What precautions/Steps can be taken to secure a PC?

There are many ways to secure a computer/system from hackers. Some are as -

- ***Use a Firewall ->*** Firewalls prevent unauthorized access to your business network and alert us of any intrusion attempts. The first thing to do with a new computer (or the computer we now use) is to make sure the firewall is enabled before you go online. However, you can also purchase a hardware firewall from companies like Cisco, Sophos or Fortinet, depending on our broadband router, which also has a built-in firewall that protects your network. If we have a larger business, we can purchase an additional business networking firewall.

- ***Install Antivirus Software ->*** Antivirus software plays a major role in protecting our system by detecting real-time threats to ensure our data is safe. Some advanced antivirus programs provide automatic updates, further protecting our machine from the new viruses that generate every day. Antivirus programs such as Bitdefender, Panda Cloud Antivirus, Malwarebytes and Avast immunize our computer against unauthorized code or software that threatens our operating system.

- ***Install an Anti-Spyware Package ->*** Spyware is a special kind of software that secretly monitors and collects personal or organizational information. It is designed to be hard to detect and difficult to remove, and tends to serve up unwanted ads or search results to direct us to certain websites. Anti-spyware packages provide real-time protection by scanning all incoming information and blocking threats.

- ***Use Complex Passwords ->*** Using secure passwords is the most important way to prevent illegal intrusions onto our computer network. The more secure our passwords, the harder it is for a hacker to invade our system. More secure often means longer and more complex: Use a password that has at least eight characters and a combination of numbers, upper- and lowercase letters, and computer symbols. Hackers have an arsenal of tools to break short, easy passwords in minutes.

- ***Secure our Network ->*** If we've got a new router, chances are it comes with no set security. We should always log in to the router and set a password using a secure, encrypted setup. This prevents intruders from infiltrating our network and messing with our settings.

- ***Use two-factor Authentication ->*** Passwords are the first line of defense against computer hackers, but a second layer boosts protection. Major online companies like Facebook, Google, Apple and Microsoft let us enable two-factor authentication, which requires us to type in a numerical code in addition to our password when logging in. This hardens our account to the outside world.

- ***Use Encryption ->*** Even if someone is able to steal our data or monitor our internet connection, encryption can prevent hackers from accessing any of that information. We can encrypt your Windows or macOS hard drive with BitLocker or FileVault, encrypt any USB flash drive that contains sensitive information, and use a VPN to encrypt our web traffic. Only shop at encrypted websites – we can spot them immediately by the "https" in the address bar accompanied by a closed padlock icon.