Denver Tech Squad

So you're a computer savvy person, you use one on a daily basis, you shop online, do your bills, write reports, you feel comfortable on a computer. So one night your doing your usual nightly news catch up and your antivirus pops up and states that a threat has been detected please "click here" to clear it. So you click on it & it starts to run a scan, after a few minutes it comes up stating that it has detected numerous viruses, trojans, and worms. However it needs you to install another program to remove these detected threats and prompts you to click on the installer, which you do since it all appears to be coming from your virus protection, the installer runs and then states that it needs you to pay $19.99 to re-register it so that it can safely remove all threats. You're a little upset about having to pay as you pay a yearly fee as it is, but you think, what's another $19.99 to pay verse keeping my data and computer safe, so you shell out the $19.99, the program finishes running. Then you realize something went very wrong as you try to access a web page and you get a pop saying xp security tools 2010 has detected a threat, the program you just paid for and downloaded, you close out of it this time, but you have no internet access. A sinking feeling begins as you try to click on internet explorer and just get pop ups, you try to play a game, and you get just the xp security tools window, no matter where you go or what you do all you get is pop ups of this security tool.

So what happened? The answer: you downloaded a virus and gave it complete access and paid to get it.

How did this happen? The newest and latest viruses now are aimed to emulate your current operating system and virus protection, so you will get a pop up that looks like it was sent from either windows or you virus protection, it looks so similar that that's why so many people end up downloading it because they believe it is coming from their virus protection or operating system.

Why Didn't my virus protection catch it and stop it? On an ongoing basis new viruses are released and these viruses are made specifically to still be able to install and run no matter what virus protection you have. It is then an ongoing battle for your virus protection to come up with a way to block the newest virus, while new viruses continue to come out. Virus protection is great for viruses, trojans or worms that they have found the "cures" for, but it can take a while for your virus protection to find a cure to newest and latest intrusions, so in the interim you are vulnerable.

What is going to happen to my PC now? Is my data safe? Most viruses now are aimed at getting you to purchase things either the protection itself or various products that have paid for advertising. There are some like the one mentioned above that blocks all internet access and any executable from running such as games, or your actual virus protection. In most cases your actual information is safe, unless you used a credit card to purchase in which case that credit card could be vulnerable. The information that is sent back if any is internet habits, and what is sent is that this computer goes to this website followed by that one every day, not any actual details on you. If you were infected from an e-mail that was sent it could replicate itself and send it to everyone in your address book.

How do I fix it? Depending on what virus you have depends on the method of removal, some viruses you can run your antivirus protection and they will be removed, however some viruses imbed themselves into the window directory and when you remove them with your virus protection it could take part of the directory with it, and then there is no cure but reinstallation of the operating system. The most effective and guaranteed way to remove a virus is to re-install the operating system, but you will lose all data not backed up and will have to re-install any program you previously installed. When in doubt call your local computer technician.

How I prevent it from happening? First of all never click on any pop ups even if it looks like it is coming from your operating system or virus protection. If you get a pop up that looks like it came from your virus protection, go into your virus protection and run a scan from there. Do not open any attachments in e-mails from people you don't know, and even if you do know the sender make sure they have wrote something to you in the body of the e-mail, even if its hello, the reason for that is the self-replicating virused emails can only resend to everyone in your address book, they are unable to send anything in the body of the e-mail.