Securing a computer on Campus

Issue

You are contacted by IT with regards to securing your computer due to an OIT (Office of Information Technology) report with regards to vulnerability.

Cause

Majority of the systems on campus are on a Public Addressable IP. This means the computer is available to be directly accessed based on what software that may be running on the computer.

The Campus Network will block some Network Ports, however, the Campus Network is configured to allow reasonable access for most computer network activity and relies on users of the network to secure their computer.

Resolution

Here is a list of what you can do to secure your computer (or device) for the Campus Network...

Use Strong Passwords

Any user account that is on the machine that is used to access the machine should use strong passwords, as define here What is a 'strong' password?

No outside (Non-university) users access

Computers on campus are strictly for use of University purposes only.

While you maybe collaborating with off-campus people, computers on campus is strictly for University users and should only be accessed with supervision by on campus users.

Use a Firewall

Most computers will have firewall capability.

If there are services on the computer that you need to access remotely (i.e. Access the computer from home), it may be wisest to have the computer's firewall configured to block the service you need to a very specific IP Range.

Given the various kinds of Operating Systems and Firewall Software that is available, we will not be able to go into detail on how to set it up, but we can recommend the IP range you will want to define to secure the system a bit better.

To computers on the Campus Network:

• 128.111.0.0/16 (128.111.0.0-128.111.254.254)

For computers using the Campus VPN and not wanting to include Resnet ranges:

• 169.231.80.0/20 (Campus wireless users)
• 169.231.96.0/19 (Campus wireless users)
• 169.231.128.0/20 (Campus wireless users)
• 169.231.144.0/20 (Campus wireless users)
• 169.231.160.0/20 (Campus wireless users)
• 169.231.208.0/20 (Campus wireless users)

For computers using the Campus VPN but allowing all Resnet, Facilities, and other internal UCSB ranges:

• 169.231.0.0/16 (169.231.0.0-169.231.254.254)

We recommend that devices use the Campus VPN service, even if they are on the Campus Wireless Network.

Disable or uninstall the service reported to you

If you aren't really using the service or application that is being reported to you, perhaps it is best to remove/uninstall the service.

Services such as:

• Bonjour
• Avahi (Linux version of Bonjour)
• Printer Sharing
• File Sharing
• Remote Desktop
If you are planning on Using Printer/File Sharing or even Remote Desktop, please configure the firewall to restrict the access to the Campus Network and use the Campus VPN if you need to access the computer from off campus.

Keep your software updated

Always make sure your software is up to date.

If it is a service or application you use, there is a chance that it has been updated to deal with the vulnerability.

If it is older software or hardware and has no update, or something you cannot get an update for it... You may have to consider either replacing it or make arrangements with your IT Staff on possible alternatives or means to isolate the computer/device for network security.

For more information

Please refer to UC Santa Barbara IT Website

- IT Security for Students
- IT Security for Faculty and Staff

Related articles

- How do I get Microsoft Office?
- How to use Zoom
- Connecting to a Network/Samba Share
- Securing a computer on Campus
- Not Recommended - Chromebooks