Email Safety Tips

Change your log-in password often.

The simple act of changing your password will increase the likelihood that your email remains secure. In addition, alpha-numeric passwords are harder to break – be sure to use both numbers and letters. **More information on passwords**.

Never share your password.

Email administrators should not ask for your password. Do not be fooled by suspicious emails asking you for your password. This is a ploy designed to fool you into sharing your password. As a simple rule, never share it with anyone. **More information on some email scams**.

Never open attachments from unknown sources.

And be cautious about attachments from people you know. They may contain **Trojan horses**, **worms**, or **viruses**, which can seriously damage your personal or work computer. Make sure your virus checker scans all attachments from your friends before you open them; this is a common way for viruses to spread. **More information about the hazards of email attachments**.

Always log out/sign off when you are finished with your computer.

It's quick, easy, and may save your account from unwanted trespassers. If you are using a public terminal, exit the browser you are using when you are ready to end your Internet session. Be sure to clear your history and your **cookies**.

Do not reply to spam e-mail messages, or other harassing or offensive mail.

By responding, you only confirm that you are an actual person with an active email address ...who can be plagued with constant unwanted email solicitations. Instead, forward the unsolicited message to the customer service department of the source's email server. **More information about spam**.

Use common sense when you're sending and receiving email.

It is good to maintain a strong sense of skepticism. Always use caution when revealing personal information, such as your social security number or physical address to anyone you communicate with through email, even if they purport to be someone of authority.

SecureFlorida.org has more information on **safe usage of online messaging services** such as Instant Messaging, IRC, or bulletin boards.