eMail Spam and Phishing

Phishing attacks, purporting to be from various Yale organizations, continue at Yale. These messages attempt to trick individuals into providing their Yale log in information. As Yale ITS identifies malicious messages, we block them from Yale email accounts, but, the individuals behind phishing messages shift their methods as we block them. Expect subject lines and from fields to vary and change quickly. It is important to know that at some point, you may see a message like this in your Inbox. If you see such messages, you can safely delete them.

Information

Phishing attacks, purporting to be from various Yale organizations, continue at Yale. The following is an example of a phishing attack:

SUBJECT: Yale.

This message is from your Yale account support desk; this email is to inform you that your Yale account is due for update and will be shutting down any moment from now. kindly click the following link and fill out all the information in the link to update your Yale account immediately to remain active

"http://firstwebabmin______--.com"

If you can’t click the link button, you can update your email account by copying and pasting (or typing) the above link into your web browser:

Tanks Account Management Team

Web Admin Yale

Reporting spam and phish is now easier

ITS implemented a new feature in Office 365 to enable easier reporting of suspected spam and phishing messages.

1. Open the message you’d like to report as spam
2. Select the Report Message button from the top/menu area within the message, and select Junk. This will immediately move the message to your Junk folder, and also adds the sender to your Blocked Addresses list so the sender cannot email you again. Additionally, these messages will be reported to our vendor, Microsoft, to improve their spam management feature in the future.

Learn more about reporting suspicious emails

Important reminders:

- Report Spam or Phishing emails and then delete the message immediately
- Don’t click on any links in a suspicious messages
- Never supply your passwords or other personal information in an email message
- Yale ITS will never ask you for your password or sensitive information (Social Security numbers, bank account numbers, etc.) via email or telephone
- Visit the ITS Secure Computing website to learn more about phishing and ways to guard your privacy: http://its.yale.edu/secure-computing

What do to if you have fallen prey to a phishing scam:

- If you believe you might have revealed sensitive Yale University information, contact ITS Information Security staff (information.security@yale.edu) immediately
- If your personal financial accounts may be compromised or if you believe you might have revealed information that could be used for identity theft or fraud, see Yale’s guide to protecting your identity: http://its.yale.edu/secure-computing/Identity-theft-and-phishing

What do you if you are notified by a member of SOM IT that your account has been compromised:

You must run an antivirus scan AND a Malwarebytes scan. Once the scans are complete, save your results and stop by the SOM IT Help Desk in room 1430 to show your computer is clear of viruses and malware. SOM IT will then be able to unlock your account and get you back on the Yale network.
Related articles

- Known Issues: Office Apps Continuously Prompting for Password (Windows)
- How to Handle Cached Global Address Entries
- What is Office365
- eMail Spam and Phishing
- Open a Departmental or Group mailbox in Outlook client (Windows)