**Do Not Become a Phishing Victim**

*Phishing* is pronounced like *fishing*. Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by impersonating as a trustworthy entity in an electronic communication.

**What to do if you're not sure if an e-mail is official**

1. *Never follow any links in an e-mail* you're uncertain about. Instead of following the link in the e-mail, visit the page by manually typing the address of the company.
2. *Never send any personal information through e-mail.* If a company is requesting you send them personal information about your account or are saying your account is invalid, visit the web page and log into the account as you normally would.
3. *Contact the Company directly* if you are still not sure about the status of your account or are concerned about your personal information. You should contact the company either through an e-mail address provided on their web site or over the phone.
4. *Finally, report the phishing scam* by forwarding the e-mail to reportphishing@antiphishing.org or spam@uce.gov and delete the e-mail.

Watch the following videos

2. *Phishing Scams in Plain English* by the commoncraft show.

**Identify a phishing e-mail**

1. *Company* - The phishing e-mails are sent out to thousands of different e-mail addresses and often the person sending these e-mails has no idea who you are. If you have no affiliation with the company the e-mail address is supposedly coming from, it's fake.
2. *Spelling and grammar* - Improper spelling and grammar is almost always a dead giveaway.
3. *No mention of account information* - If the company really was sending you information regarding errors to your
account, they would mention your account or username in the e-mail.

4. **Deadlines** – E-mail requests an immediate response or a specific deadline.

5. **Links** – Although many phishing e-mails are getting better at hiding the true URL you are visiting, often these e-mails will list a URL that is not related to the company's URL.

   I. Example of legitimate URL
      1. www.bankofamerica.com
      2. www.bankofamerica.com/smallbusiness

   II. Suspicious URL
      1. bankofamerica.xyz.com
      2. www.xyz.com/bankofamerica

6. If you’re using a banking website or conducting an online transaction with sensitive information such as your password or account number, check the address bar first! Make sure that the scheme is “https://” and there’s a **padlock icon** in your browser’s address bar. “https://” indicates that the data is being transported between the server and browser using a secure connection.