COMPUTER NEWS from the

MARCH 2015 Volume3 NO. 3

As found on the web and other sources

There are a couple of long articles this month, but I thought they were worthwhile!
Bob

Does your Computer Have VD?

Category: Security from “askbobrankin.com”.

If you bought a Lenovo laptop any time since September, 2014, it may have come with a piece of adware called Superfish that puts all of your Web browsing sessions at risk of hacking. The same flawed technology has been found in three different parental control programs, and may be incorporated in any number of other legitimate programs. Here's what you need to know, and do...

What is Superfish?

The adware, named Visual Discovery by Superfish, was installed by Lenovo on certain laptop models shipped between October and December, 2014. At first, Lenovo said the Superfish software was not a security concern, and that it merely helped consumers "discover interesting

products while shopping." Even Lenovo's Chief Technical Officer called the criticism "theoretical concerns," but those statements have turned out to be either huge lies, or stunning incompetence. Or both...

NOTE: This article is a bit more techy than most here. So if your eyes start to glaze over, skip to the "What You Need to Do" section and follow those instructions.

Superfish is a company that develops iOS and Android apps that are based on the company's "visual search" technology. Given an image, Superfish searches "billions" of online images for similar ones. The company has apps for interior decorating (match that nightstand to a dresser), flowers, and even pets. These apps get their "query" images from smartphone cameras. They're harmless.

Visual Discovery, however, gets its query images from the Web pages you visit. Then it queries a database of ads for similar images and displays "matching" ads in pop-up windows on the Web page you're viewing.

It's almost as if Superfish and Lenovo said to each other, "Let's see how much we can get people to hate us!" Well, hate they did, so loudly that in early January Lenovo "suspended" shipments of Visual Discovery and got Superfish to remotely disable Visual Discovery on all the laptops infected with it. That should have been the last anyone ever heard of this utterly daft scheme. But then it was discovered that Visual Discovery does much worse than annoy users with popup ads.

Visual Discovery eavesdrops on all of your Web traffic, including traffic encrypted using the Secure HTTP (HTTPS) protocol. It does so using a "man in the middle" subterfuge commonly found in malware. It generates fake digital certificates that fool Web browsers into thinking they are connected to trusted sites when; in fact, they are connected to Visual Discovery. It also impersonates your Web browser to the trusted site you are trying to reach.

The Lenovo laptop model numbers that got this Visual Discovery "VD" are:
E-Series: E10-30
Flex-Series: Flex2 14, Flex2 15, Flex2 14D, Flex2 15D, Flex2 14 (BTM), Flex2 15 (BTM), Flex

G-Series: G410, G510, G40-70, G40-30, G40-45, G50-70, G50-30, G50-45
M-Series: Miix2 - 8, Miix2 - 10, Miix2 - 11
S-Series: S310, S410, S415; S415 Touch, S20-30, S20-30 Touch, S40-70
U-Series: U330P, U430P, U330Touch, U430Touch, U540Touch
Y-Series: Y430P, Y40-70, Y50-70
Yoga-Series: Yoga2-11BTM, Yoga2-11HSW, Yoga2-13, Yoga2Pro-13
Z-Series: Z40-70, Z40-75, Z50-70, Z50-75

The bottom line is that Visual Discovery can read all encrypted traffic that passes between a browser and a trusted site, enabling VD to conduct its image searches and ad serving. It doesn't steal your passwords or record your bank account data, according to Superfish and Lenovo. But... it enables others to do so.

In order to generate fake certificates on the fly, Visual Discovery registers "Superfish, Inc." in Windows as a trusted "certificate authority (CA)," an entity that Windows recognizes as an authorized issuer of digital certificates. Real CAs include Verisign, Truste, Microsoft, and other well-known third parties. A program should never be able to vouch for its own legitimacy, obviously; but that's what VD does. And then it does something even worse.

Leaving the Key in the Lock

A certificate authority (CA) must "sign" every certificate it issues with an encrypted key. Real CAs guard their keys very closely. But Visual Discovery stores a copy of its key on every PC it infects. The VD key is protected by a password, but the password is available in plain text in the RAM of an infected machine as long as VD is running.

It's like leaving a key in a lock! Actually, it's worse. Imagine if Ford made all of its cars with the same exact lock, and put a spare key under the front bumper.

Robert Graham, president of Errata Security, found the password in barely three hours. Any hacker who has access to one of the VD-infected Lenovo laptops could do the same, and then he would be able to compromise all other VD-infected Lenovo machines. "I can intercept the encrypted communications of Superfish's victims while hanging out near them at a cafe wifi hotspot," Graham wrote in a blog post detailing how he did this.

That's bad enough, but it gets even worse. Visual Discovery is not the only software that breaks HTTPS (secure web connections) in this way. The password to VD's key is "komodia," Graham reports. Ironically, Komodia is the name of an ancient Greek goddess of happiness and amusement. It's also the name of the company that provided the HTTPS-breaking components of Visual Discovery to Superfish, which is not Komodia's only customer.

Three parental control software packages that use the same dangerous hijacking technique have been identified. The "Keep My Family Secure" program is marketed by Komodia itself. Another is "Quostodio," and the third is Kurupira Webfilter. All three use the password "komodia." All PCs that have any of these parental control programs installed are as vulnerable

as the Lenovo laptops infected with VD. Similarly vulnerable Komodia code has been found in Lavasoft Ad-Aware, Hide-My-IP, and a growing number of other software packages.

What You Need to Do

Finally, here is some good news: Lenovo has provided a tool that removes Visual Discovery and Superfish's bogus "trusted certificate authority" status from infected PCs. If you purchased one of the Lenovo laptops listed above recently, download and run this program, and you'll be OK.

You may have read that Microsoft's Windows Defender, McAfee and possibly other anti-malware tools were updated to remove the Superfish components. That's true, but I've read that these tools do not remove the bogus security certificates from Firefox, Thunderbird, and other software potentially compromised by Komodia. The Lenovo tool covers those bases as well as the Windows operating system.

The list of software that may be compromised by Komodia is growing. See this advisory from the U.S. CERT (Computer Emergency Response Team). Italian security consultant Filippo Valsorda has provided an online test for Superfish and other Komodia vulnerabilities. If it finds any vulnerabilities on your computer, run the Lenovo removal tool, then run the online test again. If vulnerabilities are still detected, you'll need to correct them manually.

The question that remains for me is why would Lenovo do something so stupid? The China-based firm claims that their "relationship with Superfish is not financially significant; our goal was to enhance the experience for users." Does anyone believe that? And can Lenovo be trusted going forward? Your thoughts on this topic are welcome. Post your comment or question below...

Save money by cleaning up your hard drive

By Lincoln Spector in Windows Secrets.

Like the proverbial hall closet, your internal drive — whether platter-based or solid-state — can hold only so much.

It's not just a space issue; an overstuffed drive can affect system performance, too. Here are some tips to reduce the clutter.

Not so long ago, I seriously thought that hard-drive cleaning was a dead topic. After all, hard-drive capacities were easily exceeding Moore's Law, and prices were falling faster than a notorious energy company's stock. Conventional wisdom was to simply purchase a bigger drive.

But then solid-state drives (SSDs) and online storage services went mainstream, and gigabytes became expensive commodities once again. So I'm back to helping people clean house (metaphorically speaking, of course). Now that we commonly store our data both locally and in the cloud, the need to toss out bits has never been greater.

Remove Windows' own garbage stashes

We're not the only ones who tend to collect unneeded data; Windows and our applications tend to keep outdated files. Let's start by getting rid of no-longer-needed system, update, and temporary files.

But before we do, make a full backup of your system — or, at the very least, create a restore point. To do the latter, enter "restore point" into either the Start menu search box or the charms bar's Search. When the "Create a restore point" item appears, click it. (Alternatively, click Control Panel/System/System Protection.) Under the "System Protection" tab, click the Create button and fill in a description, as requested.

Now that you're protected from overzealous cleaning, it's time to remove programs that you no longer use. Go to Control Panel and open the Program and Features tool. Next, scroll through the list of installed software and look for those you no longer use. I suggest clicking the list's Size column header; that'll move the biggest space wasters to the top of the list. Right-click any unwanted applications and click Uninstall. Keep in mind that you can uninstall only one program at a time, so make sure Windows has finished removing a program before right-clicking another.

If you've ever reinstalled Windows, the chances are good you have a huge **Windows.old** folder that's not doing much of anything. Go to your drive's root folder (typically, **C:**) and look for the **Windows.old** folder. If you see it, and you haven't reinstalled Windows within the past few months, delete it. (It can also be deleted via the Windows Disk Cleanup tool — more info.)

Next, check Windows' temp folder. In the Windows search box, type **%temp%** and press Enter. Click the **Date modified** column header to sort the files by date. You can then safely delete everything in the folder with a date prior to your last system boot. For example, if you booted Windows in the morning, you can delete anything that's not dated today.

Those are the manual methods. The more automated technique is to use Windows' built-in Disk Cleanup tool. But to access its full capabilities, you need to run it in administrator mode. Enter "cleanmgr" into the Windows search box; when it appears in the search results, right-click it and select **Run as administrator.**

Select the drive you want to clean — almost certainly **C:** — and then wait while the program scans your drive and calculates what it can remove. Eventually, it'll provide a checklist of cleanup options; note the disk space each uses, shown on the right.

The Windows Update Cleanup option (see Figure 1) might free up more space than all the others combined. But there are four things you need to know about Update Cleanup:

- You won't see this option unless you've launched Disk Cleanup as an administrator.
- The feature isn't available on Vista or earlier Windows versions.
- If you're using Windows 7, you might need to install the Disk Cleanup Wizard add-on KB 2852386 (more info).
- Once you apply this option, you'll lose the ability to uninstall past system updates; don't use it soon after installing your Patch Tuesday updates.

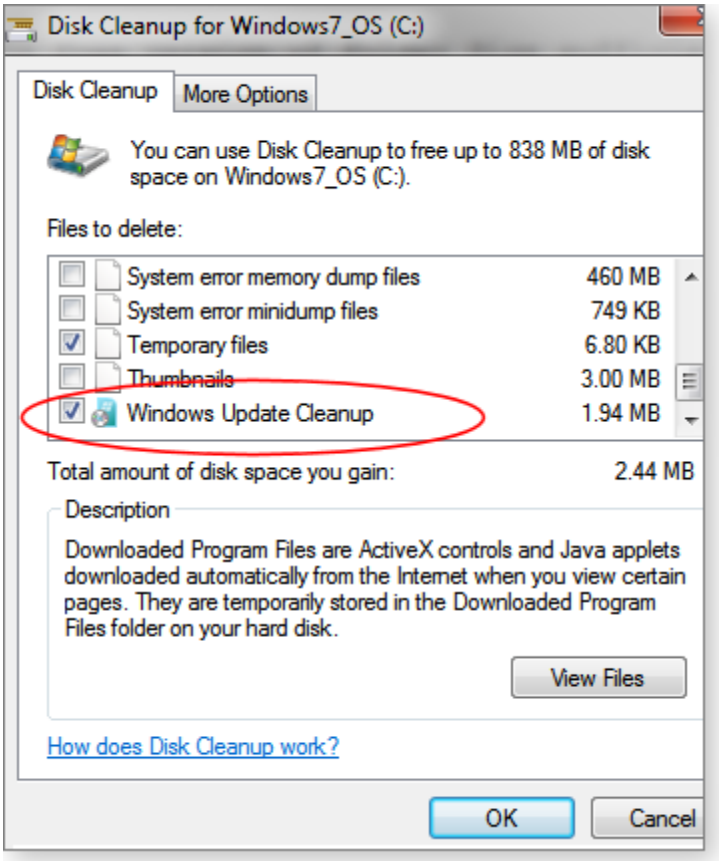

Figure 1. The Windows Update Cleanup option appears only when you run Disk Cleanup as an administrator.

If you want even more aggressive cleaning, select the More Options tab in the Disk Cleanup wizard and click the **Clean up** button in the "System Restore and Shadow Copies" section. But doing so might make it more difficult to restore your system to a previous configuration.

(Remember to empty the Windows trash after completing your various cleaning tasks.)

Find where the really big data files are hiding

That takes care of Windows' garbage. Now it's time to take out yours. This is a longer and more challenging job. Windows can figure out what files it no longer needs, but only you can decide which documents, photos, videos, music, and so forth you no longer want to keep. Fortunately, there are tools and tricks to make the task easier.

To get the biggest bang for your buck, start by going after the really big fish. Deciding whether to delete a 2K file takes as much time as deciding whether to delete a ***2GB*** one. The same principle applies to folders. A bulky folder will have either big files or a bunch of little ones.

To remove big files and folders, you first have to find them. There are numerous apps that can sort out your files and folders by size; TreeSize (site) is one popular app. I like Folder Size (download site), a handy little program that shows which folders are taking up the most space. Then, with a click, it can show the sizes of files and folders inside a selected folder.

I find the free version of Folder Size sufficient for my needs. You can choose to buy the more feature-filled Personal (U.S. $25) or Professional ($40) versions. Check the comparison page.

Folder Size can be launched like any Windows program; you can also right-click a folder or drive in Windows/File Explorer and launch it from there. After scanning the drive or folder of your choice, it displays — among other things — a pie chart of the higher-level folders such as Users, Windows, and Program Files. Click a wedge, and the chart displays the folders inside that folder (see Figure 2). By repeatedly clicking wedges, you can quickly drill down through folders to specific files. Pressing **Ctrl + E** opens a selected folder in Explorer.

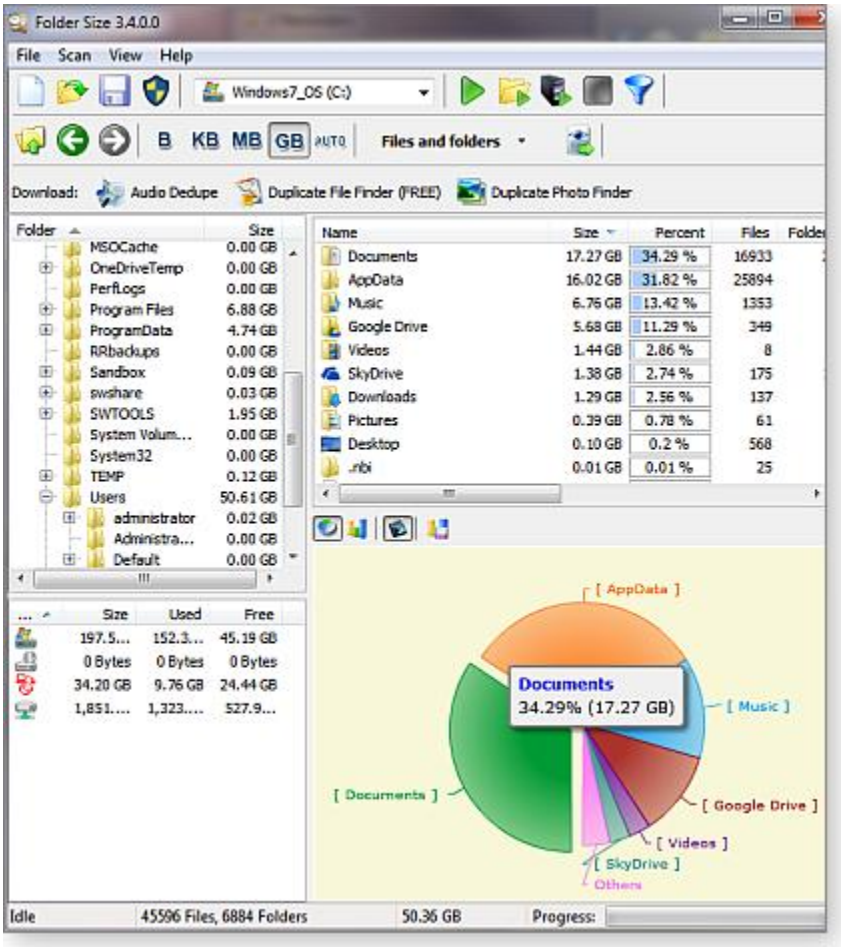

Figure 2. Folder Size offers several ways to find files and folders that are using the most disk space.

While working with Folder Size, you might want to give particular attention to the folder connected to your Dropbox, OneDrive, or other cloud-storage account — especially if you're using the service's limited free option. You really want to keep that folder small.

Do you need two (or eight) copies of that file?

There are instances when you might want multiple copies of a file, but in most cases they are simply unintended duplicates of the original. Over time, you can accumulate hundreds or even thousands of duplicate files.

It's a nearly impossible task to manage manually; you need software for finding duplicate files quickly. I use Duplicate Cleaner (download site). As with Folder Size, the free version fits my needs. A professional version costs $30; check the comparison page for what options each offers.

Duplicate Cleaner's heart is the Search Criteria tab, where you define what sort of duplicates you're looking for. In that tab's upper-left corner, you'll find another set of three subtabs. The first, **Regular**

Mode, lets you control the basics of what makes two or more files duplicates. I recommend selecting **Same Content** and leaving everything else unchecked. That way, you'll get every instance of two or more files that are truly identical — even if they have different names.

The Image Mode tab is disabled in the free version, so I'll skip that one. But as you might assume, you'd use it for finding duplicate photos. The **Audio Mode** searches for duplicate songs via metadata tags. You can, for example, search for songs with the same or similar artists and titles. The "Similar Artist" option (see Figure 3) would recognize that "Beatles" and "The Beatles" are the same group. But remember that two MP3 files of the same song, by the same artist, aren't necessarily the same recording. For example, I have three separate recordings of Bruce Springsteen singing *Badlands*, and I want to keep them all.

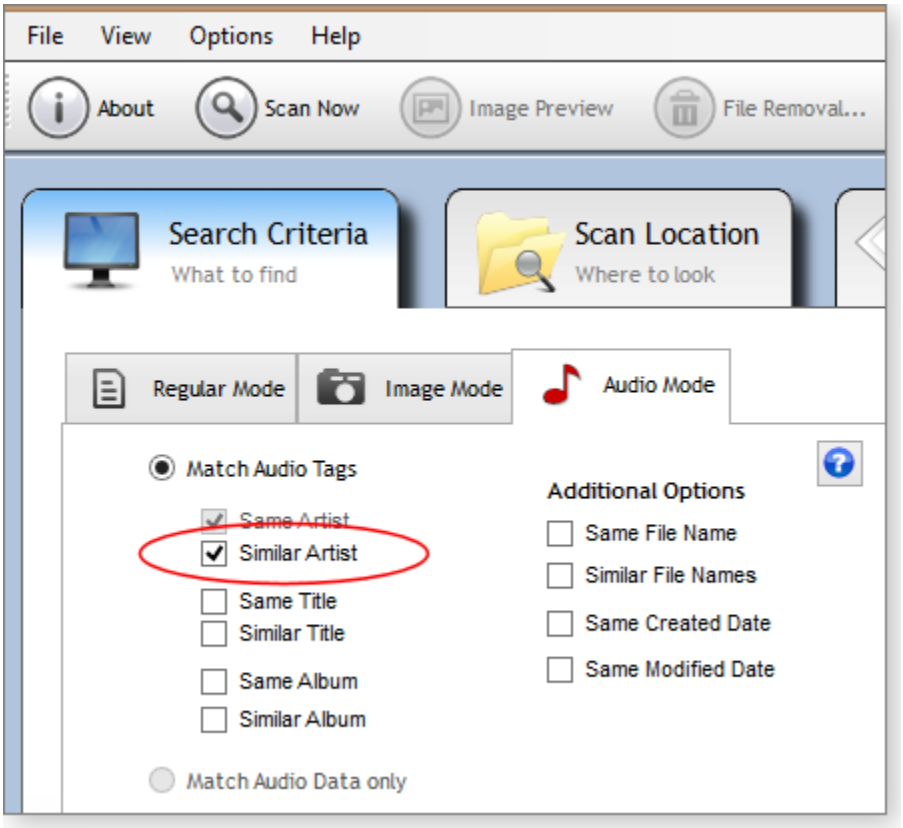

Figure 3. Duplicate Cleaner's Audio Mode flags possible duplicates by examining file metadata.

The other items on the Search Criteria tab are generally self-explanatory. However, there's one I want to call out: File Sizes. Remember my advice to go for the big fish? By setting a minimum size, you can filter out the small files that waste more time than space. With Files Sizes off, Duplicate Cleaner turned up 5,814 sets of duplicates. Scanning with File Sizes set to a 3,000KB minimum, Duplicate Cleaner found only 175 sets of duplicate files. Setting the option to 20,000KB pushed the number down to 15.

Once you've selected your choices on the Search Criteria and Scan Location tabs, you click the Scan Now button on the toolbar and wait for the results. Those results are listed in the Duplicate Files tab. (The Duplicate Folder tab is disabled in the free version.) Here, you examine duplicate-files sets: double-clicking a file opens it, right-clicking pops up various options. If you want to delete a file, simply check it.

The Selection Assistant offers tools for bulk-file selection, but it think it's safer to work through the file sets one at a time. When you're done, click the File Removal button on the toolbar to bring up the various deletion options.

All the files that fit. Follow these directions, and you'll have more free space on your drive. Better yet, you'll have disposed of old, duplicate, or otherwise unwanted files.

Was that enough to give your hard drive some much-needed headroom? If not, it's probably time to pull out the credit card and buy a new drive. Depending on your needs, it might be an external USB drive, a networked drive, or an upgraded internal disk. I'll cover these options in a subsequent article.

Keep this in mind: Storage prices, even for SSDs, continue to drop. If cleaning out your current drive today postpones the inevitable upgrade for months or a year, you might save some money.

UDF vs ISO: Why won't my CD-RW work in Another PC?

By Dennis Faas on February, 20 2015 in “Infopackets.com”.
Infopackets Reader Philip S. writes:

" Dear Dennis,

I use Windows XP and I often write my data to CD-RW (CD rewritable) discs. The problem is that some computers won't read the discs that I've created, whereas others will. I'm pretty sure the problem has to do with the format I'm using when I create the disc, but I'm not sure how to tweak the settings so that the discs are compatible on all computers. I am currently using Windows XP and Explorer to write the discs, using UDF format. Any ideas? "

My response:

You're correct -- the problem is with the UDF disc format and / or the way that you are creating the disc. When it comes to creating a CD or DVD and having the best compatibility possible (whether you're using music CD players, DVD readers, or computers to read the discs), the ISO:9660 or "disc at once" format wins hands down.

UDF vs ISO: A Quick Comparison

The ISO:9660 format has been used since 1988 whereas UDF has been around since 1995 and continues to be revised. In short, UDF has a number of revisions and newer formats may not be compatible with older operating systems.

UDF is extremely convenient because it supports **packet writing** and because it is built into most modern operating systems. In other words, you can drag and drop files to a CD or DVD whenever you want, and it writes data to the disc "on the fly".

The downside to using UDF is that the disc format may not be compatible on other systems, plus UDF isn't supported on many CD and DVD players (especially older hardware). If a computer can't read a UDF disc, you might be able to get around the issue by downloading and installing third party UDF reading software. At this time I am unaware of freeware UDF readers for Windows with up to date specifications. Anyone reading this article is welcome to chime in with suggestions.

In comparison, the ISO:9660 "disc at once" format, or "DAO" is compatible with virtually any device including CD (music) readers, and DVD (video playback) readers, and all operating systems.

The downside to using ISO:9660 format is that you might need third party software to properly write an ISO (you can use **CDBurnerXP** -- it's free). Also, you will need to write the entire contents of the disc in one go, which means it requires some planning, is not convenient, and may result in wasted media. Another ISO format supports writing multi-sessions (meaning you can write more than once to the disc) but this format is not as compatible at the disc at once method (especially for CD readers), plus it eats up memory on the disc every time you write a new session.

Further Reading

This answer only scratches the surface of the topic. If you want more reading, please review the **ISO:9660 format**, **UDF format**, **ISO:13490 (multi-session) format**, **a comparison of various CD formats**, and **reasons why UDF doesn't always work (especially with Windows XP)**. Or you can take my word on the topic, and just write an ISO disc at once.

Windows 7 Mainstream Support Ends

By John Lister on January, 15 2015 in “Infopackets.com”.

As expected and according to Microsoft's Windows lifecycle page, **Windows 7 mainstream support officially ended** on January 13, 2015. It means there will be no more significant updates to the Windows 7 operating system, other than security updates.

The end of mainstream support is in line with Microsoft's general policy of offering support for its operating systems five years after being released, followed by extended support for a further five years.

The only exception to this policy was Windows XP, where the total support period lasted for 13 years. That was largely because the system remained popular much longer than expected, thanks to the lack of interest in Windows Vista.

No More Windows 7 Service Packs or Free Support

So what does Windows 7 "end of mainstream support" mean?

In short, it means that Microsoft will no longer add any major, new features to Windows 7, and there will be no more service packs released to the public. However, Microsoft will continue to issue security updates and bug fixes free of charge for the rest of the extended support period. That's fortunate as the most recent figures suggest more than half of all PC users are currently running Windows 7.

Microsoft's free support for Windows 7 will also end. Consumers will no longer be able to get any support through phone lines or live chat; instead they will have to rely on Microsoft's website help databases or by using third party websites and solutions.

Business users will be able to choose from a selection of paid support options, which includes paying by the case, or by the hour. For the next 90 days, business users will also have the option to subscribe to a "hotfix" program that can automatically update any usability bugs without the need for IT staff to intervene. Security hotfixes, where issued, will remain free of charge for both businesses and consumers. (Source: **microsoft.com**)

Windows 7 Security Updates Should Run For 5 More Years

As things stand, the extended support period for Windows 7 is scheduled to end on January 14, 2020. Microsoft's policy says the extended support period runs for five years, or until two years after the next-but-one system is released, whichever is later. (Source: **microsoft.com**)

Given that this next-but-one system (Windows 10) is expected to be released some time this year, it's almost certain that 2020 will indeed be the final deadline. Microsoft will be hoping that's enough time that Windows 7 will no longer be widely used. That will save a repeat of the XP dilemma where Microsoft faced the unappetizing prospect of switching off security updates for a system that millions of people still used.

THAT'S ALL FOLKS!