Beware of Tech Support Scammers

DATE: 02/02/2021

What You Need to Know

Criminals posing as tech support representatives are targeting individuals and using many different tactics to trick people including stating they have found malware on your computer.

A typical example is a caller who states that they are from BT claiming that your computer or router is causing a problem on the internet. They ask if you will access your computer and type in a few commands which will then list the 'problems'. These are not problems just a normal response to the commands. They will then ask you to go to a website and click on a link which will 'fix' the issue. Once this is done they will have access to your computer to do what they will, such as:

- Encrypting files which require payment to release
- Scanning your computer for bank account details or passwords
- Installing keyloggers so they will record each key pressed when you access your online accounts.

These are just some of the many examples they will use to trick you into giving them access to your computer.

It is important to note that it's not just PC's, but any computer that can access the internet can be a target.

What You Need to Do

Tech support scammers want you to believe you have a serious problem with your computer, like a virus.

If you receive a call from "BT", "Microsoft" and any other 3rd party tech company it's more than likely a scam - please put the phone down - they might attempt to call again – remain firm and put the phone down.

Note: There is a documentary available on BBC iPlayer, based on these types of scams, that can be viewed here. It provides an insight into how big of an industry tech support scamming really is!

If you have any questions or require any support, please contact your academy's IT Department in the first instance. If any additional support is needed please contact Rebecca Meacham, Compliance & Safeguarding Officer at rebecca.meacham@dudleycol.ac.uk.