Guide to Phishing and Spam

Last Modified on 02/14/2024 1:48 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.

Table of Contents

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, or Phishing Emails Seen at Penn.

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 (many phishing attempts are crafted by non-native English speakers).
- 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 the questionable email to your Wharton Computing support team (see "Contact" below) or security@wharton.upenn.edu. It's better for everyone if you are cautious, and we are happy to confirm for you. Security is everyone's business, and the more information our Security teams receive from you, the safer everyone will be.

^Top

Compromised Account

There are several ways your Wharton account can be compromised:

- You become the victim of a virus or phishing attack.
- You leave yourself logged into a public machine on Wharton's campus or on another public machine.
- Your computer or smartphone has been stolen.
- You shared your password with someone.

> If the account compromised could have had access to your personal computer, and you have sensitive information stored on that device, be sure to change any passwords for online banking and other secure sites.

What To Do

1. **Reset** your Wharton and PennKey passwords
   - Resetting your PennKey password will also reset your Google Account password* and PennO365 password.
   - If you believe your device has been compromised, use another computer or call Student Support to help you change your passwords.
2. **Change passwords** that are similar or the same as your compromised password
   - Unique, complex passwords are one of the best ways to secure your account(s). Password managers, such as LastPass, auto-fill your credentials for you, allowing for easy and convenient account management while using long, complex, and secure passwords.
3. **Notify** the appropriate Wharton Computing support team (see "Contact" below)
4. **Complete** the Gmail Security checklist
5. Determine if your password has been exposed in a data breach athttps://haveibeenpwned.com/ and/or https://monitor.firefox.com/

* If your account was created **before December 2023**, resetting your Wharton password will reset your Google Account password

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

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 (seeHow To Protect Yourself Against Viruses).

^Top

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.

Email Spoofing

Some spammers "spoof" email addresses to make it appear as though the mail they send is coming from a university email address. Unfortunately, there is not much Wharton Computing can do to stop this. You can report the website/sender for spamming to sites like http://www.spamhaus.org/.

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

“Spoofing” and “phishing” often work in tandem - a spoofed email address may be aphishing 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: https://www.isc.upenn.edu/how-to/penno365-configuring-safe-senders-lists

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.

^Top

Need Help?

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

Students: contact support@wharton.upenn.edu or call (215) 898-8600

Faculty & PhD Students: contact your Wharton Computing representative.

Staff: email admin-support@wharton.upenn.edu