Phishing and Spam at Wharton

Last Modified on 04/17/2025 4:25 pm EDT

Phishing

What are Phishes?

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

Phishing attempts are getting increasingly sophisticated, and while we try to block phishing attempts, 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 .

Tips to Identify Phishing Attempts

- Check the email sender. Most of the time, phishing emails come from suspicious-looking addresses.
- Look for poorly worded emails or misspellings (though scammers now use AI which makes these errors less common).
- Be cautious of unusual-looking links. For example:
  - "Helpdesk requires you to upgrade webmail by clicking http://mailverificationpage14.tk "
  - *Notice that there's no reference to Wharton, PennO365, Student Gmail, or your support team in the URL, and the extension is not a standard one. Never click on a link in a suspected phishing email.*
- When you click a link in an email, pay close attention to the actual web address you've been sent to, if it looks suspicious, do not enter your Wharton credentials.
- Wharton Computing will never ask you for your username/password via email.

When in doubt, forward suspicious emails to security@wharton.upenn.edu. Security is a shared responsibility, and your caution helps protect the Wharton community.

If ISO requests the full email header, check out how to retrieve them from an email.

Already Clicked a Link?

What To Do

1. **Reset** your Wharton and PennKey passwords.
   - If you believe your device has been compromised, use another computer or contact your IT representative to help change your passwords.

2. **Change passwords** that are similar or the same as your compromised password.
3. **Notify** your IT representative and Wharton's Information Security Office.
4. Determine if your password has been exposed in a data breach at https://haveibeenpwned.com/ and/or https://monitor.firefox.com/.

Unique, complex passwords are one of the best ways to secure your account(s). Password managers, such as Dashlane (provided by Penn), auto-fill your credentials for you, allowing for easy and convenient account management while using long and secure passwords.

For security best practices, make sure you:

- Don't reuse passwords for multiple sites or services.
- Enable Two-Step Authentication whenever possible.
- Run up-to-date virus and adware scans on your computer.

Spam

What is Spam?

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

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."

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.

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

Email Spoofing

Some spammers **spoof** email addresses that make it appear as if the mail they send is coming from a university email address. Unfortunately, there is not much Wharton Computing can do except suggest that you report the website/sender for spamming to sites like and or http://www.spamhaus.org/.

If you're unsure, you can look up the site's IP address at a site like: http://get-site-ip.com/

"Spoofing" and "phishing" often work in tandem – a spoofed email address may be a phishing attempt (but not always).

Adding Addresses to your Allowlist on Gmail

Gmail offers an option to add specific addresses or domains as "safe," so they aren't automatically marked as spam. This list is known as an "Allowlist." Your Allowlists only apply to your Gmail account and must be managed and set by you. If you want to accept all email sent from a specific address, follow these instructions:

1. Log in to your **Gmail** at gmail.com.

2. Click the gear icon in the top-right, and select **See all settings.**
3. Click the **Filters and Blocked Addresses** tab.
4. Click **Create a New Filter.**
5. In the pop-up window, enter the email address you want to add to your allowlist in the From field.
    - If you want a whole domain allowlisted, you can just enter the domain (ie, "@example.com").
6. Click **Create filter.**
7. Check **Never send it to Spam**.
8. Click **Create filter.**

Adding Addresses to "Safe Senders" in Office365

Office 365 allows users to designate "Safe Senders." Safe Senders are not automatically marked as spam. This functionality is available for the Outlook web client and the Outlook Windows client. It is not available for the MacOS Outlook client. See this article from ISC for directions.

Need Help?

Contact the Information Security Office (ISO): security@wharton.upenn.edu