What is Phishing?

Phishing is the attempt to acquire sensitive information from you such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication (email) or by telephone.

To help you protect yourself from phishing, we offer the following tips:

1. **Be especially cautious of the following emails: (This includes e-mails from known or unknown associates)**
   - Messages that ask for you to confirm personal or financial information over the Internet and/or make urgent requests for this information.
   - Messages that are not personalized.
   - Messages that may try to upset you into acting quickly by threatening you with frightening information or fast –approaching deadlines.

2. **Communicate personal information only via phone or secure web sites:**
   - When conducting online transactions, look for a sign that the site is secure such as a lock icon on the browser's status bar or a "https:" URL whereby the "s" stands for "secure" rather than a "http:".
   - Also, beware of phone phishing schemes. Do not divulge personal information over the phone unless you initiate the call. Be cautious of emails that ask you to call a phone number to update your account information as well.

3. **Do not click on links, download files or open attachments in emails from unknown senders.**
   - It is best to open attachments only when you are expecting them and know what they contain, even if you know the sender. You can mouse over a link to see where it is going.
   - Beware of links in emails that ask for personal information, even if the email appears to come from an enterprise you do business with. Phishing web sites often copy the entire look of a legitimate web site, making it appear authentic. To be safe, call the legitimate enterprise first to see if they really sent that email to you. After all, businesses should not request personal information to be sent via email.

4. **Never email personal or financial information, even if you are close with the recipient.**
   - E-mail is not considered a secure form of communication.
   - You never know who may gain access to your email account, or to the person's account to whom you are emailing.

5. **Beware of pop-ups and follow these tips:**
   - Never enter personal information in a pop-up screen.
   - Do not click on links in a pop-up screen.
   - Do not copy web addresses into your browser from pop-ups.
   - Legitimate enterprises should never ask you to submit personal information in pop-up screens.

6. **Check your online accounts and bank statements regularly to ensure that no unauthorized transactions have been made.**

Reporting

The best course of action is to report your concerns to an organization that will investigate further. There are several such places on the Internet.

1. One is the U.S. government-operated website http://www.us-ert.gov/nav/report_phishing.html It provides information on where to send a copy of the email or the URL to the website so that they may be examined by experts. It also includes links with details on phishing scams and how to recognize them and protect yourself.

2. Another website to report cyberspace scams is the Anti-Phishing Working Group (APWG) located at: http://antiphishing.org/report-phishing/

3. Unlike the government-owned website, antiphishing.org features a text box in which to copy and paste the contents of the suspicious email you have received, including the header as well as the body of the message. Along the sidebar of the website, there are additional links of information to learn about phishing scams.

Phishing is a crime that has been plaguing users on the Internet for years. By reporting any suspicious contact to the proper organizations, you may have a part in helping to cut down on such unlawful activities in the future.

If you have fallen victim to a scam:

1. Change your password!
2. Report it:
   A. To the sites above.
   B. To the company who manages the account: For example, 1) Your username and password for the school district = contact the IT Helpdesk. 2) Your bank login = contact your bank.