Servium

SERVIUM'S LITTLE BOOK OF OUTDATED OS HORRORS

Prepare yourself for the Windows 7 afterlife

+44 (0)303 334 3000 www.servium.com hello@servium.com

Windows 7 is soon to give up the ghost

On 14th January 2020, Microsoft will end the extended support for its popular operating system (OS), widely used across the globe since 2009. While this doesn't mean that your existing Windows 7 devices will stop working, End of Life (EoL) will bring with it additional complications that could give your IT team some sleepless nights. These devices will no longer receive important updates or security patches, leaving them increasingly susceptible to the spectre of poor performance, application failure and cybersecurity breach.

Although there are plenty of reasons to convince yourself that sticking with an outdated OS is the right course of action, history is littered with eye-opening examples of those who chose to delay an update and unfortunately paid the price. It's difficult to predict exactly what will happen once support for Windows 7 comes to an end, but there are lessons to be learned from the mistakes of the past to ensure that you don't fall victim to a future outdated OS horror story.

MISTAKE #1: There's not enough time to upgrade before January 2020, so we'll leave it

IT Pro has stated that the average large-scale IT estate will take 10 months to upgrade its OS. With just 3 months to go you're already facing the unnerving prospect of continuing with a legacy OS after the EoL deadline. There's hardware to be replaced, applications to be updated and new programs to be learned. When you take into account the average deployment time, this is a long time to be exposed to some very ghoulish goings-on.

Horrible Happening: Bloodcurdling virus paralyses hospital

In 2016, a virus hit computers at Royal Melbourne Hospital as they were running on unsupported Windows XP machines.

Operations such as blood and tissue processing, which are usually conducted automatically, had to be manually completed. Patients also went hungry, as the virus affected computers storing information regarding meal requirements.

Theoretically, you could just wait until the next OS. Except you can't. Microsoft will not be releasing any more stand-alone OS version upgrades and will instead deliver Windows 10 as a Service with ongoing software updates, just like the experience you receive with your smartphone. If you decide to wait for the next big version release, you'll be waiting a very long time.

Horrible Happening: Travellers left flying by broomstick

In 2015, Paris Orly Airport had to close down entirely, leaving passengers stranded, after one of their mission-critical applications failed.

This application ran on Windows 3.1 OS, which ceased support in 2001, and they could not find an engineer to help them quickly repair such a dated system.

MISTAKE #2: We'll just stick with what we've got

Plenty of businesses see upgrading their OS as a choice, rather than a necessity. In making this choice, you're choosing to put both your users and your data at an increased risk. Microsoft will be focussing its resources on future innovations, not on maintaining old systems. In some circumstances you may be able to access Microsoft's Extended Support Services which will run for just three years, but are typically only available to the largest organisations. Unfortunately, this comes with a frightful annually increasing support fee charged per device. These rising maintenance costs equate to money that could be better spent preparing for the future and operating modern technology, as opposed to maintaining the past.

However, for most businesses, no more official patches will be released. Sure, 'unofficial' patches may emerge, but your OS could end up like a Franken-system and do you really want to risk your business on something you can't necessarily trust?

MISTAKE #3: We'll upgrade but won't bother replacing our hardware

Windows 7 was first released in 2009, meaning that your existing Windows 7 hardware could now be anything up to 20 years old.

And while you might consider simply upgrading the OS on your existing devices, Windows 10 is both feature-rich and demanding, which is a lot to ask of your older hardware. For example, Windows 10 is optimised for touch, something your users are well familiar with but won't be able to capitalise on if they're tethered to outdated hardware. Likewise, slow and poor performance inevitably leads to user frustration and in turn reduces productivity. It's proven that replacing your hardware with more modern, user-friendly devices has a positive impact on staff retention and employee morale.

By running an OS that is too advanced for your hardware, you'll never see the full potential. To pay for Windows 10 and not use every feature as it is intended is money wasted.

MISTAKE #4: It won't happen to us...

It's all too easy to assume that you won't be the one affected by malicious hacks, but many businesses that have thought the same have ultimately been caught out.

Many smaller organisations in particular often believe that they are not seen as worthwhile targets for hackers and cybercriminals, but the size of your business has no bearing on your vulnerability to hacks. In fact, these firms are known to have been used as attack vectors as part of wider plots to exploit larger-scale businesses.

MISTAKE #5: We think it's too expensive

IT budgets are often stretched, and the upfront cost of replacing your OS or refreshing your user devices may be an unexpected additional expense. As such, you might feel that those funds could be better spent elsewhere.

In running an unsupported OS, you are also vulnerable to malicious attacks on your data. You may find that the money you couldn't find to upgrade your OS, becomes money you simply have to find to buy back your data from a ransomware attack.

The ability to refresh your entire IT estate with a Device as a Service (DaaS) subscription makes pricing much more accessible. With DaaS, you can upgrade to world-leading HP hardware, update your applications and harness the latest Microsoft OS as part of a single monthly fee.

Horrible Happening: Hackers haunt the halls of government networks

In May 2019, Baltimore City Government found itself the latest victim in a string of ransomware attacks.

Their servers were compromised and locked out of accessing their own data. Hackers exploited a vulnerability in their unsupported Windows XP system and shut down emails, billing systems and other important services.

MISTAKE #6: The threats aren't real!

Despite repeated warnings, as well as previous incidents involving others continuing with legacy systems, there may still be some who feel that any suggestions of the risks presented by continuing with Windows 7 are unsubstantiated. After 14th January 2020, it will be an open season on Windows 7 users. Just as businesses are preparing to upgrade, criminals are preparing to take advantage of those who don't. Many security experts maintain that malware developers have devised new ways to exploit flaws in the Windows 7 system and are lying in wait until 14th January 2020 to take advantage of your unsupported system.

We can only learn from the past, with the 2017 WannaCry attack on the NHS being one of the ghastlier examples.

MISTAKE #7: We didn't consider the legal requirements

In not updating your system, you are making a choice to leave your data unprotected. Your old OS will harbour vulnerabilities that can be penetrated by criminals, causing havoc.

In order to remain GDPR compliant, it is necessary to demonstrate that your company is not storing unprotected data. This is applicable to businesses of any size, whether you have 1 outdated OS or 1000. As well as passing on your GDPR responsibilities, if your company processes card payments then you will no longer be compliant with Payment Card Industry (PCI) data security rules. Card companies are well within their rights to refuse to work with you and can even issue penalties to those who continue to process unsecure payments.

These are just two examples of the regulatory responsibilities facing many businesses. However, there are countless other compliancy standards that businesses in all kinds of industries must adhere to, many of which will have specific guidance on data security and exposing yourself to Windows 7 vulnerabilities could be an issue.

Horrible Happening: WannaCry sucks the blood of the NHS

Recovering from the WannaCry hack in 2017 cost the NHS over £92 million.

1/3 of hospital trusts were affected with more than 19,000 patient appointments and operations cancelled as a result.

Horrible Happening: Government computers so slow you'd scream

It was reported in 2014 that Veterans Affairs hospitals in the US were still running on the MS-DOS operating system, which pre-dates any of the Windows programs.

To schedule one appointment on this system took over 12 steps and input from several users, massively hampering productivity and slowing down the functioning of care services.

MISTAKE #8: Our applications won't work

You might be surprised to know that many of the business-critical applications your business uses every day are already Windows 10 compatible.

The applications currently running on your existing Windows 7 laptops and PCs will become increasingly slow and cumbersome. Persevering with Windows 7 is time wasted that could be spent learning how to use the extensive range of improved applications that have been written for Windows 10.

MISTAKE #9: Antivirus will protect us

Antivirus software is a core component of any strong security posture, but it cannot be relied upon to protect your Windows 7 OS in place of regular security upgrades.

The latest antivirus updates are designed to work best on Windows 10 products, so ensuring full effectiveness relies on your OS being updated and correctly patched to reflect all the latest threats. In asking your antivirus software to do too much and not running it on the latest OS, you are overstretching its capabilities and rendering many of the protections redundant.

Horrible Happening: Mending undead OS takes more than a pumpkin patch

An emergency patch was released for Windows XP in May 2019 after a wormable flaw in the remote desktop services was revealed.

The patch remains uninstalled on many machines, meaning that they are still exploitable. Unpatched machines were the principal cause behind the spread of WannaCry in 2017.

MISTAKE #10: We'll just update the most important machines!

Every machine in your network is important. Your entire device estate is only as strong as your weakest machine, so to selectively choose the most important devices, and leave others exposed, is to create vulnerabilities within your network.

Cybercriminals and hackers will target these vulnerabilities indiscriminately, so opting to save money by only upgrading a handful of your machines could ultimately see you end up paying a much bigger price.

Horrible Happening: Hackers use tricks to get treats

ATM machines and banks in Russia were discovered to be operating on Windows XP in 2017.

By simply using Sticky Keys, hackers were easily able to access all areas of the ATM's OS and trigger them to dispense large sums of cash.

It's not too late to act

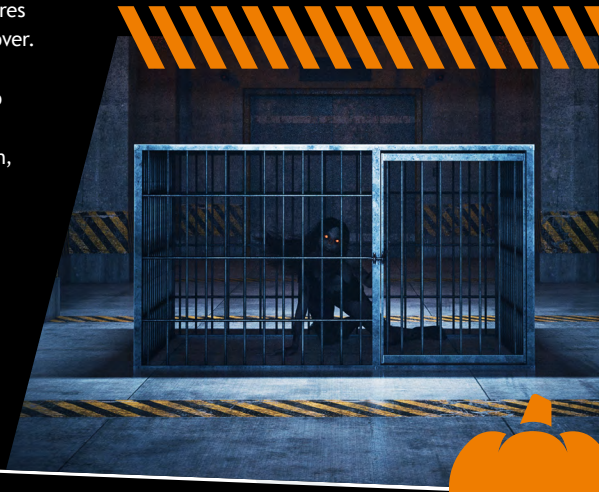
Stay safe with ultra-secure HP devices

With the latest HP devices, you can avoid the nightmare of continuing with an unsupported operating system running on outdated hardware.

HP's Premium Family of business laptops and desktops are Windows 10-ready, designed specifically to better support the next-generation Microsoft OS. By upgrading, you'll also benefit from an industry-leading hardware-embedded security posture, including innovative features such as Sure Start, Sure Click and Sure Recover.

It's never been easier or more affordable to upgrade your device estate with HP Device as a Service. You can roll up the acquisition, management and refresh of your devices into a single monthly subscription, all while shifting the financial outlay from a capital expense to a repeating operational cost.

You'll not only gain genuine transparency over your ongoing IT spend. You'll also benefit from genuine visibility into the health and performance of each device with HP TechPulse, allowing you to identify and rectify potential hardware issues before they occur and make informed choices on the hardware you select for each of your users.



Take the next step with Servium

Our HP Gold partner status means that we're ideally placed to assist you with your upgrade to Windows 10 with HP. Our longstanding partnership and HP DaaS accreditations enable us to secure you the best value commercials, and priority access to product stock and technical assistance. Upgrading your OS will never be easier.

Get in touch with your Servium Account Manager or contact us to learn more about HP DaaS and to discover the Premium Family of business machines.

Servium

+44 (0)303 334 3000 www.servium.com hello@servium.com