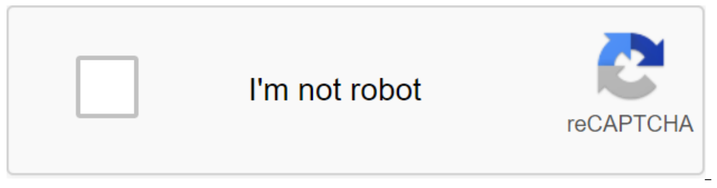

Continue

Elevate science grade 8 answer key

ConferencesThe huge social cost of every wasted moment in the search for a CURE-19 treatment unleashed an unprecedented wave of data sharing and other collaborations between pharmaceutical companies. TagsBrainstorm Health 2020coronavirusCOVID-19pandemicBristol Myers SquibbVasant NarasimhamNovartisGiovanni Caforio In a recent post, I recommended Panda Cloud Antivirus as a decent free antivirus program. Others have recommended different programs, and that's fine - after all, I don't think there's much meaningful difference between the various antivirus programs, at least in terms of security. Much more important than the antivirus software you use (or anti-spyware, or firewall, or any security software), or even if you use one at all, are practices that make up your online behavior. People who do risky things online will sooner or later get a virus, no matter how good their security software is. On the other hand, many security experts do not use antivirus software and still manage to avoid viruses. I don't recommend you follow in the footsteps of security experts - the nature of their call requires a kind of paranoia that few of us can support. I recommend a solid security software package (I run Cloud Antivirus and Windows Defender), but only as a safety net - something to pick up the slack when we make mistakes rather than the first line of defense. The thing with security, online or anywhere else, is that it is always a trade-off between protection and convenience. I can tell you how to absolutely avoid the risk of computer virus, spyware or trojans: stay offline and never install anything or use any removable storage tools. This is 100% ideal protection, but it will make it very difficult to use your computer. It's like securing a house: You could build a door less, a window-less titanium shell reinforced concrete bunker around your house and be absolutely sure the burglars couldn't get in, but you probably wouldn't want to live there. Below are tips to consider all but the most emphatic attacks on your computer. No amount of software or behavioral change can protect you from all possible attacks (if the NSA wants to get on your computer, they're probably going to do it), but you can protect yourself from virtually every attack you're likely to encounter online. I owe thanks for most of these tips to Leo Laporte and Steve Gibson, the hosts of TWiT netcast security now. If you are interested in computer security on a very deep level, this weekly show is your ticket and I heartily recommend it! Itself routers act as an effective hardware firewall, preventing computers from accessing computers on the home network from outside the network. Simply put, when you request something from the Internet - say, you click on a link, check your email or enter a URL - - the router notes which computer on the network a request has received to send a response to the desired recipient. If an attacker tries to log into your network, the router checks its list of outgoing queries and if there is no correlation with the attacker's IP address, it ignores it. He basically doesn't know which computer to send it to, so it throws it away. If you just can't use a hardware router, make sure your operating system's firewall is on. It's almost, but not quite as good. Don't open email attachments. I know someone who doesn't want to see pictures of Anna Kournikova naked, right? Email attachments are the main vector for infecting computers because it is so easy to fake the sender to make the email look like it came from someone you know and everyone loves opening attachments from people they know. It can be a funny picture of penguins, after all. But don't give the attachments at 7 p.m. If your email client automatically opens or views them, turn it off. Even if it's from your mom, and even if your mom says she opened it, and it's all right, don't open it anyway. (By the way, the next time you're at your mom's, reinstall Windows. Now, I know that sometimes you have to open attachments, so here's a simple test to know when it's most likely safe to open an attachment: You know what email from the person he says it's from. This usually means that either they said they were sending it, or they wrote a note that only they could write. You expect affection from this person. You know the person who created the file. There is a good reason to open an attachment. I'm sorry, Mom, but a good laugh isn't enough to make me risk the security of my computer. If you can't be absolutely, 100% sure of all these counts, trash it. 3. Don't download bittorent files. It sucks, I know, but since you're never absolutely sure where the file came from, where it was, or who might have changed it, bittorrent is risky. Downloading the Linux distribution from Ubuntu is probably FINE; Downloading it from Pirate's Bay is a bit dodgy. Downloading Oscar screeners movies that haven't yet been released super-duper dodgy. It's a real shame to stop sticking it to the man because of practical problems, but you take the big risk of downloading an unknown file from an unknown person about which the only thing you know is that they don't feel any remorse about breaking the law. 4. Do not download warez, or other questionable files. First they came for my bittorents, then they came for my porn! It's getting worse and worse, isn't it. But really, think about it -- people who illegal copies of illegally hacked software a) are demonstrated by lawbreakers, b) are familiar with the code of programming, and c) c) access to the code you expect to install on your computer. As for, while I'm sure there are many good Samaritans who distribute free pornography simply out of a desire for more happiness in the world, some small number of them do it for financial gain. If they give you free, they should make money from you in a different way, and one of the easiest is to install a bunch of malware on your computer, run any code they want on it, and then sell the use of your computer to spammers, phishers and other dubious varieties. Do you want to know how bad these guys are? They don't care if they give pornography a bad name!5. Don't download anything from unfamiliar sites. Again, if you're going to install something you downloaded on your computer, you should know that only people you trust have had access to it. Adobe, Microsoft and other software manufacturers are generally trustworthy, as are sites such as Download.com. Bob's free software, which I like, may not be such a safe bet. Flash ads have been used to install viruses. So is the javascript code. You don't have to do anything to get infected in this way; You just visit a site with malicious code on it and bam you are infected. Because of this, hardcore security people turn off Javascript and either block or never install Flash. Personally, I think it limits the usefulness of the Internet too much; I decided to risk running Javascript and use the FlashBlock plugin in Firefox to choose which flash objects on the page I want to run (allows me, for example, to watch YouTube videos while preventing flash ads on the same page from downloading). 7. Don't click on email links. It's very easy to hide the real destination links sent via HTML, where the text reads www.perfectlysafesiteyouknowandtrust.com, but the actual URL is www.reallybadsiterunbymeanpeoplewithnofriends.net. It's like a phishing scam work - you think you're going to PayPal or your bank, but in fact you're going to a page designed to look just like your bank's login page but hosted on the server of average people. Also, bad guys often put unique tracking documents in the links, so they know exactly who clicked on the link - which means they know which email addresses of the millions they sent spam are valid, making them worth more money to other spammers. Um, right? 7a. Don't click the abbreviated URL. I don't like this because I like Twitter and you lose a lot of functionality if you don't use the service as bit.ly or is.gd to cut urLs, but these links are scary. When The mouse over the link URL is displayed in the bar state of the email or browser, which means you can check that the link is sent to where it says it does. When you do the same with a shortened URL, it's just just abbreviated URL. There are Firefox extensions like UnTiny that will reveal the true purpose of abbreviated URLs, and some Twitter customers do as well, but until the universal solution is standardized, these URLs remain a little scary, security-wise. 8. Install all security updates. If you're not a multi-national mega-corporation run with critical custom-made software, you need to install security updates as soon as possible after release. If you don't remember to do this is not something you think you'll probably do, install a computer to automatically download and install updates. Increasingly, we are seeing 0-day exploits - viruses and trojans written to exploit security flaws before these flaws are corrected - or, in some cases, even known - by manufacturers. Keeping up to date is essential to keeping even marginally secure. I know what in the world it is, someone will think right now, hey, why don't you just switch to Mac OS X or Linux? It's true these operating systems get far fewer viruses and other problems than WINDOWS PCs, but most experts seem to agree that this is at least partly because there are so many Windows computers and so few Mac and Linux PCs. (There are many Linux servers, but those are under professional surveillance, which goes a long way to believing beyond any security weaknesses Linux has.) Bad guys program for the system that allows the greatest spread of their malware, and right now, it's Windows.But if you're still not sure, I have an even better idea for you. Both Mac OS X and Linux have demonstrated security vulnerabilities, and as they become more common, are likely to become a target for hackers. So these are not exactly safe bets. Instead, try BeOS! It can only be riddled

with security holes and only work on Pentium 4 and earlier PCs, but I can guarantee you no one writes viruses for it! For everyone else, whether you're using Windows, Mac or Linux, make sure to follow the rules above, and chances are you'll just be fine. Well done.