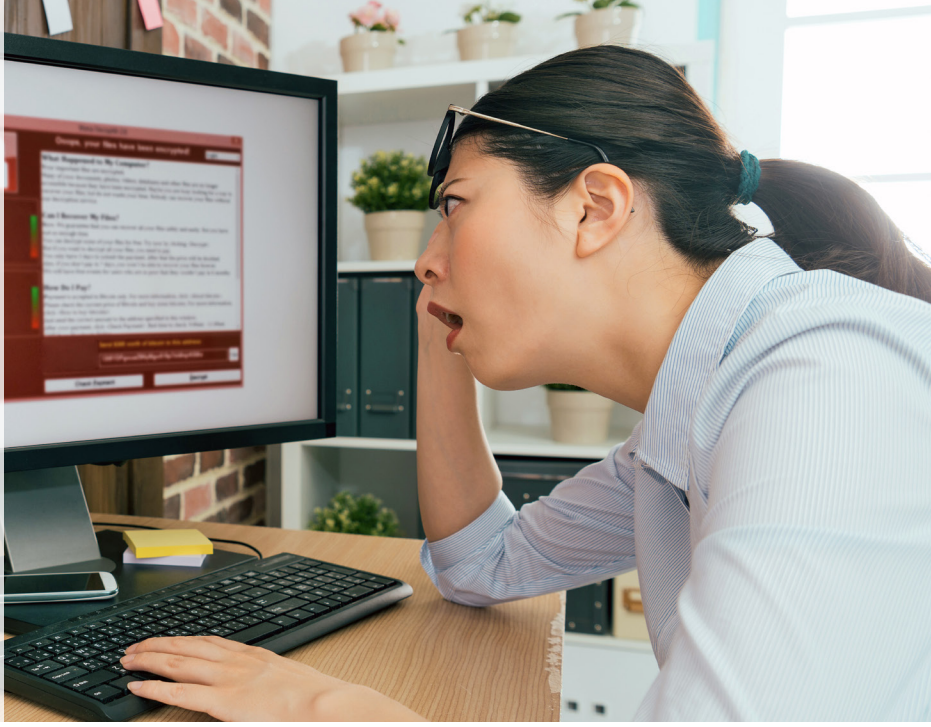
# Windows 7 End of Life:

## *Protect Yourself Against Security Threats*



*Windows 7 is going "end of life" on January 14, 2020, meaning Microsoft will no longer be regularly updating the system with fixes when a security vulnerability is found. It's likely that it also won't offer help and support if you encounter any problems. The company is urging users – both consumer and enterprise – to update their systems to the latest operating system: Windows 10.*

In this article, we'll look at why the end of support for Windows 7 is so important.

### Windows 7 End of Life: What happens next?

When Windows 7 reaches its End of Life phase on January 14, 2020, Microsoft will stop releasing updates and patches for the operating system. However, that doesn't mean Windows 7 will stop working on January 14, 2020 – you'll still be able to use Windows 7 for as long as you want. So, the good news is you're not going to wake up on January 15th to find that your Windows 7 computer no longer boots up.

**But just because you *can* continue to use Windows 7 in its End of Life status, doesn't mean you *should*.**

The biggest issue with continuing to use Windows 7 after January 14th is that it won't be patched for any new viruses or security problems once it enters End of Life, and this leaves you extremely vulnerable to any emerging threats. What's more, if a large number of people continue to use Windows 7 after the End of Life date, this could actually be a big incentive for malicious users to target viruses and other nasties at Windows 7.

So, while Windows 7 will continue to work after January 14 2020, you should start planning to upgrade to Windows 10, or an alternative operating system, as soon as possible. If you continue to use Windows 7 once it enters its End of Life phase, you'll be vulnerable to viruses and other security threats.

### The question becomes: how big of a security threat is this?

We've seen the real-world attacks that can come from unpatched vulnerabilities in an out-of-date operating system. There are also valid reasons an organization could choose to hedge its bets and not upgrade. Ultimately, it is a conversation about risk, and more specifically, how much risk is an organization willing to assume in the face of a potentially costly or complicated upgrade.

The *WannaCry* ransomware virus is a perfect example of what kind of devastating effects an unpatched, out-of-date operating system can have. The attack leveraged the *EternalBlue* vulnerability as an entry point, then spread laterally across organizations. Microsoft had issued a patch, but organizations that hadn't applied it or were running out-of-date operating systems, were still vulnerable. *WannaCry* went on to infect companies of all sizes and industries around the world, causing millions of dollars in damages. ***This is the exact type of vulnerability any person or company leaves themselves susceptible to by continuing to use any and all Windows 7 based systems.***

In order to secure the safety and support of web browsing and overall computer health, it is important to be prepared for Windows 7 End of Life and the choices this leaves you. If you have questions or need further guidance, please contact a local computer or technology professional for assistance.

*Sources:*
*techradar.com by Matt Hanson*
*and cyberscoop.com by Ellen Sundra*