E-mail - Best Practices

1. Confidential Information

   a. Do not use e-mail to send or receive confidential information. See the Guidelines for the Management and Retention of Public Record E-Mail for a definition of "Confidential".

2. Phishing Attacks

   a. UWCX Central Information Technology Services will never ask for your ID or passwords via e-mail. Any request for this information via an e-mail should be considered a Phishing attack and reported to the Central IT Service Center.

3. Viruses and Spyware

   a. UWCX e-mail users should careful consider whether to open an e-mail attachment, especially from an unknown sender. Users should not follow web links within an e-mail message unless the user is certain that the link is legitimate. Following a link in an e-mail message can cause a malicious program to be installed on the workstation.

4. Identity Theft

   a. Forms or requests for information sent via e-mail from an unknown sender should never be filled out by following a link. Doing so can result in your identity being stolen.

5. Password Protection

   a. UWCX requires the use of strong passwords for the protection of e-mail. A strong password contains a minimum combination of eight (8) capital and lower case letters, digits, or punctuation characters.

6. Credit Card Information

   a. Credit card information should never be communicated using the e-mail system. Providing credit card information via e-mail can result in the theft of a person's identity and fraudulent use of a user's credit card.

7. Using E-mail to Store Files

   a. E-mail systems are not designed for nor intended to be used as a repository for storing data. Users should not use the e-mail system as a repository for attachments. Users should follow the recommended best practices for retention of e-mail found in the Guidelines for the Management and Retention of Public Record E-Mail. E-mail attachments should be saved in an appropriate directory on a network drive.