THREAT BULLETIN

AR20221222–006 [Advisory Report] Social Engineering Awareness In Advance Of 2022 Holiday Season

TLP White

DESCRIPTION

TLP:CLEAR (TLP v1 WHITE) = Disclosure is not limited.

Summary

Social engineering continues to remain a significant threat to users worldwide, and continues to be reported by MD-ISAC members. During this end-of-year season, when attackers often take advantage of holiday celebration, end-of-year finances, and company time off, the MD-ISAC would like to remind its members to remain vigilant of cyber attacks, specifically social engineering and financial scams.

What to look out for

Social engineering can be accomplished via SMS, voice calls, and email messages. The best defense against social engineering is user training – the more social engineering red flags a user is aware of, the less likely the user is to fall for a scam or cyberattack.

Social Engineering Red Flags

- Requests for money
- Request for information validation
- Unrecognized file attachments
- Unanticipated requests
- Tech Support request remote access to a device
- Fake charity fundraising
- Spelling and grammar errors
- Communication from unknown entities

Incident Response

If administrators discover signs of attack or system compromise, the MD-ISAC recommends they:

- Immediately isolate affected systems.
- Collect and review relevant logs, data, and artifacts.
- Consider soliciting support from a third-party incident response organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
- Report activity related to this bulletin to the MD-ISAC via Maryland's 24/7 Operations Center (md-isac@maryland.gov or (410) 697-9700 - option #5).
- Report any incidents to the MDSOC by filling in this form.

Contact Information

To report suspicious or criminal activity related to information found in this Threat Bulletin, contact the Maryland Security Operations Center at (410) 697-9700 or by email at md-isac@maryland.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. Please state in the report if you are requesting incident response resources or technical assistance related to the incident.

TLP:CLEAR (TLP v1 WHITE) = Disclosure is not limited.

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