Link Safety in Email

How to protect yourself and Johns Hopkins from cyber attacks

Overview

Ransomware, malware, and data breaches of high-profile organizations continue to make headlines. From Baltimore County Public Schools to Colonial Pipeline, attackers have proven that no IT environment is completely impenetrable, and the impact of such attacks can be devastating.

Phishing is a tactic in which a bad-actor will pose as a legitimate business or personal contact in an attempt to deceive an individual into sharing sensitive information that could allow the attacker to exploit the institution. A common phishing tactic is to embed deceitful URLs that appear benign at first glance, but actually lead to a web site or file that is designed to open a door to further attacks.

Before clicking a link in an email, it is important to examine the URL (destination) of the link to gauge its legitimacy.

Your responsibility as a Johns Hopkins email user

Attackers can be exceptionally adept at disguising themselves as someone familiar or non-threatening. To protect yourself and Johns Hopkins, you should consider the following when reading your email:

- Does the topic of the email seem strange or unusual?
- Are there typos or grammatical errors in the body of the email?
- Do you recognize the sender?
    - Check their *full email address,* not just their name
- Were you expecting this email, or does it align with recent work/activity?

If the email seems suspicious, *do not open any links or attachments,* and forward the email *as an attachment* to spam@jhu.edu

Examining Links

Regardless of whether an email seems legitimate, you should always examine the URL (destination) of a link before clicking it to ensure it leads to an expected domain. Learn how to do this in the *How to view the URL of a link* section below.

What to look for

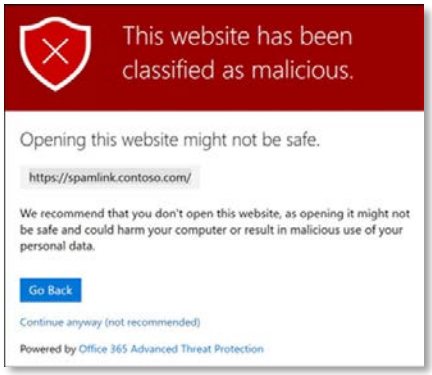
- Check that the link matches the resource you are expecting
    - E.g. you are sent a link that appears as MyLearning. If you hover over this link, you will see that it will actually take you to www.google.com.
- Make sure the domain (*x.com, x.edu,* etc.*)* is accurate. Often attackers will mimic familiar domains by making slight variations to the original
    - E.g. Instead of a link to johnshopkins.edu, they send a link to jonhopkinsedu.com

Safe Links – a built-in safeguard against malicious links

IT@JH leverages Microsoft's *Safe Links* to assist in preventing phishing and other cyber-attacks originating from links within email. Safe Links will scan the URL of any links clicked within an email to verify if it is on a block-list, thus offering a second line of defense. While Safe Links is a powerful and effective tool, it is not infallible and you should continue to examine links before clicking them.

What happens if you click on a link that Safe Links determines is unsafe?

You will be presented with a message stating the website will not be safe. DO NOT PROCEED to the website, and contact the IT Help Desk for further triage.



How to view the URL of a link

Safe Links works by rewriting URLs embedded in email so that they are scanned by Microsoft when they are opened. As a result of this process, **URLs will appear differently based on what mail client you are using. If you have any difficulty interpreting a URL or suspect the email is malicious, please send the email *as an attachment* to spam@jhmi.edu.**

In the following examples, the message appears to be sent by "Johns Hopkins HR Services," but the link in the email leads to login.028426.com, which is not a Johns Hopkins domain.

Outlook 2019 and Office365 (Windows/PC)

Hover your cursor over the link to view the URL.

Outlook 2016 (Windows/PC and macOS)

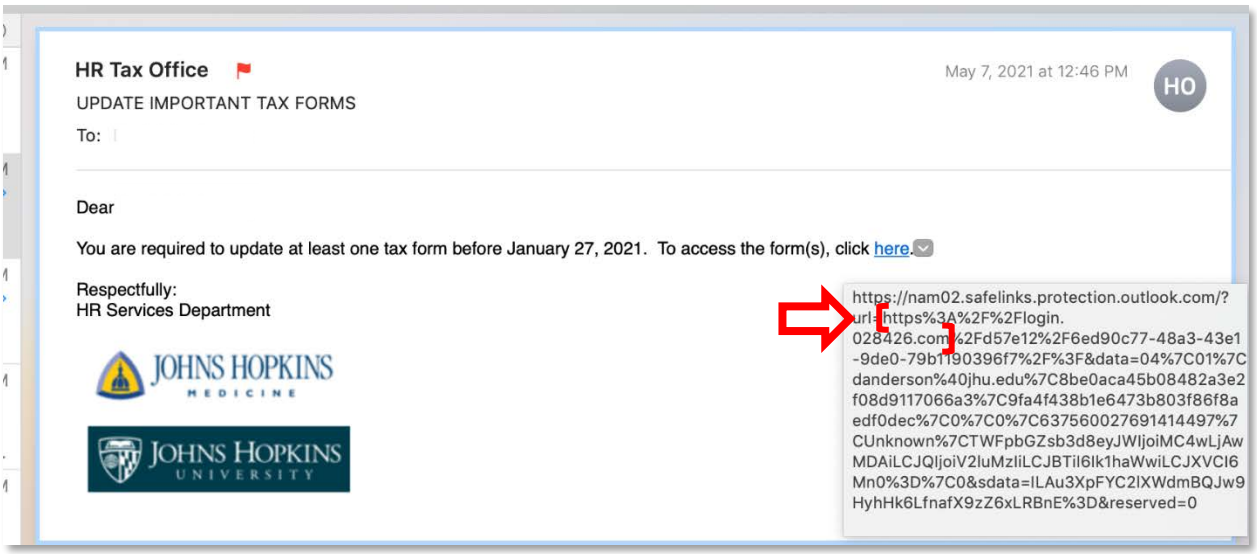
Hover your cursor over the link to view the URL that Safe Links has rewritten.

The original URL will appear after a Safe Links prefix. Check the URL after the text "…url=https://"

Mac Mail

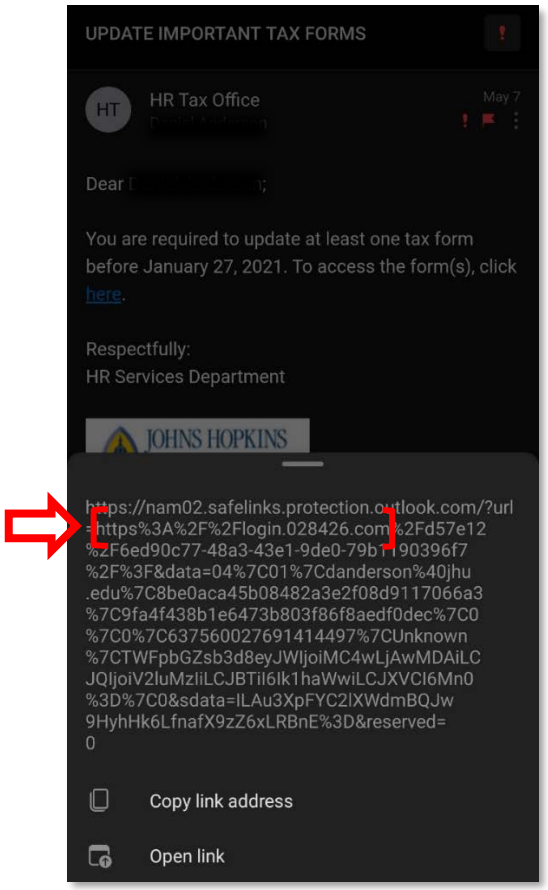
Hover your cursor over the link to view the URL that Safe Links has rewritten.

The original URL will appear after a Safe Links prefix. Check the URL after the text "…url=https://"



Outlook App (Android)

Press and hold the link – the original URL will appear after a Safe Links prefix. Check the URL after the text "…url=https://"



iOS Mail App and Outlook App (iOS)

Press and hold on the link and a preview will appear. Examine the URL domain in the upper left.