COMPUTER NEWS from the

JUNE 2018 Volume 6 NO. 6

As found on the web and other sources

Windows 10 Update: Here's What's New

By John Lister on May, 1 2018 in “Infopackets.com”.

Microsoft has released the latest major update to Windows 10 for 2018. The main changes are most useful for people who do a lot of work on their PC, particularly if they use multiple computers.

The update is part of Microsoft's new approach to evolving Windows 10. It continues to issue monthly security fixes, but has dropped the old approach of issuing new features as and when they are ready, then rounding them up in a 'service pack' every year or so before eventually moving on to the next version of Windows.

Instead, the idea is to never have a completely new version, but rather to add new features to Windows 10 around twice a year. Previous major updates have had titles such as the 'Anniversary Update', 'Creators Update', and 'Fall Creators Update', but this time round Microsoft is coming straight to the point by calling it the 'April 2018 Update'.

Timeline Makes Searching Past Month Easy

The most prominent addition is a feature called "Timeline" that aims to make it easier to find information from your activity over the past 30 days. It's designed to be a much simpler and more intuitive alternative to having to use the Windows Explorer search tool to look for files by modification date. (Source: windows.com)

Timeline covers all the files and folders you've worked on or created during the past 30 days, including on multiple computers if you use the same Microsoft account on each. It also brings in activity from the Edge browser and the Office 365 tools on mobile devices, including Android and iOS machines. It's an interesting move as it's very reminiscent of Google's approach which brings together data from your activity on computers, tablets and phones alike.

Another new feature is called Focus Assist, which will be most useful for people who have a lot of notifications and tiles activated on their Windows Desktop. Users can now either switch on Focus Assist for a set period or schedule it in advance. While it's turned on, notifications and other distractions are hidden. When it's switched off again, the user gets a quick summary of the information they missed.

Edge Browser Slowly Improving

There's also a few additions and improvements to the Edge, albeit ones that are standard in many rival browsers. These include a one-click icon to mute sound on a web page, auto fill on web forms, and an option to automatically format and clean-up a page for printing.

Perhaps the most welcome change to Windows 10 involves notifications from the Windows Defender security tools. Users can now set their computer to only tell them when there's a problem, rather than have a message pop-up after every scan even if everything is fine. (Source: theverge.com)

What's Your Opinion?

Does Timeline sound useful? Would you benefit from Focus Assist or have you switched off notifications anyway? What new features would you like to see added to Windows 10?

Tim Berners-Lee: 'Beware the weaponised web'

Pioneer of the interweb weighs in on the dangers of the corporate web

Tim Berners-Lee: 'Beware the weaponised web'

- By Chris Merriman @ChrisTheD J in “theinquirer.net”.

GODFATHER OF the three-double-yous, Sir Tim Berners-Lee, has warned against creating a 'weaponised' web, laying the responsibility for regulation with the big tech companies.

In a World Wide Web 29th birthday 'state of the union' open letter, he warns that the levels of power wielded by a small group of big names - Google, Facebook, Twitter et al - means that there is a real risk of ideas becoming brandished through concepts like fake news and propaganda spamming.

Berners-Lee points out that these key companies control which "ideas and options are seen and shared" at a key point in history, with the number of people with internet access globally to exceed 50 per cent for the first time in 2018, in line with the UN declaration that using the net is a basic human right.

He points out that these mega-corporations have been left to buy up smaller competitors. The result, he says is that: "What was once a rich selection of blogs and websites has been compressed under the powerful weight of a few dominant platforms,"

He suggests that some sort of regulation or legal framework that takes into account social objectives could at lease ease the issue.

His words come in the wake of the now recognised phenomenon of the often unwitting spread of misinformation by Russian actors during the US election.

He also points out that we need to get away from the idea that advertising in the only possible business model, branding it a myth. The second myth is the idea that it's ‘too late now' for existing platforms to change their revenue model.

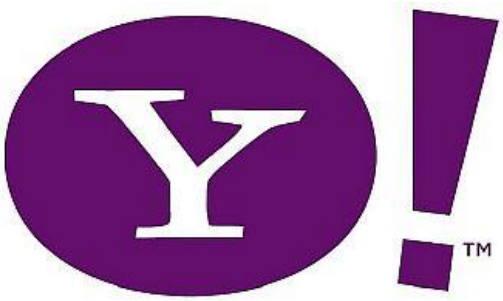
On the subject of the 50 per cent milestone, he warns that we need to concentrate now on the other 50 per cent.

"To be offline today is to be excluded from opportunities to learn and earn, to access valuable services, and to participate in democratic debate," he warns. "If we do not invest seriously in closing this gap, the last billion will not be connected until 2042. That's an entire generation left behind."

Yahoo Users Must Waive Class Action Rights Or Stop Using Service

From “Gizmo’s Freeware

Last updated by rhiannon on 26. April 2018 - 19:19



I

If you use any of Yahoo's services, especially Yahoo email, you'll be giving up any class action rights if you continue to use Yahoo services and agreeing to a privacy policy that allows your email to be analyzed and stored.

Yahoo had a data breach that involved most (if not all) of Yahoo email accounts in 2013, although the breach didn't become public knowledge until 2016. Verizon subsequently purchased Yahoo. In March of this year, a U.S. judge ruled that victims of the data breach can sue the company in the US.

Now, Verizon is requiring people who use Yahoo services to waive any class action rights and agree to settle disputes through arbitration, and has a new privacy policy impacting email users that allows Verizon to "analyze and store all communications content, including email content from incoming and outgoing mail. This allows us to deliver, personalize and develop relevant features, content, advertising and Services."
The privacy policy doesn't let users opt out of targeted ads.

More details are at Ars Technica

More details are at Ars Technica If you're looking for more privacy and security in a free email service, have a look at these two services:
Two Free Encrypted Email Services You Might Want to Use

SPEECH 2 TEXT
TCC reader Rodney Iwan sent this to me although I haven't tried it I thought I would pass it on.

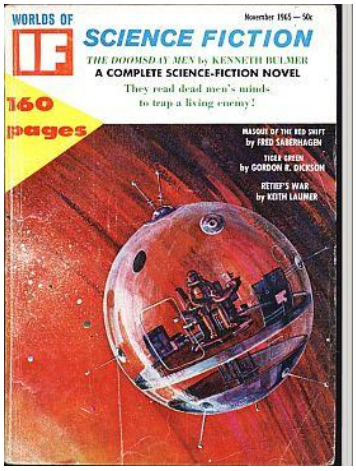
I have just been playing around with "speech to text" programs and have found one that is quite good. I thought you might want to pass the source along to anyone interested. It is www.speechtexter.com. It takes a bit of playing around to learn how to use it but I am very impressed by its accuracy and versatility. It is also easy to edit, add or delete to and save or print out. Rodney

---

Find something to read as you J Walk into the path of a truck!

Read 11,000 Pulp Magazines Online for Free

Posted: 05 Apr 2018 03:22 AM PDT



Pulp magazines (also called Pulp Fiction) were published from 1896 through the 1950's. The Pulp Magazine Archive has digitized 11,120 pulp magazines that can be read online and is made available by the Internet Archive, a non-profit library of millions of free books, movies, software, music, websites, and more.

There's a wide variety of titles including Weird Tales, Worlds of IF Science Fiction, True Detective, Witchcraft and Sorcery, Captain Billy's Whiz Bang, True Story, Adventure, and several more.

Titles are viewable by thumbnail or list, and can be sorted by title, date published, date archived, date reviewed, or by creator.The search options are pretty extensive, you can search text or metadata, by year, by topic and subject, collection, or creator.

Reading the magazines is easy, visit the site, click on a title, and the magazine opens in a dual page mode. Click on either page of the magazine to go forward or backward a page. Under each magazine there's a complete list of information including the title, content publication date, page count, collection, and other identifying information.

In keeping with the niche that pulp magazines occupied, some of the covers or content might not be safe for work or children. The science fiction titles are fine, and you'll find tales by Isaac Asimov, Poul Anderson, Arthur C. Clarke, H. G. Wells, Theodore Sturgeon, Fritz Leiber, Larry Niven, Orson Scott Card, Clifford D. Simak and more. Other titles have differing levels of content. ***Read More***

Time To Ban Caller-ID Spoofing (Again)?

Category: Telephony From “askbobrankin.com”.

Your phone rings, and a quick glance at the area code helps you decide to answer the call. But instead of a forgotten friend or a local business client, you get “Heather from Account Services,” offering to lower your credit card interest rate. Again. Just like yesterday. And the day before. Here's the scoop on what you can do about this annoying problem…

Should You Answer That Call?

The phone is ringing again. If the area code was one of the toll-free kind (800, 833, 844, 855, 866, 877 or 888) you would never have answered. By now you've learned that nothing good comes from a call made from a toll-free number. After all, toll-free numbers were created for YOUR convenience, so you could contact businesses without incurring the cost of a long-distance call.

Had it been from the Washington, DC, Area Code, 202, you would not have answered yet another fundraising call from your dully (sic) elected Congresscritter. Similarly, a call from the 702 Area Code may mean only that you left your toiletries behind at the Days Inn in Las Vegas.

But in the past year, I've been getting several calls a day that show the incoming number matching not only my area code, but also my local exchange. Ordinarily, that would mean a neighbor calling. But thanks to software that lowers the technical barriers to Caller-ID spoofing, it could be a telemarketer in Toledo, Tacoma, or Timbuktu.

And increasingly, I am getting calls that display only “PRIVATE” instead of a name or phone number. I don’t answer such calls, and if the caller does not leave a voicemail message I will not call back. This seems like a simple, obvious solution to telemarketers who hide behind “PRIVATE” phone numbers. But it has a certain medical practice up in arms.

There is a local doctor who thinks the entire world must conform to his office practices. His phone system sets all outgoing calls made by his staff and his auto-dialing appointment reminder to “private.” Patients who block calls from “private” numbers, as many people do, don’t get important calls from staff or the nuisance of yet another reminder they don’t need. This doctor tells patients that they must unblock all calls from “private” numbers or find another practice. So I found another practice.

Black, White and Gray Areas

If telemarketers are driving you nuts, there are some tools you can use to eliminate most of those calls. See my article Need Robocall Relief? Here's How to Fight Back. If you want to take it one step further, see my article on How to Sue a Telemarketer.

Another medical practice spoofed its caller-ID, sending me the number 555-555-1212. That number is so obviously fake that I blocked it instinctively. Then I got irritated because my doctor’s office was not returning my phone calls. It took two months to figure out why. I came very close to "firing" that doctor, too. I am sure I know how it happened.

An office staffer drew the short straw and the task of “programming” the new office phone system. She followed the system’s voice prompts to set things up. When it asked her for the number to send for caller-ID, she thought to herself, “Hmm... I don’t want to send our real number for patient privacy considerations. So I’ll just make one up: 555-555-1212.”

I am not a lawyer, but it seems to me that if a patient signed a form indicating that he wants you to leave all the details of his test results on his voicemail inbox, then he is not at all concerned that a passerby might catch a fleeting glimpse of a phone number and remember that it belongs to a certain medical practice. So “patient privacy considerations” are absurd, in this case. There is no good reason for your doctor to spoof caller-ID data, let alone set all outbound calls to “private.”

As you can see, the Caller-ID spoofing world is not neatly divided into good guys and bad guys. There are plenty of good guys who would call home before battle but would have to do it while disguising their identities. There are plenty of office staffers who don't think through their cunning plans. So when we debate whether to ban caller-ID spoofing, there is a lot of grey area to discuss.

Will New Laws Solve the Problem?

Kathy Afzali, a politician who represents Carroll and Frederick counties in Maryland, got a taste of caller-ID spoofing that alarmed her. "You should not be able to masquerade as someone familiar or safe to someone on the other end," Afzali said. Researching federal law on caller-ID spoofing, she found it has gaping loopholes.

That federal law is called, appropriately enough, The Truth in Caller ID Act of 2009. It authorized the FCC to come up with and enforce rules that prohibit any person or entity from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongly obtain anything of value.

Well, that lets our medical people off the hook, and a lot of bad guys. Any time a prosecutor has to prove "intent," he will back away from the case because it's nearly impossible to prove what someone else was thinking. In practice, caller-ID spoofing won't be prosecuted unless actual harm can be found that has been done to consumers. And annoying you a dozen times a day doesn't quality as "harm" in a legal sense.

Afzali's bill, which would apply only in Maryland, eliminates all of that "intent" wiggle room, and all exemptions and excuses. It's probably flawed, but it's at least a start at addressing a problem that vexes nearly everyone with a phone. Perhaps it will serve as a model for other states to adopt similar legislation, and one of them will get it right. That's the beauty of our "laboratories of democracy" in the USA.

But as we all know thanks to "Heather from Account Services" and her legion of clones, the existing federal law has not stopped caller-ID spoofing. It's not as if the FCC has not been trying, though. Penalties of up to $10,000 per violation can be assessed if someone is found to violate the spoofing law.

In August, 2017, the FCC proposed a fine of more than $82 million against a man who made more than 21 million robocalls with false called-ID data. He was trying to sell health insurance. In June, 2017, the FCC proposed a fine of nearly $120 million against a man who caused nearly 100 million robocalls with false caller-ID data to be made.

These cases and others like them are all subject to civil asset forfeiture rules. Just about any assets that may have been obtained with or used to obtain the fruits of a crime can be seized and sold by the federal government. Whether these guys have assets worth anywhere near their fines remains to be seen. But it's a start.

For now, the best defense is a combination of common sense and technology. Tools like the ones I mentioned in my article on fighting robocalls can help to weed out the spammers and scammers. For those that calls that do ring through, I recommend that you answer only calls from numbers you recognize. Voicemail is your friend. Unless of course, you enjoy toying with the telemarketers.

Your thoughts on this topic are welcome. Post your comment or question to "askbobrankin.com".

Question of the month!

CAN VEGETARIANS EAT ANIMAL CRACKERS?