Symantec Phishing Readiness Service

SaaS Listing

The definitions set out in the **Agreement** will apply to this SaaS Listing document.

The CA software program(s) ("CA Software") listed below is provided under the following terms and conditions in addition to any terms and conditions referenced on the CA quote or other transaction document entered into by you and the CA entity ("CA") through which you obtained a license for the CA Software (hereinafter referred to as the "Agreement"). These terms shall be effective from the effective date of such ordering document.

This SaaS Listing describes Symantec's Phishing Readiness Service ("Service"). All capitalized terms in this Listing have the meaning ascribed to them in the Agreement (defined below) or in the Definitions section.

Table of Contents

1: Technical/Business Functionality and Capabilities

- Service Overview
- Supported Platforms and Technical Requirements

2: Customer Responsibilities

3: Entitlement and Subscription Information

- Charge Metrics

4: Customer Assistance and Technical Support

- Customer Assistance
- Technical Support
- Maintenance to the Service and/or supporting Service Infrastructure

5: Additional Terms

- Service Conditions

6: Definitions

Symantec Phishing Readiness Service

SaaS Listing

1: Technical/Business Functionality and Capabilities

Service Overview

The Symantec Phishing Readiness Service is a phishing attack simulator used to determine the susceptibility of personnel to such attacks.

Service Features

- Customer can access the Service through a self-service online portal ("Portal"). Customer may configure and manage the Service, access reports, and view data and statistics, through the Portal, when available as part of the Service.
- The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for hardware availability, service capacity and network resource utilization. The Service is regularly monitored for service level compliance and adjustments are made as needed.
- Reporting for the Service is available through the Portal. Reporting may include activity logs and/or statistics. Customer may choose to generate raw data reports through the Portal, which can be downloaded from the Portal.
- **Stand-Alone Private Instance**: The Service is managed within Customer's dedicated instance and accessed through a secure Web interface – both hosted on CA's environment. All Emails sent to phishing targets contain uniquely encoded identifiers that only map to User details when the results are viewed within Customer's dedicated instance, making these identifiers useless to a third party.
- **Administrator Roles**: There are three (3) levels of administrator access: Full Admin, Manager, and Platform User. Customer determines which personnel resources are assigned to each type of role.
- **Phishing Assessments**: The Service includes simulated phishing assessments and templates which address the four (4) most common attack types:
    - **Open/Click Assessment**: This test will measure which of the targeted Users will open, load remote content, and subsequently click any links in messages.
    - **Data Exposure Assessment**: This test aims to convince Users to enter additional sensitive data into a form or application on a malicious website.
    - **Attachment Assessment**: This test aims to entice Users to open a malicious attachment.
- **Templates**: The Service includes pre-loaded templates for each assessment type that can be further customized by Customer to match specific organizational branding, messaging, or culture. In addition, Customer may create its own original templates. There is no limit to the number of phishing campaigns that Customer can run during the Subscription Term. Templates are provided in English. Customer is permitted to translate the templates and content into other languages for use during Subscription Term.
- **Reporting**: The Service provides a private portal to view reports, data, and metrics for each simulated phishing assessment. This data may be used in demonstrating the effectiveness of personnel awareness training and/or susceptibility to real-world phishing attacks. It also can identify persons and groups who are unintentionally exposing the Customer to the risk of compromise through the phishing attack type. Reporting types include:
    - Assessment Overview
    - Assessment Activity Detail
    - Vulnerable User IP/Geo Mapping
    - Vulnerable User Activity Summary
    - Raw Data Download
- **Training Message**: For each assessment, a specific training message and schedule can be created according to Customer policies. Users that do not complete the training immediately after clicking on a phishing link will be reminded via email to return to complete the training.
- **Phishing Training and Awareness**: The Service includes a video-based training module on phishing awareness and risks that can be used before or after executing a simulated phishing assessment. Available training topics specifically related to phishing include:

- Basics of phishing and the threat it poses to organizational security (beginner)
- Understanding and identifying malicious links (intermediate)
- Understanding and identifying malicious attachments (intermediate)
- Understanding email headers and how to use them to validate malicious Email (advanced)

Supported Platforms and Technical Requirements

- Each Customer has access to a dedicated, private instance of the Platform.
- Customer can access the Platform by using a secure password protected login. The Platform provides the ability for Customer to configure and manage the Service, access reports, and view data and statistics when available as part of the Service.
- The Platform is available on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for availability and service capacity.
- Reporting for the Service is available through the Platform. Reporting may include activity logs and/or statistics. Customer can view reports live in the Platform or downloaded the raw data (CSV) for further analysis.
- Supported browsers for the Platform:
  - Internet Explorer 9+
  - Chrome 36+
  - Firefox 25+
  - Safari 7+
  - The Platform may function adequately using other platforms/browsers, but they have not been tested and will not receive the same level of support from CA.

2: Customer Responsibilities

CA can only perform the Service if Customer provides required information or performs required actions, otherwise CA's performance of the Service may be delayed, impaired or prevented, and Customer may lose eligibility for any Service Level Agreement.

- Setup Enablement: Customer must provide information required for CA to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist CA in delivery of the Service.
- Customer must take action to authorize the authorize Symantec Phishing Readiness mail servers to send Email to Customer personnel. This may require "white-listing" by IP address, creating exceptions in Email filtering gateways, or bypassing other protection or inspection mechanisms that may block suspicious, malicious or suspect Email. The IP addresses of the Service's Email servers are available in the Symantec Phishing Readiness Help Center (accessible from the Platform). Other key filtering attributes such as Email headers and content tokens that can be used for Email filter bypass are also available in the Symantec Phishing Readiness Help Center.
- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the Portal, if applicable, or default settings will apply. In some cases, default settings do not exist and no Service will be provided until Customer chooses a setting. Configuration and use of the Service(s) are entirely in Customer's control, therefore, CA is not liable for Customer's use of the Service, nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.

3: Entitlement and Subscription Information

Charge Metrics

The Service is available under one of the following Meters as specified in the Order Confirmation:

- "***Target/*User**" means an individual person and/or device and/or email address that is installed on the platform, who will be sent a phishing assessment message, as a part of the use of the Service.

4: Customer Assistance and Technical Support

Customer Assistance

CA will provide the following assistance as part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support

If CA is providing Technical Support to Customer, Technical Support is included as part of the Service as specified below. If Technical Support is being provided by a reseller, this section does not apply.

- Support is available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration of the Service features and to resolve reported problems with the Service. Support for Services will be performed in accordance with the published terms and conditions and technical support policies published at https://support.symantec.com/en_US/article.TECH236428.html.
- Once a severity level is assigned to a Customer submission for Support, CA will make every reasonable effort to respond per the response targets defined in the table below. Faults originating from Customer's actions or requiring the actions of other service providers are beyond the control of CA and as such are specifically excluded from this Support commitment.

Problem Severity	Support (24x7) Response Targets*
Severity 1: A problem has occurred where no workaround is immediately available in one of the following situations: (i) Customer's production server or other mission critical system is down or has had a substantial loss of service; or (ii) a substantial portion of Customer's mission critical data is at a significant risk of loss or corruption.	Within 30 minutes
Severity 2: A problem has occurred where a major functionality is severely impaired. Customer's operations can continue in a restricted fashion, however long-term productivity might be adversely affected.	Within 2 hours
Severity 3: A problem has occurred with a limited adverse effect on Customer's business operations.	By same time next business day**
Severity 4: A problem has occurred where Customer's business operations have not been adversely affected.	Within the next business day; CA further recommends that Customer submit Customer's suggestion for new features or enhancements to CA's forums

The above Support Response Targets are attainable during normal service operations and do not apply during Maintenance to the Service and/or supporting infrastructure as described in the Maintenance section below.

** Target response times pertain to the time to respond to the request, and not resolution time (the time it takes to close the request).*

*** A "business day" means standard regional business hours and days of the week in Customer's local time zone, excluding weekends and local public holidays. In most cases, "business hours" mean 9:00 a.m. to 5:00 p.m. in Customer's local time zone.*

Maintenance to the Service and/or supporting Service Infrastructure

CA must perform maintenance from time to time. For information on Service status, planned maintenance and known issues, visit https://status.symantec.com/ and subscribe to Symantec Status via email, SMS, or Twitter to receive the latest updates. The following applies to such maintenance:

- **Planned Maintenance:** Planned Maintenance means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. For Planned Maintenance, CA will provide seven (7) calendar days' notification posted on Symantec Status.
- **Unplanned Maintenance**: Unplanned Maintenance means scheduled maintenance periods that do not allow for seven (7) days notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. CA will provide a minimum of one (1) calendar day notification posted on Symantec Status. During Unplanned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. At times CA will perform Emergency Maintenance. Emergency Maintenance is defined as maintenance that must be implemented as quickly as possible to resolve or prevent a major incident. Notification of Emergency Maintenance will be provided as soon as practicable.
- **Note:** For Management Console Maintenance, CA will provide fourteen (14) calendar days' notification posted on Symantec Status. CA may perform minor updates or routine maintenance to the Management Console with no prior notification as these activities do not result in Service disruption.

5: Additional Terms

Service Conditions

- Any Email templates or spoofed domains provided as part of the Service may only be used for assessments as part of this Service. CA IS NOT REPSONSIBLE FOR ANY MISUSE OF SUCH TEMPLATES AND DOMAINS NOT AUTHORIZED UNDER THE AGREEMENT.
- CA is not responsible for any errors in translation of the Service content into other languages by Customer.

6: Definitions

"**Administrator**" means Customer's designated personnel to manage the Service on behalf of Customer.

"**Email**" means any inbound or outbound SMTP message passing through a Service.

"Target" means an email address that will be sent a phishing assessment message.

"Assessment" means a simulated phishing campaign sent to a group or list of targets.

"Platform" means the Phishing Readiness browser-accessed, web-app portal.

"**Infrastructure**" means any CA or licensor technology and intellectual property used to provide the Services.

"**Phishing Readiness Help Center**" means the online Support and Knowledge Base available from within the Platform.

"**Service Credit**" means the number of days that are added to Customer's current Subscription Term.

"**Symantec Online Service Terms and Conditions**" means the terms and conditions located at or accessed through https://www.symantec.com/about/legal/repository.

"**User**" means an individual person and/or device and/or email address that is installed on the platform, who will be sent a phishing assessment message, as a part of the use of the Service.