MS-ISAC®

MS-ISAC Security Primer

Spear Phishing

July 2018, SP2018-0631

Spear phishing occurs when cyber threat actors send a targeted electronic communication to an individual or a small group of users, while masquerading as legitimate entities, in an attempt to gain unauthorized access to private, sensitive, or restricted content. Spear phishing emails are designed to socially engineer a response from the recipient. Through the response, recipients may unwittingly divulge information or click on a link that leads to a fraudulent website designed to harvest information, such as login credentials. Once collected by the cyber threat actor, the victim's information or login credentials may be used to further compromise systems and networks. Often, spear phishing attempts impose artificial time constraints to create a sense of urgency that clouds a victim's initial judgment.

TECHNICAL RECOMMENDATIONS:

- Flag emails from external sources with a warning banner.
- Implement filters at the email gateway to sift out emails with known phishing indicators, such as known malicious subject lines, and block suspicious links.
- Adhere to the Principal of Least Privilege. If a user has no need for administrative access in order to carry out their daily activities, they should not have an administrative account. This can minimize the damage caused by malicious activity carried out under the user's credentials.
- Implement Domain-based Message Authentication, Reporting, & Conformance (DMARC), a validation system that minimizes spam emails by detecting email spoofing using Domain Name System (DNS) records and digital signatures.

Other types of phishing include:

- ***Smishing ("SMS Phishing") involves a user opening a malicious SMS or text message on a mobile device.***
- ***Vishing involves a cyber threat actor attempting to gather information over Voice over IP (VoIP) phones.***
- ***Whaling is a spear phishing attempt directed towards a senior executive or other high profile target.***

ORGANIZATIONAL RECOMMENDATIONS:

- Provide social engineering and phishing training to employees. Urge them not to open suspicious emails, click links contained in such emails, post sensitive information online, and never provide usernames, passwords, and/or personal information to any unsolicited request.
- Conduct organized phishing exercises to test and reinforce the concepts using services such as those provided by CIS.
- Implement a standardized protocol for reporting phishing attempts to the Information Technology (IT) department.

USER RECOMMENDATIONS:

- Do not open suspicious emails or click on unknown links. The easiest way to check a link is by hovering over it with your mouse. This allows the true destination of the link to appear in the bottom left corner of your browser window or next to your mouse pointer in Microsoft Outlook.
- Never reveal personal or financial information in response to an email. Legitimate organizations will never ask for this information in an unsolicited email.
- If the message appears to be a phishing email, do not respond. Report it to the IT department immediately and await further instruction.

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.