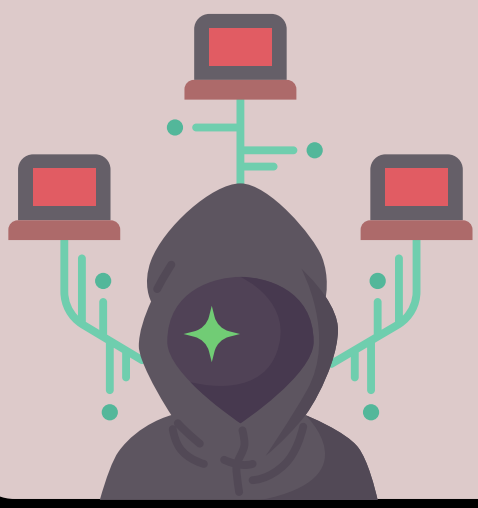
FOUR IMPORTANT STEPS FOR PREVENTING & DETECTING BOTNETS



A botnet is a collection of compromised devices that are utilized by bad actors to attack targets en masse They may coordinate for scamming (such as phishing attacks) or to bring a network down (as in a DDoS attack) or even to brute force passwords or in cryptomining schemes. Your device can be compromised and used by a botnet without you even being aware of it - which is where this guide comes in. These are four things to look for.

Check to see if your IP address is part of a known compromise

One of the easiest ways to detect whether your devices are currently being used by a botnet group is through your IP address, you can check to see if your IP addressed has been used in a botnet attack recently at https://checkip.kaspersky.com (there are also other sites that provide this service). If your IP address comes up then you know to take a closer look at your devices.

Protect Yourself Through DNS

DNS or Domain Name Service handles the communication on your device between websites and IP addresses. While normally your ISP handles this, some DNS services like OpenDNS will provide the extra service of warning you if you're about to access a malicious website.

Always Have a Good Router

Having a good router with proper firmware updates is another piece of the puzzle, many modern routers also have the capability to warn you or even block malicious websites.

For Windows Devices, Check What's Running Through Task Manager

Lastly, if you're worried your personal computer has been compromised, another place to look is your task manager. If you see processes running you don't recognize and it also seems like they're using a lot of your devices power this could be an indication your device is being used for nefarious purposes. It's good time to call in the experts to handle it.

Need assistance on this topic?
Visit ValleyTechlogic.com To Learn More.