Security Checklist

Purpose

This is a Security Checklist on security your Computer and/or Device for the Campus network.

Grad Students and Faculty should do this, at least, once a quarter to avoid problems in the future, such as needing to scramble to get a computer up to date or needing to replace something at the last minute with little or no notice.

Checklist

All Accounts have a strong password.

As defined in this link, What is a ‘strong’ password?, all accounts, regardless of what it is, should have a strong password.

Delete or repassword old accounts every 3 months.

If the user is no longer using the system or device, delete their access.

If you wish to keep the account due to archival date, change the password or archive their data off the machine.

In either case, quarterly cleanup of accounts should be done on a shared system.

Disable services you are not using

Disable services that are sometimes enabled on a computer.

Services like:

- Bonjour
- Avahi
- File Sharing
- Printer Sharing
- mDNS
- mDNS
- RPCBind

These are often left ‘enabled’ for convenience, but are not designed for a Public Internet Network, which is what the Campus Network is.

These services should be disabled on your machine as they serve no purpose other than to make you computer or device more vulnerable.

Enable and Configure the Firewall on the device

Any device put on the campus network should have a Firewall and configured to allow what you want to allow with regards to services on your device.

We recommend limiting inbound connections only from the Campus Network (128.111.0.0/16 or 128.111.1.1 to 128.111.254.254) and/or the Campus Wireless (169.231.0.0/16 or 169.231.1.1 to 169.231.254.254)

You can access the system off campus by using the Campus VPN.

Refer to:

- IPTables - Basics - Linux Firewall Basics
- Configure Windows Firewall in Windows 10/8/7 - Rough guide on how to configure the Windows Firewall
- VPN FAQ - Campus VPN information.

You can also check what ports the system is leaving open by using nmap (https://nmap.org/) to see what ports

Make sure your system is up to date.
Make sure all devices have the latest security software or firmware updates.

This check should be done at least every quarter, if not monthly basis.

The only exception is Mac OSX updates and Windows 10 Creator's Updates, these should be on hold for at least a month or two upon release, but you should be able to do normal updates on the current OS.

Linux OS upgrades like Ubuntu (the non-LTS version) and Fedora should be done ‘as soon as possible’, as their support model for the OS version is only 2 years.

**Document Everything.**

You should document somewhere what is related to the machine.

Document the following:

- What applications are running or should be on the machine/device.
- What accounts are related to applications (Some applications will use specific accounts)
- Who is responsible for what on the machine/device.
- What the purpose of the machine/device is.
- When the last time something was added and by whom.

While this may seem to be a hassle, this is the best way to make sure what has happened to the machine that was intentional by the owner of the machine/device versus a hacker who has compromised it.

**Related articles**

- How should I report a phishing attempt?
- How to Password Protect a Web Page
- Security Checklist
- Securing Linux Computer
- UFW - Special Cases