***NOTICE****: The following has been provided by WBA committee and section volunteers for use by member banks.
It should be reviewed and revised as appropriate to the user-bank’s own policies, procedures, and practices.*

**What is Spear Phishing?**

Phishing is an attempt to gain personal information by sending e-mails to a general population or group. Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or website with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the purported source of the e-mail is likely to be an individual within the recipient's own company, and generally someone in a position of authority. The actual source is usually out of the United States.

Spear phishing attempts are often targeted at publicly-known individuals in a company, often upper and middle managers or officers. Many spear phishing emails include information about the addressee's business or company that tends to make the email appear more credible.

Always remember to not give out any personal information to anyone by e-mail no matter who they say they are.