# Is Your Business VULNERABLE IN 2020?

## MICROSOFT PRODUCT END OF LIFE


DP COMPUTING

# SUMMARY

Worried about the looming end of life deadline for your Microsoft products? Microsoft is ending support for a number of popular products (including Windows 7) on January 14th, 2020. Yes, it is a hassle, but this change doesn't have to be a bad thing. Here's what's happening and how to take advantage of this opportunity to future proof your businesses IT.



# R.I.P. To Your MS Products

RIP Windows 7. For many businesses it's a tough parting. As late as September 2018 some 41% of Windows 7 users still hadn't moved on to the latest operating system. Yet sticking with existing systems until 2020 or beyond could lead to a truly bitter and sad end.

But which products are coming to an end?

- Windows 7.
- Office 2010 (including Word 2010, Excel 2010, Outlook 2010, Publisher 2010 & Access 2010).
- Server 2008 and Server 2008 R2.
- Exchange 2010.
- Small Business Server 2011 (SBS 2011).

Before we talk about why it's such an issue, let us make sure we're all on the same page about what end of life really means.

# Understanding End of Life

What does end of life mean for your business? When you first buy a product, Microsoft provides mainstream support such as:

- Offering security patches.
- Releasing design changes.
- Adding new or improved features.
- Providing complimentary support.
- Warranty claims.

For most products Microsoft stops all but security patches five years after the product's release. After all, they want to put resources behind the versions they are currently selling in stores and online.



OK, so you might be thinking that you don't need new features or design, and you have never used the warranty. Plus, at this point, most people think they know the product inside-out, so they believe they can continue on without Microsoft's help and just rely on their local IT support company.

But in 2020, Microsoft will also stop the security upgrades that provide patches and bug fixes for products you are using. Microsoft have already stopped answering posts on the Windows 7 Community forums.

You may be thinking you haven't been doing updates, so this won't make much difference for you? Try again. The updates were probably taking place without you knowing through Microsoft auto updates. That is not going to happen anymore.

# What This Means for Your Business

Come January 14th, 2020, you can still continue using your computers and servers as before. But without ongoing security support, your business runs the risk of cyberattack.

Your users will keep working to improve processes, sell product and increase revenues. Meanwhile, hackers will work just as hard to find weak points they can attack.

It is a little like pest control. Ants, spiders, roaches and other bugs are always looking for a way into your home. What do you do? Try and close any gaps they might use to get in and regularly bug bomb to keep the creepy crawlies at bay.

Microsoft was once your pest control service. The company provided the fixes needed to plug the holes and protect your business from these cyber criminals.

# What a Cyber-Attack Might Look Like

Once inside your network or systems these cyber criminals can wreck havoc. Some of ways they may mess with your systems include:

- using malicious software (malware) to take over your business computers and demand you pay a ransom to regain control.
- They might take important data for use in identity theft.
- Gain access to your bank accounts.
- Using your computers power to mine cryptocurrencies.
- Attempt to shut your business down using a distributed denial of server attack (DDOS).
- Delete all your data.

# It's Not Worth the Risk

Cybersecurity attacks are costly. Take 2017's WannaCry attack infecting more than 230,000 computers in 150 countries. The perpetrators demanded $300 ransom per computer.

The average data breach costs a company $3.86 million, according to the Ponemon Institute.  And the average denial of service attack costs a company $2.5 million.

Beyond these hefty price tags, a cyber-attack can also put your business at risk of:

- Compliance issues.
- Massive fines.
- Costly downtime.
- Brand reputation damage.
- Customers jumping to a competitor.

Where does this leave businesses still using Windows 7 and other legacy products? Let us consider the options.


# Preparing Your PCs for 2020

The good news is that you have a number of options. The first one is not so good as it involves still using these EOL products and hope for the best. While you're doing that, malicious hackers are looking to exploit that loyalty.

Microsoft is offering to still supply security updates to users for a fee! A second approach, is to pay yearly to keep getting these updates from Microsoft. This is paying now to put off what is inevitable as Microsoft is only offering three years of extended, paid support. For example, a Windows 7 Pro User can pay roughly $US50 per device for the first year of Extended Security Updates (ESUs). The price doubles in year 2 ($US100 per device) and again in year three ($US200). That’s a total of at least $350 per device until the ESUs expire in January 2023, when you will be out of luck all over again.

Antivirus and security service providers are offering a third option. Seeing an opportunity, they will offer patches and bug fixes for paying customers. The problem is that these companies offer only limited, reactionary support. Plus, they will only be in it if it proves to be profitable, so their help could end without suddenly and without warning.

Looking long-term and being proactive, you will want to go with the best option which is to upgrade and we will discuss that next.



# Future-proofing Your PC Assets

Upgrading to the latest versions of Microsoft products is an opportunity. This investment will improve productivity while future-proofing your PCs. Some examples are:

## Windows 7 to Windows 10 Upgrade

- Microsoft will provide free security updates regularly.
- Phone and online technical support provided by MS.
- An online users community to help and assist with any issues.
- Have no issues running the latest version of other 3rd party applications and utilities.

## Office 2010 to Office 365 Upgrade

- No potential security issues.
- Office 365 can improve collaboration.
- Users can access email, calendar sharing and files in real time from any device, wherever they are.
- No file compatibility issues with clients and suppliers.

# Why not wait until 2020?

Why is it a good idea to begin migration sooner rather than later? Here are our top five reasons.

1. **Risk.** Data breaches and other cyber threats are costly.
2. **Difficulty.** Migrating isn’t always easy. Depending on your IT infrastructure, it could take a lot of work.
3. **Availability.** Don't scramble to find partners to support your migration efforts at the last minute.
4. **Flexible Rollout.** By upgrading now, you can schedule a good time for your business to change over its systems.
5. **Gradual Rollout.** You can schedule the changes to be implemented gradually rather than rushing to get them all done at the same time.

Migrating data to a new system, securely and efficiently, takes work and knowhow. A reliable IT support provider can help you with the upgrade.



## Take Advantage of Our Expert IT Services

We provide a reliable IT support service.

We can ensure a proper implementation of your new products.

# DP Computing

Adelaide, South Australia


Phone: 08 8326 4364

Email: support@dpcomputing.com.au

Web: www.dpcomputing.com.au

Facebook: facebook.com/dpcomputing