E-mail/Password Usage Advisory

Whether information of a sensitive-nature is transported via e-mail, either as text or as an attachment, we remind our constituents to adhere to the following practices.

1. Passwords, PIN or any type of security or access code should not be transmitted as part of an e-mail message (either as in-line text or attachment) without the data being encrypted. The decryption key must be transmitted separately from the encrypted data.

2. The communication of passwords, PIN, or other type of security or access code should be communicated over a land-based telephone line or secured wireless telephone equipment.

3. Transmission of other private or sensitive information should be handled similarly to passwords, PIN, or any type of security or access code.

4. Private or sensitive information would be data elements or collection of data elements that could be used to attribute directly to an individual. Examples would include, but are not limited to, social security number, drivers' license number, credit/debit card numbers, salary, and medical information.

5. In some cases, electronic mail messages created from CUNY electronic mail systems are automatically forwarded to non-CUNY electronic mail systems. This practice potentially exposes private or sensitive information to the public Internet or misuse or diversion on non-CUNY provided computers. It is recommended disabling automatic fowarding if sensitive information could be a part of email messages and/or attachments.

6. Sometimes individuals are asked to disclose their passwords because of absences (planned or otherwise) from the office. The practice of sharing passwords is not allowed and computer access should only be allowed through a user ID belonging to a specific individual.

Carl Cammarata

CUNY Information Security Officer