Beware of phone calls and pop-up warnings about any sort of computer problem on your computer.

These scams are widespread, including many instances in Westbrook. The scams are based on fear, uncertainty and doubt and can be very alarming to the unknowing person. The scammers try to scare you into thinking that you MUST act now to resolve a significant problem. The latest scams are targeting both Windows and Apple computers.

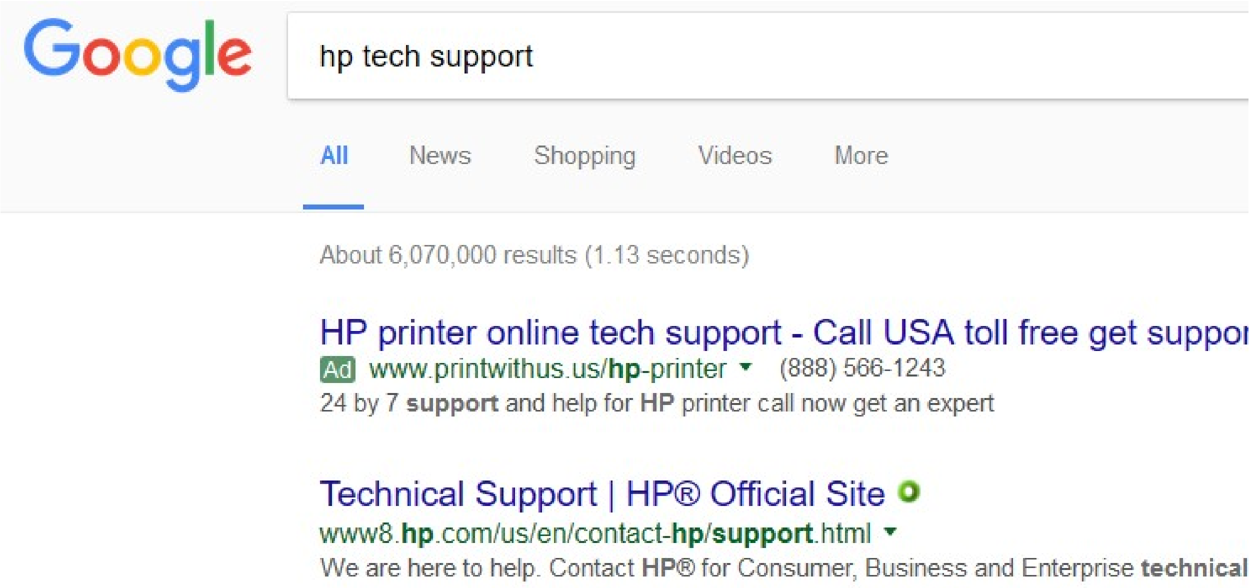
The scams usually say something about your computer has been detected as having a virus or some other problem that needs to be removed or repaired and they often say something about being with Microsoft. In some phone scam instances, ***they even know your name and address……HANG UP***. Here are some examples, all from Westbrook users.

1. The POPUP Scam. A message pops up on your computer with a warning about some problem or "virus" and asks you to immediately call a phone number for support. The computer appears to lockup (you can't get out of the webpage that shows) and you are told to call a phone number to have an expert assist you (usually claims a Microsoft affiliation). If your computer is inoperable, hold the power button down for at least 6 seconds to cause the computer to shut off. Then restart the computer and see if it acts normally. The problem usually happens when you have an internet browser open and may or may not recur. Running CCleaner before you open any browser may help by cleaning the browser history. If not, you may need to seek help.

2. The PHONE Scam: A phone caller claiming some sort of industry affiliation (usually Microsoft) says some kind of problem has been detected with your computer and needs to be fixed. Don't discuss anything with them, even if they use your name (in many cases, they know your name and address) ----HANG UP.

3. The EMAIL Scam: An old scam on businesses is now being used on individuals via email. You get email with an official looking bill for annual renewal of commonly purchased name brand computer protection software. A link to an online method of payment is included with the hope you will mistakenly pay the bill.

4. The PHONE number search scam: You decide you need help from a well-known tech industry company that you hope can help with your tech problem. You type in the name and lots of results show. The example below show results from requesting HP support. Notice that the first several do not have any hp.com in the main part of the website address. The first result is from printwithus.us and the second is actually hp.com. Lots of companies claim to be what you are looking so be careful about clicking on the first thing you see, especially if it claims 'free support' as the first result claims.



About 6,070,000 results (1.13 seconds)

HP printer online tech support - Call USA toll free get suppoı
Ad www.printwithus.us/**hp**-printer ▾ (888) 566-1243
24 by 7 **support** and help for **HP** printer call now get an expert

Technical Support | HP® Official Site
www8.**hp**.com/us/en/contact-**hp**/**support**.html ▾
We are here to help. Contact HP® for Consumer, Business and Enterprise **technical**

Knowing the name of the protection that is running on your computer is important and comforting, so you can ignore pop-up messages that are not related to your installed protection products. If messages persist, seek help to figure out why. The scams work because many of us DO NOT REALLY KNOW exactly what protection we have

Most common thing slowing computers down.

Malware has a lot of variations, and most commonly you will encounter the non-malicious type called commonly referred to as PUP's (potentially unwanted programs) that keep warning you or nagging to buy something or perform an action.

You've probably noticed new programs or notifications appear on your computer and you have no idea where they are coming from. They just seem to pop-up on your computer over time and it's most likely the result of installing new apps or programs on your system. The best way to catch these unwanted programs and unnecessary changes to your system is to pay very close attention to what the installation software says it is going to install.

Another way junk programs get into to your computer is through updates like Java and Adobe Flashplayer, just to name a couple. They are paid to install certain software and rely on you to just keep hitting next, next, next, I agree. Watch all of the updates from names you know because most of them pre-check some optional software to install. Uncheck anything you can, because the things you need are generally not uncheckable. This is really common when you download and install free utility programs. I have even seen free utility programs that as part of the uninstall process, will install as many as 3 additional programs while removing the one you agreed to remove (a good example of click, click, click and don't read).

Many, but not all, of these programs are detected and blocked or removed by a good malware removal program like MalwareBytes.

To learn more about this and what the Federal Trade Commission is doing, see this link to the FTC website.
https://www.consumer.ftc.gov/blog/shutting-down-scammers-and-their-pop-ads
The above article has a link to report a scam that you inadvertently responded to: report it to the FTC.
MalwareBytes has much information available on their website about Tech Support scams. The following link has a lot of good information about Tech Support scams. https://blog.malwarebytes.com/tech-support-scams/