# Clock Ticking for Windows 7

The clock is counting down for 40% of the world's private and public organisations. Why? Because on the 14th January 2020 the incredibly popular Windows 7 computer operating system goes end-of-life. That does not mean your Windows 7 desktops and laptops will suddenly stop working. However, it does mean that Microsoft will stop providing upgrades, bug fixes, support and, most importantly, security patches. Certainly, Windows 7 has robust security features. Nevertheless, being one of the world's most popular operating systems makes Windows 7 a favourite target for hackers and malware.

## Cyber Attacks

One of the biggest malware attacks in history, WannaCry infected 230,000 computers across 150 countries in May 2017. Later, it emerged that WannaCry exploited a security vulnerability in Windows 7. The NHS had over 70,000 devices hit, from computers and MRI scanners to blood storage units. WannaCry and other forms of ransomware work by locking you out of your computer or encrypting your data and then demanding a ransom to release it.

## Non-Compliance

The longer you run Windows 7 the riskier things will become. Of course, it's not just Windows 7 but the older, more vulnerable software applications running on it that increase your overall threat levels. Organisations that continue to run Windows 7 after the 2020 deadline will find themselves out of compliance with many regulatory authorities. You might also find that running Windows 7 will invalidate some insurance policies.

## Trouble Ahead

In some cases, organisations rely on bespoke software specially written for Windows 7. These applications are often 'business critical' but have fallen behind in terms of upgrades. Replacing such applications can be technically difficult or prohibitively expensive. However, come January 2020 these applications will represent a compliance problem and major security risk.

# Clock Ticking for Windows 7

## Aging Hardware

If your computer came with Windows 7 preinstalled then it is due to be replaced. Computers that are over three years old start to show signs of aging like loss of performance. If your computer is slow to start-up, slow to shut down, and has difficulty running two or more applications at the same time then it needs replacing. You might also find that an older PC has trouble running the latest operating systems, such as Windows 10. Today's, computers are smaller, lighter, faster, more reliable and power-efficient thanks to solid-state hard drives (SSD), for example.

## A Simple Plan

Moving one or two users from Windows 7 to Windows 10 is a fairly simple, straightforward process. Nevertheless, users will take a little while to become familiar with a new operating system. Migrating a department or entire company to Windows 10 is a different story, and requires time to plan. Changing operating system is a good opportunity to replace aging devices, so you might want to conduct a device inventory as a first step in your migration plan. Similarly, you will want to look at what applications people are actually using, and dispense with the rest.

## Work Anywhere

For users, one of the great benefits of Windows 10 is the ability to work seamless between desktops, laptops and mobile devices. You might want to consider this ability to work anywhere, on any device, when buying new hardware. As well as the technical challenges of moving to a new operating system, you will need to consider staff training to ensure a smooth transition.

## Time to Act

Perhaps you think there is no urgency to upgrade, but the clock is ticking for Windows 7. What's more, you and your colleagues might have become used to the poor performance of your existing computers and software applications. Slow, buggy PCs that keep crashing are certainly costing you money, frustrating your staff and annoying your customers. Now is the time to act. Set your budget, make a plan, move to Windows 10 and replace aging hardware.