Downloaded from: justpaste.it/bas1b

How to defend against Viruses?

We use our internet-connected devices to achieve all our daily activities right from home, such as online shopping, banking, playing games, and communicating with family and friends through social networking. But some questions might scare us, like: Are our online activities secure? Is our device infected with viruses?

By implementing the best practices and security measures, we can protect our devices from various security threats and viruses. This informative blog is about how to defend against viruses.

Use strong passwords

Using strong passwords with at least eight characters, a combination of alphabets, numbers, and special symbols could protect your devices from hackers' guesses. Choose unique passwords for each online account, such as financial institutions, social media, or email. We should update the password periodically to prevent brute-force password cracks.

Install anti-virus software

Anti-virus software actively scans for viruses that could invade your system files, email, or operating system. Choosing the best anti-virus software package is the best way to secure the organization’s data from viruses and other such threats.

Use your firewall

A firewall is an essential tool that blocks unauthorized access to the system. When setting up the firewall in the system, provide built-in firewall abilities of the operating system. You can update firewall settings based on your preferences.

Install anti-spyware and anti-malware software

Malware and spyware can damage your device and network as a virus. Installing anti-malware and anti-spyware software would help to defend against viruses. This software runs in the device and scans for viruses to protect the devices from affecting.

Regular scan

Viruses, spyware, and malware continuously evolve to infect a system and distract the system's protection methods. Implement regular scans through your anti-virus, anti-spyware, and anti-malware software to identify, isolate, and remove any suspicious elements in the network before any damage can occur.

Regular Backup Schedule

Various malicious elements can destroy the data in the system. Backing up the system would help to ensure the data is retrievable even if there is some destruction in the system. Cloud service offers backing up the data online and allows you to connect a personal external hard drive to the system and copy the updated data manually.

Regularly update your computer system

It is essential to run regular system updates to fix any bugs and anomalies. If you don't update the system, the bugs and anomalies will remain in the system and can allow hackers to exploit it.

About InfosecTrain

InfosecTrain is a global-leading provider of Information security and Cybersecurity training. It offers an instructor-led certification training program on **Network Security** certification, which helps you to achieve a complete understanding of networking methods, tools, and techniques used to identify network security threats in the organization. Check out and enroll now.