# Cyber Threat Intelligence (CTI) Submission Form: Suspicious Message

## Attack Summary

Received time: Click or tap to enter a date.

Sender: Click or tap here to enter text.

Recipient: Click or tap here to enter text.

Subject: Click or tap here to enter text.

Header attached: ☐

What kind of message are you reporting?

☐ Phishing ☐ Spear Phishing ☐ Scam ☐Business Email Compromise (BEC)

☐ Smishing ☐ Other: Click or tap here to enter text.

What was the goal of the message sender?

☐ Financial Gain ☐ Credential Harvest ☐ Deliver Malware

☐Obtain/Gather PII ☐ Other: Click or tap here to enter text.

## Analysis

Was this message spoofed?

☐ Yes ☐ No ☐ Unsure

Was this message sent by a compromised Maryland organization’s email address?

☐ Yes ☐ No ☐ Unsure

If yes, which organization was compromised? Click or tap here to enter text.

If the affected organization was not your own, has your organization notified the affected organization? ☐ Yes ☐ No

Did the message contain any attachments?

☐ Yes ☐ No

If yes, have the attachments been analyzed? What were the findings?

Click or tap here to enter text.

Did the message contain any links?

☐ Yes ☐ No

If yes, have the links been analyzed? What were the findings?

Click or tap here to enter text.

## Scope

How many users received this message? Click or tap here to enter text.

## Reporting

**Indicators of Compromise (IOC) or Indicators of Attack (IOA):**

*List all indicators and describe malicious behavior associated.*

Email Address(es):

Sender email address: Click or tap here to enter text.

If different than sender:

Reply-to email address: Click or tap here to enter text.

Original sender email address: Click or tap here to enter text.

Other related email address(es): Click or tap here to enter text.

Message Subject(s): Click or tap here to enter text.

Domain(s): Click or tap here to enter text.

IP(s): Click or tap here to enter text.

URL(s): Click or tap here to enter text.

Filename(s): Click or tap here to enter text.

Hash Value(s): Click or tap here to enter text.

Other: Click or tap here to enter text.

**Non-Malicious (Legitimate Application Malicious Execution [LAME]) Observables**

*List all indicators and describe malicious behavior associated.*

Email Address(es): Click or tap here to enter text.

Message Subject(s): Click or tap here to enter text.

Domain(s): Click or tap here to enter text.

IP(s): Click or tap here to enter text.

URL(s): Click or tap here to enter text.

Filename(s): Click or tap here to enter text.

Hash Value(s): Click or tap here to enter text.

Other: Click or tap here to enter text.

## Attribution

The above information is ok to be share with:

☐ Members without attribution ☐ Members with attribution ☐ The public without attribution

☐ The public with attribution ☐ Do not share

The above information is being shared with the following TLP classification:

☐ RED ☐ AMBER+STRICT ☐ AMBER ☐ GREEN ☐ CLEAR

For more information about Traffic Light Protocol (TLP) definitions and usage: <https://www.cisa.gov/tlp>

## Questions/Comments/Additional Information

Click or tap here to enter text.

## Incident Reporting

In the case of a cybersecurity incident related to information found in this threat bulletin, Md. Code, Public Safety Article § 14-104.1 (c)(2) and Md. Code, State Finance & Procurement Article § 3.5- 406(b)(2)) mandate that you report this via the [Maryland Incident Reporting System](https://doitmaryland.service-now.com/cybersecurityincident/). It is also recommended that you submit any shareable cyber threat intelligence to the MD-ISAC via the MD-ISAC Threat Intelligence Platform (TIP).