For your safety, turn on the auto-update feature for all your devices and applications

Software update is a 'headache' issue. Speaking of headaches may seem a bit too much, but actually updating the software gives them no trouble in many situations.

Earlier this week, Google announced that it had successfully patched a dangerous security vulnerability that appeared on Chrome - the world's most commonly used browser, and deployed the patch as a small update. Not only that, the search giant also confirmed that hackers have been actively exploiting this bug, along with another error found in Windows, causing some unfortunate damage to users.

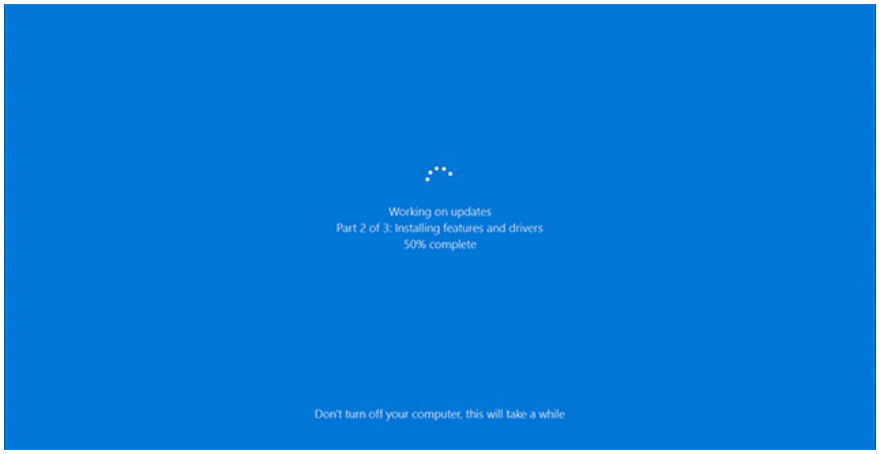
Soon there was a wave of announcements calling for people to update Chrome to the new version immediately. Although it is urgent and important, but not everyone has access to this notice, which leads to many people still at risk of becoming victims of hackers just because they do not know the patch. New security is deployed. However, luckily, the worst scenarios didn't happen thanks to the efficient operation of Chrome's auto-update feature, which made it possible for most users of the browser to have access to the patch in a timely manner. New security before unfortunate incidents occur.

1. Post-MWC 2019: 5G has a long and tough road ahead

Through the above situation, we partly understand the necessity of updating the software. However, things are not so simple in reality. Software update is a 'headache' issue. Speaking of headaches may seem a bit too much, but actually updating the software gives them no trouble in many situations. MacOS users are no stranger to the type of software update spam reminder wherever it is. Or for Windows 10 it is worse when it often forces you to update and restart the system at the most 'unexpected' times, not to mention the new updates of Windows 10 often contain dozens of errors, making Microsoft have to re-release several times to fix the problem.

However, temporarily putting those troubles aside, we all know that keeping our system up to date is the simplest way to protect you from hackers. , and at the same time activating the auto update feature is also the

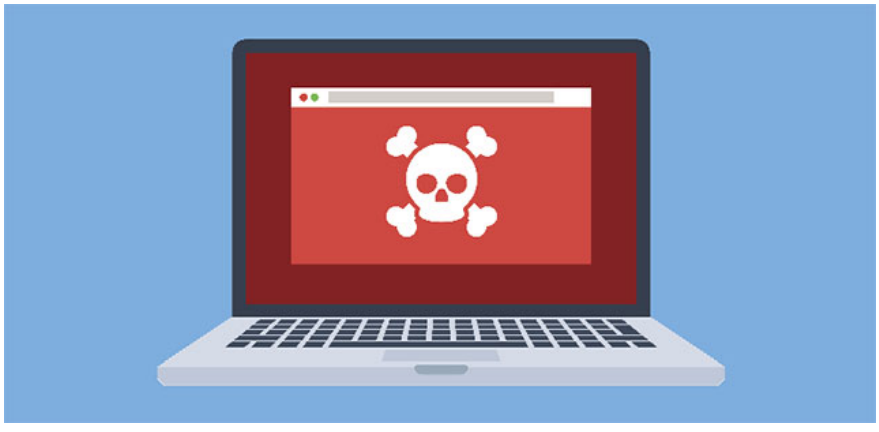
best way to ensure that you don't miss any patches. Jérôme Segura, head of cyber security intelligence at Malwarebytes, said: 'As a security expert, I strongly support that updates should be deployed and installed. set automatically, especially for font spectrum users, because these people don't always know the current security threats and patch information. '



1. Things on Windows 10 make users disappointed

For example, the case of zero-day vulnerability has recently appeared on Chrome (has just been patched), instead of giving a forced notification showing a tab on the browser to remind you about installing a new version. - which can make many people uncomfortable and click skip as a habit, the Google team has a much less "unobtrusive" approach, which is silently let the update be Fully automatic installation. Well, it seems that this measure is quite positive. Although in this case, users still have to restart the browser to apply the changes of the new version because this is a vulnerability targeting Chrome code rather than a plug-in like Flash, but the method This method of silent and automatic software update is obviously more effective, as evidenced by the fact that the number of Chrome users has been updated to the new version.

'My impression of talking about software updates is that most people do not care too much about security, instead they usually only pay attention to what is new or not, if not not yet updated what to do. However, this habit is completely wrong. In fact, security is one of the most important factors contained in an update, 'said Josiah Dykstra, technical director at the US National Security Agency (NSA).



1. Never upgrade the operating system from the first day

Of course there are some obvious exceptions here. Updates in medical or industrial systems cannot be blindly applied, because simply any unintentional error can lead to disaster with tremendous damage. Besides the case of people who trust their software, security researchers, etc. Those are situations where updating the new version automatically is often not a welcome idea. .

But for subjects, smaller systems like smartphones or laptops? In this case, it can be strongly asserted that automatic updates will bring more benefits than harms. But saying so does not mean that you must fully accept all risks that may be caused by automatic updates.

'Publishers need to do better, more effectively in checking and reviewing patches before launching. And also must immediately provide a rollback option to the end user when a problem occurs'. That is shared by Gene Spafford, a computer scientist at Purdue University and a famous cyber security researcher, in an essay written last year about so-called cyber security is disappearing (disappearing cybersecurity). A mechanism like Gene Spafford suggests may help quickly undo an automatic update in the worst situations, instead of having to wait for the publisher to fix it and then send the additional patch as it is now. now on.

At the present time, Windows 10 has been equipped with the automatic update feature by default. Apple also provided this option for the first time in iOS 12, but you have to confirm it before you want to join. To do so, navigate to **Settings> General> Software Update> Automatic Updates** and enable this feature. For Android, and at the same time with all apps on Android, the software auto-update feature will depend on the device you are using, but in general, you will still have to wait until you get the message. reported that the update is ready to install.

1. Windows is not a service, it's just an operating system, don't update it too much like that!

And for the internet of things - the 'Wild West' of the technology world, many IoT devices are not only equipped with automatic updates, but even manual software updates. There are many problems. This is really a sad fact, because there are no devices that benefit much from continuous improvement and updates over IoT devices. This is a very interesting issue. If IoT devices are not patched for security vulnerabilities in time, the damage will be very serious, on a large scale because of their nature of being interconnected and synchronized.

1. 6 things to know about IoT security

The good news is that our vast consumer technology industry seems to be starting to pay more attention to the implementation of automatic updates, although as mentioned, security benefits are one thing. It is difficult for publishers to show to consumers:

'If users actually see the value in automatic updates, they tend to only see value in product stability for features, rather than on security issues'.

This will still be a long way, requiring effort and change from both the publisher and the user.