Dear [Department/College],

In an effort to better protect the University’s cyber resources and your personal information, the [Department/College] is partnering with UD Information Technologies (UD IT) to increase campus-wide awareness of an emerging cyber threat: phishing emails impersonating University officials.

In this type of cyberattack, scammers send an email that appears to come from a University official, for example: a president, dean, chairperson, or other position, in an attempt to commit fraud by persuading you to purchase gift cards, initiate payments or wire transfers, or divulge sensitive information.

While it is not an absolute guarantee that an email is legitimate, official communications should always come from an email address ending in “@udel.edu” - to verify the legitimacy of any email, contact the alleged sender through a verifiable method.

To avoid these types of phishing scams, please observe the following email best practices:

**Always inspect the sender’s email address.** Scammers commonly use fake email addresses that look similar to our “@udel.edu” domain or existing UDelNet IDs. Be wary of email messages received from non-University email domains that request money, gift cards, wire transfers or other sensitive information.

**Don’t feel pressured by a sense of urgency.** Scammers will often ask you to send gift cards or money immediately, stating that they are busy or in a meeting, and cannot do it themselves. Often these phishing emails use phrases like “Are you available?” or “Are you on campus?” or “I need your help on something very important right away”.

**Contact the alleged sender through a verifiable method.** For example, use the UD Directory to find the sender’s phone number to call and independently verify the request.

**Do not click on links or download attachments from senders that you do not recognize.** Be especially wary of .zip or other compressed or executable file type attachments.

If you receive a suspicious email, please do not respond. Instead, forward the email to reportaphish@udel.edu and UD IT Security staff will help you assess its legitimacy.

To learn more about the University’s comprehensive approach to computer and information security (including security awareness and phishing training), please visit the Secure UD website: <https://www1.udel.edu/security/>

Thank you for helping to keep the University community safe from these cyber threats!

Best,

[Sender Signature]