Radiology Information Security Guidelines:

DO NOT: click on any web link in any email that you did not specifically ask someone for.
Instead DO: open web sites by manually typing the web address into the browser or using previously saved shortcuts.

DO NOT: Open any email attachment that you did not specifically ask someone to send to you.
Instead DO: Delete any email with any attachment that you did not specifically ask for.

DO NOT: Save any clinical images with patient demographics displayed.
Instead DO: Turn off display of patient demographics before you save an image.

DO NOT: Save any patient information in any document on any of your computers or devices
Instead DO: Make a patient list inside epic. Only save de-identified information outside of EPIC. Delete any files with sensitive data from your devices RIGHT NOW, then empty trash/recycle. If you must store sensitive information store it on UNC managed file shares only.

DO NOT: Send patient information over insecure email or text message.
Instead DO: Use your voice over the phone or send sensitive information only between your own UNC SOM email and another UNC SOM email.

DO NOT: Risk sensitive data loss from portable devices or portable storage.
Instead DO: Turn on whole disk encryption for any portable device RIGHT NOW. (Apple file vault, Windows Bitlocker, set password on phone, use encrypted USB drive; disable automatic login on all devices)

DO NOT: Store sensitive information on third party servers such as DropBox, iCloud, google drive, google docs, etc.
Instead DO: If you need to share or access files with sensitive information, set up access using UNC file shares.

DO NOT: Reveal private or sensitive information by careless WiFi use, such as free WiFi at Starbucks, McDonalds, etc.
Instead DO: Use your cellular phone service data connection, which is more resistant to hacking than free WiFi hotspots. Use a VPN if you must access sensitive information while off campus.

DO NOT: Let your computer be taken over by hackers due to your own complacency.
Instead DO: Turn on automatic Operating system updates, update web browsers and other software, especially web browser plugins such as Java or Flash. Use Chrome or Firefox for web browsing instead of Internet Explorer. Use a content blocker such as uBlock Origin. Remove any web browser plugins you don't need.

DO NOT: Let your on line accounts be taken over by hackers due to your own complacency.
Instead DO: Use a password manager to make complex unique password for each online account. Do not re-use the same password for different on line accounts. Do not share your UNC passwords with anyone.

Helpful Web Sites:

UNC Software download for VPN software antivirus, etc:
http://software.sites.unc.edu/shareware/

File vault instructions (Apple):
https://support.apple.com/en-us/HT204837

Guide to bitlocker (Windows):
http://www.pcworld.com/article/2308725/encryption/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html

Excellent detailed privacy advice:
https://www.privacytools.io/#ukusa

uBlock Origin, an excellent Ad/malware blocker for web browsing:
https://github.com/gorhill/uBlock

HTTPS everywhere, an excellent browser add on to enable secure web connection by default to many common web sites:
https://www.eff.org/https-everywhere

Password Managers:
https://1password.com/downloads/
https://sourceforge.net/projects/keepass/

VPN service provider:
https://airvpn.org