



## Phishing and Spam User Mitigation Guide (NEW)

### Identifying Spam & Phishing Email Differences

- What are the main differences between Phishing emails and Spam emails?
  - Phishing: The main goal of Phishing emails is to entice you to either click on an embedded link within the email (which will result in Malware being loaded onto your computer) or to entice you to give Personally Identifiable Information (PII) usually by asking you to fill out an online form. Here is an example of Phishing:

**Sent:** Tuesday, August 7, 2018 2:27 PM  
**Subject:** [BULK] Your Outlook Exceeded its storage limit  
**Importance:** Low

Your Email Address Has exceed its storage Limit '[Click-Here](#)' And Fill the blank space and click SUBMIT.  
Note: Failure to submit the required details your account will be deactivated from our database.

- Spam: The main goal of Spam is to entice you to buy products and services via unsolicited marketing emails. Email can also be considered Spam even if you have done business with a certain company or institution before and they constantly bombard your inbox with marketing emails (abuse). Here is an example of Spam:

**Subject:** [BULK] Pregnancy Discrimination: Title IX, Title VII and Single Mothers on Campus  
**Importance:** Low

*Live Virtual Boot Camp*

**The Changing Shape of Title IX Compliance: 5 Essentials for Your Institution & What They Mean for You**

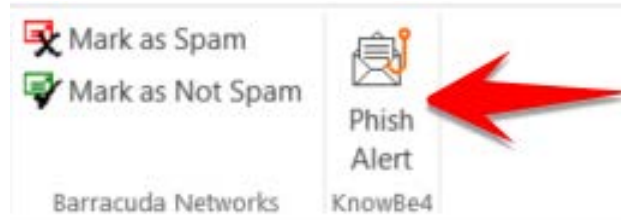
**Thu, Sep 18, 2018 | Time: 9:00 am ET | 8:00 am CT | Duration: 360 Minutes | Presented By: Dr. Susan Strauss, Dr. Jennifer L. Martin, Dr. Susan Fineran**

[Register For Webinar](#)

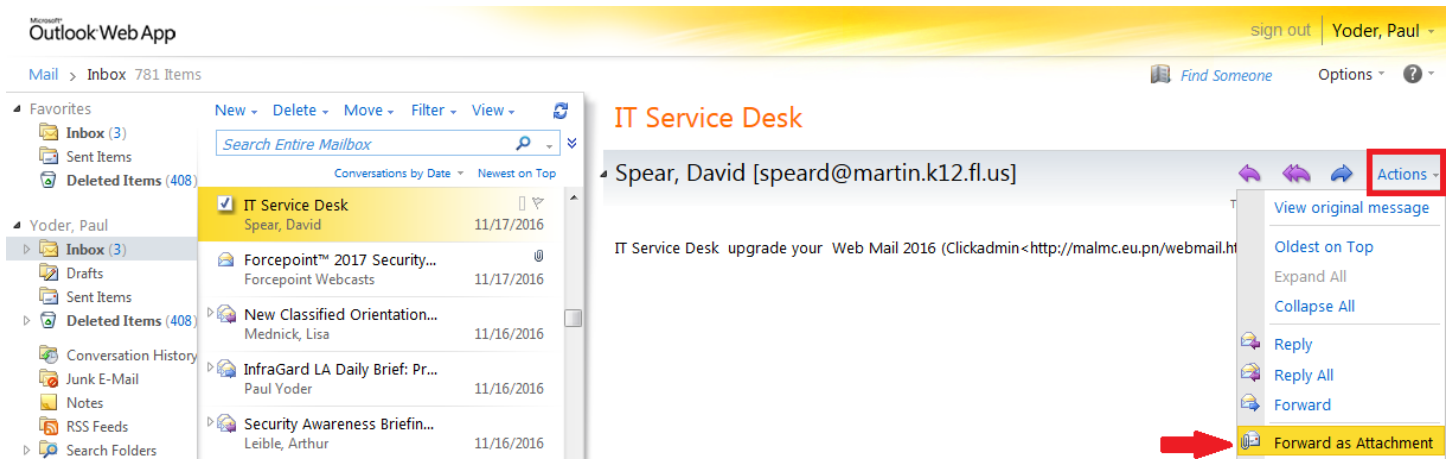
- Do I report Phishing and Spam emails the same way? **ANSWER: No - Phishing & Spam emails should be reported differently as shown below!**

## Reporting Phishing Emails

- PhishAlert button: Emails that are clearly Phishing attempts should be reported via the **Phish Alert** button in Outlook (unless you are using Outlook Web – then you only have the option of sending the email as an attachment to [spamalert@elcamino.edu](mailto:spamalert@elcamino.edu)):



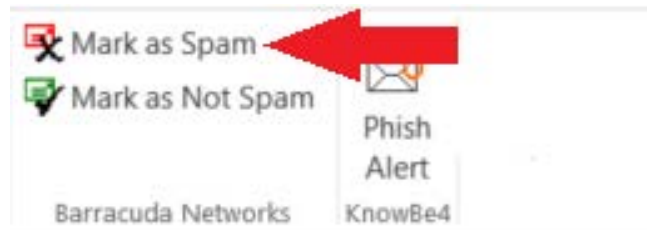
- If you are using the Outlook Web application:
  - Forward the email as an attachment to:
    - To: [spamalert@elcamino.edu](mailto:spamalert@elcamino.edu)
    - Subject: Phishing Email



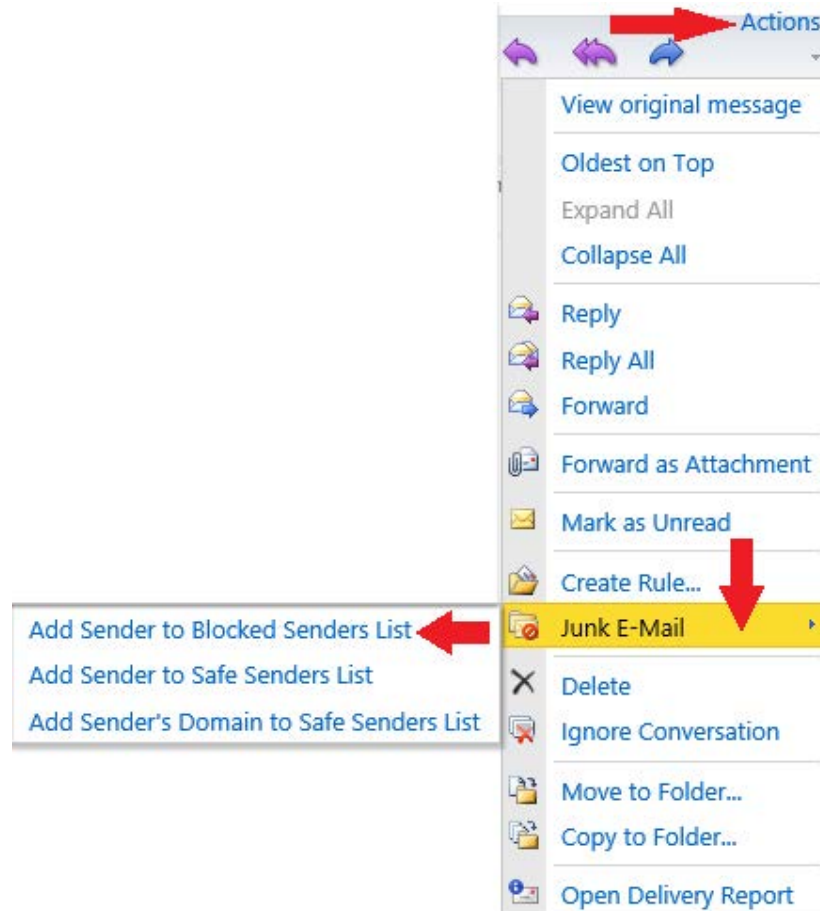
■

## Reporting Spam Emails

- Mark as Spam button: Emails that are clearly Spam marketing emails should be submitted by clicking the **Mark as Spam** button in Outlook:



- If you are using the Outlook Web application:



## Questions & Answers

- Why is the method of reporting unwanted emails different for the Outlook application on my desktop and the Outlook Web application I access from my browser?
  - **ANSWER: Because some features that are available on the desktop application of Outlook are not available in the Outlook Web version!**
- What happens to all of these emails that I report?
  - **ANSWER: Actually, a couple of different things happen to those emails that you report depending on the submission method used:**
    - Submitted via **Phish Alert** button: These emails get registered within our KnowBe4 Phishing training software and statistics are generated as to how many emails were submitted, who submitted them, and when.
    - Submitted via **Mark as Spam** button: These emails get marked within our Barracuda Spam Firewall and may end up in your personal Barracuda Spam Quarantine folder.
    - Submitted as an attachment to [spamalert@elcamino.edu](mailto:spamalert@elcamino.edu): These emails get sent to the Spam team within the Network Services and Cybersecurity departments and are handled accordingly based on the perceived threat level. At times, we will contact Barracuda to place a “block” on certain malicious emails if they pose a significant threat to the campus.
- Why are certain emails marked as [EXTERNAL] in my inbox?
  - **ANSWER: This new feature was implemented in January, 2019 so that it would be harder for hackers to spoof email messages that appear to be coming from ECC employees by providing an immediate visual clue as to when messages are actually coming from outside the elcamino.edu domain**