**Information Technology**

**Unethical issues in I.T and Cybercrimes**

**Kumeren Govender**

**Content Page**

1. Introduction
2. What is hacking?
3. Types of Cyber Crimes – Spamming\ Hacking
4. Hacking
5. Phishing
6. Spoofing
7. Viruses
8. Classification of Viruses
9. Classification of Viruses
10. Classification of Viruses
11. Trojans
12. Software Piracy
13. Survey \ results
14. Conclusion \ Bibliography



**Introduction**

Over the last decade the internet has grown rapidly. It has given rise to many avenues in every field we can think have be it education, entertainment, business, or sports. However with every great invention there is a curse too. This curse is Cybercrime – illegal activities committed over the internet. The internet, along with its advantages, has also exposed us to security risks. Computers today are being misused for unlawful activities like e-mail espionage, credit card fraud, spam, software piracy, spreading of viruses and so on, which invade our privacy and offend our senses. Criminal activities over internet are on the rise.

Cybercrime is a term used broadly to describe criminal activity in which computers or networks are a tool, a target, or a place of criminal activity. Although the term cybercrime is usually restricted to describing criminal activity in which the computer or network is an essential part of the crime, this term is also used to include traditional crimes in which computers or networks are used to enable the illegal activity

****

*"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb". – National Research Council, "Computers at Risk", 1991*

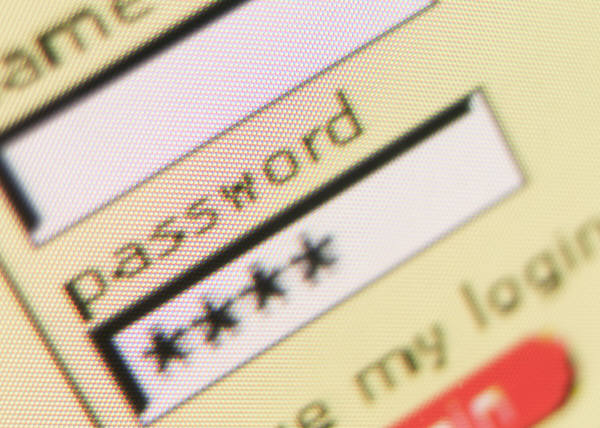
**What is Hacking?**

Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator’s original purpose. People who engage in computer hacking activities are often called hackers.

Computer hacking is most common among teenagers and young adults, although there are many older hackers as well. Many hackers are true technology experts who enjoy learning more about how computers work and consider computer hacking an “art” form. They often enjoy programming and have expert-level skills in one particular program. For these individuals, computer hacking is a real life application of their problem-solving skills. It’s a chance to demonstrate their abilities, and sometimes an opportunity to harm others.

**Hacking as a profession!?!**

Since a large number of hackers are self-taught geniuses, some corporations actually employ computer hackers as part of their technical support staff. These individuals use their skills to find flaws in the company’s security system so that they can be repaired quickly. In many cases, this type of computer hacking helps prevent identity theft and other serious computer-related crimes.



**Types of Cyber Crimes**

1. Spamming

Spamming is the abuse of electronic messaging systems to send unwanted bulk messages, which are generally undesired. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, mobile phone messaging spam, internet forum spam and junk fax transmissions.

Spamming is economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unwanted mail has become very high. The costs, such as lost productivity and fraud, are exposed to the public and Internet service providers, which have been forced to add extra capacity to cope with the surge in data transfer. Spamming is widely hated, and has been marked at illegal by many government authorities around the world.

1. Hacking

Hacking in simple terms means illegal invasion into a computer system without the permission of the computer owner. The most important definition of hacking is the act of gaining access without legal authorization to a computer or computer network. A hacker first attacks an easy target, and then uses it to hide his or her traces for launching attacks at more secure sites. The goal of an attack is to gain complete control of the system (so you can edit, delete, install, or execute any file in any user’s directory), often by gaining access to a "super-user" account. This will allow both maximum access and the ability to hide your presence.

Often attacks are based on software bugs that a hacker can use to give himself or herself super-user status. The example above was used by West German hacker "Pengo" who exploited the fact that many systems came with default usernames and passwords which some buyers neglected to change. He succeeded by persistence.

Also one can get a copy of the password file (which stores usernames and encrypted passwords and is often publicly accessible) and either do a brute-force attack trying all possible combinations, or encrypt a dictionary and compare the results to see if anyone chose a password that is a dictionary word. Another method of hacking is to email someone a program that either automatically runs, or that runs when they click on an attachment. This can install a program that will give you control of their computer. L0pht Heavy Industry’s Back Orifice 2000 (a simple copy of Microsoft’s Office 2000) allows someone to have nearly complete control (running programs, deleting files, viewing the screen, logging typed keys, etc.) over the target computer without being noticed. One complicated method, known as IP spoofing, is to get one computer to pretend that it is another one which is trusted by the target system, thus gaining the access privileges of the computer.



1. Phishing

Phishing is essentially an online con game, and phishers are nothing more than knowledgeable con artists and identity thieves. They use spam, fake Web sites, crimeware and other techniques to trick people into revealing account sign-in information.

In most cases, phishers send out a wave of spam email, sometimes up to millions of messages. Each email contains a message that appears to come from a well-known and trusted company. Usually the message includes the company's logo and name, and it often tries to evoke an emotional response to a false crisis. implied in urgent, business-like language, the email often makes a request of the user’s personal information. Sometimes the email directs the recipient to a spoofed Web site. The Web site, like the email, appears authentic and in some instances its URL has been masked so the Web address looks real.

The fake Web site urges the visitor to provide confidential information — social security numbers, account numbers, passwords, etc. Since the email and corresponding Web site seem legitimate, the phisher hopes at least a fraction of recipients are fooled into submitting their data. While it is impossible to know the actual victim response rates to all phishing attacks, it is commonly believed that about 1 to 10 percent of recipients are duped with a “successful” phisher campaign having a response rate around 5 percent. To put this in perspective, spam campaigns typically have a less than 1 percent response rate.



1. Spoofing

Spoofing is the creation of TCP/IP packets using somebody else's IP address. Routers use the "destination IP" address in order to forward packets through the Internet, but ignore the "source IP" address. That address is only used by the destination machine when it responds back to the source. Basically it is using someone else’s computer from your computer as your own.

A common misconception is that "IP spoofing" can be used to hide your IP address while surfing the Internet, chatting on-line, sending e-mail, and so forth. This is generally not true. Forging the source IP address causes the responses to be misdirected, meaning you cannot create a normal network connection.  However, IP spoofing is an integral part of many network attacks that do not need to see responses (blind spoofing).

In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by “spoofing” the IP address of that machine.

**Non binding spoofing** attack takes place when the attacker is on the same subnet as the victim. The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the data stream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine. Using this technique, an attacker could effectively bypass any authentication measures taken place to build the connection.

**Binding Spoofing** is a more sophisticated attack, because the sequence and acknowledgement numbers are unreachable. In order to avoid this, several packets are sent to the target machine in order to sample sequence numbers. Today, most OSs implement random sequence number generation, making it difficult to predict them accurately. If, however, the sequence number was compromised, data could be sent to the target. A properly planned attack could add the necessary data to a system (i.e. a new user account), blindly, enabling full access for the attacker who was impersonating a trusted host.

1. Viruses

A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. The original may modify the copies or the copies may modify themselves. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over a network or carrying it on a removable medium such as a floppy disk, CD, or USB drive. Additionally, viruses can spread to other computers by infecting files on a network file system or a file system that is accessed by another computer.

The term comes from the term virus in biology. A computer virus reproduces by making, possibly modified, copies of itself in the computer's memory, storage, or over a network. This is similar to the way a biological virus works.

Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk. Others are not designed to do any damage, but simply replicate themselves and perhaps make their presence known by presenting text, video, or audio messages. Even these benign viruses can create problems for the computer user. They typically take up computer memory used by legitimate programs. As a result, they often cause unreliable behaviour and can result in system crashes. In addition, many viruses are bug-ridden, and these bugs may lead to system crashes and data loss.

 A program called "Elk Cloner" is credited with being the first computer virus to appear "in the wild" — that is, outside the single computer or lab where it was created. The first PC virus was a boot sector virus called (c)Brain, created in 1986 by two brothers, Basit and Amjad Farooq Alvi, operating out of Lahore, Pakistan.



Classification of Viruses

Viruses can be subdivided into a number of types based on their features.

Macro viruses

A macro virus is often written in the specific languages for programs such as Word and Excel and is spread by infecting documents and spreadsheets. Since macro viruses are written in the language of the application and not in that of the operating system, they are known to be platform-independent. They can spread between Windows, Mac and any other system, so long as they are running the required application. With the ever-increasing capabilities of macro languages in applications, and the possibility of infections spreading over networks, these viruses are major threats.

The first macro virus was written for Microsoft Word and was discovered in August 1995. Today, there are thousands of macro viruses in existence—some examples are Relax, Melissa.A and Bablas.

Network viruses

This kind of virus is quickly spread across a Local Area Network (LAN) or even over the Internet. Usually, it propagates through shared resources, such as shared drives and folders. Once it infects a new system, it searches for potential targets by searching the network for other vulnerable systems. Once a new vulnerable system is found, the network virus infects the other system, and thus spreads over the network. Some of the most notorious network viruses are Nimda and SQLSlammer.

Logic bomb

A logic bomb employs code that lies dormant until specific conditions are met. The activated conditions will trigger a certain function (such as printing a message to the user and/or deleting files). Logic bombs may be within standalone programs, or they may be part of worms or viruses. An example of a logic bomb would be a virus that waits to execute until it has infected a certain number of hosts.

Cross-site scripting virus

A cross-site scripting virus (XSSV) is a type of virus that utilizes cross-site scripting vulnerabilities to replicate. A XSSV is spread between vulnerable web applications and web browsers creating a relationship.

Sentinels

A sentinel is a highly advanced virus capable of empowering the creator of the virus with remote access control over the computers that are infected. They are used to form vast networks of zombie or slave computers which in turn can be used for malicious purposes such as a Distributed Denial-of-service attack.

Companion virus

A companion virus does not have host file but exploits MS-DOS. A companion virus creates new files (typically .COM but can also use other extensions such as ".EXD") that have the same file names as legitimate .EXE files. When a user types in the name of a desired program, if a user does not type in ".EXE" but instead does not specify a file extension, DOS will assume he meant the file with the extension that comes first in alphabetical order and run the virus. For instance, if a user had "(filename).COM" (the virus) and "(filename).EXE" and the user typed "filename", he will run "(filename).COM" and run the virus. The virus will spread and do other tasks before redirecting to the legitimate file, which operates normally. Path companion viruses create files that have the same name as the legitimate file and place new virus copies earlier in the directory paths. These viruses have become increasingly rare with the introduction of Windows XP, which does not use the MS-DOS command prompt.

Boot sector viruses

A boot sector virus alters or hides in the boot sector, usually the 1st sector, of a bootable disk or hard drive. The boot sector is where your computer starts reading your operating system. By inserting its code into the boot sector, a virus guarantees that it loads into memory during every boot sequence. A boot virus does not affect files; instead, it affects the disks that contain them.

In the 1980s boot sector viruses were common and spread rapidly from one computer to another on rewritable floppy disks which contained programs. However, with the CD-ROM revolution, it became impossible to infect read-only CDs. Though boot viruses still exist, they are much less common than in the 1980s. Additionally, modern operating systems do not allow ordinary programs to write to the boot sector. Examples of boot viruses are Polyboot.B and AntiEXE.

Multipartite viruses

Multipartite viruses are a combination of boot sector viruses and file viruses. These viruses come in through infected media and stays in memory. They then move on to the boot sector of the hard drive. From there, the virus infects executable files on the hard drive and spreads across the system.

There aren’t too many multipartite viruses in existence today, but in the 1980s, they accounted for some major problems due to their capacity to combine different infection techniques. A well-known multipartite virus is Ywinz.



1. Trojans

A Trojan Horse is a destructive program that pretends to be a normal application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most dangerous types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from the Greek story of the Trojan War, in which the Greeks give a giant wooden horse to their enemies, the Trojans, apparently as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their allies to pour in and capture Troy.

Types of Computer Trojan:

         Remote Access Trojan: Abbreviated as RATs, a Remote Access Trojan is one of seven major types of Trojan horse designed to provide the attacker with complete control of the victim's system. Attackers usually hide these Trojan horses in games and other small programs that unsuspecting users then execute on their PCs.

        Data Sending Trojan: A type of a Trojan horse that is designed to provide the attacker with sensitive data such as passwords, credit card information, log files, e-mail address or IM contact lists. These Trojans can look for specific pre-defined data (e.g., just credit card information or passwords), or they could install a keylogger and send all recorded keystrokes back to the attacker.

          Destructive Trojan: A type of Trojan horse designed to destroy and delete files, and is more like a virus than any other Trojan. It can often go undetected by antivirus software.

          Proxy Trojan: A type of Trojan horse designed to use the victim's computer as a proxy server. This gives the attacker the opportunity to do everything from your computer, including the possibility of conducting credit card fraud and other illegal activities, or even to use your system to launch malicious attacks against other networks.

          FTP Trojan: A type of Trojan horse designed to open port 21 (the port for FTP transfer) and lets the attacker connect to your computer using File Transfer Protocol (FTP).

          Security Software Disabler Trojan: A type of Trojan horse designed stop or kill security programs such as an antivirus program or firewall without the user knowing.

          Denial-of-Service Attack Trojan: A type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being dreamed up by hackers.

1. Software Piracy

Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to resemble the original. Retail revenue losses worldwide are ever increasing due to this crime. This can be done in various ways-End user copying, Hard disk loading, Counterfeiting, Illegal downloads from the internet etc..



**Survey**

This was a survey conducted to see the various people affected by Cyber-Crimes.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Person Asked** | **Daily Job** | **Answer** | **How?** | **When?** | **Degree of seriousness(1-10)** |
| Nadaraj Govender | Lecturer | Yes | Spam, viruses, Phishing | continous spam all the time | 3 |
| Sarojini Govender | Teacher | No |  |  | - |
| Anurag Arnag | Student | Yes | Spam, viruses, Phishing, Trogans | A serious virus attack a month ago, all data lost | 7 |
| Yevania Naidoo | Student | yes | Spam, viruses, Phishing, Trogans | Emails are requestin private info | 5 |
| Jarred Reddy | Teacher | yes | phishing, spam | A year ago Funds were tansferred from my account | 9 |
| Prekash Moodley | IT technition | yes | Viruses, Spam, Trogens | From the time he had a PC | 6 |
| Donovan Naicker | Mechanic | No |  |  | - |
| Merushka Reddy | Student | yes | Spam, Viruses | A year ago all files were deleted | 8 |
| Kivan Moonsamy | Salesman | yes | Spam, phishing, virus | Received an email requesting credit account details | 7 |
| Tompson Naicker | Student | yes | spam, viruses, trojans | 3 months ago a virus attack | 6 |

**Results**

Most of the people questioned were affected by cyber crime. Some had serious attempts of phishing where money was transferred out of their account and others keep on receiving spam.

Average degree of seriousness of Cyber Crime: (3+7+5+9+6+8+7+6) ÷8 =6.4 Out of 10. This proves that cyber crimes need to be address due to many people being victims of such activities.

Every person affected by Cyber Crime has also been affected by spam. This could infer about the large amount of spam that is being sent to everyone. The time period shows that Cyber Crime is not new but still exists in full force.

**Conclusion**

Cyber Crime existed many years ago and is still in full force in this era. With every great advantage a disadvantage manifests itself. This is evident as cyber crime has popped up after the Information Technology age has been designed.

There are many different types of Cyber Crime, some serious and others not so bad. All computer users should have a general understanding of the different types of Cyber Crimes including Spamming, phishing, Viruses, Trojans, Worms, Hacking and spoofing. Hence this will reduce the impact of these crimes on ordinary citizens. This assignment will provide the basis to the concepts of computer information fraud as well as provide results for a survey done to put into retrospect the impact and vastness of these crimes.

**Bibliography**

Books

A textbook for Information Technology by Chris Noome

Hacking revealed by H. Smith

Past year SA NSC matric exam papers

A guide to Cyber Crimes by H. Hatton

Internet Pages

[**www.cybercrime.gov/**](http://www.cybercrime.gov/)

[**www.cybercitizenship.org/crime/crime.html**](http://www.cybercitizenship.org/crime/crime.html)

**www.howstuffworks.com › ... ›** [**Computer & Internet Security**](http://www.google.com/url?url=http://computer.howstuffworks.com/computer-internet-security-channel.htm&rct=j&sa=X&ei=E458TaubEoHmvQPC9rXrBw&ved=0CFQQ6QUoADAD&q=viruses&usg=AFQjCNFsqlDTv-O_nnj3mhNLIi5zOvm0gA)**.html**

[**www.webopedia.com/TERM/T/Trojan\_horse.html**](http://www.webopedia.com/TERM/T/Trojan_horse.html)

**http://spam.abuse.net/overview/whatisspam.html**