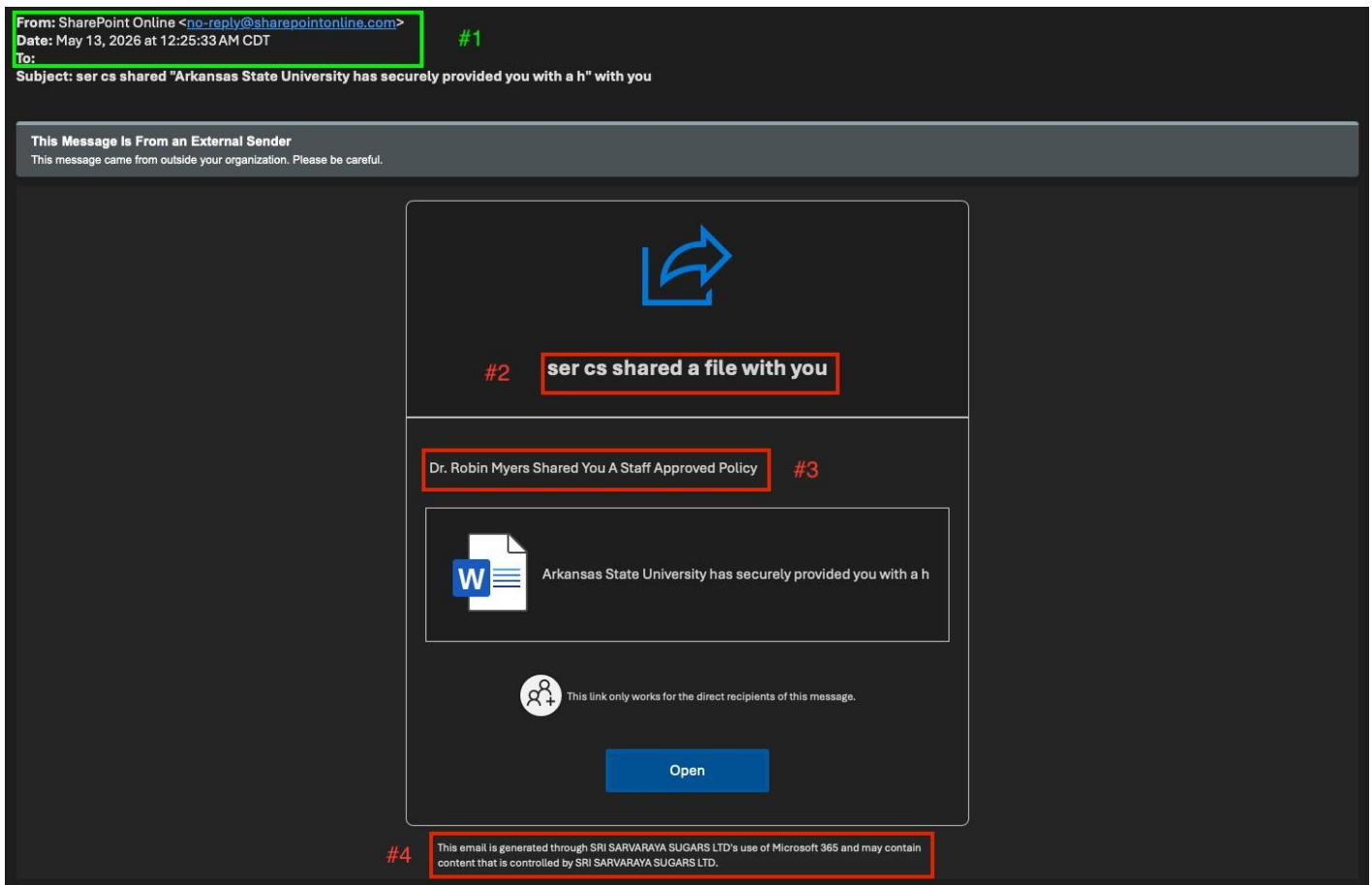


SharePoint Phishing Campaign

This article highlights a campaign seen on campus during the second week of May 2026. This malicious phishing campaign saw users receive legitimate SharePoint file sharing emails from threat actors external to our organization. The following details specific components of this email and takes a deeper dive into what indicators exist within the email.



- **#1 – Header information:** A solid first stop in identifying potentially malicious emails. In this attack however, the traffic is **legitimate** SharePoint traffic. This occurs because another organization has either been maliciously created or has had a security incident leading to their users being able to share malicious documents.
- **#2 - “Who” is sharing the file with you:** It can be tricky for a threat actor to perfectly manipulate the necessary fields in a malicious email where there are no suspicious gaps. In this instance, that is displayed in the “who” is sharing a file with you.
- **#3 – Creating a sense of urgency:** Threat actors will lean on publicly available information to help create a sense of urgency and legitimize some content in the attack. In this instance, the threat actor is doing this by manipulating fields to imply this message comes from Dr. Robin Myers. Sometimes traffic like this can be legitimate, so reviewing the message as a whole helps to narrow things down.

- **#4 – Footer information:** In this instance, the largest crack in this attacks foundation is the footer information SharePoint has automatically added to their traffic. This clearly conveys that the message originates from SRI SARVARAYA SUGARS LTD's SharePoint, which is not associated with Arkansas State University.

Having reviewed all components of the email and not just the header, we can safely confirm this email is malicious and should be reported to security@astate.edu so that it can be removed from everyone's inbox.

What You Should Do

Be Skeptical of Unknown Senders: If you receive an unexpected or unusual email, verify its legitimacy by contacting the sender through a known and trusted channel.

- **Requests to Respond to Personal E-Mails:** If you receive an e-mail from an A-State student or faculty, and there is a request to respond with information to a personal e-mail (e.g. Gmail, Yahoo, Hotmail etc.) please do not respond and forward to security@AState.edu for review to determine the legitimacy of the sender/e-mail.
- **Report Suspicious Emails:** If you receive a suspicious email, do not respond, click any links, or download attachments. Instead, report it by forwarding the email to security@AState.edu.
- **A Suspicious Email Was Interacted With:** If you received and interacted with an email before determining it was suspicious, please take the following steps:
 - Immediately take steps to reset your account password. This crucial step helps ensure that any access a threat actor may have gained is revoked.
 - If malicious attachments are downloaded to your asset, be sure to delete them.
 - Contact security@AState.edu to report the incident. Be sure to provide details of the incident, including forwarding the malicious email to our team and detailing if attachments were downloaded.

Interested in additional information security training? The A-State IT Security team holds regular in-

person training sessions on campus. Be sure to check the Daily Digest for advertisements on the next training session.

Revision #3

Created 2026-05-15 14:38:53 UTC by Jacob Weaver

Updated 2026-05-15 16:22:34 UTC by Jacob Weaver