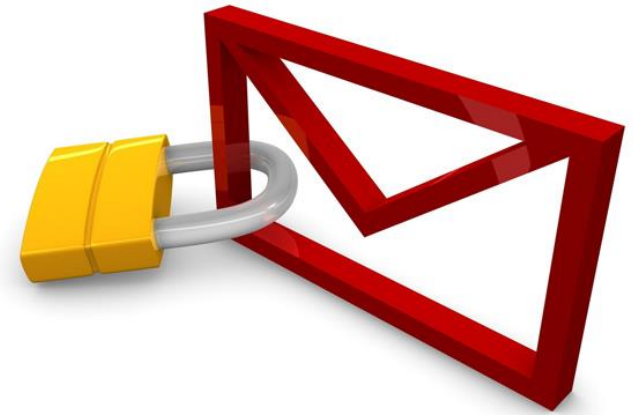
Staying Secure @ Austin College

Protecting your password

- Don’t write it down where others can see or find it
  - Anyone who finds your password can act as you and access your mailbox and file shares.
  - Just "hidden" in a drawer or under your keyboard is not a safe place.
- Don’t share it with anyone
  - No one else should need to log in as you. Once you share it with someone else, you don’t know who else may have it.
- IT will never ask you for your password
  - IT will not need you to tell them your password. Anyone who claims to be from IT and asks for your password is probably an imposter.

Email Protection



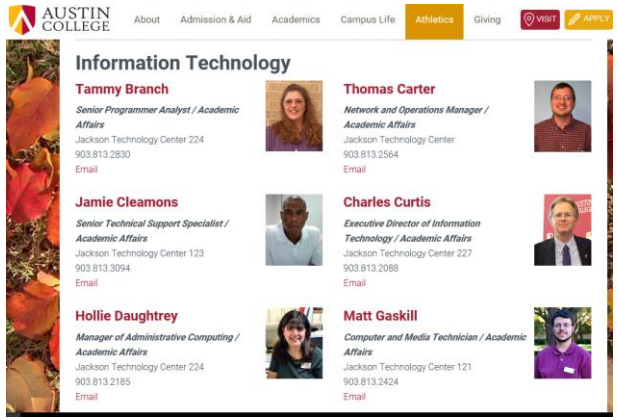
- Don't trust who the email claims to be from
  - The From address can be "spoofed" to pretend to be anyone. If the message is a surprise to you and asks you to do or click something, verify the sender by phone or in person before taking action.
- Don’t trust links or attachments in emails
  - Links and attachments may not be what they claim to be and may harm your computer just by clicking.
  - If you are not sure of the sender, do not click the link or open the attachment.
- Legitimate emails from IT will have a subject that starts with "IT@AC"
- Lock your mobile device if you check email on it
  - If you check your AC email on a phone or tablet, enable a passcode or other screen lock to prevent access to your email if you lose the device.

Information Protection

- Don't store personal/sensitive data on laptops, tablets, or phones
  - These devices could be lost or stolen, putting that information at risk. If it must be stored in a file, it is better placed on a network share.
- Don’t store sensitive college files on a personally owned computer
  - College-owned computers are configured to improve their security; a personal computer may not be as secure and may place this data at risk.
- Be suspicious of unknown memory sticks/thumb drives
  - USB media (memory sticks / thumb drives) can contain malware that may automatically execute when plugged into your computer. If you do not know or do not trust where it came from, keep it away from your computer.

Information Protection

- Be careful of the websites you visit
  - Malicious websites may attempt to steal login information or trick you into installing malware on your computer.
- Do not download or install software
  - If you need additional software on your computer, contact the Help Desk.
- Verify anyone claiming to be from IT support



- If you don't already know the person, verify anyone who contacts you in person, by phone, or by email. You can see if they are from AC IT using the AC website directory. Someone claiming to be from an outside company should never contact you without an IT person being present.

Be Safe!

- When in doubt, take the safe action
- Contact the Help Desk if you are unsure or encounter something malicious
  - Email: helpdesk@austincollege.edu
  - Phone: extension 2063 (903.813.2063)
  - Office: Jackson Technology Center east end 1st floor