LE MOYNE
Greatness meets Goodness

Acceptable Behaviors for Computing @ Le Moyne (ABC's)

A. Stay Informed – "You are the shield!"
   a. Be conscious of your role in promoting information security at Le Moyne
   b. Be aware of the non-public, protected, and sensitive data and information that you are permitted to access and utilize.
   c. Leverage the Securing the Human training available to every Le Moyne employee.

B. Protect your account(s) and passwords
   a. Don't share your account or password or allow any other individual to use these.
   b. Shut down, screen lock, or log off your devices when you are not using them and make sure your device(s) require a password to resume use.

C. Use strong authentication
   a. Good: use complex passwords (at least 8 characters including upper and lower case letters, a number, and a special character). Password managers, such as KeePass, are useful for generating and storing complex passwords.
   b. Better: use a passphrase (e.g. "4 Score and 7 Years Ago!")
   c. Best: use two-factor/two-step authentication where available (e.g. a simple password and the Google Authenticator smartphone app).
   d. Never: re-use your Le Moyne password for another service (e.g. your Amazon shopping account).

D. Protect Information
   a. Pause and verify content and recipients before sending any information via electronic communications.
   b. Never transmit privileged or confidential information (e.g. SSN, driver's license, government id, passport id, credit card numbers) via electronic communications (e.g. e-mail, instant message) unless encrypted via an IT approved method.

E. Protect Devices
   a. Do not remove information technology or data from the campus unless approved (e.g. Le Moyne has issued you a portable computing device)
   b. Ensure that any personal and portable technology uses a password screen lock, is configured for remote data destruction if lost, and/or encrypts all data stored on the device.

F. "Don't Get Hooked"
   a. Be alert for Phishing and Social Engineering attacks
   b. "When in doubt, throw it out!"
   c. Do not open email attachments you are not expecting, even if they are from someone you know. Email and instant messaging are not secure forms of communication, and may not be from who you think. Many forms of internet fraud use these to launch their attacks.

G. Approved Software & Approved Sources.
   a. Don't install or download unapproved software or add-ons.

H. Backup, Backup, Backup
   a. Use the M: drive and H: drive whenever possible. These drives are backed up regularly to reduce the risk of data loss.
   b. Use Google Drive for personal (non-work related) files and where appropriate for administrative and academic activities. Google Drive provides unlimited storage for @lemoyne.edu accounts.
   c. Do not use Google Drive for protected information
   d. Never use a personal file sharing or data backup service (e.g. DropBox) for non-public Le Moyne information.