Phishing Warning

What is phishing?

Phishing is an attempt to steal your personal information. Dishonest people pretend to be legitimate businesses to get you to disclose sensitive personal information such as credit and debit card numbers, bank information, account passwords, or Social Security numbers. One of the most common phishing scams involves sending emails that pretend to be from well-known companies. However, the scam can also be carried out in person, by mail, over the phone, via malicious pop-up windows, and spoof or fake websites. A legitimate company **will not** ask you for personal information by email or phone.

How phishing works…

1. A criminal sends emails to people that appear to be from a well-known company. One very common tactic involves a fabricated story designed to lure you into clicking on a link or calling a phone number.
2. The phishing email may ask you to fill out a form or click on a link that takes you to a fraudulent website.
3. The fraudulent website mimics the company referenced in the email and aims to trick you into volunteering sensitive, personal data.
4. You think you're giving your information to a trusted company when, in fact, you're giving it to a criminal.

Note that phishing emails can also lure you to open suspicious attachments or visit websites that can infect your computer with malicious software or malware.

You can learn more about phishing by visiting these websites:
http://www.ncdoj.gov/getdoc/64264d79-a408-4607-9e18-21222ba2b33e/Scams-Booklet-2-10-2017.aspx
https://www.dshs.wa.gov/sites/default/files/DDA/dda/documents/Phishing%20and%20Vishing.pdf
https://www.consumer.ftc.gov/articles/0003-phishing
https://www.usa.gov/online-safety