THRIVE℠

SERVICE DESCRIPTION

Anti-Phishing and Security Awareness Training

Executive Summary

Thrive Anti-Phishing and Security Awareness Training Service Definition

Thrive Anti-Phishing and Security Awareness Training service provides ongoing security testing and training for your users to increase awareness of risks associated with phishing, spear phishing, malware, ransomware and social engineering attacks with targeted user campaigns and responsive training aimed at improving awareness of and avoiding security threats. Improving user awareness of these threats reduces risk of human error resulting in security breaches and ransomware.

Services Scope

The service shall include:

- Fully managed monthly email phishing campaigns
- Quarterly user security training campaigns
- Authentic simulated email phishing template library
- Comprehensive library of remedial training content
- Client dashboard for visibility into campaign details and user scores
- Custom email templates and training library available
- Automated user sync with Microsoft 365 tenant
- Executive Summary reporting via Client dashboard

Thrive Scope of Work and Deliverables

- Thrive shall create a Client tenant within the Thrive Anti-Phishing and Security Awareness Training platform.
- Thrive shall import all users into the Thrive Anti-Phishing and Security Awareness Training platform via automated sync with Microsoft 365.
- Thrive shall send an initial email welcoming the end users to the platform and a link to the training.
- Thrive shall create and conduct monthly phishing tests to all subscribed end users after the initial phishing training completion.

- Thrive shall consult with the Client contact on a quarterly basis to setup new trainings. Training schedules can be modified as needed.
- Thrive shall send weekly email reminder notifications to end users that have not completed training.

Client Responsibilities

- Client shall provide the Thrive security team with admin credentials to the Client Microsoft 365 tenant or a Microsoft Excel.csv file with use names and email addresses of those participating in the Anti-Phishing and Security Awareness Training program.
- Client shall provide Thrive with a list of any Microsoft 365 users that should be excluded from the service.
- Clients that are running Microsoft Exchange shall notify Thrive when new users need to be added to the Anti-Phishing and Security Awareness Training Platform.
- Client shall be responsible for user training program compliance.
- Client shall provide Thrive with a primary point of contact for the Anti-Phishing and Security Awareness Training service.

Service Exclusions

Any service not explicitly included in the Security Awareness Training Definition above is considered optional and may be provided under separate agreement for an additional fee.