ECS
Serving Your IT Needs

Cyber Security Fundamentals

Before developing and implementing security measures to prevent cyberattacks, you must understand basic concepts associated with cyber security and what cyberattacks are. The method(s) of cyber security that a company uses should be tailored to fit the needs of the organization.

What is Cyberspace?

Cyberspace is the environment where computer transactions take place. This specifically refers to computer-to-computer activity. Although there is no "physical" space that makes up cyberspace, with the stroke of a few keys on a keyboard, one can connect with others around the world.

Examples of items included in cyberspace are:

- Networks
- Devices
- Software
- Processes
- Information storage
- Applications

What is Cyber Security?

As previously mentioned, cyber security is the implementation of methods to prevent attacks on a company's information systems. This is done to avoid disruption of the company's productivity. Not only does cyber security include controlling physical access to the system's hardware, it protects from danger that may come via network access or the injection of code.

Copyrighted: 2009-2022. All Rights Reserved. No Reproduction or reprinting allowed for distribution.

ECS
Serving Your IT Needs

Why is Cyber Security Important?

Cyber security is crucial to a business for a myriad of reasons. The two this section will focus on are data security breaches and sabotage. Each can have dire effects on a company and/or its clients.

Data security breaches can compromise secure information such as:

- Names and social security numbers
- Credit card and bank details
- Trade secrets
- Intellectual property

Computer sabotage serves to disable a company's computers or network to impede the company's ability to conduct business.

What is a Hacker?

In simple terms, a hacker is an individual, or group of individuals, who use their knowledge of technology to break into computer systems and networks, using a variety of tools to gain access to, and utilize other people's data for devious reasons.

There are 3 main types of hackers. They are:

- Grey hats: These hackers do so "for the fun of it".
- Black hats: These hackers have malevolent reasons for doing so, such as stealing and/or selling data for monetary gain.
- White hats: These hackers are employed by companies to hack into systems to find where the company is vulnerable, with the intention of ensuring the safety of the data from hackers with ill intentions.

Copyrighted: 2009-2022. All Rights Reserved. No Reproduction or reprinting allowed for distribution.

Practical Illustration

Patrick and Willow are in the process of opening a small answering service business. They are discussing the various needs of the company, including the type of security they are going to use for their computer systems. Patrick tells Willow that he doesn't believe it's necessary to implement any type of computer security because their business is small. Willow states even though their business will start out small, they are still vulnerable and there are many hackers out there that can break into their system and disrupt business.

Review Questions (Please watch Video or listen to audio file for right answers)

1. Cyberspace refers to which of the following?
    a. Computer-to-computer activity
    b. Individual-to-individual activity
    c. Supervisor-to-employee activity
    d. Computer-to-physical location activity

2. What is an item that is included in cyberspace?
    a. Network
    b. Software
    c. Application
    d. All of the above

3. Why is cyber security implemented?
    a. To speed up the network of a company's computers
    b. To avoid the disruption of a company's business
    c. To increase the number of clients a company has
    d. To lessen the number of employees a company employs

Copyrighted: 2009-2022. All Rights Reserved. No Reproduction or reprinting allowed for distribution.

4. Cyber security helps control physical access to and prevents danger that may come in from:
    a. Hardware
    b. Network access
    c. Code injection
    d. All of the above

5. What type of information is NOT secure information that is likely to be compromised in a data security breach?
    a. Intellectual property
    b. Credit card information
    c. The name of a company's CEO
    d. Social security numbers

6. What is the main purpose of computer sabotage?
    a. To disable a company's computers or networks to prevent it from conducting business.
    b. To disable a company's computers or networks to prevent it from being able to obtain a business license.
    c. To disable a company's computers or networks to prevent it from being able to hire employees.
    d. To disable a company's computers or networks to prevent it from being able to give its employees raises.

7. Why do "grey hat" hackers typically hack into computers?
    a. To steal data for monetary gain
    b. For the fun of it
    c. To find vulnerabilities in a computer system so the company can fix them before hackers with bad intentions can exploit them
    d. To sell data for monetary gain

Copyrighted: 2009-2022. All Rights Reserved. No Reproduction or reprinting allowed for distribution.

8. Why do “white hat” hackers typically hack into computers?
    a. To steal data for monetary gain
    b. For the fun of it
    c. To find vulnerabilities in a computer system so the company can fix them before hackers with bad intentions can exploit them
    d. To sell data for monetary gain

9. The method(s) of cyber security that a company uses should be tailored to fit the needs of the _____.
    a. Hacker
    b. Employees
    c. Organization
    d. Manager

10. _____ is the environment where computer transactions take place.
    a. An office
    b. Cyberspace
    c. A mall
    d. None of the above

Copyrighted: 2009-2022. All Rights Reserved. No Reproduction or reprinting allowed for distribution.