

SERVICE BRIEF FOR **PHISHING CAMPAIGN ASSESSMENT**



Lodestone's Phishing Campaign Assessment prepares your personnel to combat one of the most common initial intrusion vectors used by threat actors. Threat actors use phishing to imitate legitimate online services, other businesses, or individuals to manipulate their victims into clicking malicious links or downloading malicious files that could enable unauthorized network access or a data breach.

Our assessment measures your employees' susceptibility to email phishing lures that are commonly used to steal sensitive information or obtain initial, unauthorized access to a network. Arm yourself to understand your employees' security awareness and identify critical areas where additional training and planning can strengthen your security posture.

Lodestone's Phishing Campaign Assessment measures your company's susceptibility to the phishing emails that are often used to steal sensitive information or provide an initial access point into a network via a malicious link or attachment. Our experts give you the experience of a realistic phishing campaign without the risk to your organization, gathering critical metrics at every phase of the attack, including the number of employees that opened the phishing email, clicked the malicious link, and submitted user credentials.

The information gathered during the campaign's initial phase is compiled into a report describing the number and details of each email sent, along with the statistics of how many employees opened, clicked, and submitted user credentials.

BENEFITS

- Decreasing security risks to your organization due to social engineering attacks involving human manipulation and deception.
- Increasing employee awareness to form a solid first line of defense against malicious emails. Fostering a strong security posture and ensuring that everyone is accountable for making policies, procedures, and tech solutions genuinely effective.
- Fulfilling your organization's regulations and standards, conducting regular training sessions for employees and monitoring the effectiveness of such training sessions.

METHODOLOGY

Lodestone's Email Phishing Campaign Assessment simulates a real-world phishing scenario to identify personnel security awareness gaps. The assessment aims to understand whether employees can identify a suspicious or malicious email and what action they take upon identifying it.

Lodestone employs a standard methodology that includes the assessment in multiple phases:

- **Information Gathering and Open-Source Intelligence** - Gathering as much information as possible about the target. Lodestone can either conduct a black box-style campaign or an open-source intelligence (OSINT) gathering to obtain employee email addresses, names, and roles to develop relevant pretexts for phishing emails. We will also work collaboratively with you to design the right phishing campaign to meet your testing needs.
- **Attack Planning and Pretexting** - Lodestone engineers register a phishing domain and configure the DNS zones for the SMTP provider. The planning phase also includes generating SSL certificates and creating a users list in the SMTP provider. Configuration of the phishing campaign launch instance and the development of an appropriate HTML "lure" also occur in this phase. Finally, we develop an HTML credential-stealing landing page or education page to capture user-typed credentials.
- **Phishing Campaign Execution** - Once the above phases are complete, Lodestone engineers execute the actual campaign and monitor the results. Phishing emails are sent out in a phased manner over a period of hours or days, depending on the number of employees in scope, and the email campaign stays open and active for typically one to two weeks to ensure the email is seen by all intended recipients.
- **Reporting** - Reports are a crucial step in a phishing campaign assessment as the cornerstone deliverable that provides meaningful insights regarding your organization's security posture, especially the human element. Our experts share the campaign results so you can use them to develop or enhance your security awareness training. We are also here to guide you in developing more mature security awareness training as well.
- **Report Review** - We provide our clients at least two weeks to review the reports and formulate any questions or requests for clarification. At the end of every engagement, a report review call is scheduled to ensure that all of your concerns are addressed.

ENGAGEMENT ARTIFACTS




This is the information that we gather based on how the engagement is scoped:

- A list of client personnel that were targeted
- Credentials gathered through the campaign

DURATION AND DELIVERABLES

The Phishing Campaign Assessment varies in duration based on the size of your environment, the number of systems, and findings, but typically takes two to three weeks. It can be delivered on-premises or remotely.

Lodestone will provide the following deliverables to you as part of the engagement:

	Weekly Status Reporting – Lodestone will provide a weekly or bi-weekly status report to the project sponsor once the kickoff call is complete. Lodestone can accommodate your preferred communications, including via phone call or email.
	Executive Summary Report – Lodestone will provide a high-level report on the engagement, findings, and any recommendations, if applicable.
	Final Report – After the engagement completion, Lodestone will provide a final report that details the engagement, findings, and recommendations for mitigating the findings.

Connect with us:
www.lodestone.com
320 East Main Street, Lewisville, TX 75057, USA
Tel: +1-203-307-4984
info@lodestone.com

©2023 Lodestone

Lodestone is a global cybersecurity firm committed to helping clients prevent and investigate security incidents. It is comprised of top talent from private industry, government, intelligence, and law enforcement specializing in incident response, digital forensics, offensive security, risk management, and threat detection.