

[Print](#) | [Close Window](#)

THE ENQUIRER

Last Updated: 10:28 am | Sunday, March 18, 2007

NKU fends off e-mail scams, spam

IT department constantly trying to improve security

BY HOWARD MCEWEN | ENQUIRER CONTRIBUTOR

In January, NKU server operations manager Jason Allen sent a campuswide e-mail warning of a "phishing" scam. The scammers send e-mails posing as Fifth Third Bank, asking students for very sensitive information such as bank account and Social Security numbers.

Last week, a Thomas More College staff member got an e-mail from a sender posing as U.S. Bank. The e-mail carried U.S. Bank's logo. It asked the receivers to confirm some information through a link that began www.usbank.com.

"The phishing Web site was done really well in that the first part of the URL looks really legit, but upon really closer observation you see that the domain is hktech.hk," said Bill Swisher, Thomas More's director of information technology.

The "HK" stands for Hong Kong. HKTECH is the domain registration used by a Hong Kong company to set up Web sites.

Phishing, the act of using various ruses to get personal information, is a growing concern to college IT departments.

A 2006 CompUSA TechInsights survey of college students found that 88 percent of college students keep personal information on their computers.

The survey also found that - as in other areas of their lives - while college students are aware of online dangers, many don't protect themselves.

At Thomas More, it's Swisher's job to help the student protect themselves. "Our major line of defense is to block these types of e-mails. Here at Thomas More College we use a spam-filtering solution on all incoming e-mails from outside the college," he said.

Thomas More only has 1,600 e-mail users and they receive 35,000 e-mails each day. Swisher said that 95 percent of those e-mails are spam.

"We are constantly tuning our spam filters to make sure legit e-mails get to the users and bogus e-mails are blocked," he said. "This is done by examining the daily archives to see what is getting through the filters that should not as well as what didn't get through that should have."

Swisher doesn't just defend Thomas More. Once spam is blocked, he goes on offense.

"Blocking the e-mail is not the end of what I do," said Swisher. "I also try to contact the 'true' site to make them aware of the phishing attempt. Most sites have an e-mail address of abuse@domain.com or spoofof@domain.com to report these issues. I even go one step further in trying to determine who is the owner of the site that the fake, bogus Web site is operating from, but I usually get nowhere with this, especially if the site is operating overseas. I also notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their Web site."

[Print](#) | [Close Window](#) | Copyright 2007, *Enquirer.com*