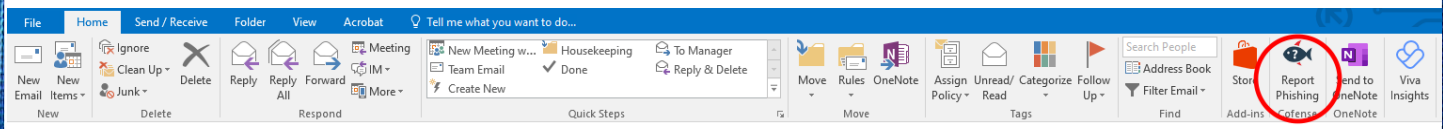
How to **Safeguard** Your Inbox:

Differentiating between **Spam** and **Phishing** in the New Year

Office of Information Technology
Division of Information Security
JANUARY 2024

As we welcome the New Year, we must understand the difference between spam and phishing in order to have a secure year. The IHS Messaging Services Team has various tools in place at IHS to filter and block phishing or spam emails from being delivered to your inbox. Please be advised that even with these tools occasionally emails get past our tools and get into your inbox. Understanding the difference between spam and phishing emails makes you better equipped to handle each one. With this knowledge, you can outsmart the phisher in 2024 and beyond!

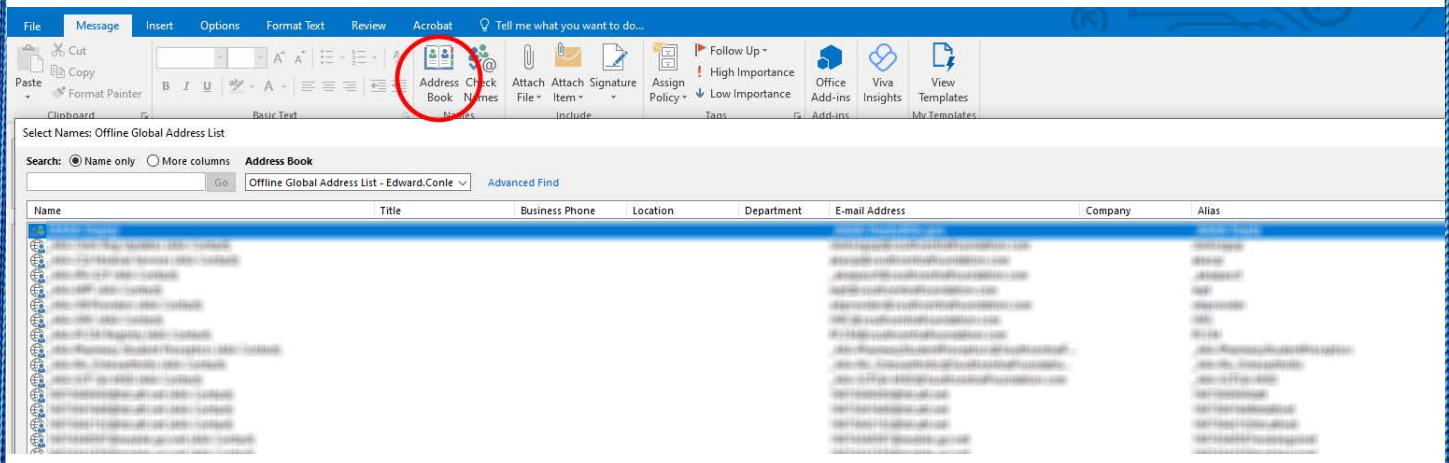
The Indian Health Service (IHS) has recently implemented Cofense Reporter, which is a tool used to assist organizations in defending against phishing attacks and other email threats. The IHS CSIRT has recently seen an influx of incidents with employees using the Cofense Reporter button to report spam. The IHS strongly recommends that Agency employees report emails they feel are suspicious by using the Cofense button located on the Outlook email home tab.



Please note that Cofense is not a replacement for the junk mail feature in Outlook. Apart from Webinar invitations asking for personal information, passive emails like notifications, advertisements, or other solicitations have a very low threat probability once investigated. Most of the real occurrences that are reported through Cofense here at IHS are marketing or advertisement emails that don't target IHS, the federal government, IT, or healthcare employees.

Before using the Cofense button to report a phishing incident, remember to check the following:

- Report emails that appear to single out the recipient personally, because of their profession or role, or because they're associated with the federal government, the healthcare industry, or the IT industry.
- IHS employees should use the HHS global address list to confirm whether the sender is an HHS or IHS employee. If the sender is a current HHS employee, hovering on the sender's email address in Outlook displays a populated contact card that does not read "Presence Unknown" and that does include the sender's avatar and contact information.

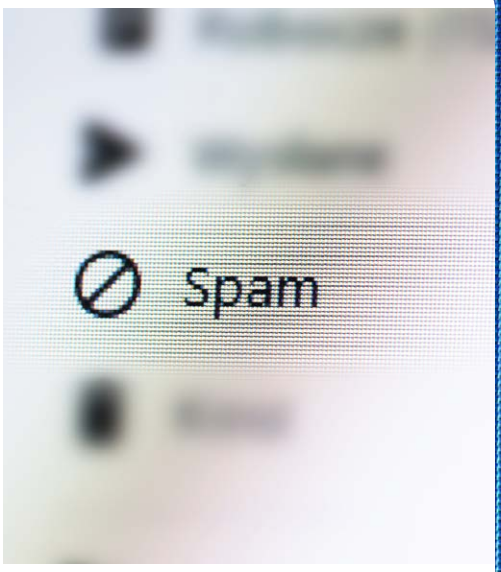


IHS employees' properly using Cofense to report phishing threats the Reporter button can significantly enhance IHS's security posture.

Please read on to learn how to distinguish between Spam and Phishing.

Spam

Spam is an unwanted or irrelevant commercial email typically sent to large number of recipients for the sole purpose of advertising a product. These messages can come in the form of emails, instant messages, social media posts, comments, and more. Although spam messages can be annoying and unwanted, they are not generally considered malicious. Spam is also known as junk mail. Spammers often obtain email addresses through data breaches, publicly available information from forums, or unsubscribe links located in spam emails.



Common examples of Spam:

Ads:
- People trying to sell goods or services you don't need or didn't request. Common examples of this are copier ink cartridges, office supplies, or car warrantees.

Chain Letters:
- A letter claiming that if you pass it on something good will happen or if you don't something bad will happen.

What is not Spam?

Personal communication, work-related communication, or educational communication emails:
- Emails received from family, friends, coworkers related to general business or personal communication.

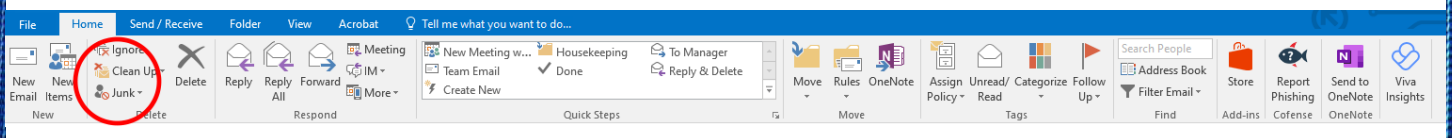
Subscription Emails:
- Advertisements, updates, and communications from organizations that you have willingly subscribed to and are interested in receiving.

Official Updates:
- Email received from online services providing legitimate updates, announcement, or security updates related to your account.

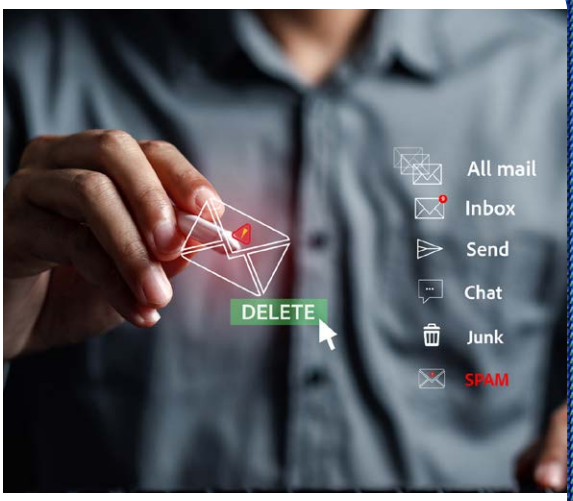
How to handle Spam received at IHS:

Do not respond:
- Avoid opening the spam message or clicking on any links located in the message. By responding, you allow the sender to confirm that your email address or phone number is correct, leading to more spam.

Mark as Spam:
- Use your email provider's spam or junk option to mark the message as spam. Using this feature allows you to automatically identify and block potential spam from your main inbox.



Delete the Message:
- Delete the spam message from your inbox or message folder immediately. Make sure that you also empty your trash or deleted items folder to permanently remove the message.



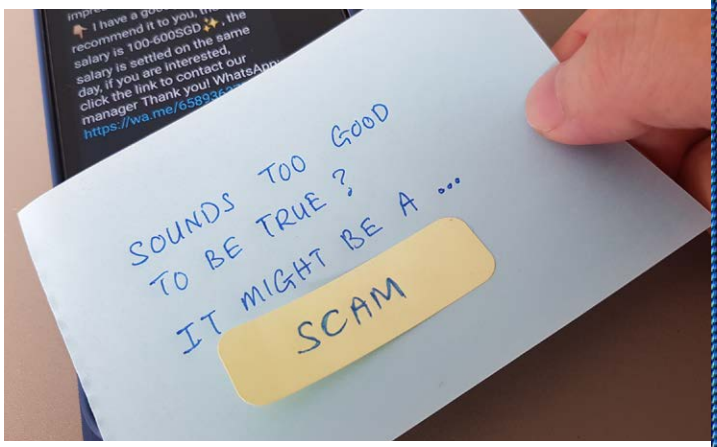
Phishing

Phishing is when cybercriminals use deceptive tactics such as sending fake emails, messages, links, or social media posts to trick individuals into disclosing login credentials, financial details, or personal information. The term “phishing” originated as a play on the word “fishing”, as cybercriminals attempt to lure or hook unsuspecting users.

Common examples of Phishing:

Emails from Government Agencies, Banks, or Financial institution:
- Emails pretending to be from a government agencies, banks or financial institutions requesting users to update their account information or confirm their identity.

Business Email Compromise (BEC):
- Cybercriminals impersonate company executives and send emails to employees, requesting sensitive information or wire transfers.



Phishing Websites:
- Fraudulent websites are designed to copy log-in pages from legit websites, misleading users to provide their login credentials, which is then stolen.

What is not a phishing email?

Expected Communication:
- Emails received from known or organizations that you have a relationship with and are expecting to receive communication from.

Employer Communication:
- Work-related emails from your employer, coworkers, or management, especially if they pertain to company policies, announcements, or tasks.

Transactional Emails:
- Emails including order confirmations, receipts, or shipping notifications from legitimate retailers or service providers.

The IHS OIT Division of Information Security wishes you a secure and prosperous year 2024!

NOTE: The links in this document are for informational purposes only and do not signify an endorsement of any products contained within the linked sites/files.

If you have any questions about this newsletter, please email Cybersecurity@ihs.gov.