Top 10 Ways to Keep Your Information and Data Safe Online

1. **Install Antivirus Software**
   Install the University’s FREE antivirus software, available to all students, faculty, and staff. Download at [www.rochester.edu/antivirus](http://www.rochester.edu/antivirus)

2. **Create Strong Passwords**
   Create strong passwords that combine at least eight characters including letters, numbers, and symbols. Consider using a memorable passphrase (a sequence of abbreviated words, numbers, and symbols).

3. **Secure Your Mobile Devices**
   Passwords, PINs, and fingerprint scanning are vital methods for protecting your devices from thieves. Set an inactivity timeout and encrypt.

4. **Keep Your Devices Updated**
   Operating system and application software should be supported with up-to-date security patches.

5. **Lock or Log Off Unattended Devices**
   When using a computer in a public area, be sure to log off completely when you are finished. When leaving your computer unattended, lock the screen with a password to safeguard data.

6. **Download Files Legally**
   Avoid peer-to-peer (P2P) networks and remove from your system any file-sharing clients used to download content illegally.

7. **Beware of Phishing Scams**
   Phishing scams come in all forms (email, phone, text, etc.). Never respond to communications asking you to disclose any personal information. The University will never email you asking for your personal information including your user ID and password.

8. **Limit Your Public Online Presence**
   Protect your social networking presence, such as Facebook, by limiting the amount of personal identifying information you disclose.

9. **Be Careful What You Store Online**
   Do not store personal or legally restricted information in cloud-based applications due to the varying levels of security offered. Be informed of content stored in applications that automatically sync to the cloud.

10. **Regularly Check Your Online Accounts**
    Check online accounts often that contain personal information. Look for fraudulent charges in your bank accounts and credit card statements. Never check these accounts using public Wi-Fi.