How to...
set up or adjust your computer's settings for accessibility and security

Setting up a computer can be overwhelming. Faced with technical jargon and a wide range of options how do you configure your settings to ensure your computer is secure, and runs as efficiently as possible?

Here are some basic guidelines for Windows' users setting up a new computer or adjusting settings to maximise performance.

Set up safe access to your computer

Protect your files and privacy by ensuring your computer is password-protected. To set up a password follow these steps:

- Go to 'Start' in the corner of the screen
- Select 'Control Panel'
- Click 'Add or remove user accounts' (under 'User Accounts and Family Safety')
- Click 'Continue' when asked for permission to make the change
- Select your account name in the list, and choose 'Create a password'
- Enter your choice of password, making sure it is a tricky combination of letters, numbers and symbols. It should be at least eight characters long
- Type a password hint into the text bar
- Click 'Create password'
- Reboot your computer and log into your account with your new password

Understanding and adjusting your computer settings

- **General Settings**

In the 'Settings' tab on the navigation panel, select 'General' and you will be presented with a list of settings to configure. Here's how to make sense of them:

- **Run Scan on Windows start-up**: This gives you various scanning options when Windows starts up (Intelli-Scan, Full Scan or Custom Scan).
- **Notify me about available updates**: Select this if you would like to be alerted to available security updates to download.
- **Download and install updates (silently)**: Select this option if you would like your machine's Internet Security to check for and download updates without notifying you.

- **Program Language**: This setting lets you choose the language your system communicates to you in.

- **IntelliGuard to detect potentially unwanted products**: By default this setting is disabled. Select if you would like IntelliGuard to detect potentially unwanted products that could contain malware but don't necessarily pose a risk to your computer.

- **Scan to detect potentially unwanted products**: Enabled by default, this allows PC Tools Internet Security to search for potentially unwanted products in scans.

- **IntelliGuard tools to display popup alert windows**: Enabled by default so PC Tools Internet Security displays IntelliGuard pop-up notifications.

- **Enable quiet mode**: Enabled by default, this stops unnecessary alerts and notifications from being displayed.

- **Password protection**: Disabled by default, this setting allows you to set up a password to protect different areas of your computer system. To do this:
- Select the 'Password Protection' checkbox
- A window will pop up asking you to enter your password. Type one in and confirm it. Add an optional hint to remind you of your password in case you forget it
- Choose which area or areas you would like to protect from the list of options
- Click 'Apply'

How to configure Advanced Settings

Go to the 'Settings' tab in the navigation panel and click 'Advanced' and a list of 'Advanced Settings' will come up.

- **Enable Power Saving Mode Detection**: Disabled by default but can be selected if you would like your systems Internet Security to detect the remaining power in your laptop battery and to delay scheduled tasks when running your laptop on battery.

- **Enable Behaviour Guard Compatibility Mode**: Disabled by default, enabling this setting will ensure Behaviour Guard adapts with other security applications that monitor the browser to prevent conflicts.

- **Enable Background Scans on System Idle**: Disabled by default, enabling this will let background scans run when your system is idle.

- **Detect Master Boot Record threats**: This is enabled by default to detect threats to the Master Boot Record. The Master Boot Record provides information to load the operating system and boot the system.

- **Enable Game Mode**: Disabled by default as it would allow Internet Security to skip all scheduled scans, updates and backup tasks, and to disable all alerts and pop-ups. This option offers less protection.

How to configure Performance Settings

Select helpful Performance 'pre-sets' by adjusting the slider bar to get the optimum level of protection and performance.

- Go to the 'Settings' tab in the navigation panel
- Select 'Performance'
- Select one of the following options from the slider bar:
- **Performance**: Minimises the number of system resources your computer security uses to give you optimal protection while having the least impact on your activities.
- **Balanced**: Provides the best balance between high-level protection and low performance impact. Usually the default setting.
- **Protection**: Provides maximum protection to detect and prevent malware at every point. This setting uses more system resources than the two other options.

How to configure Scanning Settings

- Go to the 'Settings' tab in the navigation panel
- Select 'Scan Settings' and select **Enable Cloud Scanning** if you want to activate a feature that compares files on your computer against those in a cloud-based database. The feature helps your computer detect and destroy the latest threats.

- Select ‘Play sounds’ for PC Tools Internet Security to play a sound notifying you that an infection has been found at the end of a scan.

- **Scan Alternative Data Streams:** Enabled by default, this will ensure PC Tools Internet Security scans for alternative data streams. Hackers take advantage of Alternate Data Streams (ADS), hiding root kits or hackers’ tools in them without the system administrator’s knowledge.

- **Scan for hidden files**: This is enabled by default to scan and remove hidden files associated with complex threats. These threats may hide in the operating system where they would be extremely difficult to remove so this preventative method should be enabled.

- **Lower scan priority to reduce CPU usage**: This is enabled to run background scans.

- **Show disclaimer when repairing**: This is disabled by default to prevent a disclaimer from showing each time malware infections are removed or quarantined.

- **Quarantine infections before removal**: Enabled by default to send dubious files to quarantine before deleting them off your system.

- **Scan Archives**: This is enabled to scan archived files for embedded viruses and related malware.

- **File Exclusions**: If you want to exclude any file types from scans, select.

Finally, make sure you click ‘Apply’ to save your changes.