May 2019

TechTidbit.com

brought to you by Tech Experts

Your Guide To Microsoft's End Of Windows 7 Support

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Support for Windows 7 is coming to end this year. The operating system is 10 years old, and in the near future, Microsoft will discontinue all support - including security updates - for this version of Microsoft Windows.

This means the end of Microsoft security updates and this means many 3rd-party security tools like anti-virus may no longer function.

"Malicious Actors" a. k. a. "Hackers" will quickly exploit any Windows 7 computer the moment security updates stop and any future security vulnerability is discovered.

Microsoft tells us that as of October 2018, about 39% of business computers are still running Windows 7. Clearly, there is a lot of work to do over the coming months to prepare businesses for the end of support of Windows 7.

What does it mean if a Microsoft Windows product is not supported?

In the most general terms, "not supported" means that Windows is no longer eligible for the downloadable bug fixes, security patches, and other updates from the Windows Update service. It means that the product has exceeded the standard lifecycle support services.

Each Microsoft product and service pack will fall into different support schedules, but you can also track the overall support lifecycle as well, so that you can plan for the inevitable end of a product for personal and professional use.

If Windows is not supported, is it still functional? Can you use it?

When Microsoft no longer supports a version of Windows, and your install is no longer protected from known security risks, compatibility issues, and other bugs, you can still use the operating system.

In most cases, you will still be able to start and run your version of Windows Vista, XP, 7, 8.1, etc.; but you will experience increasing instances of software incompatibility and likely security risks. You may also experience error messages or other support issues related to your hardware and software.

The compatibility issues can be frustrating, but you will likely still be able to use the product. For those individuals and companies who love the "old" product, and don't want to change, they don't really have to, unless the company is subject to industry regulation, such as HIPAA or FINRA.

What is the timeline for service packs and the Microsoft lifecycle?

When a new Windows (OS) service pack is released, the previous service pack is on a 2-year cease-of-support updates countdown. While that timeline would seem to give you a general sense of how long you have before your product is no longer supported, there are caveats.

Microsoft sometimes extends the length of time for support services, or just allows the support timeframe to inexplicably continue. It can be welcome news for the general Windows user, but it's not something that is promised or assured. So, the consensus is that you should take support when and if you can, but expect that it could end.

How do you make sure Microsoft Windows will be supported?

With the Modern Lifecycle Policy, you can pay for Software Assurance (SA), a subscription that offers additional licensing and professional services.

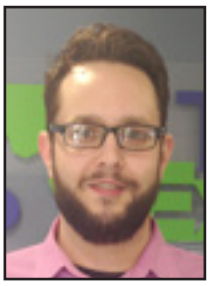
For professionals and business owners, SA offers peace of mind that they will receive support services even when the standard product is

Continued on Page 4

Microsoft tells us that as of October 2018, about 39% of business computers are still running Windows 7. Clearly, there is a lot of work to do over the coming months to prepare businesses for the end of support of Windows 7.

How To Reduce Pop-Ups And Other Browser Best Practices

"Maintaining a generally healthy system is also a key to browser speed. Malware and adware can often specifically affect browsers. Any malware affecting the entire system would affect your browsing speed as well."



Jason Cooley is Support Services Manager at Tech Experts.

One of the most annoying things about browsing the web are pop-ups. Depending on your browser, your ability to limit or block pop-ups is probably built-in. If it's not, there is definitely an extension for that purpose.

There are also other ways to ensure you have the best and fastest browsing experience possible.

Before we get into which browsers have which kind of pop-up blocker, let's examine a fact. Pop-ups are annoying, but not always intrusive or unwanted.

There are instances where I need a pop-up from a site as it may be an internal page that has been requested or a log-in box. This can be frustrating as we may not know a pop-up is coming from a link. It may appear that nothing has happened.

So how do you know? The best practice and safest way is to allow pop-ups from sites you trust (as needed).

Say you're on your banking site and you click log-in. Normally, a pop-up log-in box is displayed, but nothing happens. The pop-up has been blocked.

In the browser, you can enable this webpage to allow pop-ups, thus restoring your access and keeping you secure in the process.

In addition to pop-ups, users must also be on the lookout for pop-under windows. These are typically pages that open with other pages, like a tag along. They also frequently occur when attempting to leave a web page. They pop underneath other windows, hence the name. In most cases, pop-up blockers will stop most pop-unders.

So what about the browsers? Well, let's just cover the Big Three: Chrome, Edge, and Firefox.

These browsers all come with a built-in pop-up blocker – all of which can be enabled in the settings page of the browser.

In most cases, these will do what you want them to: stop pop-ups. However, there are some instances where pop-ups or pop-unders make it through. There are third party extensions for most browsers that will typically offer more security.

Now that these pop-ups are handled, what else can we do to make a better browser experience? There are a few things you can do to perform sort of "maintenance" on your browser.

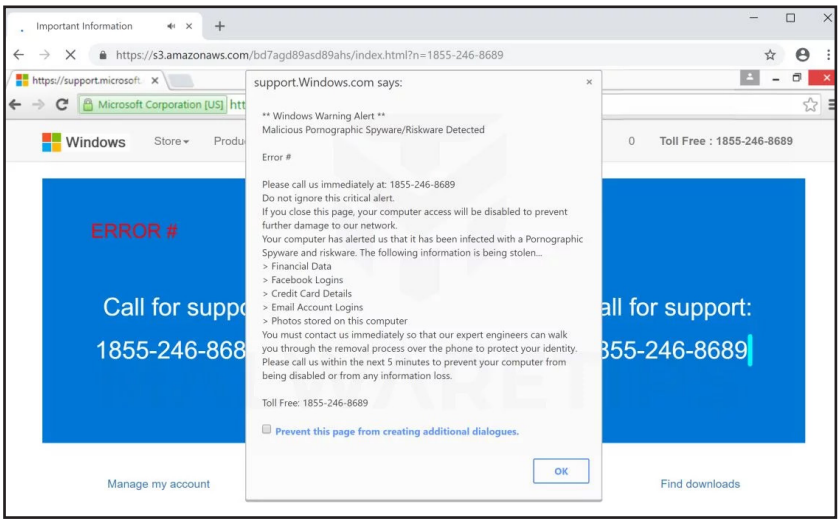
Clearing your cache (stored data) can help a website that doesn't want to load very quickly. Most people know about clearing your browsing history, but there are other clean-up methods available.

There are a few different types of stored data associated with browser use. Some of this is background information, temporary data, passwords, and preferences. You can choose which parts to remove, so you can still keep your saved information without having to reenter it.

Another quick and easy tune up process is to remove any unused browser extensions. This can help with basic browser speed and performance.

Maintaining a generally healthy system is also a key to browser speed. Malware and adware can often specifically affect browsers. Any malware affecting the entire system would affect your browsing speed as well.

The best practice you can have is to use a strong antivirus and scan your computer regularly. There are many factors at play and paying attention to all of them is key to the best browsing experience.



New Whaling Schemes: CEO Fraud Continues To Grow

In previous years, the first clue that your corporate email has been compromised would be a poorly-spelled and grammatically incorrect email message asking you to send thousands of dollars overseas.

While annoying, it was pretty easy to train staff members to see these as fraud and report the emails. Today's cybercriminals are much more tech-savvy and sophisticated in their messaging, sending emails that purport to be from top executives in your organization, making a seemingly-reasonable request for you to transfer funds to them as they travel.

It's much more likely that well-meaning financial managers will bite at this phishing scheme, making CEO and CFO fraud one of the fastest-growing ways for cybercriminals to defraud organizations of thousands of dollars at a time.

Here's how to spot these so-called whaling schemes that target the "big fish" at an organization using social engineering and other advanced targeting mechanisms.

What Are Whaling Attacks?

Phishing emails are often a bit more basic, in that they may be targeted to any individual in the organization and ask for a limited amount of funds.

Whaling emails, on the other hand, are definitely going for the big haul, as they attempt to spoof the email address of the sender and aim pointed attacks based on information gathered from LinkedIn, corporate websites and social media.

This more sophisticated type of attack is more likely to trick people into wiring funds or passing along PII (Personally Identifiable Information) that can then be sold on the black market. Few industries are safe from this type of cyberattack, while larger and geographically dispersed organizations are more likely to become easy targets.

The Dangers of Whaling Emails

What is particularly troubling about this type of email is that they show an intimate knowledge of your organization and your operating principles. This could include everything from targeting exactly the individual who is most likely to respond to a financial request from their CEO to compromising the legitimate email accounts of your organization.

You may think that a reasonably alert finance or accounting manager would be able to see through this type of request, but the level of sophistication involved in these emails continues to grow. Scammers include insider information to make the emails look even more realistic, especially for globe-trotting CEOs who regularly need an infusion of cash from the home office.

According to Kaspersky, no one is really safe from these attacks — even the famed toy maker Mattel fell to the tactics of a fraudster to the tune of $3 million. The Snapchat human resources department also fell prey to scammers, only they were after personal information on current and past employees.

How Do You Protect Your Organization From Advanced Phishing Attacks?

The primary method of protection is ongoing education of staff at all levels of the organization. Some phishing or whaling attacks are easier to interpret than others and could include simple cues that something isn't quite right. Here are some ways that you can potentially avoid phishing attacks:

- Train staff to be on the lookout for fake (spoofed) email addresses or names. Show individuals how to hover over the email address and look closely to ensure that the domain name is spelled correctly.
- Encourage individuals in a position of leadership to limit their social media presence and avoid sharing personal information online such as anniversaries, birthdays, promotions and relationships — all information that can be leveraged to add sophistication to an attack.
- Deploy anti-phishing software that includes options such as link validation and URL screening.
- Create internal best practices that include a secondary level of validation when large sums of money or sensitive information is requested. This can be as simple as a phone call to a company-owned phone to validate that the request is legitimate.
- Request that your technology department or managed services provider add a flag to all emails that come from outside your corporate domain. That way, users can be trained to be wary of anything that appears to be internal to the organization, yet has that "external" flag.

There are no hard and fast rules that guarantee your organization will not be the victim of a phishing attack. However, ongoing education and strict security processes and procedures are two of the best ways to help keep your company's finances — and personal information — safe from cyberattack.

"According to Kaspersky, no one is really safe from these attacks — even the famed toy maker Mattel fell to the tactics of a fraudster to the tune of $3 million. The Snapchat human resources department also fell prey to scammers, only they were after personal information on current and past employees."

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Your Guide To Microsoft's End Of Windows 7 Support, from page 1

no longer supported. Some companies also rely on the additional licensing rights and professional services, including: Dedicated support services, training or online certifications, and access to Microsoft partners.

For companies who need help with additional training or services, the SA solution can more than pay for itself. The alternative (or additional) scenario is to hire or use existing IT infrastructure to support your Microsoft support or training needs. Even with your paid support services (for SA), Microsoft can still end all support for a product with a 12-month notification of support cessation.

Why would you use Windows when it is no longer supported?

There are a number of reasons why you might need to use a version of Windows that is no longer supported. For example, your hardware may not support a new version of Windows, or your software may not be compatible.

Another reason to stay with a deprecated version is because you just prefer it, because you don't want to upgrade, or even due to security restrictions from your company. Some companies still use Windows 7 for security reasons, or because there are rumors (often well-founded) of issues with the new release. There's always a trade-off when you decide to use a deprecated or unsupported product.

You probably won't be able to install or access new programs, websites, or other more current functionality, but you also may not need all those bells and whistles. If you prefer the old system, and you don't want to change, then nobody can force you to upgrade. You have options to keep your system and programs in the exact same, stable state you've always enjoyed.

Five Ways to Deal With Aging Computer Equipment

While upgrading your tech equipment marks an exciting time in the office, it also presents a problem. With the introduction of new technology, you must decide what to do with your old equipment.

Provided those items are still in good working order, they may continue to be helpful in other avenues. Consider one of these five ways to give your old, replaced technology a new home:

Find a fresh purpose for it

Old equipment may not be up to task in one arena anymore, but it may be useful for something else. For example, old computers could power dummy terminals or be used for browser testing.

Connect with a local nonprofit

Your obsolete equipment may build a bridge with a local nonprofit. If you don't have a particular organization in mind, ask your team for suggestions.

Donating your items to a nonprofit can elevate your company's image in the public eye and be tax deductible down the road.

Donate it to a school

Whether your old equipment is best put to use actively or as the technological equivalent of a cadaver in a computer assembly class, schools are always in need of computers for students to use.

Be charitable

Similarly, you can donate your outdated technology to a charity and allow it to either sell your old items or put it to use in their office. This method can even net you and your business a tax break.

Hand it down

What is old to you can be new to someone else. Review the age and functionality of your employees' equipment, and you might find what you wish to discard constitutes an upgrade to another member of your team.

Create new service requests, check ticket status, and review invoices in our client portal:
http://TechSupportRequest.com