

SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-2730 SOCIAL ENGINEERING (EMAIL) TESTING

1 OVERVIEW

This Statement of Work (“SOW”), with any appendices included by reference, is part of any agreement which incorporates this document by reference.

1.1 Service Summary

The purpose of the Social Engineering (Email) Testing service (the “Service”) is to examine Customer employees’ overall awareness and knowledge of social engineering tactics to ensure they do not improperly disclose confidential or sensitive information to unauthorized or suspicious persons. SilverSky’s social engineering testing emulates common techniques and methods used by hackers. SilverSky will work with Customer’s project team to determine the scope of the testing and ‘rules of engagement.’ This includes clarifying or determining specific aspects such as the email template, target selections, notification requirements, and timing.

The Email (Malicious Website) Social Engineering test is performed remotely from the SilverSky offices and typically there is minimal interaction required on the Customer’s part once the rules of engagement are established.

Project Deliverables:

- Comprehensive Report

1.2 Project Summary

SilverSky will provide the following primary tasks, subject to modification or extension based on the engagement.

1. Kick-off Meeting
2. Information Gathering/Discovery
3. Content Creation
4. Security Testing
5. Analysis of Findings
6. Reporting

2 SCOPE

2.1 SilverSky Obligations:

Kick-off Meeting - Meet to discuss and agree upon the rules of engagement for the project. This includes project scoping, the timeframe for testing, and procedures to follow should any issues occur during the testing. Any additional precautions or provisions are also considered before testing.

SilverSky Proprietary

Information Gathering Phase - Use Customer input to identify or a supplied list of users and departments to test against. SilverSky recommends sampling from several high-risk departments, such as executive, finance, help desk, and/or customer support, to help determine if certain departments require more extensive training and oversight.

Content Creation Phase - Draft email content designed to gain the users' trust. SilverSky works with the Customer project manager to select from our large library of crafted emails, selecting one to adapt to Customer specifics. The resulting lure appears to come from a trusted source, either an internal or an outside partner. If the customer wishes to further fine-tune the lure, additional customization is available as a surcharged service. During the testing, SilverSky will build an email containing junk advertising ("spam") content, words and phrases and a link that points back to a test server.

Security Testing Phase – Testing is performed in two phases. Phase one is a simple pre-test of the Customer's email filter to determine if the email is blocked by the existing email security before reaching a user's inbox. If the content is blocked, SilverSky will note this in its testing and then will work with Customer technical staff to determine how to allow the content temporarily through the filters. SilverSky will provide best practices in security configuration to get the phishing email into the user's inbox, but it is ultimately the responsibility of the customer to assure delivery from the server into the user's inbox. SilverSky will provide multiple pre-test deliveries if required to help the Customer's test inbox delivery. The second phase of testing will include testing the agreed-upon email user list to determine user reaction to the lure.

Analysis of Findings Phase – SilverSky will compile and analyze the data generated from the assessment, and categorize statistics from the test. This analysis is the basis for recommendations on the effectiveness of social engineering education among the user population and specific users who may need to be targeted for additional training opportunities.

2.2 Deliverables

At the conclusion of the assessment, SilverSky will provide a comprehensive report composed of an executive summary and a detailed findings section. The Customer will have an opportunity to review drafts of the report and SilverSky will deliver a final version after a joint review with Customer.

Executive Summary - The executive summary summarizes the results of the assessment. It is intended for upper management and the Board of Directors and includes:

- Overview of assessment results
- Key findings and recommendations

Detailed Findings - The detailed findings section describes the assessment results in detail. It is intended for management, administrators, and other operations personnel and includes:

- Outline the terms of the engagement
- Social Engineering results detail

- Details of pass/fail of each target
- Template(s) details used during the test.

2.3 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope. In the event that the Customer requests additional services, such services will be the subject of a change request.

3 CUSTOMER OBLIGATIONS AND ASSUMPTIONS

Services, fees and work schedules are based on the assumptions, representations and information supplied by the Customer. The Customer's fulfillment of these responsibilities is critical to the success of the engagement.

3.1 Customer Obligations

- **Project Liaison** - Designate an authorized representative to authorize the completion of key project phases, assign resources, and serve as project liaison
- **Access** - Ensure SilverSky consultants have access to key personnel and data requested
- **Resources** - Furnish SilverSky with Customer personnel, facilities, resources and information and perform tasks promptly
- **Cooperation** - Ensure all of the Customer's employees and contractors cooperate fully with SilverSky and in a timely manner. SilverSky will advise the Customer if increased Customer participation is required in order for SilverSky to perform the Service under this SOW.
- **Documentation** - Timely delivery of all documentation requested by SilverSky including Customer's security policies, network diagrams, server listings, and procedures

3.2 SilverSky Assumptions

- Customer will provide SilverSky with reasonably requested information upon which SilverSky can rely to be current, accurate, and complete.
- Customer will provide access to Customer's personnel who have detailed knowledge of Customer security architecture, network architecture, computing environment, and related matters.
- Customer will provide access to Customer's personnel who have an understanding of Customer's security policies, regulations, and requirements.
- Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky obligations.
- SilverSky will immediately notify the Customer of any perceived problems or issues regarding Customer obligations.
- Customer is responsible for any additional costs if SilverSky is unable to perform the Service due to Customer's delay or other failure to fulfill its obligations under this Statement of Work.

4 PROJECT PARAMETERS

4.1 Project Scope

The scope of the project is based on the above description with the additional details listed as follows:

Project Component	Parameter(s)
Project Start Date	Typically within 30 days of the Effective Date
Project Duration	Approximately 1 week, subject to project variables
S-266-2730 Social engineering (email) testing Tier 2	Up to 500 Email addresses in scope. Work hours not to exceed 60.
S-266-2730 Social engineering (email) testing Tier 1	Up to 100 Email addresses in scope. Work hours not to exceed 40

4.2 Location and Travel Reimbursement

The Service defined in this SOW does not require onsite participation by SilverSky staff at Customer location(s).

4.3 Acceptance

Delivery of all stated project deliverables will constitute acceptance of services provided under this SOW.