Computer security and the threat of hacking computer science essay

Technology, Computer

Computer security is a safety operating system that is an important feature to install on a computer. It ensures safety and protection from unknown users and threats. If a safety operating system is weak, unknown users, or hackers, are able to break into the database and install harmful viruses, as well as steal personal information. Computer security and hacking can have both disadvantages and advantages. Computer security has evolved from early on to being a key component to own. Hacking, as well as computer security, has developed into a more harmful and dangerous activity. Currently, security programs have been developed to stop hacking and viruses from encroach onto a user's computer. Computer security and hacking have had impact on society today, globally and locally. Users use computer security to their benefit when keeping personal information stored on their database. Hacking can destroy a users' identity, or possibly their reputation. Businesses and organizations have benefited from security, by its protection of information and protection from outside harm. Hacking can be used as a good way to check a computer's sustainability to dangers through networks and the internet. Computer security and hacking are two important issues discussed and recognized today.

Computer Security is an important element of safety precaution when using a computer. These operating systems run on computers to ensure the safety of personal and financial information, along with protection. Computer security can be a very useful component to acquire [1]. If an unknown user tries to access a computer database, computer security will ensure that that user will not be let in [2]. Besides keeping unknown users out of others' computer databases, computer security also provides protection from

harmful threats and viruses. Once these viruses find their way onto a user's computer, information and control access can be stolen [3]. There are significant advantages and disadvantages of having a strong computer system, one advantage being protection from viruses and other harmful attacks [4].

Hacking has found its way into the world of computers. Hacking can be destructive, harmful, and can have some bad impact on peoples' lives. If a computer system is not protected by a security operating system, hackers can find their way into that database easily. Once in, hackers can obtain personal, financial, and important information [5]. This can cause ruin in a user's business and personal life, and much more. While being branded a bad thing, hacking can help many as well. Some hackers are able to test the reliability of a computer's security system, to find weak spots in the barrier [6]. Like computer security, hacking can have both costs, but benefits too [2].

The purpose of this report is to allow computer users to gain insight on the aspects of computer security and the ethical issue of hacking. Computer security can allow users to feel comfortable knowing their personal information is being kept hidden. But even with a high-level computer security system, one is still vulnerable to a hacking intrusion. A computer user's private information, such as social security, credit card numbers, passwords, email addresses, and other information is at risk to being taken.

There are a number of objectives covered in this report. First, computer security is used to keep personal, financial, and other private information kept confidential. Second, computer security blocks viruses and attackers from encroaching on one’s computer. Third, even with this security, one is still susceptible to a hacking attack. And lastly, hacking can be easily hurtful, but could in some cases be just as helpful for users.

The main contents of this report include computer security, and the issue of hacking. Computer security is described as a protection technique for personal information, and for blocking unwanted threats from the internet. Hacking is described as being a harmful way to obtain information from other users’ databases. Viruses and threats are each described in order for other users to know the differences between them all. Also in this report are ways to check a computer’s security and ways to keep it protected from harm too.

2 Background

2. 1Computer security is an operating system used on computer databases to protect and provide safety to users. Besides preventing unauthorized access, computer security provides protection for personal, financial, and classified information [1]. One type of this security system requires a validation of a username and password provided by the user, in order to gain access into the computer database [2, pg. 267]. Besides validating who the user is, it also confirms that the user is not trying to attempt an unlawful operation [2, pg. 31]. As shown in Figure 1, computer security requires a “

key,” or username and password, in order to access the database. Many businesses and organizations have benefited greatly from this operating system, because it allows their private information to stay confidential and secret [1].

http://comtrec. com/wp-content/uploads/2010/05/Computer-Internet-Security. jpg

Figure 1 Picture representing the security operating system,
with the binary representation inside a computer.

Computer security had begun physically in the 1950-60s. Computer systems then were guarded by security officers, to stop the attempt of gaining unauthorized access. Later on in the 60s and 70s, access could be granted over telephone lines, which caused a change in the way computers were externally guarded [2, 266-7]. By the 90s, companies sprang up to provide a more modern way of securing computer systems. Secure Sockets Layer (SSL) was developed by Netscape Communications, (which was an early web browser) to get secure transfer of info when buying online. By 1999, the Transport Layer Security (TLS) had been developed, and was very similar to the Secure Sockets Layer, but with a few important improvements [2, 350-1].

Hacking can be defined as the encroachment of one’s personal or business computer system by an outside source [7]. Hackers, or the outside sources encroaching on the personal computer, can have many motives to these intrusions. Some hackers have admitted to only wanting to enjoy the challenge of overcoming a security system [8]. Other hackers have admitted

to wanting private or financial information for their own personal gain [7]. There are different ways a computer can be hacked into. These ways include: through downloads, internet-based programs, and through fraud emails. Through these, hackers can plant viruses and attacks which make it possible to overcome a security system [3].

A “ hacker” has had many definitions from early on. In the Middle Ages, a “ hacker” was in the business of creating tools known as hoes. Later on into the 17th Century, a “ hacker” had become a strong worker that handled a hoe. Today, a “ hacker” has nothing to do with an actual tool, but is capable of being a strong worker, when it comes to intruding upon another’s computer system [2, pgs. 657-8]. The earliest form of hacking was known as “ phreaking.” This involved hacking using telephone lines [9, pgs. 12- 13].

2. 2There are a number of advantages and disadvantages when it comes to computer security. Some advantages include: greater storage space, resource and file sharing, an increase in cost efficiency, and security of private information. Some disadvantages include: the expensive cost, it could have a number of weak spots, and some security issues [4].

Hacking has some important costs and benefits when it comes into play. Some costs include: the owner loses control over his or her information, harmful viruses and threats on users’ computers, and loss of data either being intentional or unintentional by hacker. An important benefit is ethical hacking, because users can determine where the weak spots in their system are [2, pg. 659].

2. 3 There are some theories to deciding whether hacking can be good or bad. In some ways, it can be dangerous, hurtful, and devastating. Many can lose their personal information, such as social security, credit card numbers, emails, addresses, and much more, and can be left with nothing. In some ways, hacking could be a good thing. This is true because many hire ethical hackers to test their computer's security strength to find weak areas in their systems. It is an undecided theory, because hacking can be labeled good and bad, and each argument can be supported [2, 659].

2. 4 A class for viruses, threats, worms, Trojans, spyware, and other forms of attacks is known as " malware." [7]. A small portion of software that can enter a user's computer secretly and in other easy ways is known as a virus. Trojans are similar to a virus, but different in the fact that once installed, it allows the Trojan horse's creator the ability to see everything on the user's computer. Spyware is capable of being installed within a user's database with or without the user having knowledge of it [3]. These types of threats and attacks are hidden within programs that come as fake emails, internet-programs, and downloads. Figure 2 below demonstrates all the different types of harmful threats that can be uploaded onto your computer by hackers.

http://www. dreamstime. com/computer-and-network-security-hand-thumb4123007. jpg

Figure 2 This is a collection of all the different
types of viruses and threats that can be harmful

for a user’s computer.

3 Computer Security and Hacking

3. 1Society has been impacted by computer security in a number of ways. Computer security ensures users that their personal, financial, and other information will be kept secret from the eyes of others. It impacts businesses and organizations by keeping their confidential data safe from view and harm and helping them in staying successful [1]. It allows users to share files and resources, an increased amount of storage space, and an increase in cost efficiency [4]. As well as protecting information, computer security has impacted users and their computers from nasty viruses, threats, and malware as well [3]. Computer security is an important piece of technology that has impacted society since its beginning.

Hacking is impacting society today in many ways. Hacking impacts users by taking their personal information, and could possibly display it over the internet [7]. It is causing an increase in cost for companies and organizations to fix their computer systems after a security breach, and to obtain better security. There has been recent documentation dealing with an increased amount of threats found in web sites that can easily be uploaded onto databases. [10]. Hacking impacts businesses and organizations if these do not have a strong security system. Hacking can have a number of impacts on society, especially taking personal information from other users [5].

3. 2 Computer security involves another component, called a “ firewall.” This component, software or hardware, is made to block unwanted threats and

viruses from a user’s computer. A firewall is used to prevent the intrusion of hackers, viruses, and many other threats from gaining access and information onto a computer [11]. An example of a strong firewall that provides protection and dependability is the Cisco PIX Firewall [10].

A well-known security system used by many is called Symantec. Symantec had originated in 1982. It has become the world’s largest software company, with business internationally, and with over 17, 000 workers. Symantec ensures security of the computer, its infrastructure, and all the components within it. Symantec has a research lab where new technologies are developed to ensure even more security [12].

Norton AntiVirus is Symantec’s current security program. Norton provides safe networking, protection online, and a scanner to check for viruses and threats. Norton is a very trusting program, because it ensures safety for users and for their computers. Figure 4 is a picture of the program Norton AntiVirus. Figure 5 represents the Norton program at work. This main screen alerts the user if their system is not secure, and what types of protection the user would like to be on or off. [12]

http://www. amitbhawani. com/blog/wp-content/uploads/2010/06/Norton360-Box-Package. png http://www. windows7hacker. com/wp-content/uploads/blog/DownloadNortonAntivirus2010BetaonWindows_E88F/NewNortonAntiVirus. png

Figure 3 Picture of the Norton Figure 4 This figure represents the Norton AntiVirus program AntiVirus main screen

3. 3 Even though hacking is labeled as dangerous, some have found hacking to be a blessing. Some computer users hire “ ethical hackers,” which are those who imitate an actual attack onto a user’s computer system, in order to test that computer’s security system and its blocking power. While imitating this attack, ethical hackers are also looking for weaknesses within the system, and what could be stolen in a real hacking attack [6]. Another way to check a network’s security is by sending a vulnerability scanner over the computer. Like ethical hacking, a vulnerability scanner will check for weaknesses in the security, and will increase the security as well. Besides scanning for weaknesses in the security wall, users should consistently be checking their computers for any type of threats or attacks. If these threats or attacks are not resolved, all types of malware could corrupt the database [10].

4 Conclusion

Computer Security is described as being a protection mechanism for computer databases. This mechanism can come in different shapes, styles, and forms [1]. One of the types of computer security is a validation code. The user of the computer must provide his/her own username and password to access the database [2]. Another type is AntiVirus security, such as Norton AntiVirus by Symantec. This program will provide protection from harmful threats and viruses, and hackers as well [12]. Computer security has provided many with comfort knowing that their private and financial information will be kept safe from other eyes on their computers. Big companies and organizations have benefited from computer security,

because with it they have a comforting feeling that their important information will be kept safe [1].

Hacking is a dangerous and unfortunate activity that occurs on vulnerable computers [7]. Hackers find their way into other user's systems, and depending on what they want, credit card numbers, social security, or anything of the like, they are likely to succeed in getting [5]. Hackers can plant harmful viruses and threats into a user's system with or without that user knowing [7]. It can be a very upsetting and unlucky event to happen, because users are susceptible to having their personal information stolen or revealed to the public [2, pg. 659]. But in the light of things, hacking could be a good thing for some users. Ethical hacking can be a useful method for checking a computer's security barrier. It finds the weak spots that a computer hacker, virus or threat could enter the database through [6].

There are ways to improve computer security and to keep hackers and viruses out of computer systems. Ethical hacking could be a method used to find the vulnerable areas in the security, which would inform the user that better security is needed [6]. Similar to ethical hacking, a vulnerability scanner runs over the system scanning for weak spots, and improves security too [10]. Certain antiviral programs could be purchased and installed to increase security. Such programs as Norton AntiVirus will alert the user of any threats, scans the system, and will keep a computer safe [12].

There are conclusions I've drawn from researching computer security and hacking. First, computer security is a very important component to have on a computer. Businesses and companies have impacted from it, because they are able to keep valuable information stored on their computers. Without it, users should not be on the internet or network at all. Hacking can be a very uncomforting and hurtful activity to users and their computers. Users can have their private and financial information taken from them, as well as being made public. There are many types of viruses and threats that can harm users' computers, especially the ones thought to be low risk. The reason I drew these conclusions is because they are important things to know and understand. If one is naA? A? ve to the risks of the internet and hackers, their computers, as well as themselves are in peril.

There are some issues that I would like to address in future studies. I would like address the issue of weak spots in a computer's security. I would like to see this security to not have these weak spots, and to fix them before using them on computers. Second, I want users to realize how dangerous it is to not have a computer security operating system, before they find it is too late. I would like to see programs such as Facebook and MySpace not allow users to put as much information as they allow now. Because of this displaying of information, many are susceptible to danger. I would like these issues to be addressed in future studies.