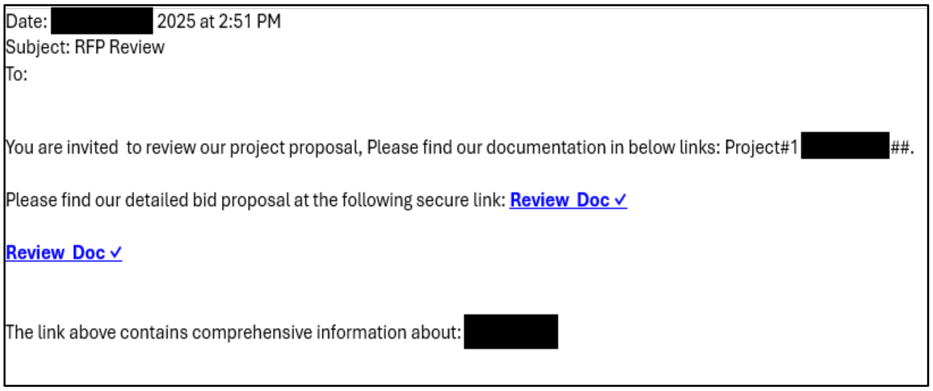
Cybersecurity Awareness Bulletin

Malicious URLs

Overview: The Mississippi Cyber Unit (MCU) is warning stakeholders of active phishing schemes in Mississippi that distribute malicious URLs. An employee received an email from a threat actor posing as a legitimate vendor that included relevant information and an attachment about a project on which the entity was actively engaged (see *Figure 1*). Malicious URLs are designed to deceive users into downloading malware, stealing personal information, or engaging in other harmful activities. These URLs often impersonate legitimate websites and/or business documents from reputable companies and vendors, making it crucial to be vigilant about checking any URLs before interacting with them. In this case, upon opening the attachment, an email was automatically sent from the employee's address to other employees. This subsequent email contained a link to a credential-harvesting website (see *Figure 2).* Credential harvesting is a technique where attackers steal users' login information, such as usernames and passwords, through fake websites or login portals. This stolen data can then be used to gain unauthorized access to accounts, leading to potential data breaches and identity theft.



Date: [redacted] 2025 at 2:51 PM
Subject: RFP Review
To:

You are invited to review our project proposal, Please find our documentation in below links: Project#1[redacted]##.

Please find our detailed bid proposal at the following secure link: **Review Doc ✓**

Review Doc ✓

The link above contains comprehensive information about: [redacted]

Figure 1: Example of the Phishing Email sent to Mississippi entity

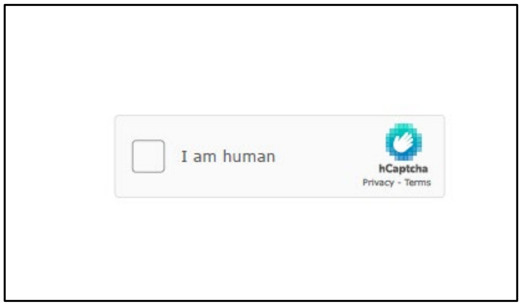


Figure 2: Example of Credential Harvesting Portal

The MCU assesses with high confidence that threat actors will continue to actively target entities in Mississippi through phishing emails, SMS messages, and other communication avenues to distribute malicious URLs.

Recommendations: The Mississippi Cyber Unit offers these recommendations to organizations to address the likelihood of succumbing to an attack.

- Hover over all links to preview the address without clicking, ensuring it matches the expected domain. Look for misspelled words or letters replaced by numbers (i.e., “O” for “0”).

- Use tools like URL scanners or browser extensions that analyze links for potential threats.

- Use URL expanders to reveal the full address of shortened URLs before clicking on them.

- Check the File Extension. Be cautious of attachments with unusual or double file extensions.

- Avoid giving personal or financial information without verifying its authenticity. Confirm its legitimacy by reaching out through a verified communication avenue. Confirm contact info sent in emails or text messages.

Resources

The links below contain information on this advisory and are not maintained by the Mississippi Office of Homeland Security (MOHS). Links to are provided for the reader's convenience and do not represent an endorsement by MOHS or the Department of Public Safety (DPS) of any commercial or private issues, products, or services.

- Five ways to check shortened links for safety | by James White | Medium
- VirusTotal - Home
- Convert any URL or Web Page to PDF. Online HTML to PDF API service.

Report Suspicious Activity

Stakeholders can report suspicious activity to ms-cyber@dps.ms.gov or by phone at 601-933-7200; or 1-888-4SAFE-MS. This email is not monitored 24 hours a day, and if there is an emergency, please dial 911. Citizens should always call local law enforcement.

(U) Standing Information Needs (SINS) Supported

HSEC-1.1: Cyber Attacks and Exploitation

MS-14000-09: Cyber Crime