

Quarantine

What is quarantine?

Quarantine is imposed on faceplates that are sending signals that interfere with the campus network. Computers attached to the faceplate have limited access to the network.

Why do computers get quarantined?

CWRU ITS Information Security and Network Engineering monitor network sensors to track malicious activity and overuse of campus resources. Quarantine is imposed on an entire faceplate in order to isolate the threat from the rest of the campus network, if a host registered in your name has been detected in the act of:

- Aggressively port-scanning hosts on- or off-campus
- Connecting to a known botnet Command-and-Control node
- Performing activities in violation of the CWRU Acceptable Use Policy (including man-in-the-middle attacks, unsanctioned 'security testing' of hosts on the network, or utilizing excessive bandwidth)

How do I get out of quarantine?

Once quarantined, you have 30 calendar days from the original quarantine date to contact the Service Desk at 216.368.HELP (4357) and address problems with your computer. Quarantined hosts that spend longer than 30 days in un-addressed quarantines will have their network registrations disabled.

Restoring the faceplate to service

Please do not unplug or move your computer to another faceplate.

1. Call the ITS Service Desk at 216.368.HELP (4357) and tell the analyst to whom you speak that you are seeing the Quarantine notification page.
2. The analyst will ask for details about your system including the registered Hostname, MAC address, or MalwareBytes log, and may request to remotely connect to your desktop in order to diagnose the problem.

Note: If there are multiple computers sharing the same faceplate (e.g. your room-mate or other lab computers), then your computer may not be the infected one, or may not be the only infected one.

3. The analyst can assist you with cleaning off malicious programs, but be advised that experience shows it is often more time-effective and thorough to back up your documents and reload your operating system to a secure configuration.
4. The Service Desk analyst will verify that the minimum standards for release from quarantine have been met, including:
 - a. Antivirus software installed and running up-to-date definitions
 - b. Automatic Updates configured
 - c. Operating System fully patched and up-to-date
 - i. The quarantine network will allow traffic to and from Symantec Automatic Updates and Microsoft Windows Updates.