 What is the main difference between a virus and a Trojan?

Step 1:

A computer virus is a form of malware, or malicious software, that travels between computers and corrupts software and data. Computer viruses are designed to interfere with systems, lead to serious functional problems, and cause data loss and leakage.

A Trojan Horse Virus is a form of malware that installs itself on a computer by impersonating a trustworthy application. The delivery technique often involves an attacker hiding malicious malware in genuine software using social engineering in an effort to get users' system access

Step 2: Explanation

The key distinction between a virus and a Trojan is that the former dissimulates as helpful software and, once installed, opens a backdoor that gives malicious actors access to a system, whilst the latter attaches itself to a system right away or file and infects systems as it travels from one to the other.

2. A virus or malware can impact which of the three tenets of information systems security (confidentiality, integrity, or availability)? In what way?

Step 1:

Malware is created with the intention of harming standalone or networked computers. Therefore, whenever the phrase "malware" is used, it refers to a programme intended to harm your computer, such as a virus, worm, or Trojan horse. Virus. A virus is a computer programme designed to infiltrate your system and corrupt or change your files and data.

Step 2:

All three principles of information system security can be affected by a virus or malware: confidentiality by allowing unauthorised remote access; integrity by altering and stealing data; and availability by slowing down the system and deleting files.

3. Why is it recommended to do an antivirus signature file update before performing an antivirus scan on your computer?

Step 1:

A security programme downloads a file or set of files called a virus signature (sometimes called a virus definition) to identify a computer infection. The files allow antivirus (and other antimalware) software in customary file scanning and breach detection systems to detect malware.

Step 2:

Before running an antivirus scan on your computer, updating your antivirus signature file is advised since it enables the antivirus to search for new malware.

A virus can be found in a computer file system using antivirus software, which then allows for its detection, quarantining, and removal.

4. Why might your coworker suggest encrypting an archive file before e-mailing it?

Step 1:

Your data is protected via file encryption, which encrypts it. It cannot be unencrypted without the proper encryption key, which is typically a password. It is not possible to encrypt files on Windows 10 Home. To access the Properties menu, right-click (or click while holding) a file or folder. Strong encryption based on a passphrase is used to protect the archive.

Step 2:

The archive can be opened and decrypted by anyone who knows the passphrase. This approach combines elements of the Passphrase and Recipient List approaches. Strong encryption is used to encrypt the archive, together with a recipient list and a passcode.

Someone at work might propose encrypting an archive file before emailing it because it makes sure that no one, even if they have access, can view the information.

5. What kind of network traffic can you filter with the Windows Firewall with Advanced Security?

Step 1:

Microsoft Windows includes a firewall feature known as Windows Firewall (officially known as Windows Defender Firewall in Windows 10). Initially, Windows XP and Windows Server 2003 both included it.

Step 2:

A layered security strategy includes Windows Defender Firewall with Advanced Security, which is crucial. Windows Defender Firewall prevents illegal network traffic from entering or leaving a local device by offering host-based, two-way network traffic filtering for that device.

Inbound and outgoing traffic can be filtered by Windows Firewall with Advanced Security, permitting or preventing particular connections to the machine.

6. What are typical indicators that your computer system is compromised?

Step 1:

Any computing resource whose confidentiality, integrity, or availability has been negatively impacted, either purposefully or unintentionally, by an untrusted source is referred to as a compromised computer. Automation or manual engagement by an unreliable source are both potential ways that a compromise can happen.

Step 2:

Strange network bandwidth utilisation, unusual background services and programmes, missing or inaccessible files, and general poor performance are signs that your computer system has been exploited.

7. What elements are needed in a workstation domain policy regarding use of antivirus and malicious software prevention tools?

Step 1:

Workstation domain regulations apply to every computer a user uses. A user's desktop or laptop computer counts as a device. Any user device that accesses data, such a smartphone, can be a workstation. It's possible that these gadgets are not working in a secure office or data centre.

Step 2:

Regarding the use of antivirus and harmful software prevention tools, a workstation domain policy must address tool selection and configuration, regularity of email and file filtering/quarantining, and regularity of upgrading anti-virus databases.

A good firewall on the server should be able to prevent unauthorised access while still allowing those who are permitted access. To prevent corruption and simple access for data thieves, there should be protection on the system's weak points.