"Top 10 List" of Good Computing Practices

General good computing practices and tips that apply to most people who use a computer.

For questions relating to any of the information contained on this page, please contact the Cecil College Helpdesk.

THE QUICK LIST
Click on each item for additional information

1. Use Passwords that can't be easily guessed, and protect your passwords.
2. Minimize storage of sensitive information.
3. Beware of scams: Never reveal your password or click on unknown links or attachments. Be careful who you share your private information with.
4. Protect information when using the Internet and email.
5. Make sure your computer is protected with anti-virus and all necessary security "patches" and updates, and that you know what you need to do, if anything, to keep them current.
6. Secure laptop computers and mobile devices at all times: Lock them up or carry them with you.
7. Shut down, lock, log off, or put your computer and other devices to sleep before leaving them unattended, and make sure they require a secure password to start up or wake-up.
8. Don't install or download unknown or unsolicited programs/apps to your computer, phone, or other devices.
9. Secure your area before leaving it unattended.
10. Make backup copies of files or data you are not willing to lose -- and store the copies very securely.

Reporting Computer Security Incidents

THE DETAILS:

1. Use Passwords that can't be easily guessed, and protect your passwords.

- Don't share your passwords and avoid writing them down.
- Characteristics of good, cryptic passwords:
  - Contain a mixture of upper and lower case letters, numbers, and symbols
  - At least 8 characters in length (or longer if they're less complex)
  - Difficult to guess (e.g. don't include real words or personal information like user name, names of family members, places, pets, birthdays, addresses, hobbies, etc.)
  - Easy to remember (so you don't have to write them down)
- Password protect all of your devices.

2. Minimize storage of sensitive information.

- Delete sensitive information whenever you can. Keep it off of your workstation, laptop computer, and other electronic devices if at all possible.
- Don't keep sensitive information or your only copy of critical data, projects, files, etc. on portable or mobile devices (such as laptop computers, tablets, phones, memory sticks, CDs/DVDs, etc.) unless they are properly protected. These items are extra vulnerable to theft or loss.

3. Beware of scams: Never reveal your password or click on unknown links or attachments. Be careful who you share your private information with.

- Don't respond to email, instant messages (IM), texts, phone calls, etc., asking you for your password. You should never disclose your password to anyone, even if they say they work for Cecil College, ITS, or other campus organizations.
- Only click on links from trusted sources. Never click on an unfamiliar link unless you have a way to independently verify that it is safe. This includes tiny URLs and any link where you can't tell where it will take you.
- Don't open unsolicited or unexpected attachments. If you can't verify an attachment is legitimate, delete it.
- Don't give private information to anyone you don't know or who doesn't have a

legitimate need for it -- in person, over the phone, via e-mail, IM, text, Facebook, Twitter, etc.

- Beware of IRS scams and phony computer support scams. These are usually over the phone and threaten dire consequences if you don't act immediately.

4. Protect information when using the Internet and email.

- Only use trusted, secure web pages when entering personal or sensitive information online. Don't log in to web sites or online applications unless the login page is secure.
  - Look for https (not http) in the URL to indicate that there is a secure connection.
- Be especially careful about what you do over wireless. Information and passwords sent via standard, unencrypted wireless are especially easy for hackers to intercept (most public access wireless is unencrypted).
  - Check your wireless preferences/settings to make sure your devices aren't set up to auto-connect to any wireless network they detect. Auto-connecting to unknown networks could put your device and data at risk.
- Don't send restricted data[1] via email, text or instant message (IM). These are not generally secure methods of communication.
- Be extremely careful with file sharing software. File sharing opens your computer to the risk of malicious files and attackers. Also, if you share copyrighted files, you risk being disconnected from the campus network, as well as serious legal consequences.

[1]**Restricted data or information:** Any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit.

5. Make sure your computer is protected with anti-virus and all necessary security "patches" and updates, and that you know what you need to do, if anything, to keep them current.

- Shut down or restart your computer at least weekly -- and whenever your programs tell you to in order to install updates. This helps to make sure software and security updates are properly installed.
- If you get an antivirus alert that there is malware on your computer, contact the ITS Support Center (info below) for assistance.
- Talk to your computer support person or the Cecil College Helpdesk, or call (410) 287-4357 for assistance.

6. Secure laptop computers and mobile devices at all times: Lock them up or carry them with you.

- In your office or dorm room, at coffee shops, meetings, conferences, etc.
  Remember: Phones and laptops get stolen from cars, houses, and offices all the time.
- Make sure it is locked to or in something permanent.
- Laptop lockdown cables are available at the Bay Tree Bookstore and most computer or office supply stores.

---

7. Shut down, lock, log off, or put your computer and other devices to sleep before leaving them unattended, and make sure they require a secure password to start up or wake-up.

- <ctrl><alt><delete> or <Windows><L> on a PC; Apple menu or power button on a Mac.
- Also set your computer and portable devices to automatically lock when they're not being used.

---

8. Don't install or download unknown or unsolicited programs/apps to your computer, phone, or other devices.

- These can harbor behind-the-scenes viruses or open a "back door" giving others access to your devices without your knowledge.

---

9. Secure your area before leaving it unattended.

- Lock windows and doors, take keys out of drawers and doors, and never share your access code, card or key.
- Be sure to lock up portable equipment and sensitive material before you leave an area unattended.

---

10. Make backup copies of files or data you are not willing to lose – and store the copies very securely.

Reporting computer security incidents...

...because sometimes you can do everything right and things still happen.

- Report any suspected compromise (hacking, unauthorized access, etc.) of computing systems

  or data to your supervisor and the Cecil College Helpdesk.
- Also report lost or missing Cecil College computing equipment to the Campus Public Safety Office

  (and to the local authorities if the incident occurred away from campus).