Global Information Assurance Certification Paper

Erin Milana
13 Oct 03
GSEC Option 1
Version: V.1.4b

Protecting Your Home Computer before Going On-Line
(For the Not So Computer Literate Home User)

Abstract

This paper will discuss why it's important to protect your home computer before going on-line, how to protect your computer against attack, examples of cyber crimes, the law against cyber crime, and Informational resources/Points of Contact to help you protect your computer.

My approach for this discussion is to appeal to first-time users of home computers who already have or are about to plug into the internet, and don't know or understand what the inherent risks are in using the Internet without protection. And, through review of several cyber related crimes, drive home the need to protect their personal PC at all times.

Introduction

From 1998 through today, serious to catastrophic hacker attacks via the Internet have paralyzed and denied home users, corporations, and government agencies access to websites, business information, and sensitive or secret (classified) data. The disruption from hacker attacks on normal day-to-day events transacted via the Internet has now totaled billions of dollars in terms of damage. Your home computer is a popular target for hackers because they either want what's stored there, or they want to use your computer's resources such as disk space or processor.

I. Why You Should Protect Your Home Computer Before Going On-line

A. What is a hacker?

A hacker, also known as a cracker, attacker or intruder, is someone who, via the Internet, uses your computer or information stored on your computer without your permission. According to the Committee on National Security Systems (CNSS) Instruction 4009, the National Information Assurance Glossary (online, 2003), a Hacker is an unauthorized user who attempts to or gains access to an information system (IS). Your home computer is an (IS) because it is made up of a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Therefore, a hacker is any child, teen, or adult who attempts to break into and/or gain access to someone else's IS via the Internet, without permission of the owner. Is this act punishable by law? Yes it is punishable by

law. But we'll discuss the law used to punish cyber criminals later. Now, let's look at what motivates a Hacker.

B. What Motivates a Hacker?

Hackers can be motivated by many or one thing. According to the CISSP Certification Exam Guide (Harris, 2002), hackers have to have Mom--Motivations, opportunities, and Means. Many hackers are motivated by $dollars-for financial gain, to make a political statement, out of curiosity, for bragging rights among other hackers, for the excitement or challenge, an intellectual game, and to be disruptive or destructive. Opportunity usually arises when certain vulnerabilities or weaknesses are present in an operating system or application. If a person's computer isn't protected by a Router/Firewall, firewall and antivirus software, then hackers have all types of opportunity to easily exploit weaknesses within that home users computer. Means pertains to the capabilities a criminal would need to be successful, such as "know-how," equipment and time.

C. How Does a Hacker Launch an Attack

1. From the moment you connect to the Internet, be it via a dial-up Internet Service Provider (ISP) such as CompuServe®, a Digital Subscriber Line (dial-up) such as VERIZON®, or cable modem access such as COMCAST®, you become susceptible to attack. On any given day, thousands of scans and probes are scurrying through the Internet looking for "open doors," vulnerabilities of which the easiest to find and compromise are on those computers that don't have the protection of a Firewall and Antivirus software installed and operating correctly. The scans and probes are looking for computers that can be turned into zombies or drones, which are used as "robots" to potentially cause a Distributed Denial of Service (DDoS)[1] attack.

2. Another common attack method is the use of hidden file extensions and/or email borne viruses that arrive as attachments. One example of this vulnerability is in the Windows operating system. Windows operating system by default hides file extensions, so all you see in your mailbox are the first two fields of the email, i.e., LOVE-LETTER-FOR-YOU.TXT. vbs; the vbs (Virtual Basic Script) is the executable command you don't see. Multiple email borne viruses are known to exploit hidden file extensions, and use clever address/title schemes to get you to open your email (see Fig. 1, Pg. 5). The virus is sent to you from an address you know, such as a friends email address, or with a title of some

[1] A DDoS overwhelms its victim by sending bad packets or continually requesting services until the victim's resources are all tied up and cannot honor any further requests. The attack uses hundreds or thousands of other unwitting computers as slaves in the process. The attacker creates master controllers that can in turn control slaves, or zombie machines. The master controllers are systems in which an attacker is able to achieve administrative rights, so that programs can be loaded that will wait and listen for further instructions.

company or help desk you are waiting to hear from, also called email spoofing. Examples include:

- Subj: ILOVEYOU – Love Letter worm
- Subj: Re: Your Application – Sobig worm

Other examples can be found at http://www.f-secure.com/virus-info/wild.shtml.

3. Let's take a more detailed look at viruses. According to PCWorld (online, 2003), a computer virus is like its biological equivalent. A computer virus is a program that spreads unwanted and unexpected actions through the insides of your PC. Not all viruses are malicious, but many are written to damage particular types of files, applications or operating systems. Viruses cannot replicate on their own. Much like human viruses, they need a host. Computer viruses infect files by inserting or attaching a copy of itself to the file or program (host application). Several viruses have been released that achieved self-perpetuation by mailing themselves to every entry in a victim's personal address book, using programs such as, MS Outlook and Outlook Express.

There are three main types of viruses in circulation: boot sector viruses, macro viruses, and file infecting viruses.

A. The boot sector is the very first sector on a floppy or hard disk. It contains executable code which helps to operate the PC. Because the PC's hard disk boot sector is referred to every time the PC powers on "boots" up, and is rewritten whenever you configure or format the set-up of the system, it is a vulnerable place for viruses to attack.

Boot sector viruses are usually spread through the boot sector of floppy disks left in disk drives when systems are rebooted. From there, they infect the boot sector of hard disks, loading themselves into memory each time the system is booted and waiting for an opportunity to write themselves to more floppy disks to spread. This kind of virus can prevent you from being able to boot your hard disk.

B. Macro viruses are by far the most common viruses in circulation, accounting for around 75 per cent of viruses found "in the wild[2]". These can be obtained through disks, a network, the Internet, or an e-mail attachment. Macro viruses do not directly infect programs, but instead, infiltrate the files from applications that use internal macro programming languages, such as Microsoft Excel or Word documents. They are then able to execute commands when the infected file is opened, which spreads the virus to other vulnerable documents. In turn, users who share files can also spread the virus to other systems.

C. File infecting viruses infect executable files, such as EXE and COM files, loading into memory when executed and spreading their payload (see illustration 1).

4. Worms are different from viruses in that they can reproduce on their own with no need for a host application, because they are self-contained programs. A

[2] "In the Wild" refers to a computer exploit that is suspected to currently be propagating through and/or infecting users via the Internet, such as a worm, virus or malicious code.

worm can propagate itself by using email, TCP/IP[3] and disk drives. Because viruses are acting more like worms, the definition of a worm and virus is continually merging, thus sometime the terms worm and virus are used synonymously.

D. Why attack you?

1. Don't take it personally. Some probes are looking for specific types of computers using Unix, Microsoft, Macintosh operating systems, or functioning as web servers, or databases because the attacker wants to exploit specific vulnerabilities of those types of operating systems or applications running on those systems. Once the vulnerability is identified via the scan or probe, the computer is often infiltrated or exploited by planted Trojan horses, back doors and remote administration programs. The hacker uses these hacker in the hopes of using those computers at some later date to cause destruction or DDoS attacks. Also in using someone else's compromised computer, a hacker is able to hide/disguise where he is located and what his/her Internet Protocol Address[4] is. These types of probes scan thousands of networks and computers with no one person or target in mind. They just look for any and all vulnerabilities, and the attacker does not necessarily care where the vulnerable system happens to be located, or who it belongs to. A Home User is likely to face or become an unknowing accomplice to, a probe, scan or DdoS attack.

2. Additionally, you could be targeted because a hacker wants to steal and use your private information, such as your identity, your credit card numbers, your banking or financial information, passwords to your accounts, and other sensitive information.

II. Protecting Your Computer against Attack

A. What is a Router/Firewall, Firewall, and Antivirus Software?

Before identifying what you'll need to do to protect your computer, here are a few terms you'll need to know to help get you started:

1. A **Router (with Firewall capability)** is a network device that filters incoming data based upon a permissions list, called Access Control List. The router directs/sends data to its appropriate IP address. The Router/Firewall has limited firewall capability, but can also help protect your computer. It can be programmed somewhat to look for and block worms, viruses and malicious codes before they reach your internal firewall and/or computer's hard drive.

[3] Transmission Control Protocol over Internet Protocol (TCP/IP) is one of a standard set of rules that determine how systems will communicate across the networks, i.e., computer to computer communication.
[4] Internet Protocol address is the address which identifies where the computer is located, and possibly who lives at that address, much like your home address.

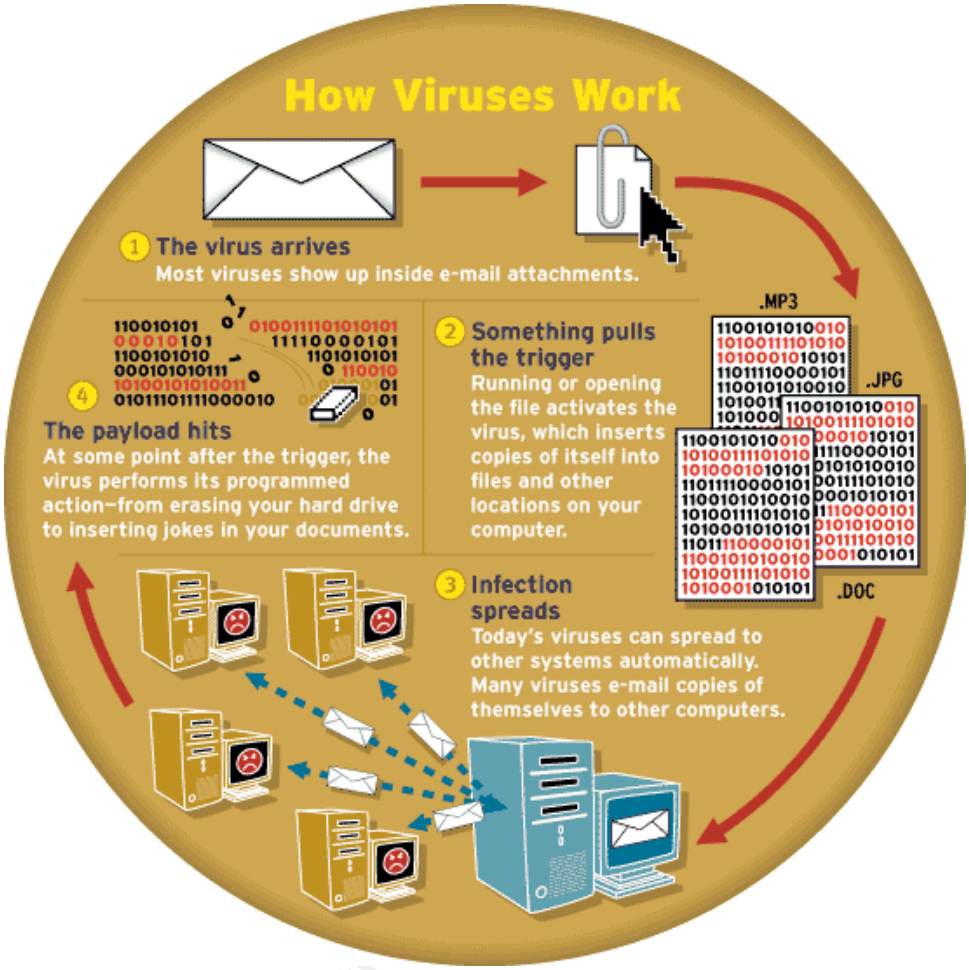

Illustration1 (PCWorld, 2003). How Viruses Work

1. The virus arrives, usually inside an email attachment.
2. Running or opening the attachment activates the virus, which inserts copies of itself into files and other locations on your computer.
3. The infection spreads, most often by emailing itself to addresses listed in your personal address book, or when you forward/send the email to someone else and they open the email.
4. Once the virus is activated or triggered, it performs its job according to the programmed instructions it is carrying, known as the payload.
5. (Not depicted.) The virus continues to propagate if instructed, or completes it mission on the infected computer, and stops because it is finished, or awaiting new instructions.

2. A **Firewall** is a network device used to restrict access from one network (your pc) to another network (the Internet). It acts as a chock point for all incoming and outgoing traffic. It can be placed externally to provide a buffer zone between your internal, private data, and external gateway, the Internet. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized intranet (internal to a business) users from accessing private networks connected to the Internet. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

3. **Antivirus software** works in conjunction with your router/firewall, specifically looking for malicious code (viruses or worms), identified by its digital signature, and automatically refuses to let the virus or worm in. It searches your hard drive and/or removable drives/disks for viruses and removes any that are found. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses, so that it can check for the new viruses as soon as they are discovered (in the wild).

B. **Table of some Name Brands on the Market for Routers, Firewalls and Antivirus Software**

To assist you choose a Router, Firewall, and Antivirus software, below is a link to finding reviews of the products I've listed in Table 1, below. http://www.firewallguide.com/.

Table1. List of Routers, Firewalls, and Antivirus software by name.

Routers	Firewalls	Antivirus Software
2Wire	Norton Personal Firewall 2003	Norton AntiVirus
D-Link	Symantec	F-Secure Anti-Virus 2003
Hawking	Sygate Personal Firewall Pro 5	GeCad Software RAV AntiVirus for Windows 8.6
Linksys	ZoneAlarm, Zone Lab	Network Associates
Microsoft	BlackICE PC Protection	McAfee VirusScan
Netgear	Internet Security Systems	Panda Software Antivirus Platinum 7
SMC	eTrust EZ Firewall	Symantec Norton AntiVirus 2003
		Trend Micro PC-cillin

Snapgear	Computer Associates	2003
SonicWall	McAfee Firewall	Kaspersky Anti-Virus Personal 4
WatchGuard	Kerio Personal Firewall 2, Kerio Technologies	Spybot Search & Destroy

C. **Steps to protecting your computer**

In order to protect your PC and keep your private information private, you will need to do the following:

1. Before accessing the Internet, block access to your computer by using front-end protection devices such as a router and firewall.
2. Install an Antivirus software package.
3. Install anti-spam, anti-Trojan, anti-spyware and privacy software, which are usually a part of an Internet Security Software package.
4. Choose an Internet Service Provider (ISP) that already provides on-line spam, virus and content filters, if available.
5. Ensure your protection devices/software applications are updated regularly. One solution to follow is to use or subscribe to the automated update services offered, which will update your protections every time you log-in or access the Internet.
6. Upgrade or update to more secure operating systems, applications and protocols regularly, because newer versions contain patches to old vulnerabilities.
7. Visit vendor websites regularly for new information or subscribe to receive newsletters announcing the latest flaws/vulnerabilities, patches, and informational news.
8. Disable the "Hide file extensions for known file types" option on your system, thus enabling you to readily see all extensions/executables.
9. Don't open email messages when you don't know who sent them.
10. Turn off your computer when you're not using it.

III. Examples of Cyber Crimes

Commentary: As you read through the different topics depicting different cyber crimes, keep in mind that while some of the crimes are committed by knowledgeable computer hackers, many of the crimes could have been prevented by having computer protection mechanisms already in place.

A. **Convicted Cyber Thieves and their Crimes**

There are many cases still pending sentencing, and even more cyber crimes not reported. Here are three cyber crimes already prosecuted that I've chosen to share with you, which demonstrates the benefits of protecting your computer. If you'd like to read more of the details, click on the link provided (if already on-

line), or log on to the Internet and paste the link in the search box and click “go”; the cases will appear; URL: http://www.usdoj.gov/criminal/cybercrime/cccases.html.

1. United States of America v Alexey V. Ivanov. Charges stemmed from the activities of Ivanov and others who operated from Russia and hacked into dozens of computers throughout the United States, stealing usernames, passwords, credit card information, and other financial data, and then extorting those victims with the threat of deleting their data and destroying their computer systems.

2. Sacramento, California – Adil Yahya Zakaria Shakour, 19, of Los Angeles, California was sentenced. During the hacking into a North Carolina site, he obtained credit card and personal information from the website, which he then used to purchase items for his personal use. The fraudulent credit card purchases totaled approximately $7, 167.

3. Pittsburgh, Pennsylvania--Ferguson, age 43, of 414 Dewalt Drive was tried for breaking into the America Online account of Common Pleas Court Judge Kim D. Eaton on three occasions. He obtained personal e-mail messages belonging to Judge Eaton, files, and other information that were part of her AOL account.

B. **A Well-Known Recent Cyber Crime – W32Blaster -- Parsons**

On August 29, 2003, the arrest of an 18 year-old high school student suspected of creating a variant of the W32/Blaster worm was arrested. The W32/Blaster worm is the worm that during the month of August had brought the internet to a crawl. I was watching CNN when “latest breaking news” flashed across the screen; stating Federal Agents had arrested an 18 year-old located in Minneapolis, Minnesota in connection with the blaster worm. By Saturday, August 30th, many people woke up to headlines and the face of the 18 year-old boy. According to The Baltimore Sun, Jeffrey Parson was charged with creating and launching a secondary version of the damaging “Blaster” worm that was said to have infected at least 7,000 computers, as well as a Microsoft Web site.

The Baltimore Sun reported, officials said Parson did not create or disseminate the original Blaster computer worm, which since August 11th had attacked hundreds of thousands of computers and networks worldwide. It also forced a one-day shutdown of Maryland’s Motor Vehicle Administration. The person or people who had created that cyber-worm, or several other variants of it, have not been caught.

Authorities said Parson essentially copied the Blaster worm August 13th, slightly altered the code, and relaunched it. The complaint says Parson modified the cyber-worm to instruct computers it infected to attack a Microsoft Web site, www.windowsupdate.com, which provides updated software. Microsoft was able to quickly block the worm. But company officials said it still caused millions of dollars in damage. According to John McKay, the U.S. attorney in Seattle, near Microsoft’s headquarters, “the teenager’s arrest would make clear that federal authorities will vigorously pursue those who commit cyber crimes. He said it was a significant attack not only against Microsoft, but against thousands of home

computer owners and business computer owners." It is estimated that the Blaster variants caused between $5 and $10 million in damage to Microsoft alone. Authorities also said Parson might have been able to access infected computers and to view personal communications and financial information, though it is not clear whether he did so.

Parson's was caught only after one of his friends came forward and reported his activity to Federal authorities. Parson was arrested for violation of U.S.C. Title 18, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(b), and 1030(c)(4)(A), and Section 2. The charge is "Intentionally Causing and Attempting to Cause Damage to a Protected Computer." For a complete reading of the Warrant for Arrest and Complaint, click on the following link: http://news.findlaw.com/hdocs/docs/cyberlaw/usparson82803cmp.pdf.

C. **Timeline of the Cyber Crime -- W32/Blaster Worm**

Again, reinforcing why you should protect your home computer before going on-line, with a Firewall and Antivirus program, the following timeline demonstrates how quickly an attack spreads. The timeline identifies the first notification of the particular Microsoft operating system vulnerability, the call for MS operating system users to patch their system, and the subsequent events that escalated the problem, see http://news.findlaw.com/legalnews/documents.

1. On **July 14, 2003**, Microsoft Corporation (Microsoft) was contacted confidentially by a research group known as Last Stage of Delirium (LSD). LSD had found vulnerability in Microsoft's Windows family of operating system software (Symantec, Infoworld).
2. On **July 16, 2003**, Microsoft made available for download, the patch identified in Microsoft Security Bulletin MS03-026.
3. On **July 24, 2003**, a Chinese group of computer experts named "XFocus" reverse-engineered the patch and found the vulnerability. XFocus then identified the source code to exploit the MS operating system vulnerability, as well as developed a scanning tool that searches the Internet for computers that have the vulnerability, and that have not been patched. Then they posted their source code and scanning tool on the Internet.
4. On or about **August 11, 2003**, MS became aware of an Internet worm named Blaster. The worm was based on the XFocus exploit code, scanning the Internet for targets, attacking them, and then installing itself on the targeted computers.
5. On **August 13, 2003**, CNET reports, to gauge how fast computers were becoming infected with Blaster, a security company put an **"unprotected" PC** on the Internet. At one point, the machine **became infected in 5 1/2 minutes; later in the day, it took only 27 seconds**. Among the entities hit by Blaster are the Maryland Motor Vehicle Administration, the Federal Reserve Bank of Atlanta (GA) and German automaker BMW.
6. On or about **August 14, 2003**, MS became aware of several variants of the Blaster code; one in particular was referred to as "W32/Lovesan.worm.b" or Lovesan B."

7. On **August 14, 2003**, a rolling power outage; black out, cascades across parts of Canada and parts of the U.S. North western and eastern states.

8. By **August 15, 2003**, estimates of infected computers were more than one million (SANS Newsbites Vol. 5, 34)

9. On **August 18, 2003**, Washington Post notes that another Blaster variant, dubbed the "Good Worm" {Nachi/Welchia} is launched, to eradicate the previous Blaster worms.

10. On or about **August 18, 2003**, CNET reports a more virulent form of the W32/SoBiG.F mass emailing worm, "the fastest proliferating worm to date is wreaking havoc on the Internet."

11. On **August 19, 2003**, Sophos Virus News reports: Sobig-F Worm Spreading Fast, Sophos Suspects Author Is Using Spam Techniques.

12. On **August 20, 2003**, Sophos posts its Anti SoBIG-F patch.

13. On **August 20, 2003**, Microsoft in coordination with the FBI locate the website hosting the Adult (porno) site where the SoBIG.F virus was launched, and take offline 19 of the 20 drone/zombies scheduled to launch a new {DDoS} attack on August 22, 2003.

14. On **August 21, 2003**, Sophos states a new variant of the Blaster is out.

15. On **August 21, 2003**, a CSX spokesman states a worm penetrated CSX Corp.'s computer system, shutting down train signaling and dispatching systems in the eastern US. It is unclear which worm caused the problems (Associated Press; Washington Post).

16. On **August 22, 2003**, the SoBIG.F new attack is thwarted.

17. On **August 23, 2003**, Sophos reports Nachi A. SoBIG.F, Panol.B and Caraga Macro virus were all transiting the Internet.

18. On **August 25, 2003**, the FBI serves a subpoena to Usenet access provider EasyNews, an adult Usenet newsgroup, regarding an account that may have been used to post the SoBIG.F virus. FBI finds the account was established with a **stolen credit card number** just minutes before the worm was posted! (Computerworld, Williams)

19. On **August 29, 2003**, Panda's Software Virus Laboratory reports a new variant of Blaster, Blaster.E on the Internet. This version performs the same exploit, but gets into the computers directly from the Internet through port 135. The file it creates is called MSLAUGH.EXE. It is programmed to run between August 16 through December 31, 2003 and causes infected machines to conduct a DDoS attack against itself.

20. On **September 1, 2003**, Computerworld reports the W32.Blaster worm may have contributed to the cascading effect of the Aug. 14 blackout, according to government and industry experts (Computerworld, Verton).

Now, let's turn to the law by which the above cases were prosecuted.

IV. <u>The Law used to Prosecute Cyber Crime</u>

United States Code (U.S.C.) Title 18, Part I Chapter 47, Section 1030

While there are several laws regarding computer intrusions, the Federal Criminal Code most often cited for cyber crimes is Title 18, Part I, Chapter 47, Section 1030: United States Code Annotated Title 18. Crimes and Criminal Procedure; Part I—Crimes, Chapter 47—Fraud and False Statements, Section 1030; Fraud and related activity in connection with computers. Below is an excerpt of the code. For complete details, click on the following link: http://www.usdoj.gov/criminal/cybercrime/1030NEW.htm

(a) **Whoever--**

(1) having knowingly accessed a computer without authorization or exceeding authorized access, …that has been determined by the United States Government …to require protection against unauthorized disclosure for reasons of national defense or foreign relations...

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains...

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States...

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value...

(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer...

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if...

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer.

V. Computer and Internet Security Points of Contact

1. **Who to report to if you suspect or have been hacked?**

A. NIPC -- If you suspect or believe you have been hacked or attacked there is an organization you can call or email regarding the incident; the National Infrastructure Protection Center (NIPC).

The NIPC, URL: http://www.nipc.gov/contact.html
For private citizens and companies - Phone: (202) 323-3205, 1-888-585-9078
Email: http://www.nipc.watch@fbi.gov
Online: http://www.nipc.gov/incident/incident.html

B. Under the new Department of Homeland Security (DHS) , the NIPC now falls under the umbrella of the Information Analysis Infrastructure Protection (IAIP) Directorate. Not to worry, the above contact information still holds true today. If you forget who to contact, think DHS, and you'll still be able to reach the appropriate office.

Here is some additional contact information, listed under DHS:

http://www.dhs.gov/. Then click on: Threats and Protection. This will currently take you to the NIPC Incident Reporting Form page.

2. **Other Computer and Internet Security Resources**

A. Computer Expert Response Team CERT® Coordination Center
Email: www.cert.org
Phone: 1(412)-268-7090 (24-hour hotline)
Established in 1988, the CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

B. SANS Institute - Internet Storm Center
Email: (isc.incidents.org) SANS is the trusted leader in information security research, certification and education. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization.

C. Computer Incident Advisory Capability – U.S. Department of Energy
Email: ciac@ciac.org
Phone: 1(925)422-8193

D. iDefense
Email: www.idefense.com
The nation's first private security intelligence firm, iDEFENSE uniquely addresses the challenges faced by both public- and private-sector organizations in protecting critical information assets.

Conclusion

In conclusion, it's paramount that you protect your home computer before going on-line. If you don't, it's just a matter of seconds or minutes before your computer is compromised by a hacker.

There are many products available for protecting your home computer. Once you've installed a Firewall, Antivirus software package, and followed the 10 steps to help you protect against hacker attacks, you will be better prepared to confront the inherent dangers of the Internet.

And, while examining true cyber crimes, it became evident that the creators of the original worms and viruses have not been found, and probably won't be. Virus and worm writers are becoming more sophisticated than ever, and make it nearly impossible to trace them. Everyday someone's computer or Information System becomes an unwitting accomplice to an attack. Everyday someone's credit card or identity is stolen via the Internet. Thus, you must be extra cautious when opening attachments, or responding to information solicitation on the Internet.

Furthermore, while the United States Code, Title 18, Section 1030 has been written to prosecute cyber criminals, it's still not enough to hope the criminals will

be caught. A hacker has many places to hide, and many opportunities, means, and motives to continue hacking without the immediate fear of being caught.

Fortunately, private citizens have organizations they can turn to for help. The National Infrastructure Protection Center is but one of the organizations established to help private citizens as well as business owners protect their Information Systems and networks against attacks; and after attacks have occurred.

Finally, this quote from Stephen Northcutt, President of SANS Institute wraps things up perfectly:

“If you accept the theory that a lot of the worm activity you have seen to date is aimed at testing for potential information warfare attacks, then this had to happen. Code Red may have been testing Internet scale infection; Nimda may have been testing multiple vectors for infection; Slammer may have been testing rapid infection; "Good" worm may have been testing countermeasures. The bottom line is simple: if your computers are not actively protected, you have nearly a 100% chance of being used by whatever future worm comes your way.”

REFERENCES

Associated Press. "CSX Blames Virus for Delays." Washingtonpost.com. August 21, 2003; page E05. URL: http://www.washingtonpost.com/ac2/wp-dyn/A23020-2003Aug20? (11 Oct 2003)

CNET Asia Staff. "World Squirms as Sobig returns." CNET News.com. August 19, 2003; 8:47p.m. URL: http://news.com.com/2100-1002-5065494.html?tag=nl (11 Oct 2003)

Cole, Eric. Hackers Beware. Indianapolis, New Riders, 2002.

The Committee on National Security Systems (CNSS) Instruction 4009. National Information Assurance Glossary. Revised May 2003. URL: http://www.nstissc.gov/Assets/pdf/4009.pdf (11 Oct 2003)

Department of Homeland Security. 2003. http://www.dhs.gov/. (11 Oct 2003)

Department of Homeland Security. 2003. "The National Infrastructure Protection Center." URLs: http://www.nipc.watch@fbi.gov; http://www.nipc.gov/contact.html; http://www.nipc.gov/incident/incident.html. (11 Oct 2003)

Harris, Shon. "All-in-One Certified Information Systems Security Professional (CISSP) Certification Exam Guide." Berkley: McGraw-Hill/Osborne, 2002. 641-642.

Findlaw.com. 2003. "United States of America vs. Jeffrey Lee Parson." URL: http://news.findlaw.com/hdocs/docs/cyberlaw/usparson82803cmp.pdf (11 Oct 2003)

Firewall Guide. 2003. URL: http://www.firewallguide.com (11 Oct 2003)

Krebs, Brian. "'Good' Worm Fixes Infected Computers." Washingtonpost.com. August 18, 2003; 2:55 pm. URL: http://www.washingtonpost.com/ac2/wp-dyn/A9531-2003Aug18? (11 Oct 2003)

Laura Sullivan & Stephen Kiehl. "Youth Charged in Virus Attack." The Baltimore Sun Newspaper. August 20, 2003. (2003): 1A.

Microsoft.com. "What You Should Know About the Blaster Worm and Its Variants Security Bulletins; MS03-026." Revised August 22, 2003. URL: http://www.microsoft.com/security/incident/blast.asp. (11 Oct 2003)

Northcutt, Stephen. SANS NewsBites;News About Blaster. August 20, 2003 Vol. 5, Num. 33. URL: http://www.sans.org/newsletters/newsbites/vol5num33.php and http://www.sans.org/newsletters/newsbites/vol5_34.php. (11 Oct 2003)

Panda Software. “Weekly Virus Report; The New E Variant of Blaster Worm. August 29, 2003. : URL: http://www.pandasoftware.com/about/press/viewNews.aspx?noticia=4099&ver=2003,3&pagina=2&numprod=&entorno=. (11 Oct 2003)

PCWorld. “Antivirus Software.” 2003. URLs: http://pcworld.idg.com.au/pp.php?id=316975074&pp=1&taxid=117 , and http://demo.idg.com.au/images/howvirusworks.gif. (11 Oct 2003)

Sophos. “Top 10 Viruses Reported to Sophos in August 2003.” URLs: http://www.sophos.com/virusinfo/topten/200308.html and “Virus Articles ‘August’.” http://www.sophos.com/virusinfo/articles. (11 Oct 2003)

Symantec.com. “Concerns Mount Over Possible Big Net Attack.” Reprinted from InfoWorld. August 4, 2003. URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=2381. (11 Oct 2003)

United States Department of Justice. “Computer Intrusion Cases.” Revised 9 October 2003. URL: http://www.usdoj.gov/criminal/cybercrime/cccases.html (11 Oct 2003)

United States Department of Justice. “1030**.** Fraud and Related Activity in Connection with Computers.” Revised 8 February 2003. URL: http://www.usdoj.gov/criminal/cybercrime/1030NEW.htm (11 Oct 2003)

Verton, Dan. “Blaster Worm Linked to Severity of Blackout.” Computerworld.com. September 1, 2003. URL: http://www.computerworld.com/securitytopics/security/virus/story/0,10801,84519,00.html. (11 Oct 2003)

Wells, Joe. “Virus Descriptions of Viruses in the Wild.” Wildlist Vol. E01. 2003. URL: http://www.f-secure.com/virus-info/wild.shtml (11 Oct 2003).

Williams, Martyn. “Sobig.F Worm Could have Originated on Usenet.” August 25, 2003. URL: http://www.computerworld.com/securitytopics/security/virus/story/0,10801,84326,00.html. (11 Oct 2003)

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event