

*This document is intended to be used as a resource to help prepare a funding or approval request for use of the PhishingBox Security Awareness Ecosystem. The information contained within this document should be incorporated into your organization’s specific funding format. The context of the text is from the point of view of you making a request for funding internally; this is not a sales proposal per se.*

**BUSINESS CASE:**

**IMPROVE SECURITY THROUGH SECURITY AWARNESS TRAINING**

# EXECUTIVE SUMMARY

Social engineering, or the act of attacking the human element of security, poses a risk to our industry. In order to improve our overall information security, we are recommending that we establish a security awareness training and testing program. Through this program, we will enroll staff in security awareness training, and test employees though simulated phishing attacks. The testing will provide realistic information to evaluate our employees’ susceptibility to social engineering attacks.

This document provides support for obtaining a license to use a hosted software system that will allow us to deploy training courses, and conduct realistic, but non-intrusive, social engineering attacks via phishing. In addition, the platform provides additional tools to help identity and report suspicious emails.

We are recommending a solution from PhishingBox. Their system will provide us with the ability to perform testing for all of our employees for an annual investment of $xxxx.

# SITUATION

Social engineering attacks are a significant threat to businesses. This is a concern for us as many data breaches begin with a phishing email. Key facts about phishing are available here: https://www.phishingbox.com/resources/phishing-facts

As an organization, we need to maintain an adequate control environment. Our stakeholders, clients, and regulators expect it, and we need to protect our trade secrets and other business information. A data breach could be expensive and negatively affect our reputation. We have invested in security systems and software, such as firewalls and anti-virus software; however, we are not adequately prepared for social engineering attacks. As part of a layered defense, we need to improve and test the human link of our security chain.

The primary method to improving the human element of security is through training and testing. Using phishing simulation will do more to improve our security than upgrading our computers or increasing password complexity. We expect the following benefits from implementing phishing simulation training and testing.

**PHISHING SIMULATION BENEFITS**

# Increased Security

Phishing simulations provide quantifiable results that can be measured.

These measurements allow improvement to be identified and tracked. Initially, we expect a 33 percent failure rate. After subsequent training, we expect an ongoing failure rate of approximately 5 percent. We do not expect the success rate to be 100 percent due to employee turnover, forgetfulness, and other reasons. This fact is the reason for ongoing training and testing.

# Demonstrated Responsibility

As a responsible organization, we need to demonstrate to our stakeholders that we understand the current threat environment and are taking steps to reduce our risk. By ignoring the threats from social engineering attacks, we could be exposing ourselves to litigation.

# Improved Training Retention

We can provide training on what to do and what to avoid, but until an employee experiences it, their actions are unknown. After seeing what is capable, employees understand and are more security conscious.

# Net Reduced Training Cost

By pinpointing employees that are more susceptible, such as repeat failures, we can provide additional training to those employees without the cost and burden to other employees.

# ALTERNATIVES CONSIDERED

We considered several alternatives. These options included creating systems internally, obtaining a commercial system, and contracting for phishing as part of an external social engineering test. Below are key points relating to each of the alternatives.

|  |  |  |
| --- | --- | --- |
| Option  | Pro  | Cons  |
|  Internally Developed / Open Source Systems    |   ~ Total control  | ~ Resource Intensive ~ Needed Expertise ~ Install Software ~ Support Software  |
| Third-Party Hosted Software |  ~ Low cost ~ Good controls ~ Vendor support  |  ~ Vendor reliance  |
|  Outsourced Managed Services |  ~ Good expertise  |  ~ Expensive  |

# RECOMMENDED SOLUTION

We are recommending the purchase of a license to use a web-based solution from PhishingBox LLC. We selected PhishingBox because the system is affordable, easy to-use, and powerful. The system includes free training content, and allows us to perform phishing testing. The system also allows us to incorporate our own training as well.

The PhishingBox system will provide us the ability to launch training, conduct testing for all of our employees for an investment of $xxxx annually.