

*This document is intended to be used as a resource to help prepare a funding or approval request for phishing simulation at your organization. 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 PHISHING SIMULATION**

# 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 conduct simulated social engineering attacks to evaluate our employees’ susceptibility to such tactics.

This document provides support for obtaining a license to use a hosted software system that will allow us to easily conduct realistic, but non-intrusive, social engineering attacks via phishing, which is the most common tactic. Such testing will promote employee awareness of the threat and allow us to identify employees that may need additional training.

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 91% of hacking attacks begin with a phishing or spear-phishing email and the average cost of data breach is $7.2 million or $156 per compromised record. In 2015, the number of spear-phishing campaigns targeting employees increased by 55%. In addition, the threat is increasing every day. The number of phishing attacks in Q1 2016 was higher than any total since 2004. At the same time, social engineering prevention and testing is often overlooked. Less than 46 percent of companies perform any type of social engineering training or testing.

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 phishing simulation 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  |
|  Hosted Phishing Simulation System  |  ~ Low cost ~ Good controls ~ Vendor support  |  ~ Vendor reliance  |
|  Outsource Social Engineering Test  |  ~ Good expertise  |  ~ OneTime ~ 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, easyto-use, and powerful.

The PhishingBox system will provide us the ability to perform testing for all of our employees for an investment of $xxxx annually. Their Investment Summary is detailed in the proposal.



#  Social Engineering Facts and Figures

|  |  |
| --- | --- |
| 89% of all attacks involve financial or espionage motivations.  | Verizon Data Breach Investigations Report 2016  |
| 63% of confirmed data breaches involve using weak, default or stolen passwords.  | Verizon Data Breach Investigations Report 2016  |
| 95% of breaches and 86% of security incidents fall into nine patterns.  | Verizon Data Breach Investigations Report 2016  |
| Ransomware attacks increased by 16% over 2015 findings.  | Verizon Data Breach Investigations Report 2016  |
| 30% of phishing messages were opened in 2016 – up from 23% in the 2015 report.  | Verizon Data Breach Investigations Report 2016  |
| Web application attacks climbed to the #1 spot for data breaches, up 33% over prior year.  | Verizon Data Breach Investigations Report 2016  |
| If stolen devices are encrypted, it’s much harder for attackers to access the data.  | Verizon Data Breach Investigations Report 2016  |
| In 2015, there were 38% more security incidents detected than in 2014.  | The Global State of Information Security Survey 2016  |
| The median number of days that attackers stay dormant within a network before detection is over 200 days.  | Microsoft Advanced Threat Analytics  |
| As much as 70% of cyberattacks use a combination of phishing and hacking techniques.  | Verizon Data Breach Investigations Report 2015  |
| Phishing, malware and zero-days give IT security the most headaches.  | 2015 Cyberthreat Defense Report North America & Europe  |
| The top 3 industries affected by data breaches are Public, Information & Financial Services  | Verizon Data Breach Investigations Report 2015  |
| Phishing has been on the rise since 2011.  | Verizon Data Breach Investigations Report 2015  |
| Phishing campaigns have evolved to incorporate installation of malware as the second stage of the attack.  | Verizon Data Breach Investigations Report 2015  |
| 23% of recipients now open phishing messages and 11% click on attachments.  | Verizon Data Breach Investigations Report 2015  |
| For 2 years, more than two-thirds of incidents that comprise the Cyber-Espionage pattern have featured phishing.  | Verizon Data Breach Investigations Report 2015  |
| Nearly 50% open e-mails and click on phishing links within the first hour.  | Verizon Data Breach Investigations Report 2015  |

|  |  |
| --- | --- |
| The reality is that you don’t have time on your side when it comes to detecting and reacting to phishing events.  | Verizon Data Breach Investigations Report 2015  |
| e-Mail phishing rate in 2015 was 1 in 1,846.  | Symantec Internet Security Threat Report 2016  |
| In 2015, the number of spear-phishing e-Mail campaigns increased.  | Symantec Internet Security Threat Report 2016  |
| In 2015, 34.9% of all spear-phishing e-mail was directed at an organization in the financial industry.  | Symantec Internet Security Threat Report 2016  |
| Spear-phishing attacks against small businesses continued to grow in 2015.  | Symantec Internet Security Threat Report 2016  |
| The number of spear-phishing campaigns targeting employees increased by 55% in 2015.  | Symantec Internet Security Threat Report 2016  |
| 66% of IS professionals feel it is likely that they will be subjected to an APT attack.  | ISACA 2014 Advanced Persistent Threat Awareness Study  |
| 70% of respondents are spending greater than 5% of their IT budgets on security.  | 2015 Cyberthreat Defense Report North America & Europe  |
| 92% of IS professionals believe that social network use increases the likelihood of a successful APT attack.  | ISACA 2014 Advanced Persistent Threat Awareness Study  |
| 34% of companies do not have a crisis response plan for a data breach or cyberattack event.  | Assessing the Results of Protiviti’s 2014 IT Security & Privacy Survey  |
| 72% of security incidents at financial services organizations involved a current or former employee.  | The Global State of Information Security Survey 2015  |
| 62% of security incidents at industrial product organizations involved a current or former employee.  | The Global State of Information Security Survey 2015  |
| 56% of organizations say it is unlikely or highly unlikely that they would be able to detect a sophisticated attack.  | EY’S Global Information Security Survey 2014  |
| In 2015, 34.33% of phishing attacks targeted clients of financial organizations.  | 2016 AO Kaspersky Lab: Securelist  |
| Phishing messages usually take the form of fake notifications from banks, providers, e-pay systems and other organizations.  | 2016 AO Kaspersky Lab: Securelist  |
| The average lifetime of a phishing site is 5 days.  | 2016 AO Kaspersky Lab: Securelist  |
| Phishing URLs often closely resemble the genuine URL of a legitimate company.  | 2016 AO Kaspersky Lab: Securelist  |
| An estimated 91% of hacking attacks begin with a phishing or spear-phishing email.  | Wired.com/Hacker Lexicon  |
| The amount of phishing websites increased from 24,864 to 33,571 between 2014 and 2015.  | Google’s Safe Browsing Service  |
| Financial sector is targeted most for cyber-attacks, especially with phishing and spear-phishing.  | NTT Group  |
| On May 24, 2016, the APWG announced that the number of observed phishing attacks in Q1 2016 was higher than any total since 2004.  | Anti-Phishing Working Group (APWG)  |
| More than 75% of the phishing websites observed in Q1 2016 were hosted in the U.S.  | Anti-Phishing Working Group (APWG)  |