Security awareness: Today, let's talk about **Phishing**. What is phishing? **Phishing** (pronounced fishing) is a clever e-mail identity theft scam. The online encyclopedia, Webopedia (www.webopedia.com) defines it as: "the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information."

Boring, right? Not if you take the bait. Just like real fishing, the bait is usually very, very appealing; or, it might be very, very frightening. Carrot or the stick: the promise someone owes you money, or maybe that your credit card has been stolen. No matter what the bait, they'll ask you for your confidential information, and make it seem urgent that you give it. Things that will usually make you react, even panic, before you think it through. That's what they're counting on.

What makes phishing so easy to fall for is that it seems the request comes from a legitimate source, and for usually what seems to be a very legitimate reason. Often, the e-mail or website may contain official brand images, disclaimers, even case numbers, all to make you think its on the up and up. This type of tactic, tricking you to give out information, comes under a broader topic called **social engineering**. We'll have more on that in future articles.

An example of phishing is a fraudulent e-mail from the "IRS" claiming there is a tax refund waiting for the recipient. The message points the user to a link requesting confidential information like Social Security Numbers and credit card information. Unfortunately, its not from the IRS, and no, there is no refund waiting. (http://www.irs.gov/newsroom/article/0,,id=151065,00.html):

Here are some simple "do's and don'ts" if you get an e-mail like this:
DON'T reply, it will just let them know the e-mail address they tried is valid, and that means more spam for you;
DON'T give out confidential information, no legitimate institution or business is going to ask you to provide that kind of information in an e-mail;
DON'T click on any links in the e-mail, they'll probably take you to a "bad guy's" website;
DON'T open any attachments to the e-mail, they probably carry a nasty payload;
DO contact an institution you are involved with at the phone number, e-mail address, etc. ***you*** have on file, not the one in the e-mail. Let them know you got something suspicious;
DO be careful, and treat any unsolicited e-mail as suspicious;
DO be skeptical. Better safe, than sorry.

If you have any questions about this or any other type of suspicious activity, contact IT Security at **ITSecurity@hofstra.edu**.