Cybersecurity Information for Students, Faculty, & Staff

Quicklinks

There are many cyber security threats out there, but it is important to remember that most of them are avoidable. For additional cyber security do's and don'ts, check out ITS' "Top 10 List" of Good Computing Practices.

PROTECT YOUR PASSWORDS

Make sure others don't have the chance to use your accounts maliciously!

- Don't share your password with anyone. ITS will never ask you for your password. Neither should anyone else.
- Always use cryptic passwords that can't be easily guessed.

PHISHING AND OTHER SCAMS

Criminals and hackers continue to come up with schemes designed to compromise computers, steal personal or private information or passwords, or trick you out of money. Scams commonly use email, the internet, or the telephone. Social media sites, texts and your personal computer can also be used as phishing tools. Don't get fooled!

INTERNET PRIVACY (Facebook, Twitter, blogs, etc.)

A good rule of thumb is to *only post information you would be willing to put on a banner in a public place.*
Assume that any information you enter online is public unless you are using a known, trusted, secure site. Social networking sites (Facebook, Twitter, etc.), personal web pages, and blogs are great places for people to find personal information about you – and once you post something, you can't take it back!

ENABLE AUTOMATIC UPDATES

Updates fix problems in your operating system (the basic program that runs your computer/device) software, and apps. Out-of-date and unpatched devices are especially vulnerable to viruses and hackers. To protect yourself:

- Turn on automatic updates for your computer, antivirus, and all apps that you have.
- Install updates when your programs tell you they are available.
- **Shut down or restart your computer once a week.** This helps make sure software and security updates are properly installed to protect your computer and keep it running smoothly.
- For mobile devices, remember to sync often so you get available updates. Always install updates when your carrier tells you they are available.

FILE SHARING RISKS / COPYRIGHT

File sharing can expose your computer to a number of security risks.

- Although file sharing is not in itself illegal, if you share or download copyrighted material without permission – even unwittingly – you are breaking the law and could be subject to College, criminal, and/or civil sanctions. Please see Cecil College's policy on copyrights for more information.
- Improperly configured file sharing software can allow others access to your entire

computer, not just to the files you intend to share.

- Viruses and malware can be transmitted by file sharing software.
- Files offered by others may not always be what they say they are.

What can you do?

- **#1:** Run up-to-date anti-malware software. This is required for Macs and PCs on campus!
- **#2:** Make sure your file sharing software is configured only to share the files you intend to share.
- Also, turn file sharing off when you're not actively using it to avoid unknowingly sharing personal or copyrighted files.

  Other tips to avoid malware…

- Additional information about file sharing is also available on OnGuardOnline.gov's web site.

Legal File Sharing Services

We strongly encourage you to use legal file sharing services for obtaining music, movies, TV, games, books, etc. on the Internet. A large list of digital music, videos, and other services is available from Educause at http://www.educause.edu/legalcontent.

SAFE AND SECURE USE OF GOOGLE@CECIL COLLEGE

Google is great for email and all of its many apps and tools. Google drive provides unlimited storage for documents and can be used to back up any local data or folders you have on a device. However, don't forget to protect your account and any private information. Google security and privacy information is available