**Install antivirus software**
Install the University’s FREE antivirus software, available to all students, faculty, and staff. Download at: www.rochester.edu/antivirus

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

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

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

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

**Keep your computer updated**
Keep your computer’s software up to date including your anti-spyware.

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

**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 including your user ID and password.

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

**Secure your mobile device**
Secure your mobile device with a password or PIN. Set an inactivity timeout and encrypt.