March 2017

TechTidbit.com

brought to you by Tech Experts

Free Windows 10 Upgrade for SMBs: What You Need to Know

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

While Microsoft has recently accounted that free Windows 10 upgrades have been reinstated, there is a caveat: They are only available to SMBs that have previously declined the offer.

If you fall into that particular category, now is the time to reconsider.

Here are some frequently asked questions about the free Windows 10 upgrade and how it affects you.

Is it open to everyone?

No. It is open to SMB customers on Enterprise plans that are running personal computers on Windows 7 or 8.1.

Will my monthly subscriptions increase?

No. The Enterprise E3 and E5 plans will remain priced at $7 and $14 per user per month respectively, or $84 and $168 per user annually.

Do I need to sign a long-term licensing agreement?

No. The licenses that are issued for the E3 and E5 plans are provided on a per-user basis. To continue running the operating system, you need to ensure you pay the associated monthly payments. You can cancel at any time.

Do I need any other software?

To use the Windows 10 Enterprise E3 or E5 plans, you need to be running Windows 10 Pro. If you don't have the license for this OS, Microsoft is now giving you a chance to upgrade free of charge when you subscribe to the E3 or E5 plans. This license will never expire.

Will I need a PC upgrade?

You may need to upgrade your OS from Windows 10 Pro to Windows 10 Enterprise. In addition, if you have yet to subscribe to the E3 or E5 plans, you will need to do so first.

It is important to remember that Windows 10 is a more powerful operating system. Older PCs with slower hard drives or low memory may not perform well.

Is this a time-limited patch?

According to representatives from Microsoft, the offer to upgrade Windows 7 and 8.1 to Windows 10 Pro is permanent for subscribers to Windows 10 Enterprise E3 and E5.

The Purpose Of Routine Maintenance On Your PC Or Server

Anthony Glover is a Senior Network Engineer and Service Manager at Tech Experts.

Workstations and servers are valuable assets for any small business. This is why it's very important that we take proper care of these vital attributes.

Computers can be great, long-lasting tools if taken care of correctly and routinely. This ensures that your PCs and servers will continue to run as they should, as long as possible. There are several steps to maintain your PC or server.

Monthly Hardware Cleaning

This will keep your fans running efficiently and keep your PC or server clear of dust and debris that can potentially cause a few issues (such as heating problems, fan malfunctions, or damage to devices like your power supply).

Heat also can cause computers to run slow or sluggish. This is extremely important and should be monitored and managed by an IT professional such as Tech Experts.

Monthly Software Management

This is to ensure you provide a safe operating environment for your business. It helps to keep the functionality of all your programs and keep your computer running smoothly. By clearing caches, you eliminate temp files that could potentially cause problems for some programs and will also free up space on your hard drive. This is another key process to keep your PCs and servers running at their full potential.

Registry Cleaning

Throughout use of your PC or server, you will accumulate registry errors from programs being installed, updates, etc.

This should be cleaned and corrected on a monthly basis to ensure proper operation of your PC. When it comes to speed when booting and operating your PC or server, this is an especially big factor.

Monthly Hardware Monitoring and Recording

When you are operating a business that needs your equipment to work efficiently (which is the case for most businesses), you'll want to check your PC and servers on a monthly basis.

Having your vital components like hard drives scanned, checked, and recorded will let you know if anything needs replaced before it fails and leaves you in a bind.

Thermal Monitoring

Heat is a vital threat that should never be overlooked as it's essential to speed and safe operation of your PC or server.

Heat can destroy components and cause Blue Screens Of Death due to heating issues, causing the PC or server to not function at all unless it's corrected.

You want to make sure the environment of the equipment is clean, clear, and cool to avoid overheating.

Process Monitoring

This can catch potential threats like malicious software, of course, but it can also help you and your IT department find more subtle unwanted issues such as backdoors or even rootkits that allow onboarding of your PC or server without the end-user knowing at all.

Here at Tech Experts, we provide a preventative maintenance service that can be utilized on both PCs and servers at your business. So why hassle at all if you don't have to?

You could have an IT professional manage your computers, saving your business money and saving you time. It could even save your computers or server.

The Importance Of Having Ad-Blockers

Luke Gruden is a Help Desk Specialist at Tech Experts.

Every day, millions of people go online and go to a familiar website, just to get an advertisement pop-up that disrupts their online experience.

Ads are a way of life for many websites to generate profit from viewers visiting their website and, when clicked, these ads can take a person to another website, usually for their product.

While annoying and harmless when used as intended, issues in this system start to happen when the intentions of an "advertiser" go beyond just advertisement.

There are malicious people on the Internet utilizing advertisements to leave our computers and information vulnerable for theft and abuse.

Some advertisements will come in as scareware trying to pressure people into calling their number or download a harmful program.

Scareware is a common pop-up that thousands have fallen victim to – giving up Social Security numbers or access to bank accounts, allowing malicious connections to their computers, leaving networks vulnerable and infected, and more.

Some advertisements, if not filtered by a website correctly, can actually contain viruses and infections that don't allow a person an opportunity to protect their own browser and computer.

These infections usually leave spyware and trojans that try to steal your information from your computer.

Surprisingly, the websites with these sorts of advertisements may have never intended for you to fall victim to scareware or other infections.

Usually, websites with these ads tend to be smaller websites using an advertisement agency that does not fully screen all the advertisements they are receiving, allowing malicious people to send their harmful information out onto the Internet.

There is a very simple solution to these real threats: ad-blocking software. If you use Firefox or Google Chrome, there are two good options that you can attach to your browser.

The first option is Adblock Plus, which is a common choice that works well. There is also uBlock Origin that uses less processing power than Adblock Plus that also blocks most advertisements. Both of these options will go a very long way in protecting your computer.

If you are using Internet Explorer or Microsoft Edge, these web browsers do not support add-ons and have weak advertisement blocking capabilities.

Firefox and Chrome on their own, even without add-ons, are more secure than Internet Explorer. If you have not switched to Chrome or Firefox, I highly recommend you make the change soon.

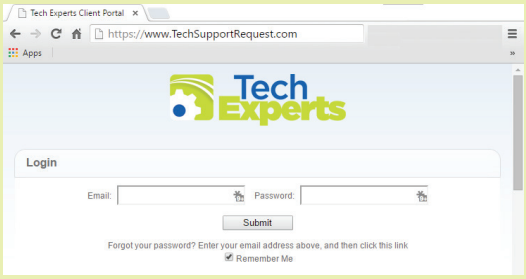
The installation processes for Adblock Plus and uBlock Origins are very straightforward and easy on Chrome and Firefox. You can Google the ad-blocker you want to use and go to either the Chrome web store or Add-ons For Firefox, based on which browser you are using.

Keep in mind that this isn't a substitute for anti-virus. Ad-blocking extensions for your browser simply help to block the things that could become nasty infections.

For a more protected computer, you should absolutely use both anti-virus and ad-blockers.

If you need help setting up ad-block software or have questions, you can always contact Tech Experts.

Stay safe and remember to use ad-blocking software to keep your Internet experience safe.



Create new service requests, check ticket status, and review invoices in our client portal:

http://www.TechSupportRequest.com

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

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

Sales Inquiries
(734) 457-5001
(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) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

2017 Will See Worst Cyber Attacks To Date

Jared Stemeye is a help desk specialist at Tech Experts.

At least, according to cybersecurity experts. There were around 500 million people with personal information leaked and over $2 billion stolen or lost in damages between 2015 and 2016 alone – and, chances are, you heard of at least one of the many high-profile data breaches during this time. Experian, Target and Yahoo all experienced massive data breaches within the past two years.

Beyond the private sector, government agencies such as the Office of Personnel Management (the bureau in charge of background checks on all government employees) were hit with cyberattacks, causing data leaks of over 22 million individuals who had undergone federal screening.

These numbers are quite alarming as top cybersecurity firms and analysts agree 2017 will see even more data breaches through the creation of ever-evolving and sophisticated malware.

Size Doesn't Matter

In the cyber world, there are few things being bought and sold faster than data. Personal records, financial information, and even intellectual property are being distributed and exchanged for money or other data – and business is booming.

Organizations of all sizes were not fully aware of how this deeply embedded malware could potentially be infecting their systems without their knowledge until just recently.

The prevalence of zero-day attacks was not fully understood either. This has allowed attackers to prepare and disseminate virtually undetectable software to perform data dragnets across many networks, big and small.

It would be naïve to assume that all the data breaches occurring are currently exposed and being corrected. This is even truer for smaller, community-driven businesses that may have little to no persistent network security monitoring.

The Cost

Per the non-profit online security analysts Online Trust Alliance (OTA), approximately 82,000 cybersecurity incidents impacting more than 225 organizations worldwide were reported in 2016.

"As the majority of incidents are never reported to executives, law enforcement or regulators, the actual number of incidents causing harm combining all vectors including DDoS attacks could exceed 250,000," OTA said.

Given this, it is well known by those affected that data breaches are expensive - and the longer the breach takes to discover, the more these costs can compound.

"If a breach took a long time to be found, then something about the existing infrastructure made it hard to discover the weakness sooner. That calls for rearchitecting the infrastructure, typically an expensive and time-consuming project. But that imperative is not always heeded," says OTA. However, the cost of notifying victims and hiring security consultants to investigate, identify, and fix the problem can cost a company a lot more.

This is only the beginning as the costs of such an attack continue to rise when downtime, lost productivity, and the resulting lost revenue are considered.

Today's Need For Cyber Defense

The scale of small business networks is becoming more complex as even basic technologies evolve. Cloud deployment, fluid transfer of data across multiple devices, and the incorporation of all things Internet have made it increasingly difficult for your everyday office worker to navigate and detect threats.

For the attackers, though, nothing has changed. Malware will keep infecting these new systems and attackers will keep hunting for data to steal. "Cyber-attacks and cyber-defense is not a battle of attrition, it's an arms race," Ray Rothrock, CEO of Red Seal Security Analytics, says.

It is important to always be ahead in this race and, for businesses, it is becoming increasingly evident that having a full-time cybersecurity team at the ready is necessary for a fluent and successful operation.

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