Guide to Phishing and Spam

Last Modified on 02/19/2025 2:26 pm EST

This article explains the differences between phishing attempts (email messages that try to steal private information) and spam (unwanted, mass email messages). It also details what to do if a Wharton account has been compromised.

> If you have any questions or concerns about anything in this article, please reach out to the Wharton Information Security Office at security@wharton.upenn.edu.

Phishing

What is Phishing?

Phishing emails are scams sent to you by people or programs who are looking for access to your accounts or to learn valuable information about you. They often appear to be from an administrator of the email system or another user on the system. The content of the email generally is one of the following:

- a warning that your account may close if you don't use your account credentials to log into their website
- a call to click on a link to address financial or other issues
- a request to update your work data

> **Etymology of Phish:** "Phishing" emerged in the 1990s as an internet slang version of "fishing," describing the process of using messaging to lure or "fish" for users' sensitive information. The convention of replacing "f" with "ph" has its roots in the name given to early hackers -- Phreaks -- and the act of hacking was called Phreaking. The process of fishing for information became known as Phishing as these "Phreaks" were fishing for a person's information.

Phishing attempts are getting increasingly sophisticated, and while we try to block any phishing attempts of which we are made aware, no system is 100% effective. To test your knowledge of identifying these scams, check out this phishing quiz.

> ISC offers an informative training on Information Security Essentials that can teach you how to protect your data best. For more information, see Phishing & Spear Phishing .

Spam

What is Spam?

Spam emails are unsolicited messages sent in bulk. Many spam emails are sent for straightforward commercial purposes, but some are harmful phishing emails that will attempt to gather your sensitive information.

> **Etymology of SPAM:** The term "Spam" was coined in the 1990s to describe excessive, unwanted and repeated online posting and messaging. It was rooted in early internet forums and chat rooms in which users repeated

quotes from the Monty Python “Spam” comedy sketch. This sketch featured the popular Spam meat product and characters annoyingly singing "Spam" repeatedly.

Email providers (Gmail, O365) have spam filters that try to ensure untrustworthy, or possibly malicious, email doesn't make its way to your Inbox. Gmail provides basic spam filtering that will automatically move suspicious mail to your spam folder. Some email providers call this folder "Junk," so keep an eye out for either term.

For more information on spam filtering at Wharton, see our article, Spam Filtering Overview.

Check your Spam or Junk folder

It’s a good idea to occasionally look in your spam folder (sometimes called Junk, depending on the mail platform) to make sure there aren’t any important messages that were improperly marked as spam. If there are legitimate messages there, you can click **Report Not Spam** or **Mark as Not Junk** to restore them to your inbox.

Need Help?

Contact the Wharton Information Security Office: security@wharton.upenn.edu