

NEWSLETTER



Is your computer slowing down? You are not imagining it!



Why Do Computers Slow Down Over Time?

Remember the awe you felt when you turned on your new computer and it loaded in a flash? Your computer was the envy of your friends and you weren't afraid to bathe in that glory. Button on, ready to go, those were the days!

After a year or two though, it doesn't seem to be quite as zippy...no, you're not imagining it. It really has slowed down, not just in comparison to newer models and your expectations...There's a measurable drop in speed and power that has nothing to do with worn out parts. The good news is a little maintenance can have that baby cruising at top speed again. Let's take a leisurely walk through the system and spot the culprits:

Start-up applications: It's super convenient to have Skype start automatically and your anti-virus too. In fact, many of the applications starting themselves with the computer are essential to your experience. But some of them are getting a little too 'helpful'.

For example, iTunes helper loads in the background to speed things up when you connect your device – but if you can't even remember the last time you ran iTunes on your computer, then it can go. Programs like that are holding onto a portion of your processing power and adding to your speed issues. The average home computer

automatically loads around 75 programs at start-up!

Temporary junk: Computers are kind of messy. They leave temporary files and snippets of information all over your hard drive, each action leaving a trail rather like a roaming toddler with a sticky sandwich. Every webpage, every image on that webpage, every program you run and every game you play leaves something behind.

It may be the tidbits of information called "cookies", saved game files, auto-restore files or even a log so that you can hit the undo button 100 times while it remembers your actions for you.

The more junk your computer builds up, the slower it gets.

Viruses and malware: These infections sit in the background consuming resources while doing various nightmarish things. They may be spying on your actions, stealing your information or reaching out through your network to infect others. Occasionally, the impact is limited to seeing your computer slow to a crawl, however the flow-on financial costs of an infection can easily reach into the thousands.

Bloating: With every new version of

software comes a new set of features, introductory sequences and design improvements. The problem with this is the application becomes larger and larger with each new version, requiring more system resources to install and run – and slowing your computer down.

Just like a car, computers need regular maintenance - we offer a Tune-Up service to bring your computer back to its original speed and extend its life.

Give us a call at 0113 2579992 to book in a Tune Up.

In this newsletter, we talk about why computers seem to slow down over time, and make you aware of a dangerous threat on the internet that could cost you money.



“Hackers targeted everyone and everything, including home PCs – and they were astoundingly successful.”

Will That Click Cost You Thousands?

Ransomware has undeniably been the biggest security threat of 2016. No-one was safe. Hackers targeted everyone and everything, including home PCs – and they were astoundingly successful – earning themselves upwards of \$846million from US reported incidents alone. Business is booming for hackers, with thousands of attacks each day bringing in an average of \$640 per target. Perhaps even more alarmingly, the financial cost of each individual attack is on the rise – the more ransomware proves to be an easy earner for them, the more they demand each time.

For a quick payday, some hackers offer to ‘rescue’ you from immediate danger – for a fee. One method is to trick you into thinking you have a virus that will spread if you don’t pay money to remove it immediately. Another much scarier method is to pretend to be the FBI and say your computer was involved in a crime (anything from money laundering to child pornography) and you can avoid going to prison by paying a few hundred dollars.

Thousands of regular people are also waking up every day to discover they’ve been locked out of their own files. Entire music and video libraries, digital photos from the past 5 years, personal budget files and even their secret novel draft ...all held hostage until the user pays a ransom. The encryption is so strong and unbreakable that paying the ransom often becomes the only solution.

The way ransomware gets onto your computer is deviously simple. Generally, the hackers convince you to click an email attachment/link or pop-



up. With both approaches, the hacker usually offers helpful information, for example:

- Tracking an unclaimed parcel
- Alerting that a virus was found and needs to be removed
- Advising details of a recent traffic fine

It’s so tempting to click through for more details and that’s what the hackers count on. Their messages and pop-ups aren’t obvious threats and so slip easily under our radar. Unfortunately, they’re not the most trustworthy bunch so paying may not actually unlock your files, and one payment can quickly become several.

To make matters worse, they can encrypt any backups connected to your computer too, like a USB drive. Having a backup is super important in any situation, but in cases like this, the right backup is needed. Not only one stored separate from your network, but one created recently with all the files you can’t bear to lose. Before restoring your backup, however, you’ll need to make sure the malware isn’t lurking in the background, ready to not just re-infect your restored files but also the backup drive itself.

To avoid finding yourself up to the waist in ransom demands or sending hackers money each month, we recommend being wary of email

attachments, even from friends and family. If you’re not sure what the file is, don’t click it. They may not have sent that email intentionally; their infected system may be auto-emailing everyone in the address book. You should also be careful with any popups that appear out of place, especially ones that try to make you panic. If it doesn’t sound right or look right, don’t click it. Ransomware is just too dangerous to risk.

Call us to set your computer up with protections against ransomware, and put backups in place that will keep your important files safe.



Unit 39g, Springfield
Bagley Lane
Farsley, Leeds LS28 5LY
0113 2579992
info@emeraldict.co.uk
www.emeraldict.co.uk