Global Information Assurance Certification Paper

Cyber Crime – The Intelligent Criminal

Candice Barry

01/03/2005

© SANS Institute 2000 - 2005 Author retains full rights.

Cyber Crime – The Intelligent Criminal

Introduction

"Cyber crime is any criminal activity, which uses network access to commit a criminal act. With the exponential growth of Internet connection, the opportunities for the exploitation of any weaknesses in Information Security are multiplying.[1]" Some use the Internet for entertainment, knowledge, work or play. Others use the Internet to get rich quick with a barrage of illegal activities that can go unnoticed for months and sometimes, they never get caught. Cyber crime can disrupt your life so suddenly and strip you from your identity almost instantly.

With cyber crime on the rise, we need to be proactive on the war against criminals on the web. The purpose of this paper is to discuss different types of Cyber Crime. I will offer a brief history on hacking and offer tips to protect your computer, your assets, and yourself. I will also be discussing several types of viruses, the harm they can do to your system and how to protect your computer from becoming a victim. Phishing and Identify Theft go hand in hand. When you are phished, the criminal is looking for you to expose your private and personal information. Once they have obtained this information, they have the ability to steal your identity. I will be discussing in detail, the phishing scheme and offering tips on how to keep your identity safe. I will also offer suggestions on what to do if you feel your identity has been compromised.

Hacking

"Hacking is the deliberate and unauthorized access, use, disclosure, and/or taking of electronic data on a computer. It is illegal and covered under federal and various state criminal statutes. The computer crime of hacking is committed when a person willfully, knowingly, and without authorization, attempts or achieves access, to a computer or computer network.[2] "

While the term hacking was not coined until the 1960's, hacking has been around as early as 1870. A group of teenage boys hired to run the switchboard for Bell Telephone were considered the first "hackers." They would misdirect calls, eavesdrop on conversations, and play other harmless pranks. Subsequently, they were fired and replaced with more reliable girls. Nonetheless, with the rise of technology came the rise of computer hacking.

---

[1] Cyber Crime
http://www.yourwindow.to/information-security/gl_cybercrime.htm

[2] Computer Crime (Hacking) Law and Legal Definition
http://www.uslegalforms.com/lawdigest/legal-definitions.php/US/US-COMPUTER_CRIME.htm

The early 60's brought the real hackers. At first, the term hacker was considered a compliment to describe a person who could push programs beyond what they were designed to do. MIT reported the first generation of computer hackers. A group of MIT programmers would create shortcuts or "hacks" to make the computer process quicker. These MIT employees were considered geniuses by the hacks they created.

In 1972, John Drapper, also known as Cap N' Crunch discovered that a toy plastic whistle given away in Cap N' Crunch cereal boxes would enable him to hack phone systems. This whistle emitted a 2,600-hertz tone. With practice and one hole glued shut, the whistle could open telephone lines by blowing a precise tone into a telephone and make it possible to conduct free long-distance calls.

The Great Hacker War started in 1984. A guy calling himself Lex Luthor founded the Legion of Doom, which was named after a Saturday morning cartoon. The Legion of Doom's members consisted of the best of the best hackers until one of the gang's members, Phiber Optik, feuded with another member, Erik Bloodaxe and got him thrown out of the club. Phiber Optik and some of his friends formed a rival group called the Masters of Deception. For almost 2 years in 1990, Legion of Doom and Masters of Deception feuded by jamming phone lines, monitoring calls, and trespassing in each other's computers. Soon enough, the Federal Government cracked down and subsequently sent the gang members to jail.

In December of 1988, Kevin Mitnick was arrested for stealing programs and tapping into Digital Equipment's computer network. Digital Equipment officials claimed that Mitnick had caused $4 million in damage to computer operations and stole over $1 million in computer software. In 1989, he was convicted and served one year in prison.

In 1992 the FBI went to question Kevin Mitnick about some computer break-ins at Pacific Bell. When they arrived to question him, they discovered that he had fled. Mitnick was "on the run" from the FBI, and many times, he stayed just out of reach from getting caught. He went from city to city consistently while he continued to hack into computers through laptops and cell phones. On Christmas Day, 1994 Kevin Mitnick hacked into the computer of Tsutomu Shimomura, a well-known security expert. Shimomura was determined to find the intruder and worked with the FBI to track Mitnick to Raleigh, North Carolina. Mitnick was soon arrested at his apartment at 1:30 am on February 15, 1995

. More recently, in 2001, a teenager who is known by the handle "Mafiaboy" was arrested and charged with two counts of mischief to data. "Mafiaboy" was single handedly responsible for attacking several major websites including Yahoo! Amazon.com, eBay, CNN.com, and ZDNet. "The attacks involved using one computer to launch an attack via 'slave' computers worldwide. The slave computers can be used without their owners' knowledge -- the hacker has the computers send large amounts of data to the target site in a short period of time, essentially overloading the targeted site.

It's the equivalent of having millions of people make a phone call to the same number.[3]" These Denial of Service (DOS) attacks caused over 1 billion dollars in damages.

There are a several different ways to prevent your computer from being hacked:

1. **Patch your system!** Make sure you perform the critical and necessary updates to your operating system. Many updates contain security patches to keep your computer safe. If you are using a Microsoft operating system, you can set your updates to install and run automatically.
2. **Install anti-virus software and maintain it!** Update your virus definitions and run scans of your hard drive daily. If a virus is found, disconnect from your network and allow your anti-virus software to quarantine and fix the virus. One small worm can equal one giant problem.
3. **Install a firewall!** Firewall software will help prevent unauthorized incoming and outgoing communications to and from your computer while you are connected to the Internet. Port scanning is extremely common. It is used to find any type of vulnerability within your system that can then be exploited. You can download free firewall software from a company called Sygate. If you are using Windows XP, downloading Service Pack 2 will automatically enable firewall protection on your computer as long as it is turned on.
4. **Regularly remove spy ware!** "Spy ware is any software that gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spy ware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spy ware monitors user activity on the Internet and transmits that information in the background to someone else. Spy ware can also gather information about e-mail addresses and even passwords and credit card numbers.[4]" There are a couple of different tools to use in removing spy ware. They are Ad-aware and Spybot. After installing one of these free applications, simply perform a scan on your computer to remove any spy ware.
5. **Disconnect your computer!** Make sure when you are done using your computer for the day that you log off and turn it off. Leaving your computer up and running while connected to the Internet is an open door for hackers to start their probe. [5]

---

[3] Kane, Margaret, 'Mafia boy' Busted In Dos Attacks. ZDNet News April 18, 2000
http://zdnet.com.com/2100-11-520033.html?legacy=zdnn

[4] Webopedia Online Dictionary
http://www.webopedia.com/TERM/s/spyware.html

[5] Anti Hacking Tips For Home Based Online Business
http://www.tamingthebeast.net/articles3/anti-hacking.htm

As Microsoft's CEO, Steve Ballmer states, although the engineers are trying, it is too naïve to suggest that Microsoft can eliminate all of its security vulnerabilities. "Hackers get smarter, too.[6]"

Viruses

A virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. It can be sent to you in e-mail, in downloads you make from websites, and even automatically deploy when you visit certain websites. There are several types of viruses that can infect your computer. Macro viruses, File viruses, Boot viruses, Multipartite viruses, Polymorphic or Mutation viruses, and Stealth viruses are all viruses that can put your computer out of commission indefinitely. While the Trojan Horse, Logic Bomb, and the Worm act like viruses, they are entirely different.

Macro viruses are one of the more common forms of infection. Macro viruses are written in a programming language like Visual Basic. Visual basic is supported by some software, most notably Microsoft Word and Excel. Macros are actually miniature programs embedded in a document, and therefore have many of the same rights and abilities as the user who is logged on to the system. Macros are used to enhance programs by making it more efficient with a click of a button. For example, by creating a macro in Word, you can automate your document to print immediately after saving. You record your macro in steps:

1. Create new Macro named PRINTING
2. The Macro begins recording
3. Click the save Icon
4. Click the print icon
5. Click stop on the macro box

Now when you click on your PRINTING macro, your document will automatically save and print.

The problem is that macros may be written maliciously to perform harmful tasks, such as deleting all of the text and then saving the document. Running this macro would make it impossible to recover your data. Not only can macros be written to delete your current document, but they can also be written to delete entire files and folders from your hard drive. You should never run a macro unless you created it or it is from a trusted sender.

File viruses infect executable or program files by inserting their code into some part of the executable or program file so that it can be executed when the file is accessed or they may overwrite the file entirely. Once the infected program is run, the

[6] Microsoft CEO: Hackers getting smarter
http://www.msnbc.msn.com/id/6297510/

virus is transferred to your system's memory and may replicate itself further. File infecting viruses have been written for a wide range of operating systems, including Macintosh, UNIX, DOS, and Windows. Overwriting viruses can cause irreversible damage to the files leaving your computer inoperable. **Loveletter**, which operated as an email worm, file virus, and Trojan downloader, is a notorious example of a file-overwriting virus. **Loveletter** searched for certain file types and overwrote them with its own malicious code, permanently destroying the contents of those files. Files affected by an overwriting virus cannot be disinfected and instead must be deleted and restored from backup.

Boot viruses attack the boot sector and master boot record of the fixed disk. They can be created easily without any difficulty. They infect the master boot record of the storage devices like the hard disk or floppy. Master boot record is the boot record that is situated in the first sector of hard disk or floppy that describes the disk type, sector, partition table, cluster size and file system of the device. When the computer is turned on, it runs a couple of tiny program contained in these special sectors, first the partition bootstrap and then the system bootstrap, to ready itself for work. The only way of becoming infected with these viruses is booting from the infected disk.

Tips against boot viruses:

- Change the boot sequence in the BIOS, so the floppy won't be the first in that sequence. This way, you are protected if you accidentally forget an infected floppy in your floppy drive. Booting from the floppy drive is never necessary unless you are planning to install or reinstall the operating system of your computer.

- Scan any floppy disk put into your floppy drive using an antivirus program before executing any programs on the disk. This will ensure a virus is not accidentally copied to your computer.

A Multipartite virus can also be referred to as a multi part virus. Multipartite viruses share some of the same qualities of boot viruses and file viruses. It attempts to attack both the boot sector and the executable, or program, files at the same time. When a computer boot up with an infected floppy disk, a typical multipartite virus will make itself resident in memory and then infect the boot sector of the hard drive. From there the virus will infect a computer's program or executable files and eventually infect the entire computer's environment. What makes these viruses so unique is that they do not stop infecting once the boot sector is infected. They load into the memory and start infecting the other program files too. They infect program files and when the infected program is run they start infecting the master boot record too. This type of virus can re-infect a system over and over again if all parts of the virus are not cleaned. They are generally very hard to detect and difficult to remove. To remove them you must clean both the boot sector as well as any infected files.

Polymorphic comes from the Greek for 'many forms' and was applied to viruses in the early 1990's when the first polymorphic viruses appeared. Scanners easily detect most viruses because no matter how many times a virus copies itself, each copy will look the same. Polymorphic Virus or a Mutation Virus is a virus that produces varied copies of its own self. It is a virus that can change it's own code allowing it to have hundreds, even thousands, of different variants in the hope that virus scanners will not be able to detect the virus. Essentially, the polymorphic virus changes itself each time it infects. Because of this, it is very hard to detect these viruses making it even harder to clean the infection.

A stealth virus is a virus that hides the modifications it has made to the boot records or files. To achieve this, a stealth virus uses the system functions necessary to read files or sectors from storage media and forges the results of calls to such functions. Programs that try to read infected files or sectors see the original, uninfected form instead of the actual, infected form. This makes the virus's modifications undetected by antivirus programs. If your antivirus program scans the memory, it should find these viruses and should be able to clean the infection.

Trojan Horses, Logic Bombs, and Worms act like viruses but are really programs that need to be executed. When these programs are executed, the damage can be just as extreme as a computer virus.

Trojan Horses are actually destructive programs that act as a helpful application. You may think you have software that will help your computer function better, but in reality, it is a Trojan Horse and will destroy your system. Many Trojans claim to be software that can eliminate your viruses, but when run, actually infects your computer with new viruses. Still others can allow third parties to remote into your computer and take over your system.

Logic Bombs are programs that lie dormant until something triggers them. The trigger could be a date, a number, or even a specific event, like executing your e-mail. When a Logic Bomb is triggered, it can destroy your whole system by changing or erasing data and making your hard drive unreadable. Some Logic Bombs are done unintentionally and are simply the result of a corrupt file.

A computer worm is a lot like a virus because it is designed to copy itself from one computer to another; however, a worm does not need another file to be shared in order to spread. Once a computer worm is on your computer, it takes over your computer by using features that transport files or information. Once a worm gets in your system, it can travel alone without any help from the user.

Tips you can use to protect yourself from worms and viruses are:

- Use an anti-virus program; one that includes a background scanner is the best option. It will allow you to scan your computer while continuing to work. If it finds a virus, a pop up window will alert you.

- Keep your anti-virus software updated. Some anti-virus programs will allow you to set it for automatic updates. This is the best option.

- Scan your hard-drives regularly with your anti-virus software

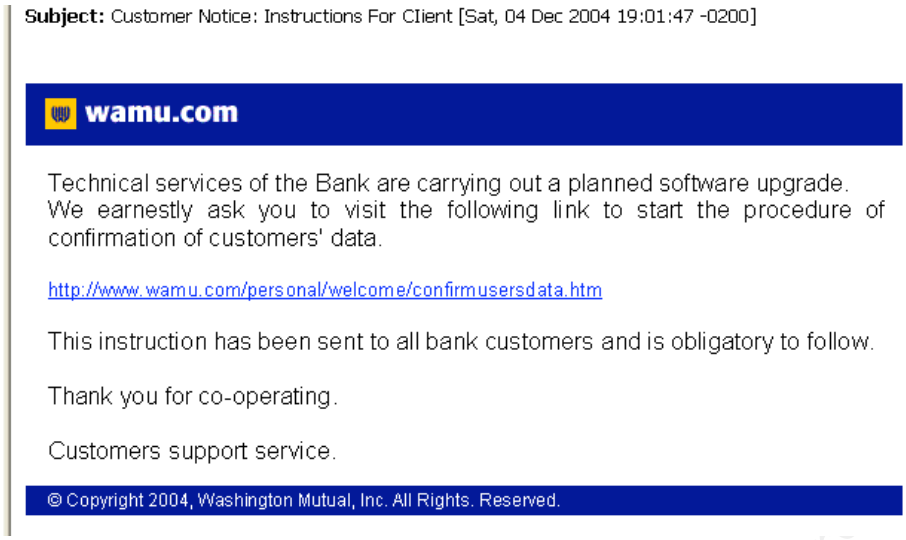
- Remove floppies from the floppy drive of your PC. If your floppy disk has Boot sector viruses, it will infect your computer when the computer attempts to boot from the floppy drive.

- If using Microsoft, apply all critical and security related patches using Windows Updates. These patches will protect your computer.[7]

Phishing and Identity Theft

Phishing and identity theft go hand in hand. Phishing is the term coined by hackers that use email to "fish" the Internet in hopes of hooking you into giving them your personal and private information such as login ID's, passwords, and credit card information. They do this by impersonating a legitimate company such as EBay, Paypal, or even your local financial institution. In the scam, you will receive an email asking you to update your personal information so that the company can "update their records." Many times, the email will also state that if you do not verify your information, you will be suspended from that site. Clicking the link within the email will send you to a bogus website made to look authentic asking you to input your name, account number, even your social security number for verification. The website then records the personal information you input, giving the criminal access to your identity and giving them the ability to wreak havoc with your life. Below is an example of a typical email Phishing scam.

[7] Hodas, Elizabeth Protecting Your Computer from Viruses
http://www.hmc.edu/comp/occ-down/vol5/iss3/viruses.html



Subject: Customer Notice: Instructions For CIient [Sat, 04 Dec 2004 19:01:47 -0200]

wamu.com

Technical services of the 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.

http://www.wamu.com/personal/welcome/confirmusersdata.htm

This instruction has been sent to all bank customers and is obligatory to follow.

Thank you for co-operating.

Customers support service.

Criminals that have created Phishing scams are getting smarter! Not only have criminals created a way to scam you and steal your identity, but also have found a way to make your computer behave as though it has a virus. With this new scam, you don't even have to click the link within the email. Merely opening the email will push code onto your computer to change a piece of software called a host file. " All Web sites have numeric Internet addresses, or IP addresses that contain a sequence of numbers. An example of an IP address is 10.243.1.15. The web sites also have simple names to remember like Cnn.com. The names and numbers are linked via the Internet through Domain Name Servers or DNS. Your local computer will always check the host file stored on your hard drive for the Domain Name Server first. That local host file overrides the information contained from the Internet's Domain Name Servers.[8] "

By changing a computer's host file, the criminal can change the Web site that your computer visits. Typing in banknewport.com, for example, could point your computer toward the criminal's instead. Due to the fact that you don't realize you have been redirected to the criminal's website, you input your personal data and at that point, you are susceptible to having your identity stolen. If your host file is changed, even after the criminal's site is pulled down, the host file still points to the criminal's website. This can cause much confusion. Imagine happily enjoying Internet Banking and all of a sudden your computer can no longer reach your banks website.

Identity theft is one of the fastest growing crimes in the United States. More than 11 million Americans have become victims of identity theft. According to CBS news, Every 79 seconds, a thief steals someone's identity, opens accounts in the victim's name and goes on a buying spree. Criminals with access to your personal information such as credit card numbers, drivers license number and social security number can bring in a hefty paycheck.

---

[8] Sullivan, Bob A New, More Sneaky Phishing Attack, MSNBC Nov. 5, 2004
http://www.msnbc.msn.com/id/6416723/

Criminals will obtain your personal information and obtain loans, credit cards, even bank accounts in your name. They will use the credit cards and loans to purchase goods and have the statements mailed to their address. Since the bills and charges incurred will be sent to the criminal, you will be unaware that debt is mounting until you have a credit check or a collection agency has tracked you down. By this time, your credit report will stricken with late payments and show many accounts in collections. It could take months to clear your credit report as credit reporting agencies need proof that you did not make these charges.

How do thieves get your data?

Thieves are getting more creative, innovative, and smarter. Here are some high and low-tech ways they are getting your data.

- Theft of Business Records: Criminals working in a company can take your data from files, bribe another employee, or even hack into a company's computer system to steal your data.

- Shoulder Surfing: Also known as standing next to you in a checkout line and memorizing your name, address and phone number as you write a check. Another newer technique of Shoulder Surfing is to take a picture of your credit card with their hi-tech camera phones.

- Dumpster Diving: Criminals go through your trash, the trash of businesses, and even landfills

- Fraud: Criminals can pose as landlords, employers, doctors or anyone else who may have legitimate need for you personal information. They will then ask for that information and use it to steal your identity.

- Skimming: Criminals steal your credit card number as your card is being processed at a restaurant, store or business using a special collection device, known as a skimmer. A skimmer is a small device that is used to store your credit card number. The waiter that took your card not only swiped it at the restaurant, but also swiped it into their skimmer. Credit card skimming has become a worldwide problem. Card losses due to skimming exceed $1 billion a year.

- Phishing: As discussed earlier, sending an e-mail to a user falsely claiming to be legal company in an attempt to scam the user into giving out private information that will be used for identity theft.

- Stealing: Good old-fashioned stealing of your wallets, purses and even your mail.

Tips for preventing identity theft:

- Review your Credit report at least once a year for any inaccuracies.
- Purchase a shredder. Shred all documents with personal information before throwing them away.
- Monitor your Bank statements. Monitor your account statements on a monthly basis to ensure they arrive at the scheduled time and there are no discrepancies.
- Do not send mail using your unsecured mailbox. If you have payments to send, mail them at your local post office.
- If your driver's license number is the same as your Social Security number have your license number changed.
- Do not pre-print your Social Security Number on your checks.
- Don't carry your Social Security Card in your wallet/purse.
- Keep items that contain your personal information in a safe place.
- Even if the e-mail states that your account is in jeopardy of being closed. Do not respond to e-mails requesting your personal Identification.

What to do if you are a victim:

- **Contact the major credit bureaus:** Obtain a copy of your credit report, which is free if you are an ID theft victim. Make sure your credit is tagged with a fraud alert. Get in writing that the fraud alert remains in place for seven years.
- **File a police report:** Even if your local police department says it isn't necessary, file a police report. You will need this to dispute unauthorized charges and for any insurance claims. Contact the Federal Trade Commission. This will enter your case in the FTC's database, which is used nationwide by law enforcement to find patterns and catch criminals.
- **Close all compromised accounts:** **"**The list may be longer than you think. This lists includes, but is not limited to accounts with banks, credit card companies phone companies, utilities, and ISPs. Dispute all unauthorized charges and follow up after submitting the paperwork.[9]**"**

Conclusion:

[9] Sullivan, Bob, ID Theft Victims Face Tough Bank Fights, MSNBC Feb. 18, 2004 http://www.msnbc.msn.com/id/4264051/

How can something so wonderful and innovative turn our lives into such a nightmare? The Internet, while working for us, can also work against us. With technology becoming more indispensable in today's society, cyber crime will continue to rise. With that rise in cyber crime, we must raise our awareness to help prevent and fight these unseen criminals.

While there are safeguards in place to protect you, the consumer, they are not full proof. Law enforcement agencies around the world are working together to make new partnerships, methods, and responses to fight cyber crime. At the same time, you must do your part in protecting your identity. It is important for you to realize that only you can protect yourself from becoming a victim to cyber crime.

References:

Author Unknown Cyber Crime
http://www.yourwindow.to/information-security/gl_cybercrime.htm

Computer Crime (Hacking) Law and Legal Definition
http://www.uslegalforms.com/lawdigest/legal-definitions.php/US/US-COMPUTER_CRIME.htm

Kane, Margaret, 'Mafia boy' Busted In Dos Attacks. ZDNet News
April 18, 2000
http://news.zdnet.com/2100-9595_22-520033.html?legacy=zdnn

Webopedia Online Dictionary
http://www.webopedia.com/TERM/s/spyware.html

Anti Hacking Tips For Home Based Online Business.
http://www.tamingthebeast.net/articles3/anti-hacking.htm

The Associated Press, Microsoft CEO: Hackers getting smarter
Oct. 21, 2004
http://www.msnbc.msn.com/id/6297510/

Hodas, Elizabeth Protecting Your Computer from Viruses
http://www.hmc.edu/comp/occ-down/vol5/iss3/viruses.html

Sullivan, Bob A New, More Sneaky Phishing Attack, MSNBC
Nov. 5, 2004
http://www.msnbc.msn.com/id/6416723/

Sullivan, Bob, ID Theft Victims Face Tough Bank Fights, MSNBC

Feb. 18, 2004
http://www.msnbc.msn.com/id/4264051/

Kremen, Stanley H. Apprehending The Computer Hacker
http://www.shk-dplc.com/cfo/articles/hack.htm

Federal Trade Commission, ID Theft: When Bad Things Happen to Your Good Name
http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

Stiller Research, Introduction to Viruses
http://www.stiller.com/vintro.htm

Types of Viruses
http://www.jconsult.com/virus/smex38help/WebRoot/at.htm