Firewalls

This information is presented as general purpose suggestions and the effects may differ on each device or based upon specific updates done to each device. The County of York assumes no liability to unintended results this may have on your specific device and will not assist in any issues that may arise from implementing these tips. This is not an all-inclusive list of all software options available, simply a partial list of some options for the reader to further research for what might work best for them.

A firewall will protect your network, and PC (as best it can) by analyzing and blocking unauthorized traffic from coming into or possibly out of your system. The most critical firewall on your network will probably be built into your router (box connected between your modem and your computer, tablet, or phone). This will usually also host your Wi-Fi access and might have an antennae on it. However, one of the first things a virus or hacker will do after infecting one system is to infect other devices on your network. For this reason, it is critical to have firewall enabled on all devices. In addition, outbound firewalls might be able to prevent a virus from uploading your data or reporting to hackers if your system does get infected. Luckily, firewalls are usually one of those "set it and forget it devices". The only time you might have an issue is when you're trying to host resources on your device to the entire world (without using a cloud type service).

Routers

The default settings for most routers require no changes since that is one of the primary purposes of this device. To access your router, while connected to your network, open your Internet browser (Chrome, Internet Explorer, Safari, Firefox, etc.). Then go to https://192.168.1.1, https://192.168.0.1, or see your router manufacturer website for how to connect. The username and password is usually printed on the router itself or again visit the website. Unfortunately, each router menu is very different and you may need to consult online documentation specific to the make and model of your router.

Microsoft Windows

Enable Firewall: Click "Start" button | click "Control Panel" | click "System and Security" | click "Windows Firewall" | on left side click "Turn Windows Firewall on or Off" | select "Turn on Windows Firewall" for all networks

Reference: https://www.dummies.com/computers/operating-systems/windows-7/how-to-enable-the-windows-7-firewall/

Macintosh

Enable Firewall: Click “Apple Menu” | click “System Preferences” | click “Security” | click “Firewall” tab | click lock in lower-left corner and enter username and password | click “Turn on Firewall” or “Start”

Reference: https://support.apple.com/en-us/HT201642

Android

Android itself does not offer a firewall option. Below are some options for apps that will serve this purpose, however some IT experts report they might cause more issue than they prevent.

1. NoRoot Firewall
2. NetGuard

iPads and iPhones (iOS devices)

At the time of this writing, Apple does not allow firewall programs on their iOS devices. This is by design, as iOS devices handle security in a very different way than other devices. You can read a more detailed article on this here: https://www.tomsguide.com/us/iphones-dont-need-antivirus-software,news-23111.html