This SPICE EduGuide applies to HSC users of Email in the HSC environment. Due to the widespread use of email, its effectiveness as a 'social engineering' tool, and the flow of messages in public places, we must maintain a heightened awareness of the security risks using it. Social engineering is the practice of manipulating you for someone else's gain – similar to the behavior of a 'con artist'.

Email Attachments/Malicious Software – Many viruses and other malicious software are distributed via email. A virus could be in an enticing attachment that professes to be the punch line of a joke, or a fun computer game to play, and activated when you open it. Email messages can contain links to malicious web sites that when visited, deposit malicious software on your computer.

Phishing – Fraud based but official "looking" email informing you that a financial account needs to be updated, or that there is a huge investment opportunity in another country, or warning you about a security problem with your account. A phishing message will instruct you to reply or click a web link and provide personal information like usernames, passwords, pins, account numbers, or your mother's maiden name. These are most likely not messages from reputable financial or other institutions—they are trying to steal your information.

Spoofing – Address books are often compromised by hackers. They can send you an email and make it appear as if it is coming from a familiar email address of someone you know. Spoofing is often done in conjunction with a phishing scam or malicious software attachment as described above, to draw you into the hoax. The content of a spoofed message is often out of context with the sender (i.e. your boss sending you a computer software game he just wrote.)

Unauthorized/inappropriate Disclosure – Confidential messages can be exposed via email in many ways. Hasty use of the 'type ahead' feature that saves users keystrokes when typing addresses often causes users to send messages to the wrong email address. Email messages often travel over the internet in a non-secured manner when sent to commercial email service providers (i.e. AOL, MSN, Yahoo, etc.) Even when a sender is cautious to send a message to another email user seemingly within their secure email system, the receiver may be using the 'auto forward' feature of their email causing the message to travel over the internet.

Safeguard Requirements and Guidelines

- An email service that you personally subscribe to may or may not be appropriate for our information and computing environment. Use the email technologies approved by your Unit Information Security Manager for work related email or for email of any kind accessed from a HSC computer.
- Messages emailed between your @ufl.edu email account, and other @ufl.edu email accounts *generally* remain within the UF network, and do not travel on the internet. However, be aware that your recipient may have set the 'auto forward' of their @ufl.edu email account to a personally subscribed or commercial email system. Check before you send anything confidential.
- If you are sending **Restricted** information via email, do not send to lists; send to single addressees only. Check the addresses before you send, to ensure accuracy. Additional requirements apply if you are emailing patient identifiable information; see http://privacy.health.ufl.edu/
- As a practice, delete messages with attachments and links from senders you do not know. The very small percentage that turns out to be legitimate can be resent.
- Validate unexpected messages with links and attachments from familiar senders. They could be 'spoofed'. If you don't have time to validate, don't open the link or attachment.

Policy & Standards References:

TS0006 Electronic Communications	TS0006 Electronic Communications Software