“Trojan emails… Protecting the Private Information of Our Constituents

We are noticing a global increase in emails containing malicious code. Therefore, we are asking everyone to be vigilant to avoid becoming a victim.

An attacker interested in breaching our University's security may use Trojan emails. Some emails will entice you to open a greeting card, install a screen saver or a game, or view a video when actually it is installing a program that allows the attacker to capture information which then is forwarded back to the attacker. Other methods may include a request to follow a link to what appears to be a reputable web site when it is actually a malicious site.

How Does It Work?

The attacker will send you an email or an instant message. The message may appear to be from an important person at a College or Central Office department, a system or network administrator, your College's security manager, a friend, a business, a government agency or some other familiar sounding entity. The emails make realistic claims or requests. For example, the email message might be an urgent request requiring you to "contact us by using this link." Another variation might be an email claiming to be from someone in authority requesting your user name and password (in violation of University information security policy and procedure). Regardless of which story the attacker provides, they emulate a legitimate individual or organization. If you fall prey to the email you may be allowing attackers access to our University's information.

What Should I Watch For To Determine if an Email is a Legitimate Email or Not?

• Does the email ask you to "verify your information" or to "confirm your user-id and password"?

• Does the email reference any consequences should you not 'verify your information'?

How Can I Avoid Becoming a Victim?

• Do not click on any links listed in email messages and do not open any attachments contained in the email. Many attackers attempt to install malicious code, like a Trojan horse, onto your computer.

• Bring suspicious or questionable emails to the attention of your College security manager.

• Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
Do not provide personal information or information about your College or University, including its structure or networks, unless you are certain of a person's authority to have the information.

Do not reveal passwords or other College or University sensitive or private information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

Don't send sensitive or private information over the Internet without first checking with your College security manager.

Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs.net).

If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a web site connected to the request; instead, verify contact information through an independent source such as an online or paper phone book.

For more information visit:
CUNY Phishing Advisory: security.cuny.edu under Advisories
NYS CSCIC security tips: www.cscic.state.ny.us/cscorner/news/
US CERT: www.us-cert.gov/cas/tips/ST04-014.html
i-Safe Phishing Video: ftc.isafe.org/phishing.html
OnGuard Online: www.onguardonline.gov/phishing.html
National Consumer League's Internet Fraud Watch: www.fraud.org/tips/internet/phishing.htm