer, IE, by Microsoft is the most common browser. Firefox by the Mozilla Organization is a newer browser that is starting to get a strong following. There are other browsers as well, but these other browsers are falling behind these first two groups of browsers.

Website as well as participate in a chat room. The child may be allowed to play the games, but be restricted from the chat room.

Sometimes it is important to restrict a whole Website. For a long time both whitehouse.com and nasa.com would take a user to a porn site. Children would often type these names when they really wanted whitehouse.gov or nasa.gov. Routers with the ability to block whole Websites can allow for the extra security of blocking these types of problems.

One thing to remember is, that by using the router to block domains and Websites, only known sites can be blocked. There is no way to block sites that have not been entered into the router. This sort of blocking can be looked at as "closing the barn door after the horses got out".

One way to be proactive is to block the chat room, or Internet messenger software, at the router. This can be achieved by blocking what are called ports. When ports are blocked, this type of software will not be allowed to work for anyone on the inside of the router. The problem is it takes more knowledge to understand how to configure and block these ports. See *Appendix 1* for a list of ports for the different software.

Content Filtering

Routers and firewalls can only do so much to protect children from the Internet. As it has already been demonstrated, routers can be very effective at blocking

A firewall is a device that is designed to keep external data on the external side of the network.[33] This is the one device that all networks should have at the edge of the network. The network edge is the router that interfaces both the internal network and the external network. A firewall is the best device to have at this edge point. All firewalls are routers, but not all routers are firewalls, it makes sense to have a firewall as the edge router.

A firewall will protect private data from the outside world better than a router. Because of this protection small networks should have some sort of device like a D-Link DI-604 for wired situations, or a D-Link DI-624 or the Linksys WRT54G for wireless situations. All of these low cost routers have configureable firewalls which make them very strong candidates for the small network use.

Beside the goal of a configureable firewall, these routers also have both domain blocking and URL blocking. What this does, is allow for the router to be configured in such a way that the router will block certain Websites or particular Web Pages of a Website. There are many reasons this is a good feature.

With the risks so high for children when they are in a chat room (as seen in the section entitled *Chat Rooms / Internet Messenger*), having a router to block the chat room is essential to internet safety. Using the router's ability to block URLs, parents can close down some chat rooms and still leave the rest of the Website open for the child. This is a good strategy in cases where a child can play games on a

A browser is no different that any other piece of software. It may contain a flaw, or defect, that allows a hacker to exploit the browser and take over the computer. The best way to reduce this risk is to make sure that all software patches for the browser have been applied to the system. The next way is to ensure that the browser's settings are set so that it makes it harder for a hacker to implant code onto the system.

The major weakness with IE is that it is insecure. Out of the box, IE is configured for ease of use. This opens the browser to hackers. The debate about IE and its security issues is not new. It has been going on for a long time and many of these security issues have been well documented. In more recent news, PC World reported (about IE), "[T]he steady increase in Internet-based viruses, worms, browser hijackings, and other attacks has made browser security a daily crisis for millions"[28]. The security risk of IE has been talked about by many security experts as well. Jeremiah Grossman, CEO of WhiteHat Security, has said "Internet Explorer's track record is such that the software just cannot be trusted right now"[29]. On the other hand, other browsers, like Firefox, come out of the box with more secure settings. These browsers are better suited to defend against hackers, but they come at the prices, that users need to be more literate with the computer and the Internet. Even with these more mature requirements, security experts still recommend that the better security decision is to use a browser other than IE. Joe Stewart, a researcher at security firm Lurhq,

says "... to stop the most recent kind of attack is recommend that customers stop using Internet Explorer"[30].

One of the most common hacks of a browser is what is called redirection. This is where code written on a Web page makes the user believe that they are on one Website when actually they are on a different Website. Most of the time this is done in a phishing scam. A user is sent an E-Mail, when the user clicks on a link in the E-Mail, the user is led to believe that they are taken to their bank's Website. The fact is that the user is taken to a different site where a hacker is waiting for the user to enter information that can be used to steal the user's identity.

The good news is that user's can tell if they are where they believe they should be. Every Website, that asks for private information, will be a secured Website. This is where encryption is used between the browser and the server to exchange information. Any time that a secure Web page is being displayed, in a browser, the browser will show the user that the page is secured. This is usually done with a lock somewhere in the browser. Most browsers will display this lock in the lower right hand corner of the browser's windows. The lock will look something like:

If a Web page is asking for private information, such as Social Security Number, Credit Card Number, Credit Card Expiration Date, there should always be a lock displayed in

hackers that are attacking from the outside trying to get to a single computer system on the internal network of the business. To advert a successful attack, the network needs to be protected from the outside world. This is as good of an idea for a home network as for a business network. It is important to remember that both types of networks are at risk of being hacked into.

One way to start to protect the internal network is to make it a separate network from the outside world. To allow the separated internal network from the outside world, the network must be set aside from the external network. This is done by configuring the internal network as a completely different network of its own. Now data can not be routed between the internal network and the external network. From a working perspective, this is useless because now the internal network can not access the outside world. There is no way that the internal network can get E-Mail, surf the Web, or even communicate with systems that are on the external network.

To allow internal computers to talk to external computers, there has to be a way to route data from the internal network to the external network. This work is done by a device called a *router*.[32] A router connects two different networks and moves traffic between the two networks. A router can only handle basic rules for traffic movement. The router can not get very sophisticated in its ability to filter data. A router can only limit certain types of data from one network to an other.

The good news is that most of the private information is entered when the user profile is created. At this point it is very easy to ensure personal information is not revealed. The bad news is that personal information can be revealed during normal conversations with other users. A watchful eye, by the wrong person, can lead a child into a bad situation. A great example of how this type of problem can occur can be found in a story at wiredsafety.org. (Already described in the section entitled *Internet and Children*)

The most important thing to remember, when it comes to online relationships: **Do not setup an off line (in person) meeting without parents involvement**. Even if parents agree to this type of meeting, it should always be done in public place. Remember never leave alone with someone you know only through the Internet. It is very hard to know if this person is really the way they present themselves in an online forum, or if they are just acting out as a different person. There have been many people find out the hard way that someone is nothing like they have presented themselves online.

Routers / Firewalls

Although there are many risks associated with the local computer system, one of the best ways to reduce problems from the Internet is to stop the problem before it enters the internal network. It may appear that most attacks are targeted on the local computer system, but these are not the only attacks that hackers make. Most business systems see

the browser. **If there is no lock, do not enter the information.**

Just because the browser is displaying a lock, it does not ensure that the Website is a valid Website. Many times a hacker will setup a scam Website to act like a secure Website. Once a secured Website is displayed in a browser, a user can check the reasonableness of the site being the expected site the user wanted to go to. This can be done by double clicking on the lock. Once the this has been done, the browser will display the security certificate. A security certificate will look something like:

By looking at the security certificate, most of the time, there will be a clue if the certificate is not from a trusted source. In the above example the certificate is from VeriSign, Inc. Companies, like VeriSign, make it their business to furnish security certificates for Websites. When a certificate is from one of these companies, the site is most likely a valid site. If a scam site was to have a certificate from one of these security certificate companies, there would be a better chance of the authorities catching the hackers committing the scam. This is the reason that most scam sites will have a security certificate from a non-business type of security authority. The best practice is simple, look at the security certificate, if it can not be verified as a valid security authority do not enter any data on that site.

Chat Rooms / Internet Messenger

One of the highest risk on the Internet comes from Internet Chat Rooms and Internet Messengers, IM. Both of these technologies can be approached the same way when it comes to Internet safety. For that reason *chat room* will be used to describe both technologies.

Chat rooms today are extremely high risk to children. Here are some facts that need to be remembered:[31]

- 30 percent of teen girls in one poll said they had been sexually harassed in a chat room. Only 7 percent, however, told their parents for fear that their Internet access would be restricted.

- 86 percent of the girls polled said they could chat online without their parents' knowledge; 54 percent could conduct a cyber relationship.
- Boys are more likely than girls to talk to strangers in “open” chat rooms. Girls are more inclined to chat in “closed” chat room situations such as Instant Messaging, without recognizing that strangers are able to eavesdrop and track kids through their online profiles.

These facts show that children are very open to using this technology to meet other people, even if their parents do not know about these contacts. It also shows that there are some risks associated with these technologies. For example many online users can read the conversation in an open chat room. On the other hand, only selected users can see a conversation in a closed chat room. For this reason there is a higher risk of problems in a closed chat room since this type of chat room is less monitored.

There are many ways to reduce the risk when using a chat room. The basic rule of thumb is not to give out personal information. This information includes, but is not limited to, the following list of information:

Name
Address
Phone Number
Where you live
School you go to
Where you work
Names of family members