

# [The vulnerability of computerised accounting information systems to computer crim...](https://assignbuster.com/the-vulnerability-of-computerised-accounting-information-systems-to-computer-crime/)

The hot debated topic in the informative age is computer crime. These crimes are committed with the help of computers which wreak havoc and completely paralyse the economy. These crimes are with high intensity and more deadly and destructive than physical crimes. There are no precise, reliable statistics on the amount of computer crime and the economic loss to victims, partly because many of these crimes are apparently not detected by victims, many of these crimes are never reported to authorities, and partly because the losses are often difficult to calculate.

These crimes are committed by those who intend to use information system for their personal benefit’s, thereby affecting the entire economy and making companies, individuals, banking or financial institutions more vulnerable towards various threats committed by computer crime professionals through misuse of internet and computer softwares. Hackers with their computer skills access various websites, break-out the passwords and manipulate accounting system of a company, celebrities etc., thereby making the people vulnerable to frauds committed through computers.

In the rapid changing technological era many developments have taken place and computerised technology with innovative user friendly packages and softwares has created a sound impact all over the globe. Due to computerised systems the modern era people can obtain comprehensive information allied to anything only at the ‘ click of a mouse’. With the advent of information systems, it has become easier and faster to stock-in and keep posted alarmingly sizeable amount of statistics / data. But these systems on the other hand have made it easier and quicker for criminals to commit fraud. When the need for computer security is ignored, an open invitation is given to criminals – these destructive minded criminals take advantage of any opportunity to defraud – a company, company’s clients and individuals.

Computer frauds / Computer crimes when looked from a wider perspective are a very destructive and dangerous weapon in the arsenal of criminals. It’s dangerous because these criminals use computers to commit dishonesty and harm by obtaining an advantage or causing loss of something of value – This could be in the form of program fraud, hacking, e-mail hoaxes, auction, retail sales schemes, investment schemes and people claiming to be experts on subject areas. That is why it is important for educational providers to have knowledge of this area of computer crime. Students in any grade level or educational providers are also vulnerable to computer crimes as the modern era studies are closely associated with computers. With the use of new technologies and many coming up – more is the vulnerability for rise of computer crimes.

Computer crimes can be divided into two main areas; ‘ THEFT’ and ‘ SABOTAGE and VANDALISM’. Computer pranks are considered as illegal activities, because they often have at least the potential for significant harm. Also these computer crimes are difficult to differentiate from sabotage and other forms of destructive behavior (http://www. aarp. org/bulletin/yourhealth/Articles/a2003-06-30-onlinefraud. html). The potential for significant damage to commercial interests, accounting systems and national defence through computer viruses and other forms of computerised sabotage has been demonstrated and can be collated from the past, the amount of destruction such crimes can commit. Mainly the perpetrators of computer crime can be divided into employees, outsiders and hackers.

Employees use their knowledge and understanding of the various activities of the business, outsiders have a difficult task to penetrate into a system and get familiar to the working of the system and finally the hackers who are less concerned about any monetary gains or damage, instead they may commit computer crime for ‘ fun’ or ‘ intellectual challenge’. Although, media highlights outsiders and hackers as the most dangerous criminals – but employees are the most dreadful perpetrators of most computer crimes / threats. Computer related crime / theft can be divided into six categories: theft of software and computer equipment, unauthorized use of access codes and financial passwords, theft by entering fraudulent transaction data, theft by stealing or modifying data, internet hoaxes for illegal gains and theft by modifying software. All the softwares and standard applications framed for the very comfort of this informative age are always prone to the vulnerability of attack from criminals.

In the innovative age accounting plays a very important role in the overall projection and building of the structure of a company. Accounting data is the lifeline of any corporate. The accounting data gives a correct and concrete picture of the financial position of a company. With the advent of computerised accounting softwares and packages, it has been a sigh of relief for the accountants. Now, the accountants are able to punch-in entries in the software and get desired reports, as required by the management within a reasonable time. Secondly, the data got with the help of computerised system is more accurate, which helps the management to take appropriate decisions, based on the past financial position. At the same time, all these softwares are also vulnerable to threats / crimes.

Many a times, it may happen that in order to show misleading figures to the outside world, the management with the help of their accountants manipulates the accounting records by inputting unrealistic figures in the software; thereby inflating the profit’s and foolproofing the folks. On the other hand, the clerical staff entering the data and preparing the reports may manipulate the input data – on being influenced by any outside or competitive sources – to avoid disclosing the true scenario of the company. Many a times the top officials of a company – invoice the customers account with an outdated / dormant item of which the current system (software) value is very low, invariably showing inflated profits. These sorts of crimes are practiced, so as to conceal the actual feeble condition of the organization and misguide the outside world such as investors, shareholders, etc.

A criminal can also impersonate someone else, access that person’s account electronically and cash-in money or information, since the computerised system transfers money based transaction on the input of a password and sort code. The criminal, will anyhow locate the password and sort code, which make him / her easily accessible to the other person’s account. With these passwords they open up the restricted area / personalized section and carry out their activities beneficial to them and harmful to others. In case if PBX Access Code, ATM passwords are known to other person than the one using the facilities, computer crime operators will misuse it by making telephone calls and withdrawing cash through ATM, without the knowledge of the concerned.

This is possible, because all these programs are stored in a computerised system and runs on the input of a ‘ PASSWORD’. Also the criminals with the help of internet create websites, projecting themselves, as one of an exceptional advertising agent, auction agent, promotion agents etc. In response to these websites – companies, individuals and others, who are interested in advertising their products or auctioning their property, make payment through internet under the impression that their work will be carried out swiftly. Later on they feel cheated, when they realise that computers were used as a base for embezzlement of money.

Entering fraudulent transaction is the most common and the easiest method of theft in computer related crime. Some type of fraudulent transactions is forgery (fake ID Cards etc.), disbursements (fictitious invoicing etc.), inventory fraud (fictitious customer account etc.), payroll fraud (embezzlement of wage payments), pension fraud (embezzlement of pension payments), cashier fraud (undervaluation of tickets etc.)

Many software professionals with their vast knowledge and professional experience create computer programs affecting the software package of a company or network and subsequently crashes the entire system, making it disabled. Such destructive programs are called ‘ VIRUS’ – Eg. Melissa, I love you etc. Since the development of computers and the wide use of internet, many cases of virus has come up – this has indulged in the pumping of huge amount of money. Such destructors are called ‘ HACKERS’.

During February, 2000, hackers launched – Distributed Denial of Service (DDS) attacks on several prominent websites. In a DDS attack, dozens or even hundreds of computers all linked to the Internet are instructed by a rogue program to bombard the target site with nonsense data (Steven Alter). This attack causes the target site’s servers to run out of memory, and thus cause it to be unresponsive to the queries of legitimate customers. Also there are many information system professionals, who with their wide knowledge of computers force their entry to the web site of banking or financial institutions, reputed companies etc. with the sole aim of manipulating the software and use it for their own benefits. These people hatch password of the respective accounts and access the records / data of others.

Computerised technology has made the informative world very small and compatible. Computers play an important role – for the task which used to take an indefinite time earlier , be now completed within a decisive short span of time, thereby increasing the efficiency and data reliability level. Data stored in computers can function as a comparison tool and can be easily compared with current performance, thereby hastening decision making. Even management can get the exact data in a standardised layout within a set time limit for strategic planning, functioning and diversification and expansion process. The only shortcoming added to these benefits is the evolvement of computer crimes. Anyway, nowadays utmost care is being taken by way of password, data encryption, so as to avoid and reduce the tendency of information system crime.

\* Bibliography

1) Philip Keir, Internet. au, Electronic Messaging Made Easy, 1998, Issue No. 37, Page No. 34

2) Steven Alter, Information Systems Foundation of E-Business, 4th edn., 2002, Pearson Education Inc., New Jersey, USA

3) Carole Fleck, Online Fraud on the Rise, June 2003, viewed 10. 05. 2004, http://www. aarp. org/bulletin/yourhealth/Articles/a2003-06-30-onlinefraud. html

4) Computer Crime and Intellectual Property Section (CCIPS), viewed 11. 05. 2004, http://www. usdoj. gov/criminal/cybercrime/compcrime. html

5) Fundamentals of Computer fraud, viewed 29. 04. 2004, http://www. marketplace. cfenet. com/products/ProductDetail. asp? CatID= 100170

6) Ginger Kastor and Wadsworth Illinois, Computer Fraud, viewed 04. 05. 2004, http://www. lrs. ed. uiuc. edu/wp/crime-2002/fraud. htm

7) Ronald B. Standler, Computer Crime, 2002, viewed 06. 05. 2004, http://www. rbs2. com/ccrime. htm