Keep your computer updated
Keep your computer’s software up to date, including your anti spyware and ensure you have installed the University’s Sophos Antivirus to keep your computer safe.

Download files legally
Avoid peer-to-peer (P2P) networks and remove any file-sharing clients already installed on your system.

Keep personal information safe
Never respond to emails asking you to disclose any personal information. The University will never email you asking for your personal information.

Lock your computer
When leaving your computer unattended, physically lock it to prevent theft and lock the screen with a password to safeguard data.

Log off public computers
When using a public area computer, be sure to completely log off when you are finished using it.

Back up important data
Make backup copies of your important computer data, store them securely, and consider storing extra copies at another location.

Scan email attachments
Scan all email attachments before you open them since they may contain viruses that could harm your computer.

Create strong passwords
Create strong passwords that combine at least eight characters including letters, numbers, and symbols.

Limit social network information
Protect your social networking presence, such as on Facebook, by limiting the disclosed amount of personal identifying information.

No multiport devices
Don’t install multiport network devices (wireless routers, switches, hubs, etc.) in your dorm room.