6 Ways to Avoid EMAIL PHISHING

1 CHECK SENDER'S EMAIL

Display names can differ from email. When receiving an unexpected email, be sure to click on the name of the sender to view the true email address.

Ex. John Smith, jsmith@test.com could be John Smith, scammer@scam.com

2 READ THE EMBEDDED LINK

Before clicking or opening a link, you can hover over with your mouse to see the embedded link. A pop-up will tell you what the link is, standard urls begin with http:// or https://

3 MARK AS JUNK OR SPAM

Right click on the message and select the "Junk" or "Move to" Spam option before deleting or sending to trash. By doing this, you're teaching your mail to recognize email from malicious senders.

4 CALL SENDER TO VERIFY

Whether it's a hacked email from a friend, or someone pretending to be a credit card login, call the person or company to verify that they did indeed send it.

5 DON'T DOWNLOAD SOFTWARE OR ENTER YOUR CREDENTIALS

The purpose of phishing is to gain access to your personal information and finances.

ex. If a financial institution sends an email reading something like, "Click here to sign in." Don't click on it. Open a browser, and type the institution's name, then go there manually.

6 KEEP AN UP-TO-DATE ANTIVIRUS

Use Webroot or SUPERantivirus. Check out our Resource Page for free downloads if you don't have anything current running.
http://www.thenoc.net/resources/

Questions? Call 904.471.0022 or email help@thenoc.net