DATA INTEGRITY

Integrity, in terms of data and network security, is the assurance that information can only be accessed or modified by those authorized to do so. Measures that the Office of Information Technology has taken to ensure integrity include controlling the physical environment of networked terminals and servers, restricting access to data, and maintaining rigorous authentication practices. Data integrity can also be threatened by environmental hazards, such as heat, dust, and electrical surges.

In order to protect data integrity in the physical environment, OIT follows best practices which include: making servers accessible only to system administrators, keeping transmission media (such as cables and connectors) covered and protected to ensure that they cannot be tapped, and protecting hardware and storage media from power surges, electrostatic discharges, and magnetism.

OIT system administration measures to ensure data integrity include: maintaining current authorization levels for all users (access is granted by functional security agents), encrypting transferred data, following change management procedures, documenting system administration procedures, parameters, and maintenance activities, and creating disaster recovery plans for occurrences such as power outages, server failure, and virus attacks

ENCRYPTING EMAIL

In an attempt to keep prying eyes from gathering sensitive information by reading your email, one of the chief solutions is to employ Encryption. Encryption basically takes your email message, and jumbles it up so that it looks like just a bunch of random numbers, letters, and symbols. While these messages look random to the illegitimate user, they do have a purpose. Each side of the email conversation (sender and recipient) have a specific key that they use to encrypt the message, and this is so each party will be able to decrypt the message with their key and clearly read the message as it was intended.

The most trusted and prolific email encryption software available on the web today is called PGP (Pretty Good Privacy) software, which you install in addition to your email client*. This software will stop efforts to harvest credit card numbers and other personal information. Encryption using PGP is easy, free, and trusted by millions all over the Internet.

While there are of course some commercial options available, the encryption strength of commercial PGP and OpenPGP (freeware) are based on the same standard (RFC2440), so you are really just paying for the use of the commercial interface.

Commercial PGP is available at: www.pgp.com

Freeware PGP is available at: www.gnupg.org

* Some mail systems such as Lotus Notes/Domino have encryption built-in, but it will only work with the same Lotus Notes/Domino environment. Emails sent outside of Lotus Notes/Domino will be left unencrypted without the use of 3rd party encryption software such as PGP.

OFFICE OF
Information Technology
UNIVERSITY OF CENTRAL OKLAHOMA

For additional help or assistance, contact the UCO Service Desk at 405.974.2255 or support@uco.edu.