Policy and Procedures for a Compromised or Suspected Spamming Account

04/03/2012

Article References: IT Systems Access Request Form, **Cellular Communication Devices and Services: 25.99.09.R0.01**, **Email for University Communication Procedure 25.99.08.R1.01, Use of Telecommunications Service 25.99.08.R1.**

If an account is suspected of being compromised or an account is known to be legitimate but is suspected of spamming the following procedures shall apply.

1.) Suspect account is to be immediately disabled for a minimum of one business day.
2.) Account will undergo immediate investigation.
3.) Damage done by aforementioned account must be corrected, and any affected services restored.
4.) Once the account has been verified to be compromised or spamming, and after corrective measures have been taken to restore services damaged by the account in question the following procedures will apply:

    a.) **If the account has been compromised**: Upon re-enabling the user's account the user will be required to change their password and retake training course "3001 Information Security Awareness" available within the TrainTraq system.

    b.) **If the account has not been compromised**: If the account was not compromised but was confirmed to be spamming the user will be required to retake training course "3001 Information Security Awareness" available within the TrainTraq system.

Definitions -

Compromise: to jeopardize the security of or expose to vulnerability, danger, or misuse.

Spamming: the act of sending unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail.