Secure Storage/Sending

Never keep information on your computer or in email that you wouldn't want to become public knowledge. This especially includes sensitive information such as (but not limited to) social security numbers, banking numbers, tax information, etc.

- The Microsoft Office 365 suite is approved at USC for secure file/information storage and sending. Use OneDrive to keep documents and share with other members of USC. It is provided free of cost with your USC Microsoft Suite. This eliminates any need to keep files on your computer and backs them up should anything happen to your device.
  - For storage and sending of legally protected, high-risk, or restricted information please reference USC policy regarding Data Classification.

- Encrypt all email messages that contain confidential information.
  - To do so, within Microsoft Outlook in the email you would like to send
    - Click Options
    - Click the arrow next to Encrypt
    - Choose most applicable option

- Encrypt confidential documents
  - Save confidential document as PDF
  - Open document in Adobe Acrobat
    - Choose Tools → Protect → Encrypt
    - Choose most applicable option

- Password managers work well for secure and quick note storage.
  - OnePassword and LastPass offer free accounts

TROJANSECURE
OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER

Secure Storage/Sending

Never keep information on your computer or in email that you wouldn't want to become public knowledge. This especially includes sensitive information such as (but not limited to) social security numbers, banking numbers, tax information, etc.

- The Microsoft Office 365 suite is approved at USC for secure file/information storage and sending. Use OneDrive to keep documents and share with other members of USC. It is provided free of cost with your USC Microsoft Suite. This eliminates any need to keep files on your computer and backs them up should anything happen to your device.
  - For storage and sending of legally protected, high-risk, or restricted information please reference USC policy regarding Data Classification.

- Encrypt all email messages that contain confidential information.
  - To do so, within Microsoft Outlook in the email you would like to send
    - Click Options
    - Click the arrow next to Encrypt
    - Choose most applicable option

- Encrypt confidential documents
  - Save confidential document as PDF
  - Open document in Adobe Acrobat
    - Choose Tools → Protect → Encrypt
    - Choose most applicable option

- Password managers work well for secure and quick note storage.
  - OnePassword and LastPass offer free accounts

TROJANSECURE
OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER

Secure Your Confidential Information

Using poor information security practice is like giving your credit card to a stranger! Follow the guidelines below to make strides in securing your sensitive information.

1. Avoid clicking on links or attachments in unsolicited emails. Be extra cautious of unexpected emails posing as legitimate entities or offering employment.
    a. Forward suspicious emails to phishing@usc.edu for evaluation
2. Use passwords with 16+ characters and avoid password reuse.
3. Setup accounts with Two-Factor Authentication (2FA) for an additional layer of security
    a. www.twofactorauth.org lists setup instructions for sites and apps that offer 2FA
4. Avoid sending confidential information in email or text message, once digitized it can be shared without your consent. See other side of brochure for tips!
5. Avoid accessing confidential information while on unsecured wi-fi (credit card information, account logins, etc.), it can be seen by others on the network. Use your phone's data plan for this type of activity.

To keep up-to-date on recent information security risks and trends, visit https://infosec.usc.edu/

To report suspicious activity or for security related questions, contact security@usc.edu

TROJANSECURE
OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER

Secure Your Confidential Information

Using poor information security practice is like giving your credit card to a stranger! Follow the guidelines below to make strides in securing your sensitive information.

1. Avoid clicking on links or attachments in unsolicited emails. Be extra cautious of unexpected emails posing as legitimate entities or offering employment.
    a. Forward suspicious emails to phishing@usc.edu for evaluation
2. Use passwords with 16+ characters and avoid password reuse.
3. Setup accounts with Two-Factor Authentication (2FA) for an additional layer of security
    a. www.twofactorauth.org lists setup instructions for sites and apps that offer 2FA
4. Avoid sending confidential information in email or text message, once digitized it can be shared without your consent. See other side of brochure for tips!
5. Avoid accessing confidential information while on unsecured wi-fi (credit card information, account logins, etc.), it can be seen by others on the network. Use your phone's data plan for this type of activity.

To keep up-to-date on recent information security risks and trends, visit https://infosec.usc.edu/

To report suspicious activity or for security related questions, contact security@usc.edu

TROJANSECURE
OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER