Belmont PD has seen a few social engineering/phishing cases recently and we wanted to get the word out to help our citizens become more informed. At no point will any entity legitimately call you to let you know of a problem with your PC and then offer to fix it for you.

Individuals were informed that their PC was having undetermined errors and to have the issue resolved they needed to contact a toll free number for assistance. The other variation is where a bad actor will call stating to be a technical support technician and state that there is a problem with the PC and they will fix it.

The next step of their plan is to get you to do some basic “troubleshooting” checks using Task Manager or Resource Monitor (shown below) and tell you that what you are seeing is abnormal and needs to be fixed. In all cases, they will name off same standard names that run on ALL Microsoft Windows based machines.

The final step of their plan is to get you to allow them to remotely access your PC. Once this is done, they can secretly install applications that can do a number of different things. Some will allow for a key logger to run on your system and send information back to them. When you go to your bank, they can gather all of the information and proceed to access accounts. They may install a backdoor which they use at a later date to secretly access your PC, go through all of your data and find anything that they can use for their gain, such as Social Security numbers, dates of birth, your address, medical information, financial information.

**How can I avoid this?**

1. Keep your Anti-virus, anti-malware, and computer system up to date with patches and updates.
2. Do not install software from unknown third parties. If you are unsure of a program, go to google.com/bing.com and search for the program name. You can usually find out if it is legitimate or not very quickly.
3. Never give strangers remote access to your PC or home networking equipment.
4. If a pop-up shows up, or an unsolicited call with a legitimate company name in caller id comes in, do not respond. Remember, they will **NOT** contact you to let you know of an issue.
What to do if you are victim of this type of Scam:

1. Contact your local police department to report it.
2. File a complaint with the FTC:
   https://www.ftccomplaintassistant.gov/#crnt&panel1-1
3. Use a different computer to change passwords to accounts.
4. Contact your bank(s), credit card companies to alert them. They have procedures that they can implement to assist in stopping/slowing fraudulent spending.
5. Keep an eye on all your financial accounts and websites you may use to perform online shopping (Amazon, eBay, etc...)

Informative links:
https://www.consumer.ftc.gov/articles/0346-tech-support-scams