Do not give sensitive information to anyone unless you are sure that they are indeed who they claim to be and that they should have access to the information.

What is a social engineering attack?
To launch a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a Phishing attack?
Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit sensitive, personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts. If you would like to know more about "phishing," some useful links are:

- Encyclopedia Entry on Phishing: http://en.wikipedia.org/wiki/Phishing
- OnGuardOnline Quick Facts on Phishing: http://onguardonline.gov/phishing.html
- FTC Consumer Alert: How Not to Get Hooked by a 'Phishing' Scam: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.pdf
- Watch Out for "Phishing" Emails Attempting to Capture Your Personal Information: http://www.privacyrights.org/ar/phishing.htm

How do you avoid being a victim?

- 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 give sensitive information to anyone unless you are sure that they are indeed who they claim to be and that they should have access to the information.

- Do not provide personal information or information about your department, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a web site's security.
- 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).

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about the University or downloaded malware contact the BSD-ISO team via the following phone numbers or e-mail addresses:

Plamen Martinov, Director of BSD Information Security	O: 773-834-1714	pmartinov@bsd.uchicago.edu
Kim Cooke, IT Security and Compliance Analyst	O: 773-834-7897	kcooke3@bsd.uchicago.edu

You may also send an e-mail to the BSD Security mailbox: security@bsd.uchicago.edu
Visit the BSD-ISO website: http://security.bsd.uchicago.edu