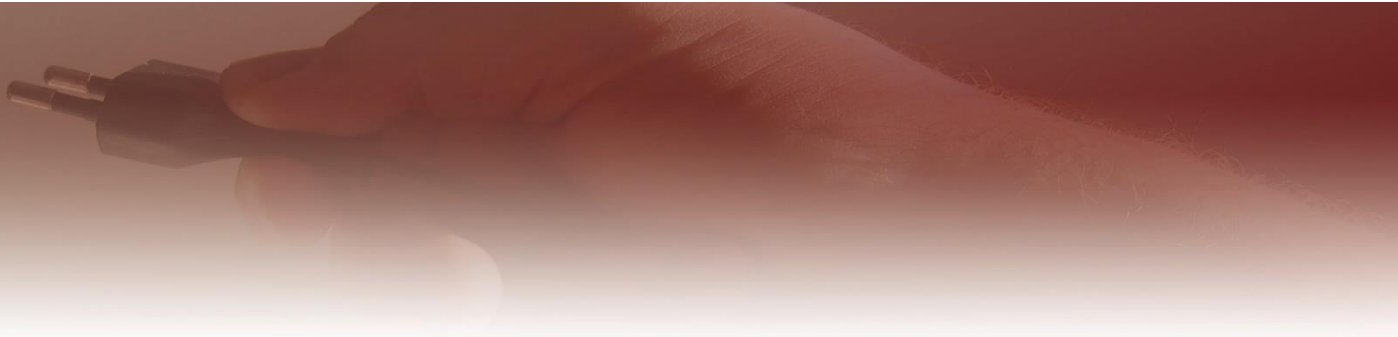Microsoft is ending support for Windows 7. If your business has ignored all the previous warnings, your time is up. Windows 7 will reach its end of life on January 14, 2020. This ebook explains what that means, why it matters, and what's next.

Business users get notifications all the time saying that such-and-such software or hardware needs an update. It can feel as if every time we turn on our computers, there's a warning of a necessary upgrade or security patch. Sometimes, we ignore the warnings. We figure we'll wait it out. How bad could it be? Well, pretty bad in the case of Windows 7, which is reaching its end of life January 14, 2020.

What Does End of Life Mean?

All good things must come to an end. In the case of software, it doesn't matter if it is a good one or not. It's still going to reach what's called "end of life." It's typically a ten-year cycle. The new software gets the manufacturer's full attention and support for five years. Then, the company starts recommending you move on to its newer software. After all, resources are limited, and they can't develop new offerings and also support old ones forever.

As Microsoft puts it, the company is discontinuing Windows 7 to focus its "investment on supporting newer technologies and great new experiences."

In Windows 7's case, Microsoft stopped fully supporting the 2009 operating system (OS) five years ago. Now, in January 2020, it's cutting off all extended support options, too. That means no more system updates or security patches. The company has stopped releasing any new features or design changes, and there's no longer any included manufacturer's support. Plus, you can't call in your warranty if something does go wrong.

You may love your Windows 7, but as the next section explains, it's not going to love you back any longer.

Why Does This Matter to Windows 7 Users?

Your operating system won't just stop working on January 15, 2020. However, there will no longer be any updates or patches for viruses or security problems.

If you remain loyal to outdated software, you are putting your business at much greater risk of cyberattack. Microsoft admits it. The head of Windows at Microsoft Germany told ZDNet that Windows 7 "does not meet the requirements of modern technology, nor the high security requirements of IT departments."

In fact, the system's security was the most widely affected in the widespread WannaCry ransomware attack. That 2017 attack infected more than 230,000 computers in 150 countries, with the perpetrators

demanding $300 ransom per computer. According to Kapersky Lab data, "roughly 98 percent of the computers affected by the ransomware were running some version of Windows 7, with less than one in a thousand running Windows XP."

Plus, it's widely known that Windows 7 is being retired. So, hackers know perfectly well that it's more vulnerable to attack. Remediating any attacks on your Windows 7 system will also be more costly. Microsoft will charge much higher fees when asked to help businesses that didn't migrate in time. It is offering extended Window 7 security updates through January 2023 for Windows 7 Pro and Windows 7 Enterprise users, but the plans aren't cheap.

Finally, there's no incentive for third-party developers to support Windows 7 applications. So, you could find that other business applications aren't secure either.

What Can You Do?

If it makes you feel any better, you're probably not alone in not having done anything yet. Windows 7 remained the most popular version of Windows worldwide until the end of the fourth quarter of 2018, according to Net Applications. That means more than a billion users were relying on nine-year-old Windows 7 globally.

Beyond user preference, there are many other reasons a business may not yet have updated its OS. Migrating to a new system isn't always easy, and it is time consuming. Depending on your IT infrastructure, it could take a lot of work. Existing software or hardware may not be equipped to run the Windows 10 solution.

With WannaCry, one reason Britain's National Health Service was hit so hard was that it couldn't upgrade some of its physical machines to the latest OS. For example, it couldn't run Windows XP on an embedded system such as a MRI machine. If this is the case for you, be safer by isolating those devices or computers from your infrastructure.

There are no more extensions. The deadline for Windows 7 users is here.

Conclusion

Despite sounding like doomsayers – "the end is nigh!" – there is no overstating the importance of acting to upgrade from Windows 7. This operating system is "extremely vulnerable," and that's in Microsoft's own words. Don't risk your business data. Do what you must now to shore up your cybersecurity with a supported system. Dragging your feet any longer could cost you revenue, IT effort, compliance and regulatory fines, customer loyalty, and brand reputation. It's time to move on.

The good news? Upgrading to the latest operating system can improve productivity. You'll likely notice increased operating speed and enjoy new features and functionality. This enhanced usability can drive productivity. Plus, you'll benefit again from regular security updates and manufacturer technical support.

We Can Help!

Your users probably know and love their Windows 7. Managing the change to a new platform is easier with the help of a Managed Service Provider. We can tackle your data migration and provide reliable service and support. Contact our IT experts today. Don't wait!

Twin Cities PC Repair

Phone: (651) 456-8655

Email: helpdesk@pcgoodguys.com

Web: www.twincitiespcrepair.com

Facebook: facebook.com/TwinCitiesPCRepair