# PHISHING:

What is phishing? We have all heard the term but many are confused about what it means.

***Definition**:* is attempting to acquire personal information such as usernames, passwords, & credit card details (and sometimes indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, businesses which have account holders, online payment processors, or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail spoofing or instant messaging, and it often directs users to enter details at a fake website, whose look and feel are almost identical to the legitimate one.

Phishing is a type of identity theft and an example of social engineering tactics used to deceive users and exploit the poor usability of current web security technologies.

The term is a variant of *fishing*, and alludes to "baits" used in hopes that the potential victim will "bite" by clicking a malicious link or opening a malicious attachment, in which case their financial information and passwords may then be stolen.

**Real-world scenarios & how to handle phishing attempts*:***

(1) At work you get an email / instant message asking for your password or PIN for a database update or some important need. Your name is part of a list. The email says it is from “the Campus IT Department”, or “your IT Dept”. What should you do?

Technology Support Services (TSS) would NOT ask for your password or PIN number, we would only use the identifier “TSS” in our email / instant message, and a TSS member’s name would be on the communication. Don’t send the information! Assume that the request is fake and simply delete the email / message. No need to contact TSS or send us anything.
***On the other hand***: If the item requesting info looks genuine and says it is from TSS, notify us promptly and forward the email to TSS! There is a problem and we need to know who got the email / message and who may have responded.

(2) At home you get an email / message asking for your password, PIN, account #, social security #, or other personal information. The communication appears to come from your bank, a business/entity, or government agency that you have an account or dealings with. What should you do?

Don’t send the information & delete the email / message! You can try to verify the source – call the business, entity, or agency that you believe may have sent it and ask to speak to the sender, the IT department, or customer service. They would never ask for that type of information. They need to know there is a problem and that customers may be impacted.

***Individuals can also report phishing to both volunteer and industry groups, such as *PhishTank* (watchdog group) & government agencies, such as the Federal Trade Commission.

Signs that point to phishing / good rules of thumb:

- the email / message requests sensitive personal information
- it does not look like it is from a genuine source with appropriate identifying information
- threatens action or account closure unless you respond
- has an origin in another country, uses bad grammar / typos
- it just looks suspicious

If you see any of these signs, assume it is probably a phishing attempt, do NOT reply, and delete the email / message! Legitimate entities / businesses already have the info they need and they would request necessary info differently.

Do not click on hyperlinks in emails or on websites unless they are from a trusted source. You could be lead to a fake website where you may open and spread malware or get tricked into providing your important personal information to an identity thief.

**SOURCES OF INFORMATION:**

PhishTank
http://www.phishtank.com/

Federal Trade Commission
http://www.ftc.gov/
https://www.ftccomplaintassistant.gov/
http://www.ftc.gov/bcp/edu/microsites/idtheft2012/