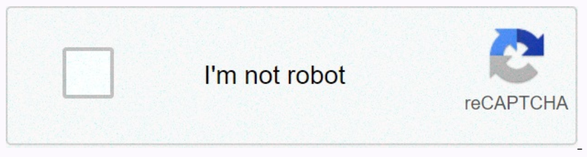

Continue

Turnitin software for pc

Geosense appears as a location sensor in the Location and Other Sensors panes in Control Panel. It would be really crazy to put a GPS sensor inside your desktop (unless maybe you're sporting one of the super small media nettops). But what if you want to enjoy the benefits of geolocation of mobile devices in your station that don't move much without the hassle of adding new hardware? Geosense for Windows 7 you've covered. Geosense leverages Windows 7 support for geolocation sensors. It uses a combination of methods to calculate your location without GPS; this includes Wi-Fi triangulation, mobile signal triangulation, and IP address search. The information it collects can be used in any application that uses geolocation data. What does that mean? For starters, it could eventually mean that you don't have to enter your location manually when searching for directions. You can also add location information on your desktop to popular social networking services like Twitter, Gowalla, and FourSquare. Of course, privacy concerns will be your full responsibility. At least on your phone when you broadcast geolocation information, it may be out of date when you move from place to place. But if you tweet about your new Samsung 3D HDTV and your location, I hope you also bought a guard dog when installing Geosense. Also, until now there have been very few Windows applications that can take advantage of geolocation, although Geosense sites link to several examples (including the Windows 7 weather gadget). Firefox 3.5 or later has built-in geolocation capabilities. Nonetheless, if you keep your head fixed and broadcast your location information responsibly, Geosense can make your desktop computing experience more efficient and interactive. Follow GeekTech on Twitter or Facebook. No geolocation required. Jaruwan Jaiyangyuen/Shutterstock Unlike other types of malware, you can't just clean up the ransomware and get on with your day. Run-of-the-mill viruses won't destroy all your data and backups. That's why ransomware is a danger you need to prepare for in advance. If you don't run ransomware protection, says Adam Kujawa, director of Malwarebytes Labs. If you haven't secured your backup before, then you're really out of luck. Are you at risk? Sure, ransomware attacks can be bad, but not all hazards carry the same level of risk. For example, a killer asteroid strike is a known danger. Should we spend trillions of dollars building defenses against threats that only occur once every 100 million years? Not necessarily, because the actual risk of impact is quite low. So when it comes to ransomware, you should consider what your level of risk is for permanent data loss. Part of your risk assessment is how ready you are for the attack. There are a few things you can do to make your data relatively secure. Because ransomware can and will encrypt any file found on the PC or connected network, select select solutions that don't make your files accessible. One such solution is water gapping your backup drive, which means it doesn't connect to your PC or network constantly. Another option is a backup tool that uses versioning, so you can recover the version of your file that preceded any disaster. If you have a secure and isolated backup, ransomware attacks may be a hassle, but you can shake them without too much trouble. Combined with common sense precautions, such as not clicking on links you do not trust, these are all fairly standard computer hygiene. There are also some easy ways you can add ransomware protection to your PC without installing other security programs. Your existing antivirus plan may already offer protection. For example, if you use Windows Defender, the default antivirus of Windows 10, it has some built-in ransomware protection, but it is turned off by default. If you enable Windows Defender Controlled Folder Access ransomware protection, the software protects public folders, such as Documents and Pictures, from unauthorized changes. If a ransomware app can't access your Documents folder, it can't encrypt your files—game, set, match! There are also free apps, such as RansomBuster Trend Micro, that work the same way. Unfortunately, this approach is not easily fooled and can interfere in practice. Many legitimate programs need to access your document folders regularly, so you may have to rival many permission popups. RELATED: Want to Survive Ransomware? Here's How to Protect Your PC Ransomware Is Still a Serious Threat Some experts think the heat is not on home computers. Criminals tend to focus their efforts on victims with deep pockets. The recently published Check Point Cyber Security Report 2020 agrees with that assessment: In 2019, we saw an escalation of sophisticated and targeted ransomware exploits. Certain industries have been severely victimized, including state and local governments as well as health organizations. The headlines in 2019 were filled with stories about these attacks, including successful attacks on more than 70 state and local governments. If you're not a bank or city government, you probably don't have to worry about ransomware in 2020 than you did a few years ago, because today's ransomware attacks are more targeted. In addition, a 2019 study of ransomware trends by RecordedFuture noted the overall number of ransomware campaigns may continue to climb, but the reality is that most of these campaigns are ineffective and die quickly. This is good news for your home computer — especially if you don't want to run other cybersecurity applications. However Not out of the woods yet. It's easy to jump to the conclusion that ransomware is no longer a problem for consumers, Kujawa said. But we know, just based on history, that cybercrimes, tactics are cyclonic. They're back around. Maybe we'll see something that utilizes some of the techniques developed to attack the business and get on the consumer side. Perhaps new exploits are becoming available, or tactics for infections are making better return on investment for cybercriminals to pursue consumers again. Jonny Pelter, CEO of SimpleCyberLife.com, agrees. The volume of ransomware attacks has started to drop, but the attack rate is still high. It's true. CrowdStrike's 2019 Global Security Attitudes Survey documented that the number of victims who paid ransom for last year's attacks doubled from 2018. Of course, this will only make the development and distribution of ransomware by cybercriminals much more profitable, Pelter said. Unfortunately, I am afraid we are entering a period of satisfaction. When ransomware attacks come out of the mainstream media, people misinterpret this as a decrease in the number of ransomware attacks, which is far from reality, unfortunately. RELATED: How to Protect Your Files From Ransomware With Windows Defender's New Controlled Folder Access Ransomware Prevention Software All this means you may be relatively safe in the short term, but it's still a good idea to protect yourself with some ransomware prevention software. Although home computers have been relatively powerless for several years, there are now plenty of anti-ransomware packages you can choose from — both free and paid. Even standard antivirus plans now routinely offer some level of anti-ransomware protection. However, many of these (and most free plans) rely on the same technology traditional antivirus programs do. They detected a software signature known to recognize malware. The downside of this approach, of course, is that it makes you vulnerable to zero-day infections. In contrast, most stand-alone ransomware packages, such as Acronis Ransomware Protection, Check Point ZoneAlarm Anti-Ransomware, and Malwarebytes Anti-Ransomware Beta, detect malware with its behavior. These programs monitor the activity of applications and quarantine processes that take suspicious actions, such as generating encryption keys or starting encrypting files. This makes these programs dramatically more effective at stopping ransomware in its tracks, whether it's known tensions, new threats, or hybrid malware (both viruses and ransomware). And yes, that's a new thing to worry about. We are seeing more malware families adopting ransomware capabilities, Kujawa said. Where previously it might have just stolen some information, now, once that happens, it might redeem your system and ask for money. Whatever method you choose to protect your PC and data, remember: When it comes to ransomware, prevention, and preparation are essential. And the problem may only get worse. As Dis lamented Kujawa: Ransomware was a nightmare in my career. RELATED: Should You Pay If You're Exposed There's a multibillion-dollar business built around the sale of PC and Mac cleaning software. They come in all shapes, sizes and prices and tout the need to clean, tune, and repair your computer so that run smoothly and efficiently. I have even written about many of these programs myself at the Geek Help Desk and Online Technology Tips. But do you really need all that software? Is there a real advantage or just a bunch of feathers? Well the answer is, it depends. Sometimes third-party programs can provide valuable services if you know how to use them. However, I have found that most of the recommended utilities on the Internet are full of options and settings that can ultimately harm your computer more than help. Not only that, many utilities themselves install malware into your system, wreaking havoc. When you talk about cleaning a computer, whether it's a Mac or a PC, it can refer to a number of things. Let's describe what each of those categories is and see if it makes sense to use them or not. Registry Cleaners A long time ago, I wrote 10 typical best registry cleaning articles and basically put out a list of popular and semi-popular registry cleaners without actually explaining anything. What does a registry cleaner actually do? Well, basically (and theoretically) it should remove entries that aren't used or old, thereby speeding up your computer. Even if you only delete unnecessary entries, the performance impact is minimal. If you try to do a search for actual performance tests performed before and after using the registry cleaner, you will find that there are very few actual tests and in tests, there is basically no difference in performance. So that's the first point. The second problem is that many registry cleaners will clean up the wrong entries. The only thing I use and continue to use is CCleaner. It's the only one that won't break your system. There's nothing else I can give you completely. It's best to download the free version to see its benefits first, but the Professional version includes real-time monitoring, automatic updates, and unlimited support, which I recommend on any PC. In the end, registry cleaners can crack your computer, not offer any real performance improvements and waste your time. If you want to speed up your computer, read my article on how to speed up boot time in Windows and five ways to speed up Windows 10. In addition, uninstall useless programs on your system. That's so much more in terms of performance than cleaning up your registry. File Cleaner Is a tool that will do your best to remove junk or files that aren't used on your computer. This includes temporary files, cookies, Windows hotfixes, cache files, history files, log files, clipboard data, etc., etc. In my view, there are only two programs worthy of this that you will ever need: CCleaner and PC CCleaner does a great job of cleaning up files you may no longer need. Again, I've never really saved a huge amount of space from using this tool, but if you really want to be super neat and tidy, that's all you need. On average, I save about 1 GB in space when I run it running it a few months. Not a large amount, but great if you have a small hard drive. You should also read my other post on how to clean up disk space in Windows by adjusting Windows settings. PC Decrapifier is a program that helps you uninstall crap software that comes with a new PC that you bought from Dell, HP, etc. I personally recommend just doing a clean installation first and then using your computer. Here's my guide to doing a clean installation of Windows 10. Uninstaller If you install a lot of software on your PC, you can easily remove it yourself. However, there are whole categories of software to help you uninstall programs. Is this necessary? That's what it is. I personally try not to install anything on my main PC that I won't use every day. If I want to try something or my kids want the game played, etc., I use a secondary machine and install all the garbage. The machine is then removed every few months and starts all over again. I also use a virtual machine and load other software there. If you don't have a second PC or don't know how a virtual PC works, you may have software on the system that you no longer want. Most software will have an uninstaller to delete all the files correctly, but often they leave things behind. In addition, some programs do not come with uninstaller, which is really annoying. In such cases, I only recommend Revo Uninstaller. It's been around a long time and done the best job. It's not free, so I'll only spend money if you have a lot of programs that don't come with the right uninstaller. Otherwise, you can uninstall it and then run CCleaner to clean up old or unfixed entries from those programs. Also, as with most of these tools, it comes with some other utilities that you really don't need. However, it is still OK in my book for some users because deleting programs is not necessarily a smooth experience in Windows. Startup Cleaners Startup cleaner is a completely useless program if you ask me. Windows has a built-in tool to view all the startup programs on your system and there is really no need to see startup drivers, DLL, etc., that some of these programs are touting. Outside of simple programs, it really makes no difference unless you're a tech geek. Many programs claim they will give you descriptions and details about each program and while this may be true, you really don't need a program for that info. Just read my article on how to change the startup program in Windows 7 / 8 / 10, then do Google on any startup item you don't believe in! I definitely don't recommend installing a startup cleaner because it is something that users can do with little time and research. Now, can disabling startup programs make a difference? Yes! Startup programs can really slow down your PC, so it's good to turn off anything you don't think you'll need. Again, this is like a registry because if you disable the wrong items, your computer may not function properly. Just do a little googling before you you something and you'll be fine. Duplicate File Finder Another set of tools is directed to delete duplicate files. I have had many occasions where I copied the same photo or video from my camera and then had a lot of extra space used because of it. Duplicate file finders can save disk space if you have lots of photos, videos, or music that might be duplicated. Also, make sure you don't buy anything. There are many great free programs that can find duplicates, so don't get sucked into buying something just to remove duplicates. Browser / History Cleaner Mostly, you really don't need a browser and history cleaner. You can delete your own history properly and make sure it can't be recovered. Most people end up buying this software because they have some shady browsing that they need to hide and they are afraid that someone will find it unless they use one of these tools that claims only their program can actually delete your browsing history. BS complete. Here are some of the previous articles I wrote about this topic: Clear Google Search History How to Delete and Delete Cookies Basically, you want to clear your browsing history using the browser and clear the cache. That's it. You don't need fancy tools to do that. No one can restore my history. I even tried to restore my own history to see if this was good enough and that. Internet speed booster Internet speed booster is another category of useless software that you should not install. These programs are more likely to disconnect your Internet connection or slow it down more than speed anything up. Do you want a faster Internet connection? Get a faster wireless router, clean up interference on your wireless network, and increase your Wifi signal. There are several occasions where changing some TCP or network settings can speed up the write/read performance of files over the network, but that is usually for LAN traffic and not your Internet connection. Contact your ISP and increase your download speed, but don't install the speed booster! Conclusion as you can see from above, I do not recommend installing too many so-called optimizer and tune-up utilities for your PC. There are some good programs out there, but the majority suck. Try to do as much as you can yourself and then just use a trusted program as I mentioned above. What do you think about cleaning utilities? Are you using anything? Enjoy! Enjoy!