COMPUTER MISUSE

COMPUTER MISUSE

- Businesses, government and academic institutions are increasingly reliant on the Internet for their day-to-day business, while consumers are using e-commerce more and more for purchasing goods and services.
- This implies ever-increasing opportunities for hackers and virus writers to disrupt the activities of their fellow citizens.
- Hacking first became a prominent issue in the 1980's, with the publicity achieved by exploits such as the Internet Worm, but at that time it was not clear how law enforcement agencies could best tackle this new threat

TYPES OF MISUSE

- Misuse of computers and communications systems comes in several forms
- **Hacking**

  Hacking is where an unauthorized person uses a *network*, Internet or *modem* connection to gain access past security passwords or other security to see data stored on another computer. Hackers sometimes use software hacking tools and often target, for example, particular sites on the Internet. Also, the act of stealing personal or private data, without the owner's knowledge or consent
- **Viruses**

  Viruses are relatively simple *programs* written by people and designed to cause trouble or damage to computers or their files.
- **Software Cracking**

  Cracking is where edit a program's source code, or you could create a program, like a key generator. Cracking is pretty much looking for a back door in software, and exploiting it for malicious use or for a copyright breaching act

CONT.

- **Data misuse and unauthorized transfer or copying**

  Copying and illegal transfer of data is very quick and easy using online computers and large storage devices such as *hard disks*, *memory sticks* and *DVDs*. Personal data, company research and written work, such as novels and textbooks, cannot be copied without the copyright holder's permission.

- **Copying and distributing copyrighted software, music and film**

  This includes copying music and movies with computer equipment and distributing it on the Internet without the *copyright* holder's permission. This is a widespread misuse of both computers and the Internet that breaks copyright regulations

CONT.

- **Email and chat room abuses**

  Internet services such as *chat rooms* and *email* have been the subject of many well-publicized cases of impersonation and deception where people who are online pretend to have a different identity. Chat rooms have been used to spread rumors about well known personalities. A growing area of abuse of the Internet is email spam, where millions of emails are sent to advertise both legal and illegal products and services.

- **Financial abuses**

  This topic includes misuse of stolen or fictional credit card numbers to obtain goods or services on the Internet, and use of computers in financial frauds.

PREVENTING MISUSE

- **The Computer Misuse Act (1990)**
  - This was passed by Parliament and made three new offences:
  - Accessing computer material without permission, e.g. looking at someone else's files.
  - Accessing computer material without permission with intent to commit further criminal offences, e.g. *hacking into the bank's computer and wanting to increase the amount in your account.*.
  - Altering computer *data* without permission, e.g. writing a *virus* to destroy someone else's data, or actually changing the money in an account.

PUNISHMENT

- The offences are punishable as follows:
- Offence 1. Up to 6 months' prison and up to £5,000 in fines.
- Offences 2 and 3. Up to 5 years in prison and any size of fine (there is no limit).

PREVENTING MISUSE

- **The Data Protection Act**
  - This was introduced to regulate personal data. This helps to provide protection against the abuse of personal information.it also provides guidance and best practice rules for organizations and the government to follow on how to use personal data including:
  - Regulating the processing of personal data
  - Enabling the Data Protection Authority to enforce rules
  - Holding organizations liable to fines in the event of a breach of the rules
- **Copyright law**
  - This provides protection to the owners of the *copyright* and covers the copying of written, musical, or film works using computers

CONT.

- **Reduce email spamming**
    - This may be reduced by:
        - Never replying to anonymous *emails*.
        - Setting filters on email accounts.
        - Reporting spammers to *ISPs*, who are beginning to get together to blacklist email abusers.
        - Governments passing laws to punish persistent spammers with heavy fines.
- **Regular backups and security**
    - Just making something illegal or setting up regulations does not stop it happening.
    - Responsible computer users need to take reasonable steps to keep their data safe.
    - This includes regular *backups* and sufficient security with passwords.

WHAT IS ETHICAL HACKING ?

- Independent computer security Professionals breaking into the computer with permission
- System neither damage the target systems nor Steal the information.
- Evaluate target system security and Report back to owner about the Vulnerabilities found .

ETHICAL HACKERS

- Ethical hackers are not criminal hackers
- Completely trustworthy
- Strong programming and computer and Networking skills
- Learn about the system and trying to find its weaknesses
- Techniques of criminal- hackers –Detection – prevention

DIFFERENCE

- **Hacker**
  - Access computer system or network without authorization and breaks the law
- **Ethical hacker**
  - Perform most of the same activities but with the owner’s permission and employed by companies to perform penetration tests .

TYPES OF HACKERS

- **White hat Hackers**
  - White hat hackers, also known as ethical hackers are the cybersecurity experts who help the Govt and organizations by performing penetration testing and identifying loopholes in their cybersecurity. They even do other methodologies and ensure protection from black hat hackers and other malicious cyber crimes.
  - These are the right people who are on your side. They will hack into your system with the good intention of finding vulnerabilities and help you remove virus and malware from your system.

CONT.

- **Black Hat Hackers**
  - **THE BAD GUYS-**their agenda may be monetary most of the time, it's not always just that. These hackers look for vulnerabilities in individual PCs, organizations and bank systems. Using any loopholes they may find, they can hack into your network and get access to your personal, business and financial information.

CONT.

- **Grey Hat Hackers**
  - Gray hat hackers fall somewhere in between white hat and black hat hackers. While they may not use their skills for personal gain, they can, however, have both good and bad intentions. For instance, a hacker who hacks into an organization and finds some vulnerability may leak it over the Internet or inform the organization about it.
  - It all depends upon the hacker. Nevertheless, as soon as hackers use their hacking skills for personal gain they become black hat hackers. There is a fine line between these two. So, let me make it simple for you.
  - Because a gray hat hacker doesn't use his skills for personal gain, he is not a black hat hacker. Also, because he is not legally authorized to hack the organization's cybersecurity, he can't be considered a white hat either.

CONT.

- **Script Kiddies**
  - A derogatory term often used by amateur hackers who don't care much about the coding skills. These hackers usually download tools or use available hacking codes written by other developers and hackers. Their primary purpose is often to impress their friends or gain attention.
  - **Use tools created by black hats**
  - However, they don't care about learning. By using off-the-shelf codes and tools, these hackers may launch some attacks without bothering for the quality of the attack.

CONT.

- **Green Hat Hackers**
  - These hackers are the amateurs in the online world of hacking. Consider them script kiddies but with a difference. These newbies have a desire to become full-blown hackers and are very curious to learn. You may find them engrossed in the hacking communities bombarding their fellow hackers with questions
- **Blue Hat Hackers**
  - These are another form of novice hackers much like script kiddies whose main agenda is to take revenge on anyone who makes them angry. They have no desire for learning and may use simple cyber attacks like flooding your IP with overloaded packets which will result in attacks.

CONT.

- **Red Hat Hackers**
  - Red Hat Hackers have an agenda similar to white hat hackers which in simple words is halting the acts of Black hat hackers. However, there is a major difference in the way they operate. They are ruthless when it comes to dealing with black hat hackers.
  - Instead of reporting a malicious attack, they believe in taking down the black hat hacker completely. Red hat hacker will launch a series of aggressive cyber attacks and malware on the hacker that the hacker may as well have to replace the whole system
- **State/Nation Sponsored Hackers**
  - State or Nation sponsored hackers are those who have been employed by their state or nation's government to snoop in and penetrate through full security to gain confidential information from other governments to stay at the top online.
  - They have an endless budget and extremely advanced tools at their disposal to target individuals, companies or rival nations.

CONT.

- **Hacktivist**
  - if you've ever come across social activists propagandizing a social, political or religious agenda, then you might as well meet hacktivist, the online version of an activist. Hacktivist is a hacker or a group of anonymous hackers who think they can bring about social changes and often hack government and organizations to gain attention or share their displeasure over opposing their line of thought
- **Malicious Insider**
  - A malicious insider can be an employee with a grudge or a strategic employee compromised or hired by rivals to garner trade secrets of their opponents to stay on top of their game.
  - These hackers may take privilege from their easy access to information and their role within the company to hack the system.