SEATTLE COLLEGES | IT Services

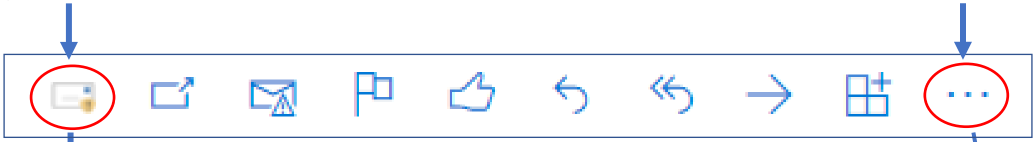
How to Report Phishing Email in Outlook (online version)

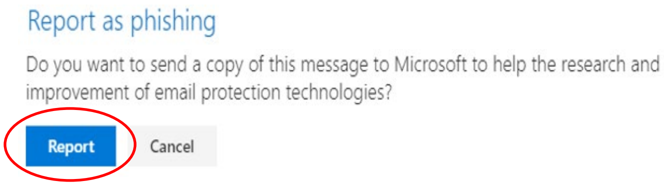
When you've opened a message and you suspect it is phishing – DO NOT RESPOND or CLICK on any links. (See How to spot a phishing email – pg. 2.)

From the task bar choose to 1. Report Phishing or 2. Report Phishing, Mark as Junk or Block Sender.

Option 1. Click this button to Report Phishing & send a report to Microsoft.

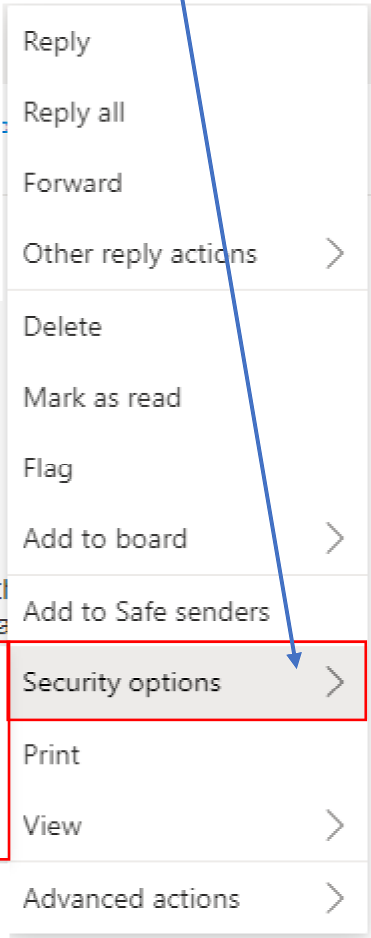
Option 2. Click the ellipses to open the options menu. Select **Security options** & select from: Report Phishing, Mark as Junk or Block *the Sender*



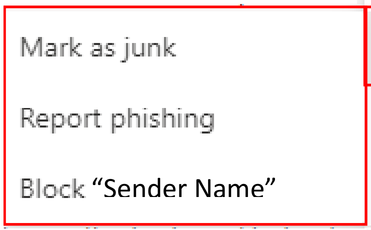


Report as phishing

Do you want to send a copy of this message to Microsoft to help the research and improvement of email protection technologies?



Security Options	What happens to the message?
Report phishing	- Sent to Microsoft for analysis & deleted.
Mark as junk	- Sent to Junk Email folder.
Block "sender"	- Deleted and future messages from this sender go to your Junk Email folder.



Note: When you mark a message as phishing, it reports the sender but doesn't block them from sending you messages in the future. To block the sender, you need to add them to your blocked senders list.

SCAN to visit us
itservices.seattlecolleges.edu

ITHelp@seattlecolleges.edu

How to spot a phishing email

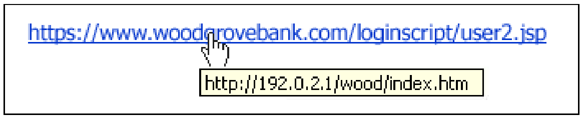
From https://support.microsoft.com/en-us/office/how-to-deal-with-phishing-in-outlookcom

A phishing email is an email that appears legitimate but is actually an attempt to get your personal information or steal your money.

Here are some of the most common types of phishing scams:

- **Emails that promise a reward**. “Click on this link to get your tax refund!”
- **A document that appears to come from a friend, bank, or other reputable organizations**. The message is something like “Your document is hosted by an online storage provider and you need to enter your email address and password to open it.”
- **An invoice** from an online retailer or supplier for purchase or order that you did not make. The attachment appears to be a protected or locked document, and you need to enter your email address and password to open it.
- **Urgent call to action or threats** - Be suspicious of emails that claim you must click, call, or open an attachment immediately. Often they'll claim you have to act now to claim a reward or avoid a penalty. Creating a false sense of urgency is a common trick of phishing attacks and scams. They do that so that you won't think about it too much, or consult with a trusted advisor who may warn you away.

  Tip: Whenever you see a message calling for immediate action take a moment, pause, and look carefully at the message. Are you sure it's real? Slow down and be safe.
- **First time or infrequent senders** - While it's not unusual to receive an email from someone for the first time, especially if they are outside your organization, this can be a sign of phishing. When you get an email from somebody you don't recognize, or that Outlook identifies as a new sender, take a moment to examine it extra carefully before you proceed.
- **Spelling and bad grammar** - Professional companies or organizations usually have an editorial staff to ensure customers get high-quality, professional content. If an email message has obvious spelling or grammatical errors, it might be a scam. These errors are sometimes the result of awkward translation from a foreign language, and sometimes they're deliberate in an attempt to evade filters that try to block these attacks.
- **Generic greetings** - An organization that works with you should know your name and these days it's easy to personalize an email. If the email starts with a generic "Dear sir or madam" that's a warning sign that it might not really be your bank or shopping site.
- **Suspicious links or unexpected attachments** - If you suspect that an email message is a scam, don't open any links or attachments that you see. Instead, hover your mouse over, but don't click, the link to see if the address matches the link that was typed in the message. In the following example, resting the mouse on the link reveals the real web address in the box with the yellow background. Note that the string of IP address numbers looks nothing like the company's web address.

  https://www.woodgrovebank.com/loginscript/user2.jsp

  http://192.0.2.1/wood/index.htm

  Tip: On Android long-press the link to get a properties page that will reveal the true destination of the link. On iOS do what Apple calls a "Light, long-press".
- **Mismatched email domains** - If the email claims to be from a reputable company, like Microsoft or your bank, but the email is being sent from another email domain like Yahoo.com, or microsoftsupport.ru it's probably a scam. Also be watchful for very subtle misspellings of the legitimate domain name. Like micros0ft.com where the second "o" has been replaced by a 0, or rnicrosoft.com, where the "m" has been replaced by an "r" and a "n". These are common tricks of scammers.