Phishing Scams and Identity Theft are two very serious issues that threaten the integrity of you and the university. Phishing Scams seek to steal confidential information by sending “official looking” e-mail messages that ask you to verify private information, such as a social security number, credit card information, passwords, etc. Phishing Scams often lead to Identity Theft, one of the fastest-growing crimes, and could ultimately corrupt the integrity of NCCU. Below are several tips to prevent us from becoming victims of phishing scams and/or identity theft.

1. A NCCU or any other reputable business will NEVER ask you for a password, social security and/or credit card number via e-mail.

2. If you are on a website and entering personal information, confirm that the website is secure. The easiest way to check is to look at the site address for https:// and/or the secure site padlock.

3. Look for typos. Legitimate businesses will take the time to proofread all communications they send to customers.

4. Don’t email personal or financial information. Email is not a secure method of transmitting personal information.

5. Forward all spam messages to spam@nccu.edu

Identity theft occurs when someone uses an individual’s personal information to impersonate the victim in financial transactions. Several recent incidents have highlighted the susceptibility of college and university data collections to theft. At the University of Texas, New York University, and elsewhere, security flaws have revealed students’ Social Security numbers and other personally identifiable information. By reporting all instances of spam, not sending confidential information through email, shredding confidential information and being cautious about the emails we respond to, you will be doing your part to protect the integrity of NCCU and yourself.