# How to Report a Suspicious Message on Outlook (Web Browser)

Designed for UTSA Faculty and Staff

To keep UTSA safe from cybercriminals and nation-state threat actors, everyone in our community should be vigilant about suspicious emails— and know how to handle them. Remember that malicious messages are designed to look like legitimate emails and typically include a call to action, such as clicking a link, opening an attachment, or even transferring money. If you receive a suspicious message, please report it right away.

How to report from web browser:

1. From your inbox right-click the suspicious message
2. Click "Security Options"
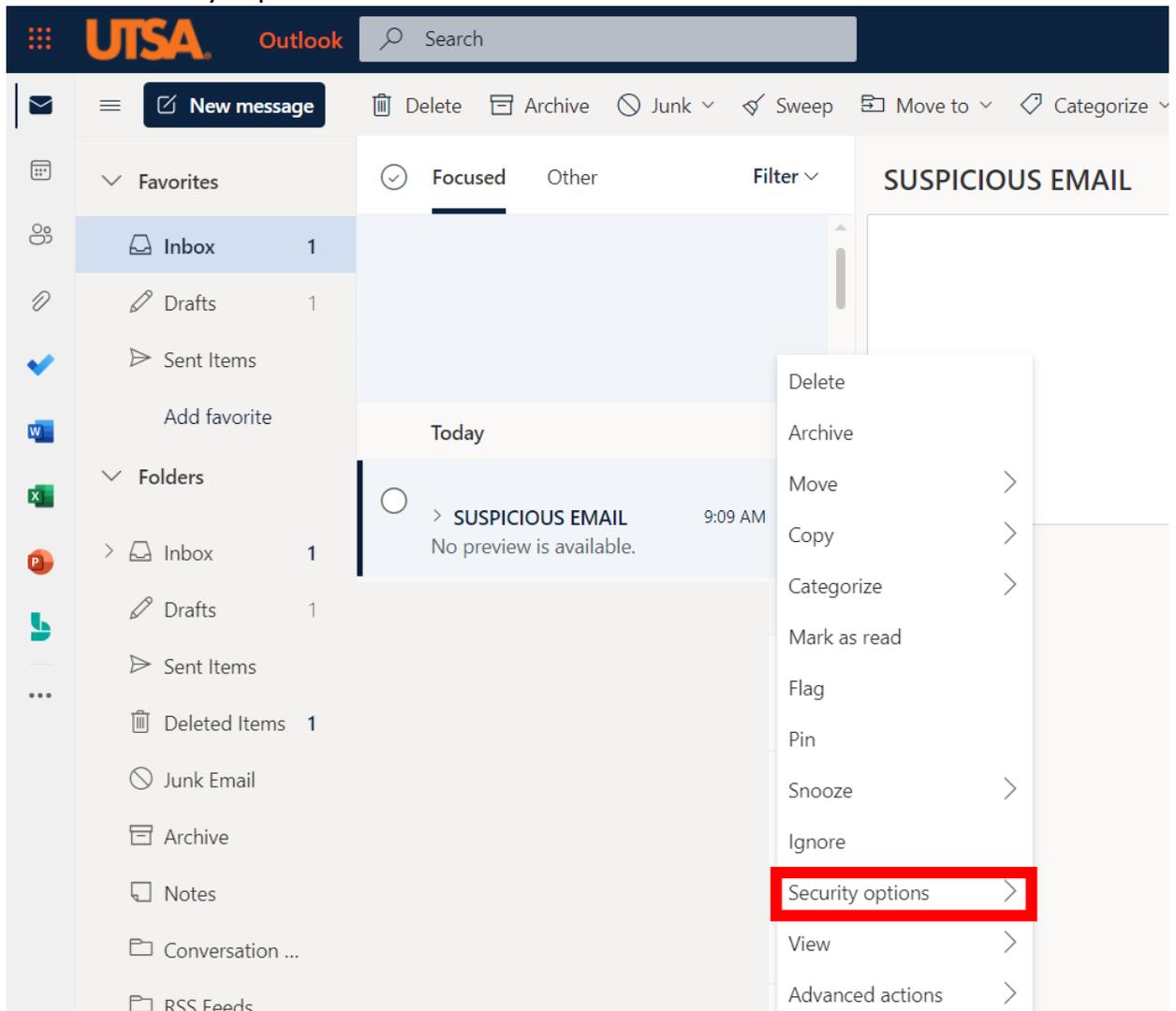
3. Select "Phishing"
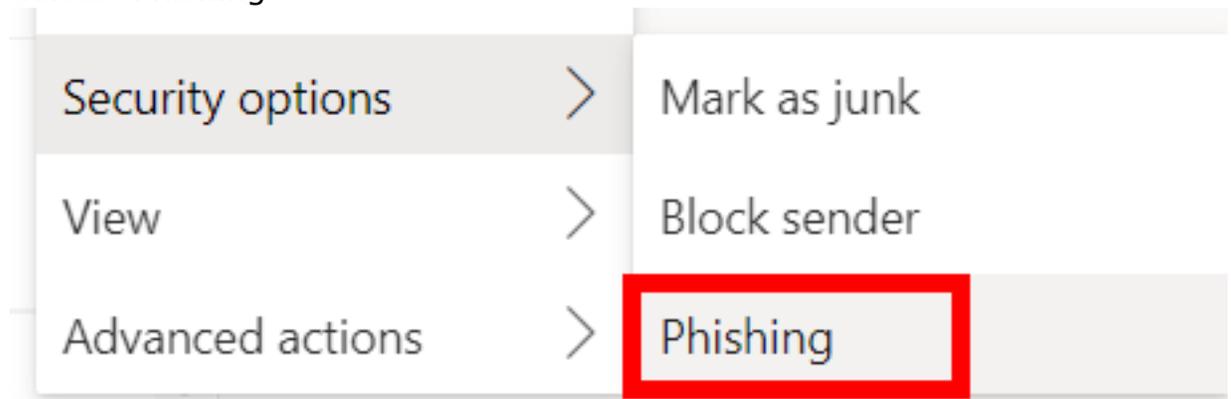
Remember, if you receive a suspicious email:

Don't reply to the email. Even if you think you know who sent the message, please do not reply. If an email account has been compromised, engaging with the sender or message content could increase the security risk.

Don't click on suspicious links or attachments. Best practice is to never click a link or open an attachment that you were not expecting.

Don't forward the email. If you receive a message with a suspicious link or attachment, you may think about forwarding the message to a colleague for insight. Never forward unusual or suspicious emails to other users. Instead, report the email as a suspected phishing attempt.

For questions or concerns please contact Tech Café.