**Best Practices on the Network**

**Do not let anyone plug in their personal laptop or computer into a network jack in the library.**

Any computer or device that is connected via Ethernet to our network has the same access to sensitive areas of the network as our staff computers. Patrons don’t have our passwords or permissions, but software can be used to capture traffic on the network, including those passwords. Given a little time and the right tools, a patron can access and take over any computer on the network, including the servers.

Most patrons that want to plug into our network do not have any bad intentions. But because we cannot vet their devices, we don’t know what sorts of malware or viruses they may have installed on them.

We are working on segmenting the network so this will be less of an issue, but it will take some time.

Patrons often want to plug in because of increased speed and security, and our wired network is somewhat faster and definitely more secure than the wireless one. But the wireless network is plenty fast enough for most patron needs I think, especially in the larger and Charter libraries.

As for security, if we let patrons plug into our wired network, it loses any guarantee of security. Unfortunately, publically available wireless is inherently insecure, and there isn’t too much we can do about that. No one should use a wireless connection outside of their home with any expectation of complete privacy. That has been true for as long as there has been wireless. Things are certainly better now because the Meraki access points do a good job of isolating each connection, but people shouldn’t expect complete privacy on the public wireless, or the public computers either.

**Do not plug a patron’s or unknown flash drive into a staff computer.**

Flash drives can be infected just like a normal computer hard drive. Often the malware or virus will automatically start itself up when the flash drive is inserted. This is similar as to when a CD begins running a program as soon as it’s put into a computer, except without the friendly warning.

I frequently see virus warnings from the public computers about malware that is trying to launch itself from a patron’s external drive. For every piece of malware that our antivirus catches, it is safe to assume there are many out there it does not catch. There are simply too many new kinds of malware every day.

From what I have heard staff will plug a patron’s flash drive into a staff computer to transfer files for printing. There are a couple of alternatives to this. The easiest way is to get the required printer installed on at least some of the public computers. Another good method to transfer files is to email them to a library email account from which the staff can print the file.

**Staff Computer Maintenance**

Once a month, I recommend you run Ninite, CCleaner, and Malwarebytes.

Ninite is a program that aggregates updates for several regularly updated, popular programs. It can be found in the Software folder on your C: drive. If it’s not there, let me know. Just double click on it and it will update Firefox, Flash, Java, Acrobat Reader and Malwarebytes. You can customize and download your own Ninite executable here: <https://ninite.com/>

CCleaner will scan your computer and remove temporary files that accumulate with daily use. This helps to keep your hard drive free of useless files, and it cleans out all the flotsam and jetsam that your web browser saves every time you visit a website. You may want to tweak the settings ahead of time so that some useful things like your ‘Recent Documents’ list and saved form information within your browser are not erased.

Malwarebytes scans your computer for and removes any adware or malware that it finds.

Doing these things regularly, along with avoiding malware (http://ides.winnefox.org/click-me-not) will help to keep your computer running smoothly.