EMAIL SECURITY
The Tele Comm Method

Most computer users are aware of the term "phishing". It is pronounced "fishing" and it is the practice of luring unsuspecting Internet users to a fake Web site by using authentic-looking email with the real organization's logo. It is an attempt to steal passwords, financial or personal information, or introduce a virus attack. Creation of these Web site replicas is meant to fool unsuspecting Internet users into submitting personal or financial information or passwords. It truly is "fishing", with bait, for your personal information.

Keeping email secure, protecting your personal information, and eliminating as much spam as possible from your in box can be accomplished by following some simple rules:

1. **NEVER INCLUDE ANY PERSONAL INFORMATION IN AN EMAIL**
    This includes but is not limited to social security numbers, credit card numbers, bank account numbers, and passwords.

2. **NEVER RESPOND TO ANY EMAIL THAT ASKS FOR PERSONAL INFORMATION**
    Fallacious emails will typically ask for your personal information because there is a problem with your account. Do not fall for this and never respond to these emails.

3. **NEVER CLICK ON ANY LINK IN AN EMAIL**
    Although the link may look legitimate in the email, clicking on the link may actually take you to a different website. If you need to go to a link in an email, open up another tab in your browser and type the address in the new tab.

4. **NEVER OPEN AN EMAIL FROM SOMEONE YOU DO NOT KNOW**
    The email subject and/or sender may entice you to open it, but it may be a ploy to get you to open the email.

5. **NEVER OPEN AN ATTACHMENT YOU ARE NOT EXPECTING**
    Even if the email is legitimate and the sender is someone you know, and attachment may have been put on the email unbeknownst to the sender. The attachment, if opened, may put a virus on your computer.