BEWARE OF PHISHING SCAMS!

In light of the growing incidences of identity theft, it is suggested that we be more watchful for possible fraudulent emails, particularly phishing emails; see http://www.cuc.claremont.edu/securityinfo/.

Phishing is a scam to trick consumers into providing personal identity data such as account names, passwords, social security numbers, and credit card information in an attempt to perpetrate a fraud. Phishing emails are often spoofed to appear to be from legitimate sources such as banks, web sites such as eBay and Amazon, and credit card companies. They try to lead consumers to counterfeit web sites where they ask you to verify personal security data.

If you receive such an email, do NOT click on any links in the email message, but instead forward the message to spam@postini.com and reportphishing@antiphishing.org then delete the item immediately and empty your email trash folder.

At home, ensure that your web browser is up to date and all security patches are applied.

Although phishing is typically carried out by email, telephone contact can also be used. If you receive such a phone call, try to obtain the caller's name and phone number and report this to reportphishing@antiphishing.org.

If you suspect that you have been a victim of identity theft, immediately contact your financial institutions and post office. You can visit the Federal Trade Commission's web site to report the activity at http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html or call 800-IDTHEFT. In addition, call the three major credit bureaus to request that a fraud alert be placed on your credit report:
- Equifax at 800-525-6285
- Experian at 888-397-3742
- TransUnion at 800-680-7289

More information on how to combat phishing can be found at:
- Microsoft phishing web site: http://www.microsoft.com/protect/youself/phishing/identify.mspx
- How to avoid phishing scams: http://www.antiphishing.org/consumer_recs.html
- Identify Theft Resource Center: http://www.idtheftcenter.org/