

March 14, 2008

Beware of Scam Soliciting Email Account Information

In general, account information is never requested by a legitimate organization via unsolicited email when you did not initiate the request yourself.

UNI has become aware of a new email phishing scam targeting educational institutions and has developed this information to help users identify this email scam. Below is a sample of one of the emails currently being used in this scam:

=====
VERIFY YOUR EMAIL ACCOUNT NOW

Dear Email Account Owner,

This message is from messaging center to all email account owners. We are currently upgrading our data base and e-mail account center. We are deleting all our email account to create more space for new accounts. To prevent your account from closing you will have to update it below so that we will know that it's a presently used account.

CONFIRM YOUR EMAIL IDENTITY BELOW

Email Username :
EMAIL Password :
Date of Birth :
Country or Territory :

Warning!!! Account owner that refuses to update his or her account within Seven days of receiving this warning will lose his or her account permanently.

Thank you for using our email account
Warning Code:VX2G99AAJ
Thanks,
Support Team

=====

UNI will NEVER request the above information from our users unless you have initiated the correspondence. ITS currently determines which email accounts to disable by a user's student or staff status with UNI, not by the account usage. Please remember to **NEVER share your password** for any system with anyone.

If you have replied to such an e-mail, please contact UNI as soon as possible at postmaster@uni.edu or the Computer Consulting Center at 319-273-5555, as your account may have been compromised.

Please inform people within your department about this scam.