New Steps for Phishing/ Spam emails

\*We are no longer using ITthreats to report suspicious emails\*

* Please take the following steps to report them

Step 1: Select the icon highlighted which is in your ribbon. This will not remove the email from your inbox but flag it for fraud/spam.

Diagram

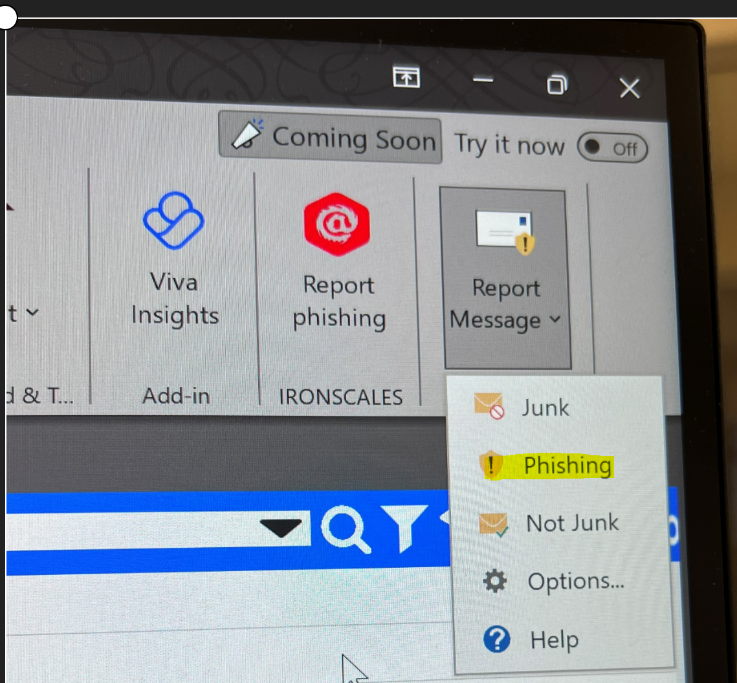
Description automatically generated with medium confidence

Step 2: Select the icon highlighted to report the message. This will not remove the email from your inbox

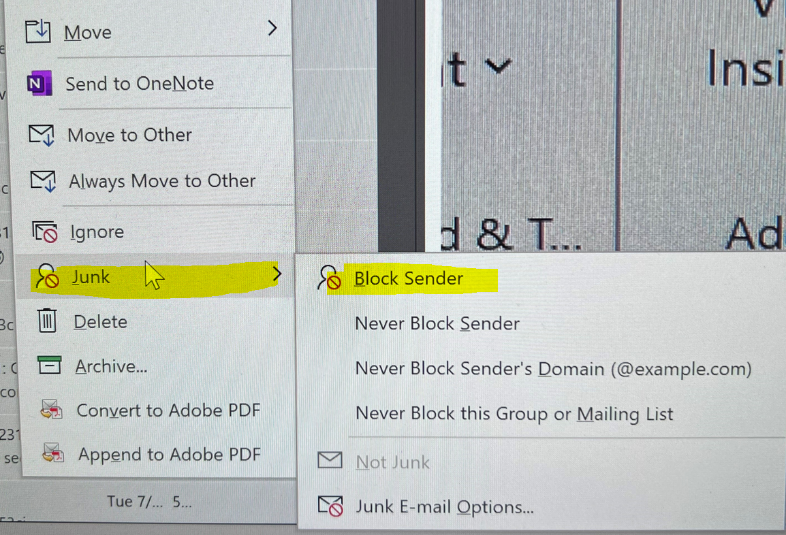
Diagram

Description automatically generated with medium confidence

Step 3: Once you open the report message dropdown- select Phishing option

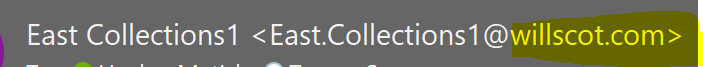


Step 4: If you want the email to be removed, you will have to right click the email and select junk, block sender. This will remove the actual email from your inbox



* Examples of fraudulent, spam, phishing emails

1. the URL is not correct- always look at the end url of the email, not just the first part before @
   * + hmatish@martinconcreet.com
     + [hmatish@martinconcrete1234.com](mailto:hmatish@martinconcrete1234.com)



1. Contains a clickable link that you don’t recognize- NEVER click links
2. Microsoft telling you your password expired- This is not how Microsoft informs you
3. Poor spelling or incorrect grammar within the body of said email
   * 1. good morning sur
     2. plese adise on mater
4. You need to purchase x amount of gift cards for client gifts- Check with upper management via a phone call to clarify if you are unsure.
5. There are attachments contained within an email that you don’t recognize- DO NOT OPEN THOSE ATTACHMENTS
6. Check the signatures in the body EX: James Cory Lee- this is not his work signature