**May 2026 Phishing Results**

OIT's May phishing simulation email was titled, *Meeting Invitation*. The scenario included a link requesting the recipient to "Launch Remote Session". The email instructed the user to download and open a file to start the remote session.

**Clues to Spot in this Scenario:**

**Issue: Unknown Sender**

The sending email address was *Jorge Powell rpowell74@securefilesshares.com*. The email domain is unknown and should not be trusted.

**What to do:**

Do not click on the link to find more information. The sender is unknown and did not provide any meeting context so you should report the email as suspicious.

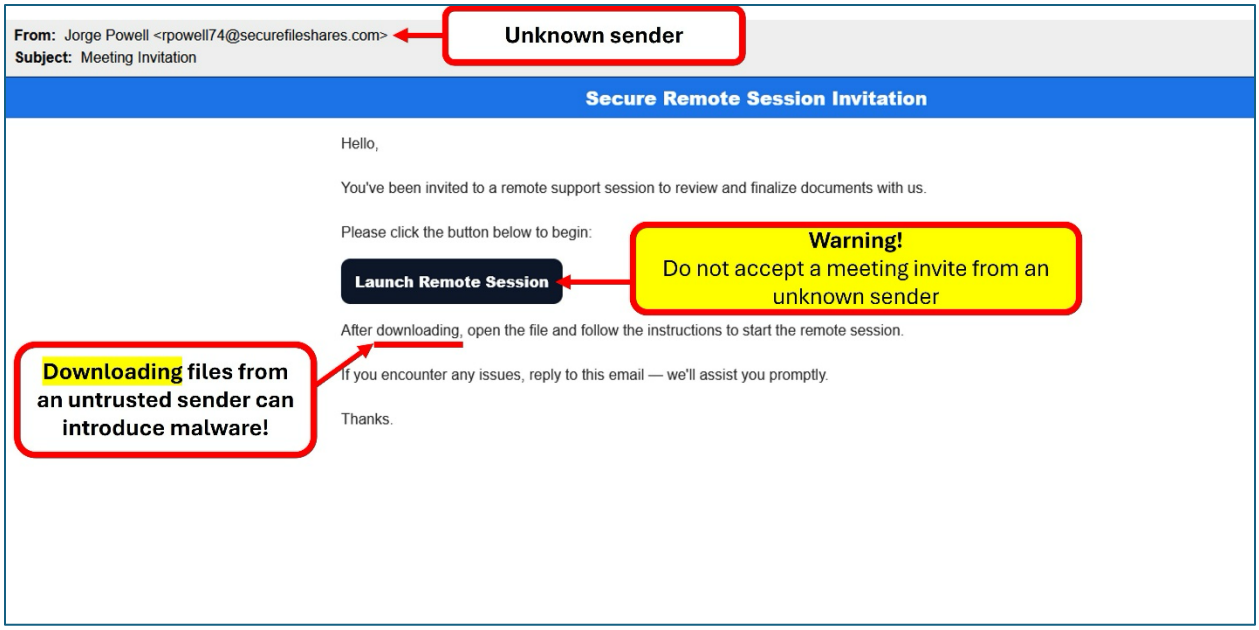
**Issue: Unknown meeting request**

Meeting invites delivered through phishing emails take advantage of our natural tendency to trust familiar workflows. Attackers rely on users accepting these requests out of routine and habit without carefully verifying the source. In this case, the invite prompted the user to download a file which is an especially high-risk action. Downloading files from unknown or untrusted senders can introduce malware, such as ransomware, spyware, or credential-stealing tools, which may silently compromise the system, spread across the network, or expose sensitive data.

**What to do:**

Review the email when you have time and are not in a hurry. Verify the sender by checking the email carefully and confirm through a trusted method, such as a phone call to the sender. Always report emails that are unexpected and from an unknown sender, especially one that lacks specific content.

View the full scenario:




## Good News

**670** employees reported the phishing scenario. Great job MC!

## Opportunities for Improvement

**27** employees clicked the link

If you suspect an email may be a phishing attempt, let IT Security analyze the email for you by Reporting the email using the report phishing button.