7.1 Introduction

Technicians need to understand computer and network security. Failure to implement proper security procedures can have an impact on users, computers, and the general public. Private information, company secrets, financial data, computer equipment, and items of national security are placed at risk if proper security procedures are not followed.

7.2 Explain why security is important

Computer and network security help to keep data and equipment functioning and provide access only to appropriate people. Everyone in an organization should give high priority to security because everyone can be affected by a lapse in security.

Theft, loss, network intrusion, and physical damage are some of the ways a network or computer can be harmed. Damage or loss of equipment can mean a loss of productivity. Repairing and replacing equipment can cost the company time and money. Unauthorized use of a network can expose confidential information and reduce network resources.

An attack that intentionally degrades the performance of a computer or network can also harm the production of an organization. Poorly implemented security measures to wireless network devices demonstrate that physical connectivity is not necessary for unauthorized access by intruders.

7.3 Describe security threats

To successfully protect computers and the network, a technician must understand both types of threats to computer security:

Physical – Events or attacks that steal, damage, or destroy equipment, such as servers, switches, and wiring

Data – Events or attacks that remove, corrupt, deny access, allow access, or steal information

Threats to security can come from the inside or outside of an organization, and the level of potential damage can vary greatly:

Internal – Employees have access to data, equipment, and the network

Malicious threats are when an employee intends to cause damage.

Accidental threats are when the user damages data or equipment unintentionally.

External – Users outside of an organization that do not have authorized access to the network or resources

Physical loss or damage to equipment can be expensive, and data loss can be detrimental to your business and reputation. Threats against data are constantly changing as attackers find new ways to gain entry and commit their crimes.

7.3.1 Define viruses, worms, and Trojans

Computer viruses are deliberately created and sent out by attackers. A virus is attached to small pieces of computer code, software, or documents. The virus executes when the software is run on a computer. If the virus is spread to other computers, those computers could continue to spread the virus.

A virus is a program written with malicious intent and sent out by attackers. The virus is transferred to another computer through e-mail, file transfers, and instant messaging. The virus hides by attaching itself to a file on the computer. When the file is accessed, the virus executes and infects the computer. A virus has the potential to corrupt or even delete files on your computer, use your e-mail to spread itself to other computers, or even erase your entire hard drive.

A worm is a self-replicating program that is harmful to networks. A worm uses the network to duplicate its code to the hosts on a network, often without any user intervention. It is different from a virus because a worm does not need to attach to a program to infect a host. Even if the worm does not damage data or applications on the hosts it infects, it is harmful to networks because it consumes bandwidth.

A Trojan is technically a worm. The Trojan does not need to be attached to other software. Instead, a Trojan threat is hidden in software that appears to do one thing, and yet behind the scenes it does another. Trojans are often disguised as useful software. The Trojan program can reproduce like a virus and spread to other computers.

Virus protection software, known as anti-virus software, is software designed specifically to detect, disable, and remove viruses, worms, and Trojans before they infect a computer. Anti-virus software becomes outdated quickly, however, and it is the responsibility of the technician to apply the most recent updates, patches, and virus definitions as part of a regular maintenance schedule. Many organizations establish a written security policy stating that employees are not permitted to install any software that is not provided by the company. Organizations also make employees aware of the dangers of opening e-mail attachments that may contain a virus or a worm.

7.3.2 Explain web security

Web security is important because so many people visit the World Wide Web every day. Some of the features that make the web useful and entertaining can also make it harmful to a computer.

7.3.3 Define adware, spyware, and grayware

Adware, spyware, and grayware are usually installed on a computer without the knowledge of the user. These programs collect information stored on the computer, change the computer configuration, or open extra windows on the computer without the user's consent.

7.3.4 Explain Denial of Service

DoS is a form of attack that prevents users from accessing normal services, such as e-mail and a web server, because the system is busy responding to abnormally large amounts of requests. DoS works by sending enough requests for a system resource that the requested service is overloaded and ceases to operate.

Common DoS attacks include the following:

Ping of death – A series of repeated, larger than normal pings that crash the receiving computer

E-mail bomb – A large quantity of bulk e-mail that overwhelms the e-mail server preventing users from accessing it

7.3.5 Describe spam and popup windows

Spam, also known as junk mail, is unsolicited e-mail. In most cases, spam is used as a method of advertising. However, spam can be used to send harmful links or deceptive content.

When used as an attack method, spam can include links to an infected website or an attachment that could infect a computer. These links or attachments can result in lots of windows designed to capture your attention and lead you to advertising sites. These windows are called popups. Uncontrolled popup windows can quickly cover the user's screen and prevent any work from getting done.

Many anti-virus and e-mail software programs automatically detect and remove spam from an e-mail inbox.

7.3.6 Explain social engineering

A social engineer is a person who is able to gain access to equipment or a network by tricking people into providing the necessary access information. Often, the social engineer gains the confidence of an employee and convinces the employee to divulge username and password information.

A social engineer might pose as a technician to try to gain entry into a facility. When inside, the social engineer might look over shoulders to gather information, seek out papers on desks with passwords and phone extensions, or obtain a company directory with e-mail addresses.

Here are some basic precautions to help protect against social engineering:

Never give out your password.

Always ask for the ID of unknown persons.

Restrict access of unexpected visitors.

Escort all visitors.

Never post your password in your work area.

Lock your computer when you leave your desk.

Do not let anyone follow you through a door that requires an access card.

7.3.7 Explain TCP/IP attacks

TCP/IP is the protocol suite that is used to control all of the communications on the Internet. Unfortunately, TCP/IP can also make a network vulnerable to attackers.

Some of the most common attacks:

SYN flood – Randomly opens TCP ports, tying up the network equipment or computer with a large amount of false requests, causing sessions to be denied to others

DoS – Sends abnormally large amounts of requests to a system preventing access to the services

Spoofing – Gains access to resources on devices by pretending to be a trusted computer

Man-in-the-middle – Intercepts or inserts false information in traffic between two hosts

DNS poisoning – Changes the DNS records on a system to point to false servers where the data is recorded

7.4 Identify security procedures

A security plan should be used to determine what will be done in a critical situation. Security plan policies should be constantly updated to reflect the latest threats to a

network. A security plan with clear security procedures is the basis for a technician to follow. Security plans should be reviewed on a yearly basis.

Part of the process of ensuring security is to conduct tests to determine areas where security is weak. Testing should be done on a regular basis. New threats are released daily. Regular testing provides details of any possible weaknesses in the current security plan that should be addressed.

There are multiple layers of security in a network, including physical, wireless, and data. Each layer is subject to security attacks. The technician needs to understand how to implement security procedures to protect equipment and data.

7.4.1 Explain what is required in a basic local security policy

A security policy should describe how a company addresses security issues. Though local security policies may vary between organizations, there are questions all organizations should ask:

What assets require protection?

What are the possible threats?

What to do in the event of a security breach?

7.4.2 Explain the tasks required to protect physical equipment

Physical security is as important as data security. When a computer is taken, the data is also stolen.

There are several methods of physically protecting computer equipment:

Control access to facilities.

Use cable locks with equipment.

Keep telecommunication rooms locked.

Fit equipment with security screws.

Use security cages around equipment.

Install physical alarms triggered by motion-detection sensors.

Use webcams with motion-detection and surveillance software.

For access to facilities, there are several means of protection:

Card keys that store user data, including level of access

Biometric sensors that identify physical characteristics of the user, such as fingerprints or retinas

Posted security guard

Sensors, such as RFID tags, to monitor equipment

7.4.3 Describe ways to protect data

The value of physical equipment is often far less than the value of the data it contains. The loss of sensitive data to a company's competitors or to criminals can be costly. Such losses can result in a lack of confidence in the company and the dismissal of computer technicians in charge of computer security. To protect data, several methods of security protection can be implemented.

Password Protection

Password protection can prevent unauthorized access to content. Attackers can gain access to unprotected computer data. All computers should be password protected. Two levels of password protection are recommended:

BIOS – Prevents the operating system from booting, and prevents BIOS settings from being changed without the appropriate password

Login – Prevents unauthorized access to the local computer and the network

Data Encryption

Encrypting data uses codes and ciphers. Traffic between resources and computers on the network can be protected from attackers monitoring or recording transactions by implementing encryption. It might not be possible to decipher captured data in time to make any use of it.

Software Firewall

Data being transported on a network is called traffic. A software firewall is a program that runs on a computer to allow or deny traffic between the computer and the network to which it is connected. Every communication using TCP/IP is associated with a port number. HTTPS, for instance, uses port 443 by default. A software firewall is capable of protecting a computer from intrusion through the ports. The user can control the type of data sent to a computer by selecting which ports will be open and which will be secured. You must create exceptions to allow certain traffic or applications to connect to the

computer. Firewalls can block incoming and outgoing network connections unless exceptions are defined to open and close the ports required by a program.

Data Backups

Data backup procedures should be included in a security plan. Data can be lost or damaged in circumstances such as theft, equipment failure, or a disaster such as a fire or flood. Backing up data is one of the most effective ways of protecting against data loss.

Smart Card Security

A smart card is a small plastic card, about the size of a credit card, with a small chip embedded in it. The chip is an intelligent data carrier, capable of processing, storing, and safeguarding thousands of bytes of data. Smart cards store private information such as bank account numbers, personal identification, medical records, and digital signatures. Smart cards provide authentication and encryption to keep data safe.

7.4.4 Describe wireless security techniques

Because traffic flows through radio waves in wireless networks, it is easy for attackers to monitor and attack data without having to physically connect to a network. Attackers gain access to a network by being within range of an unprotected wireless network. A technician needs to know how to configure access points and wireless NICs to an appropriate level of security.

When installing wireless services, you should apply wireless security techniques immediately to prevent unwanted access to the network. Wireless access points should be configured with basic security settings that are compatible with the existing network security. The following items are basic security settings that can be configured on a wireless router or access point:

Service Set Identifier (SSID) – The name of the wireless network. A wireless router or access point broadcasts the SSID by default so that wireless devices can detect the wireless network. Manually enter the SSID on wireless devices to connect to the wireless network when the SSID broadcast has been disabled on the wireless router or access point.

MAC Address Filtering – A technique used to deploy device-level security on a wireless LAN. Because every wireless device has a unique MAC address, wireless routers and access points can prevent wireless devices from connecting to the wireless network if the devices do not have authorized MAC addresses. Enable MAC address filtering, and list each wireless device MAC address to enforce MAC address filtering.