MalBlock™ FAQ

Q: What is an Internet bot?
A: An Internet bot, also known as a web robot, robot or bot, is a software application that runs automated tasks (scripts) over the Internet.

Q: What do bots do?
A: The largest use of bots is in web spidering (web crawler), in which an automated script fetches, analyzes and files information from web servers at many times the speed of a human. More than half of all web traffic is made up of bots.

Q: Are all bots bad?
A: No. Some bots are "good," e.g., search engine spiders. However, other bots can be used to launch malicious activity.

Q: Why can’t I see a MalBlock™ warning page when it detects bot activity?
A: This is expected behavior. Bots are not designed to communicate to a user, only other software. As a result, the system can block the activity, but unlike other malicious activities like phishing attacks or ransomware (which are designed to interact with a user), bot activity cannot present a normal web message.

Q: When I go to a web site that is blocked by web filtering, I see more block events than actual times I was blocked on the dashboard.
A: This can happen on some web sites: Advertising and Shopping are two categories of web sites that support HTTPS encryption and multiple active bots on the website. When a user is blocked from going to a website once, it can generate dozens of blocks because the bots reside on the website.

Q: I see “device unknown” in the portal for devices on my network. Was it blocked by security or web filtering?
A: Some Apple devices and Windows 10 machines support MAC Address Randomization. This is an optional setting in Windows 10 and can be disabled. Random hardware addresses make it difficult for people to track your location when you connect to different WiFi networks.

Notes:
Apple products only randomize the MAC address when they attach to an unknown WiFi network.

When enabled, Windows 10 will only randomize one time when it attaches to a network. The next time the subscriber attaches to the that WiFi network, the same MAC address will be used.

More information on hardware random MAC address generation can be found here:
https://www.mathyvanhoef.com/2016/03/how-mac-address-randomization-works-on.html