# COVID-19 Cybersecurity and Remote Work

- **Don't click on email website-links or download attachments from an unknown source, especially the ones with the COVID-19 subject line**. Instead, search the topic using Google, Bing, or DuckDuckGo and select the top results.

- **Do not download sensitive hospital information, including PHI** on to the computer or your personal cloud storage – Google Drive, Dropbox, One Drive, etc.

- **Power-off the computer after use.** Powered on machines are discoverable and active even when they are not in use.

- **Do not use public Wi-Fi**. Use your phone's hotspot if possible.

- **Increase home wireless security**
  - Change the default manufacture's password on your home Wi-Fi network.
  - Use a strong network administrator password. Administrator access allows router setting change.
  - Ensure strong encryption by using WPA2.
  - Ensure the built-in firewall is enabled.
  - Routers are vulnerable, just like computers, and require periodic firmware updates.
  - Old routers (5-years or older) are more vulnerable and most often not supported, if possible, replace them with the latest top-brand models.
  - Refer to the manufacture's owner's manual for instructions.

- **If you are using hospital computers**
  - Limit the hospital computer use to business purposes only.

- **If you are using personal computers to access the hospital network**
  - Use only Windows 10 computers or the latest MAC OS versions.
  - Do not use old computers - Windows 7, Vista, XP, or unsupported MAC OS versions
  - Check to make sure the computer's firewall, antivirus, and auto-updates are enabled.
  - Do not download and install programs from sketchy websites.
  - Remove unnecessary services and software.

- Report any suspicious or unusual incidents to GWUH IT Service Center at 202-715-4955 or email to itsc.gwuh@gwu-hospital.com.