WORKFORCE PHISHING AND SECURITY AWARENESS TRAINING

SERVICE DESCRIPTION

Description of Service

This document describes BlueVoyant's Workforce Phishing and Security Awareness training program being provided to you ("Customer", "Client", or "you") by BlueVoyant, executed by Client for the purchase of this Service.

Service Overview

The overwhelming majority of successful cyberattacks (91%) begin with an attack on either an employee's willingness to help or on their curiosity. These are inherently positive employee attributes that can also leave your team vulnerable to nefarious schemes to coax them into taking actions that expose sensitive data.

BlueVoyant's Workforce Phishing and Security Awareness Training Program is designed to illuminate for your team how and why they are the number one target in cyberattacks and empower them to be the very best defense against attacks in the future. We make training personal because the attacks are personal.

Our training program includes a proprietary mix of proven techniques to test and educate employees as well as ensure they are **motivated** to improve security behavior. The combination of a custom, targeted phishing campaign along with interactive training designed to motivate as well as educate employees are distinctive attributes of the BlueVoyant training program.

The BlueVoyant Workforce Phishing and Security Awareness Training Program provides the following advantages over commoditized online security awareness programs:

- Participants retain more knowledge when they have an engaging test that's designed around their specific environment followed by focused interactive and synchronous instructor-led training.
- A keystone of our program is that it incorporates motivational aspects. It's not enough to simply share facts with employees but the motivational element is left out of most training.
- Our training program is customized to your specific environment so it resonates more with employees than generic training programs.
- Studies show that companies get better results in a condensed, shorter time frame with instructor-led training vs. asynchronous online learning programs where employees are inclined to multitask.
- Our training program is designed to build a culture of security among your team along with suggestions, tools and techniques that can be used post learning to help your team continue to grow and support each other.

BlueVoyant's Workforce Security Training Methodology

BlueVoyant will work with client stakeholders to ensure that the phishing and training are relevant to their workforce and effectively and conveniently delivered.

Phase 1: Baseline Phishing

We start with a baseline phishing test using information relevant to the client's specific workforce. After the phishing campaign has been crafted and executed, we will prepare a report of findings that are incorporated with additional information we gather from management to prepare a customized synchronous, online learning experience.

Phase 2: Training Design

BlueVoyant will collect information through discussion, interviews and observation to integrate with findings from the phishing test to design a training program around the client's specific environment. Data collection may involve face-to-face, virtual media, and phone conversations with selected staff as needed. Once objectives are identified, a customized, unique training program is then developed for the specific target participants.

Phase 3: Delivery

Phase 3 involves delivery of the training to the intended audience. Training is delivered via interactive online classroom techniques including but not limited to quizzes, group work, hands-on experiences, lecture, case studies and demonstrations. The balance of activities will depend on the objectives defined in Phases 1 and 2 but all training is designed to be engaging, interactive, motivating and fun, thus memorable. The session will be capped by preventative and mitigating actions users can perform to secure themselves and the organization.

Phase 4: Review

In the final phase of training we measure both knowledge and motivation to improve habits to determine training retention. We will also develop recommendations for further training activities to include retraining, additional training topics, and future areas of focus. *Note: Final testing is done immediately following training unless otherwise specified by the client.*

BlueVoyant Workforce Phishing and Security Awareness Service Levels

Phishing, training and post training testing may be completed once, annually or quarterly. First training session is 1.5 hours.

Quarterly services include custom targeted phishing campaigns and 30 minutes of followup training each quarter. Each training session includes the phishing email to highlight how to detect phishing, additional aspects of social engineering and tips to avoid falling victim to them, as well as an infographic on current or common attack techniques.

Client Responsibilities

A member of our team will work with one or more client stakeholders or subject matter experts to understand the specific target security behaviors that should be addressed in the training program. We will prepare a recommendation for length and scope of security training. The client is responsible for ensuring that team members are adequately prepared with the devices and materials needed to complete the program.

The Client is responsible for designing and enforcing the company policies that define expected team member participation in the program.

Specific metrics and implementation methods for objectives are the responsibility of the BlueVoyant team but the Client is responsible for final sign off on the adequacy of the objectives and metrics prior to delivery of training.