# Phishing Emails: What They Are & What To Do

Last Modified on 08/13/2019 1:08 pm EDT

This article provides information on phishing emails, how they affect your accounts (Wharton or Personal), and steps you can take to avoid or address the consequences.

## What are Phishes?

Phishing emails are sent to you by people or programs who are looking for access to your accounts or any valuable information. 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:

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

>> **Common Phishing Emails Seen at Penn**

Phishing attempts are getting increasingly sophisticated, and while we block any phishing attempts no system is 100% effective.

## Tips to help identify phishing attempts

- **ALWAYS** check the email sender. Most of the time phishing emails come from suspicious-looking addresses.
- Be on the lookout for poorly worded emails or misspellings (many phishing attempts are crafted by non-native English speakers).
- Many phishing emails contain unusual looking links. Here are recent examples:
    - "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.
- Even if a link looks legitimate, be cautious and consider the other tips listed above. 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 IT support team or security@wharton.upenn.edu. It's better for everyone if you are cautious, and we are happy to confirm for you.

# Already Clicked a Link?

If you do click on a link from a phishing email, follow these steps:

1. Change your Wharton account password immediately.
2. Contact your support provider immediately for additional help identifying any unanticipated consequences.
3. If you use the same password (or similar ones) for other Wharton or Penn accounts, **change those as well**.
4. If you use the same password (or similar ones) for your personal accounts, **change those as well**.

We recommend that you maintain separate passwords for each website you log into. Consider using LastPass , the password manager service provided to the Penn Community (or a similar product) to help you keep track of your passwords.

## Password Change Links

- Wharton password change: https://password.wharton.upenn.edu
- PennKey password change: https://weblogin.pennkey.upenn.edu/changepassword
- Penn O365 password change: https://office365.password.isc.upenn.edu/

# Questions?

Students - Wharton Computing Student Support

Faculty - Academic Distributed Representatives

Staff - Administrative Support