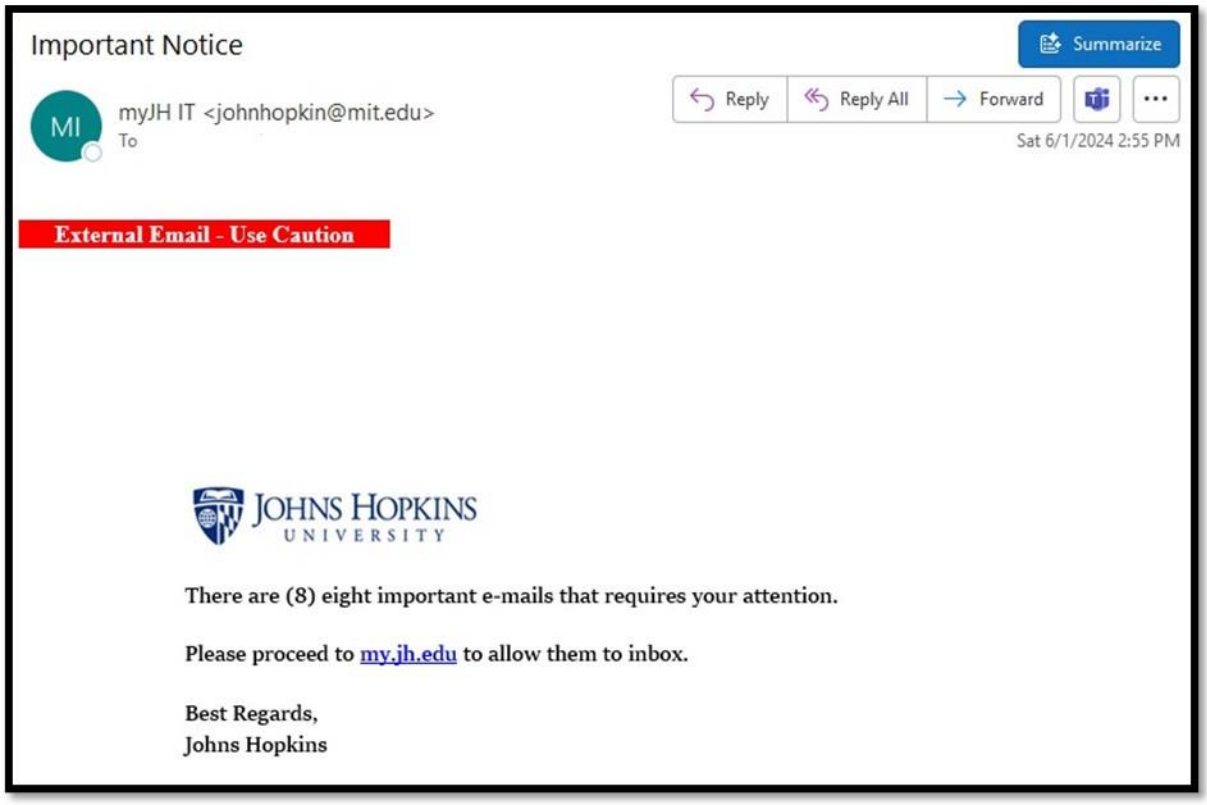
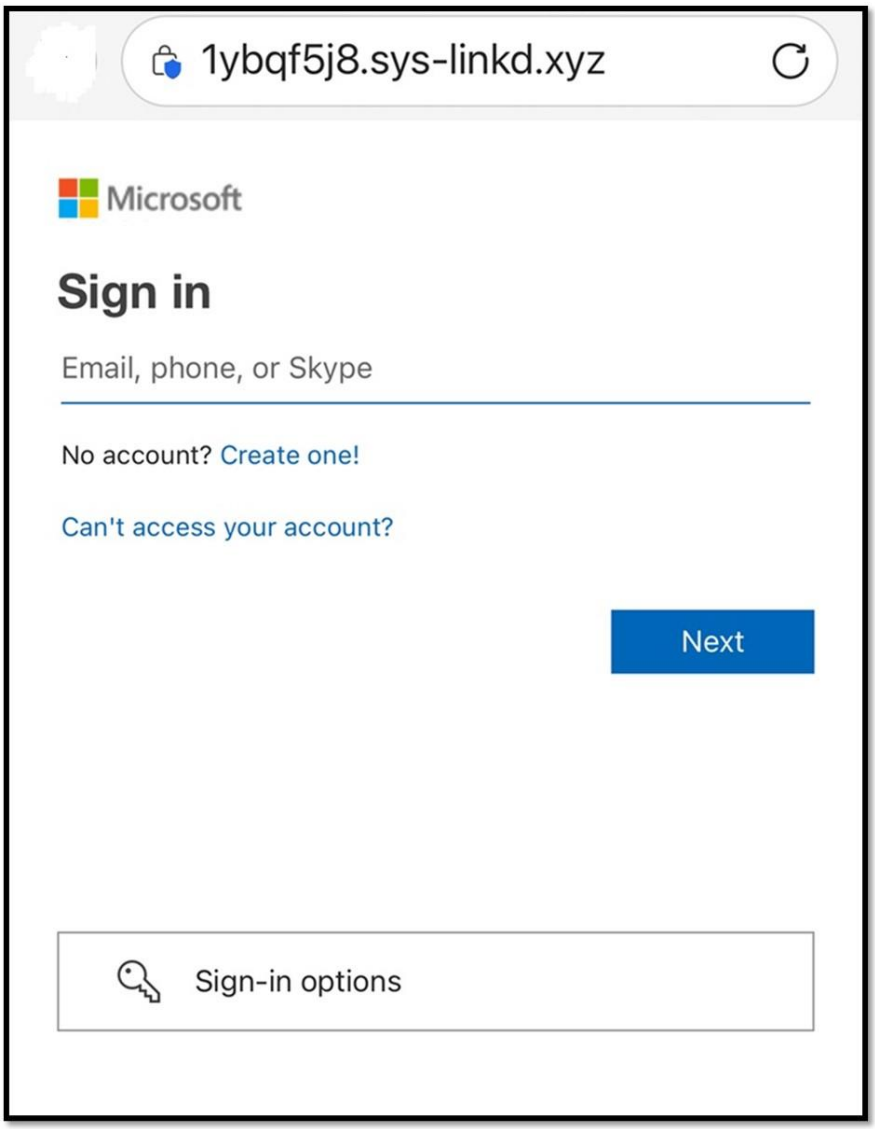
Direct Deposit Scam Targets Payroll

Payroll are now popular targets for criminals. The direct deposit scam is the latest trick hitting employees. The Internal Revenue Service (IRS) and law enforcement are warning employees to be on the lookout for this type of phishing scam.

In the scam, the criminal emails a request to the employee from a fake email address. The phishing message references myJH IT with an email address of johnhopkin@mit.edu and directs users to click on my.jh.edu, which is hyperlinked to a spoofed Microsoft login page.



The criminals will then provide a fake Microsoft login Page. The fake Microsoft login page starts with https://1ybqf. A valid Microsoft login page will begin with https://login.microsoftonline.com. The Messaging team has blocked the delivery of this phishing email and will purge those delivered.



The criminals provide new bank account and routing numbers, which leads to a new bank account the scammers control.

Scam emails usually have grammatical or spelling mistakes, but recent scam attempts include emails that were "well written, cordial and lack the misspellings, grammar mistakes and exclamation points that would trigger many popular email filters that search for spam or phishing attempts." To make the email look even more realistic, "the scammers may even spoof the forms used by the company when making these requests."

Phishing and other Email Scams: Dos and Don'ts:

1. *DON'T* send passwords or any sensitive information over email.
2. *DON'T* click on "verify your account" or "login" links in any email.
3. *DON'T* reply to, click on links in, or open attachments in spam or suspicious email.
4. *DON'T* call a phone number in an unsolicited email or give sensitive data to a caller.
5. *DO* report impersonated or suspected email to spam@jhu.edu
6. *DO* be cautious about opening attachments, even from trusted senders.

If you receive a scam email you can report them to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3). You may also file a complaint with the IC3 if you believe you have been the victim of an Internet crime at https://www.ic3.gov.