Using the “Report Phishing” Button

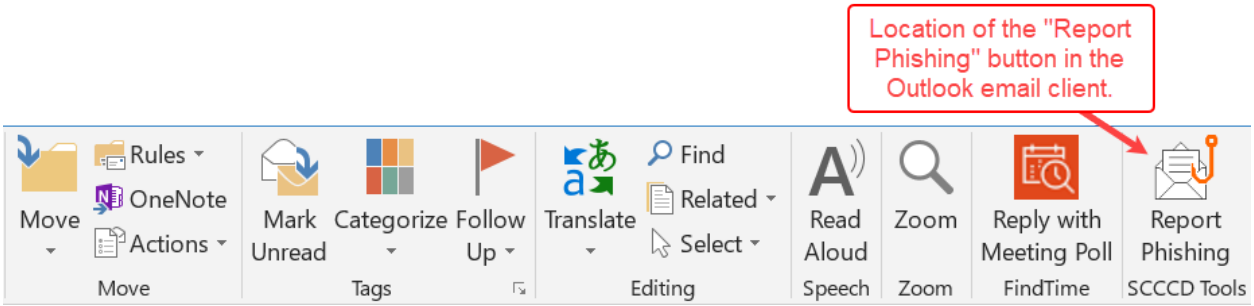
The purpose of the Report Phishing button is to allow SCCCD users to report suspicious emails that make it through to your inbox. Messages reported through the “Report Phishing” button will be analyzed and, if confirmed as a phishing message, can be safely quarantined and removed from other district mailboxes.

When to Use the Report Phishing Button

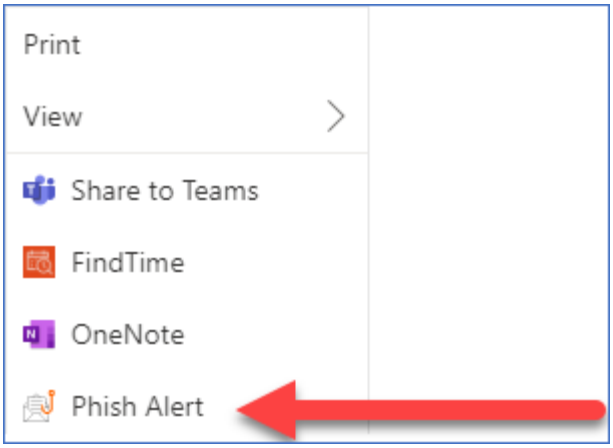
Click the Report Phishing button if you believe you have received a phishing email or any potentially dangerous email. The phishing email you report will be automatically deleted from your inbox and forwarded to the IS department for analysis. The Report Phishing button should only be used to report emails you believe may potentially contain malicious content. Do not use the Report Phishing button to report spam or marketing emails.

How to Use the Report Phishing Button

For Outlook users (Windows and OS X), the Report Phishing button will appear at the top of your Outlook client (see below).



For Outlook over the web users (Windows and OS X), the Report Phishing button is called “Phish Alert” button will appear under the ··· (ellipse) icon to the right of the message (see below).



To report an email as a phishing email:

1. Click the **Report Phishing** button while the email is open.

2. A prompt will ask you if you want to report the email as a phishing email. Click **Yes** if you'd like to report the email, or click **No** to not report the email.
3. If you click **Yes**, the email is removed from your inbox. The email will be evaluated and if it is legitimate, it will be returned to your inbox. If it is determined to be a phishing email, it may be removed from all user SCCCD email inboxes.

Getting Help and Additional Information

SCCCD users are the first and best line of defense to protect against dangerous phishing emails. Avoid clicking on links, calling phone numbers provided in unsolicited emails, or sending cash or gift cards to anyone in response to an unsolicited email that requests immediate actions. A list of cybersecurity and data protection tips can be found on the SCCCD portal.

Please call or e-mail your local helpdesk with any questions or concerns you may have.