Computer hacking is the practice of modifying computer

Technology, Computer

Since the word " hack" has long been used to describe someone who is incompetent at his/her profession, some crackers claim this term Is offensive and falls to give appropriate recognition to their skills. Computer hacking Is most common among teenagers and young adults, although there are many older hackers as well. Many hackers are true technology buffs who enjoy learning more about how computers work and consider computer hacking an " art" form. They often enjoy programming and ha eve 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, to an opportunity to harm others. Since a large number of hackers are self-taught prodigies, 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 seriouscomputer-related crimes. A number of issues arise in considering hacking from the educator perspective.

First, we need to consider the fact that the public perception of hackers s mixed, and that " hacking" and " being considered a hacker" can be quite appealing to students who are going through developmental periods In which they are defining themselves, as well as challenging authority and rules. There is often a Robin Hood mentality to early actions, though it is unclear exactly who " the poor" are, and how they are " being compensated". Second, the anonymity of actions which hackers perform against others

often enhances the severity of actions. For example, an illegal pay-per-view website that features the game of Gills Philippians vs..

Iran. These robin DOD-Like hackers are paid to hack the system of this site to malting the peace balance of Industry. Computer hacking can also lead to other constructive technological developments, since many of the skills developed from hacking apply to more mainstream pursuits. For example, the infamous hackers Dennis Ritchie and Ken Thompson went on to create the UNIX operating system in the sass. This system had a huge impact on the development of Linux, a free UNIX-Ice operating Woozier who started this hacking madness in the computer world. II. Review of Related Literature

For the past years, new ways of finding and helping solve a crime was implemented by authorities, but what shook the society was an unpractical way; Hacking. It is used to describe vivid creation of a new program or changing the existing complicated software's (Palmer, 2001). This thought happened to strike down an idea if the idea of hacking is ethical or in lay man's terms, doing the wrong actions for good intentions. At present, the purpose of the paper is to find out if students from De La Sale University - Manila find hacking for good intentions ethical as it sounds.

According to research Journal by Palmer (2001), ethical hacking was used in search for a way to approach intruder threats that breaks in different organizations by breaking in also into threats system. To put it simply, computer securities used hacking to fight against hackers or commonly said as fighting fire with fire. According to a Journal by Fearsome, et al. (2010),

ethical hackers must possess qualities such as being completely trustworthy, profound programming or networking skills and are also adept in maintaining operating systems intact.

A description by Jamie (201 1), describing ethical crackers are such highly paid professionals with status of legitimacy and can not be easily accessed. They are trained experts that can minimize the risk of impact and getting caught, even though; it would not guarantee their client's perfect security as those people that operates their computers and networks can make mistakes and the longer it has been for their tests to be performed, the lesser reliable it is Mail, 2011; Palmer, 2001).

The question, should ethical hacking be really considered as a work comes in, knowing some could even be arrested for doing it and would hacking being implemented on a regular academic basis be a good thing to the rise of the ethical hacking empire? A survey conducted by the IEEE Computer Society in Walsh College asked to their faculty if they should not teach ethical hacking or penetration testing to their college students. The results showed an overwhelming majority of 71 percent agreed by the college's faculty members (Livermore, 2007).

This can be a profound source saying that even most of the populous in their faculty, believes so that Hacking is indeed needed to be implemented on a university's education and can also qualify being an expert on hacking as a professional. On the other hand, Scaffold (1997), states that writing vandal ware or computer viruses and breaking into a computer and looking at the

files is not completely related into computer education. He believes that knowledge on ethical hacking does not stop there as he believes that the ability to hack should also come with responsibility on their actions.

Hacking is not new for most of the techno occupant societies nowadays. The idea of breaking in into something that broke in already is not new (Palmer, 2001) and the minds of the students that are learning ethical hacking today will proportionally grow Mail, 2007). Though most of the studies stated do agree on the implementation of hacking for the good intentions as an ethical practice, while for some immoral as it responds to digging in into personal information, it will still depend on whether on how the hacker uses up its capability for doing the good or bad. Ill.

Methodology The subject of this study were DULLS students from the college of Computer Studies, Business, and Liberal Arts. These students were exposed into subjects and even survey forms, both online and hardcopy that will answer questions that are related to hacking. The term 'survey is commonly used to a research methodology designed to collect data from a specific population, or a sample from that population, and typically uses a questionnaire or an interview as an instrument for the survey (Robinson, 1993). Sample surveys are an essential tool for collecting and analyzing information from selected individuals.

They are widely accepted as a key tool when conducting and applying basic social science research methodology (Rossi, Wright, ND Anderson, 1983). According to Leary (1995), there are distinct advantages in using a

questionnaire vs.. An interview methodology: questionnaires are less expensive and easier to administer compared to personal interviews, because they lend themselves to group administration and, they allow confidentiality to be assured. The survey used in this study have four main purposes. The first purpose is to know if the selected population is familiar to the term hacking.

Next is to know their impression about hacking. The third is to know if they are aware about Ethical hacking. Lastly is o know if their opinion about legalization of hacking. Factors including age, gender, and college were used to measure these perceptions. All in all, the survey constructed is used to know how students from DULLS view hacking and its use in relation to ethics. 'V. Data Analysis Our group conducted survey from different colleges in DULLS, which includes College of Computer Studies, College of Business, and College of Liberal Arts.

We chose these colleges because first, CSS is composed of students who are very familiar of computer-related concepts. Next, COB because it is composed of students who will e part of the corporate world in the future, and might use persons with hacking knowledge to protect their system. Lastly, CLAD students because they seem as the neutral college for our research. The survey we conducted is composed of questions related all about our topic, which is hacking. Some of the big questions are the familiarity of the respondents in the term " hacking".

Another one would be their awareness about " Ethical hacking". In addition, we asked their opinion about the legalization of hacking, if it was to be used in an investigation. Among the students in the college of business 42. % are familiar and 57% are very familiar of the term hacking. However, they have varied impressions of the term: Impression on hacking of business students (Table 1) Table 1 shows the impression of business students in the term hacking. Whether they see it as something that is bad or good, they are also given the option abstain.

The table illustrates that their impression is equally divided, 43% answered bad and another 43% answered good. Their impression must be based from their own experience since 57% of them have been hacked. Surprisingly, more than half of the business students want hacking to be taught in school. We infer that this result is based from their curiosity to learn new things. In addition, 86% of the COB respondents are not aware of Ethical Hacking. This may be because of the fact that they do not have computer-related subjects. All in all, these business students do not agree to the legalization of hacking. ACH choice. The reason behind this may be the fact that they will not really need hacking or any computer-related subjects in their field. Most of the students are in the field of communication arts and psychology, which obviously does not require computer concepts like hacking. However, 67% of the respondents are familiar with Ethical Hacking, but no one agreed to it. In the end, like COB students, they also do not agree in the legalization of hacking. Lastly, we distributed our survey among CSS students. We conclude that most of them, if not very familiar, are familiar with the term hacking.

The reason behind this is because of their course. In fact, there is a specialization - Network Engineering, among CSS students that tackles hacking. In addition, being exposed to computer- related subjects surely made them familiar about this concept of hacking. However, hen it comes to their point of view, 50% believed that it is good, and the other half believed that it is bad. Their point of view may be based from experience, since 58. 8% of them have been hacked and probably rude things are committed in this hacking.

As a result of being CSS students: Response of computer students with regards to teaching hacking in educational institutions (Table 2) Table 2 shows a huge percentage of respondents agreed that hacking should be taught in educational institutions. We can say that computer science students are more interested to learn hacking rather than business and liberal arts students. The reason behind this is because, CSS students are the ones who live and breathe computer, which means they know a lot about computer, and at the same time, they want to learn more about it.

Table 2 can also apply to the ones who are familiar with Ethical Hacking and the ones who are not. In the end, 94. 1% of computer science respondents agreed that the concept of hacking should be legalized. In conclusion, students of computer science, business, and liberal arts have different perspective when it comes to hacking, whether it is ethical or Just plain hacking. To put the over- al impression of the 3 colleges on hacking together we have: Impression on hacking of CSS, COB, CLAD students (Table 3) We can say that in the end, the term hacking will usually referred to as " bad".

However, 55. 5% respondents agreed to ethical hacking. Thoughts of CSS, COB, CLAD students on Ethical Hacking (Table 4) With this, we conclude that despite the fact that their impression on hacking is bad, they still believe that there is a concept of ethical hacking, which proves our claim that the meaning of hacking will always depend on its purpose. V. Results and Discussion What do you think of when I say the word " Computer Hacker"? Some people probably think of some sort of criminal bent on gaining access into your bank accounts or remote control over your computer.

Granted, hackers have gotten a bad reputation from the media, who sometimes report break-ins of databases, computers, and other virtual resources. However, this does not mean that every hacker has a desire to do harm. In fact, hackers are hardly the bad guys. The word hacker has been so warped and distorted by the media that people now believe that hackers are all criminals ND intend to do harm. The truth is, hackers are people and therefore many of them have morals that disallow them to purposely cause harm.

The results of our research believes that regardless of the stereotypical view of hackers in today's society, the majority of them help the world of computers rather than damage it. Action should be taken against the people who make the internet unsafe, not the people who make the internet safer. In this research, we learned that hacking still has the future to revolutionize. If ethical hacking was legalized by the law, this would be a great help or investigations and preventing the illegal by passers in our techno-world.

People can minimize the potential of being hacked by discipline and proper orientation to the basic securities of the internet world.