**Text 1**

**Word List**

|  |  |
| --- | --- |
| access | доступ |
| acquire | получать; приобретать |
| attempt | пытаться; стараться; прилагать усилия |
| benign virus | неопасный вирус |
| bug | ошибка (в программе); сбой; дефект |
| consider | полагать, считать; рассматривать, обсуждать |
| decrease | уменьшаться; убывать |
| denial | отказ (в доступе) |
| exploit | средство (программа) атаки |
| gain | получать, приобретать |
| increasingly | все больше и больше; в большей степени; в большей мере |
| inherent | присущий; собственный; неотъемлемый |
| legitimate | легальный; законный |
| log in  log out | входить в систему  выходить из системы |
| malicious  ~ software (malware) | злонамеренный; злоумышленный  вредоносные программы |
| means | средство; способ; метод |
| patch | заплата; вставка в программу (с целью исправления или изменения) |
| possess | иметь; обладать |
| replicate | повторять; воспроизводить |
| seek | искать; разыскивать |
| source | источник |
| tamper | вмешиваться; портить; наносить ущерб |
| variety | многообразие, разнообразие; ряд, множество |
| vulnerability | уязвимость; слабое место |

***I. Define the following words as parts of speech.***

Security, perspective, devote, variety, acquire, competitive, malicious, indirectly, exploitation, increasingly, restrict, decrease, source, partially, request.

***II. Compare the following words with the Russian ones. They may have different meanings.***

Information, electronic, individual, company, perspective, resources, attack, physical, social, secret, person, document, engineering, disk, situation, copy, original, alternatively, systematically, actually, collect, practice, operate, identification.

***III. Fill in the gaps with one of the following words:***

passwords, decrease, social, unauthorized, malicious, protecting

1. Physical attacks to acquire sensitive information are sometimes considered a type of … engineering.

2. … confidential information is a business requirement and in many cases an ethical and legal requirement.

3. Computer … provide computer access that may be used to disable a company or a person electronically.

4. People who wish to obtain secret information are called crackers, corporate spies or other … individuals.

5. There are practices to … the possibility of someone physically tampering with computer equipment.

6. Information security means protecting information and information systems from … access, use, disruption, modification or destruction.

***IV. Read paragraph 1 of the text and find out the words to prove the title of the text.***

***V. Read the text and name the problems considered in it.***

***VI. Look through the text and find:***

a) techniques used to obtain information through physical attacks;

b) reasons for protecting information by individuals and companies;

c) common physical information security practices.

**Physical Information Security**

1. Physical information security is concerned with physically protecting data and means to access that data (apart from protecting it electronically). Many individuals and companies place importance in protecting their information from a software and/or network perspective, but fewer devote resources to protecting data physically. However, physical attacks to acquire sensitive information do frequently occur. Sometimes these attacks are considered a type of social engineering.

2. Many individuals and companies consider it important to protect their information for a variety of reasons, including financial, competitive, and privacy-related purposes. People who wish to obtain this information may be computer crackers, corporate spies, or other malicious individuals. This information may be directly beneficial to them, such as industrial secrets or credit card numbers. It may also be indirectly beneficial to them. For example, computer passwords do not have inherent value. However, they provide computer system access that may be used to get other information or to disable a person/company electronically. Sometimes these malicious individuals use electronic means or social engineering to gain information. However, sometimes they use direct physical attacks.

3. There are several ways to obtain information through physical attacks or exploitations. A few examples are described below.

Dumpster divingis the practice of searching through the trash of an individual or business in attempt to obtain something useful. In the realm of information security, this frequently means looking for documents containing sensitive information. However, as more and more information is being stored electronically, it is becoming increasingly useful to those seeking information through this means to search for computer disks or other computer hardware which may contain data. Sometimes this data can be restored to provide a wealth of information.

4. Overt document stealing Sometimes attackers will simply go into a building and take the information they need. Frequently when using this strategy, an attacker will masquerade as someone who belongs in the situation. The thief may pose as a copy room employee remove a document from someone's desk, copy the document, replace the original, and leave with the copied document. Alternatively, the individual may pose as a janitor, systematically collecting information and "throwing it away." The individual may then be able to walk right out of the building with a trash bag containing documents that were left out in the open or a sticky note which had been left in a partially open desk drawer on which a user had written his/her passwords.

5. There are many practices commonly used to decrease the possibility of success for these kind of attacks. Document shredding has become common, and the practice is still growing. Also electronic storage media are often prepared for disposal by purging, which erases files which may have been "deleted" by an operating system but never overwritten with other data.

6. Many choose to restrict access to areas where information is kept to those possessing a proper identification badge and/or other form of authorization. This attempts both to decrease the ease with which someone could access documents and to decrease the possibility of someone physically tampering with computer equipment. Along the same lines, many companies train their employees to physically protect documents and other sources of sensitive information on an individual level by locking the information in a file cabinet or by some other means. Also, companies request that employees memorize their passwords rather than writing them down as the paper with the password could be seen or stolen.

***VII. Mark the following statements as True or False in relation to the text. If a statement is false, change it to make it true.***

a) Many individuals and companies devote resources to protecting data physically.

b) The data obtained by the attackers may be directly or indirectly beneficial to them.

c) Computer disks found in the trash may contain sensitive information that cannot be restored.

d) There exist many practices to decrease the possibility of stealing data.

e) In many companies employees are requested to learn their passwords by heart.

***VIII. Match the terms in A with the statements in B.***

|  |  |
| --- | --- |
| A | B |
| a) social engineering | 1. The removal of sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique. |
| b) overt document stealing | 2. The practice of searching through the trash in attempt to get documents containing important data. |
| c) dumpster diving | 3. A collection of techniques used to manipulate people into performing actions or divulging confidential information. |
| d) purging | 4. Cutting paper into very fine strips for destroying private, confidential or sensitive documents. |
| e) document shredding | 5. Practice for looking for useful information by pretending to be someone who belongs in the situation. |

***IX. Find out the equivalents to the following words and word combinations in paragraphs 2 and 3.***

Поиск, секретная информация, взломщики, мусор, восстанавливать, злонамеренный, обеспечивать доступ, средство, разгребание мусора, получать, цель, присущий, однако, область.

***X. Find words and phrases in the text which mean:***

confidential, take place, goals, profitable, in an effort, supply, pretend, diminish, limit, ask.

***XI. Choose the correct answer to the following questions.***

1. What is physical information security concerned with?

a) protecting data from a software/network perspective;

b) physically protecting information and means to access it;

c) designing techniques for breaking into computer systems.

2. Which information may be directly beneficial to crackers?

a) computer passwords;

b) industrial secrets, finances, new products;

c) phone numbers of company’s employees.

3. Which of the physical information security practices are not mentioned in the list?

a) document shredding;

b) locking documents in a file cabinet;

c) memorizing passwords.

***XII. Characterize the techniques used by attackers for obtaining sensitive information.***

***XIII. Speak about the necessity of physically protecting information and security practices suggested using the information from the text.***