AbleNet

Report Junk or Phishing Emails

Junk and Phishing emails are very prominent for anyone sending/ receiving emails, whether personally or professionally. We want to provide information on how to identify them, which in most cases is also the best way to avoid them.

Key characteristics of junk or phishing emails are the following;

- Messages from an unverified/ unfamiliar contact
- Major spelling, word placement, or punctuation errors
- Information regarding services that are unwanted/ unrequested
- Request for information, either personal or company-related details, outside of normal context
- Non-work appropriate content

Please Note: Suspicious emails may match any (or multiple) of the previous criteria

Junk email

Generally characterized as harmless, annoying emails soliciting products or services from an unwanted source.

With these messages, you can disregard, delete, or report them as Junk via Outlook. You can typically locate a link at the bottom of the email or go to the company's website to unsubscribe as well. With recent regulations put in place, companies are held accountable to honor your request to not be sent further emails once you've unsubscribed.

Phishing email

Phishing emails are very harmful messages, where the sender is attempting to get access to corporate or personal information. This is generally done by enticing someone to click web links or attachments that initiate malware/virus attacks.

If you receive a message that meets or contains any of the above criteria, please remember;

- Do NOT open any file attachments
- Do NOT click on any links
- Report emails to Microsoft

Reporting potential scam or phishing messages are crucial for Microsoft to aid in making our computers safe. If they can get valid details/ information they may be able to stop potential issues before they start. To report these messages to Microsoft follow these steps;

1. Open Microsoft Outlook
2. Create a new, blank email
3. Address the email to the Microsoft team to review each message type as follows:
4. Junk: email to junk@office365.microsoft.com.
5. Phishing: email to phish@office365.microsoft.com
6. Copy and paste the junk or phishing scam email into the new email as an attachment.

    Please note;

    ◦ You may attach multiple messages to this email, just be sure all the messages are the same type - either junk or phishing
    ◦ Leave the body your message empty, there is no further input needed