UNIT 4

Nguyễn Công Cường – 20T1

Task 1+2:

1. who break into computer systems just for fun, to steal information, or to spread viruses (see note below)
2. When buying online, credit card information passes through multiple computers, potentially exposing it to hackers.

Email can be read by people who illegally enter computer systems as it travels across the internet.

Private networks can be attacked by intruders attempting to obtain sensitive information like Social Security numbers and bank accounts.

1. Malware (malicious software) are programs designed to infiltrate or damage your  
   computer, for example viruses, worms, Trojans and spyware. A virus can enter a PC via a disc drive - if you insert an infected disc - or via the Internet.
2. If you want to protect your PC, don’t open email attachments from strangers and  
   take care when downloading files from the Web. Remember to update your anti-virus  
   software as often as possible, since new viruses are being created all the time

Task 3:

1. Security is crucial when you send confidential information online. Consider, for  
   example, the process of buying a book on the Web, you have to type your credit  
   card number into an order form which passes from computer to computer on its way  
   to the online bookstore. If one of the intermediary computers is infiltrated by hackers,  
   your data can be copied
2. To avoid risks, you should set all security alerts to high on your web browser.  
   Mozilla Firefox displays a lock when the website is secure and allows you to disable  
   or delete cookies - small files placed on your hard drive by web servers so that they  
   can recognize your PC when you return to their site.\
3. If you use online banking services, make sure they use digital certificates - files  
   that are like digital identification cards and that identify users and web servers. Also  
   be sure to use a browser that is compliant with SSL (Secure Sockets Layer), a  
   protocol which provides secure transactions.
4. The only way to protect a message is to put it in a sort of virtual envelope – that  
   is, to encode it with some form of encryption. A system designed to send email  
   privately is Pretty Good Privacy, a free ware program written by Phil Zimmerman.
5. To protect crucial data, companies hire security consultants who analyse the risks  
   and provide solutions. The most common methods of protection are passwords for  
   access control, firewalls, and encryption and decryption systems. Encryption  
   changes data into a secret code so that only someone with a key can read it.  
   Decryption converts encrypted data back into its original form.
6. A virus can enter a PC via a disc drive - if you insert an infected disc - or via the Internet
7. A worm is a self-copying program that spreads through email attachments; it replicates itself and sends a copy to everyone in an address book.

Task 4:

1-b, 2-a, 3-c, 4-d

Task 5:

1. password
2. firewall
3. hacker
4. Viruses
5. freeware
6. encryption
7. decryption
8. spyware

Task 6:

1. The hacking into the North American Defense Command in Colorado Springs
2. 1981
3. In connection with virus spreading
4. Fifteen years old

Task 7:

1. was
2. showed
3. attempted
4. launched
5. spread
6. overwrote
7. infected
8. stole
9. were not affected

Task 8:

1. The most dangerous cybercrimes are likely phishing and spreading malicious software, as they can lead to significant financial losses and security breaches.
2. Paying for digital content is generally fair and legal. Copyright infringement should not be allowed online as it violates intellectual property rights.
3. Governments can combat cybercrime through legislation, international cooperation, public education, and funding for cybersecurity initiatives.
4. Government censorship of internet content is a complex issue involving balancing security concerns with freedom of expression rights.
5. Our privacy is at risk when marketing companies hold extensive personal data. Stricter regulations on data collection, storage, and usage are needed to protect individuals' privacy.

Task 9:

1. find out
2. hand over
3. tracked ... down
4. break into
5. log on
6. go about
7. throw away
8. grown up
9. Hacking into
10. keep ahead

Task 10:

1. throw away
2. break into
3. grown up
4. set about
5. hand over
6. shut down
7. ran up
8. find out
9. keep