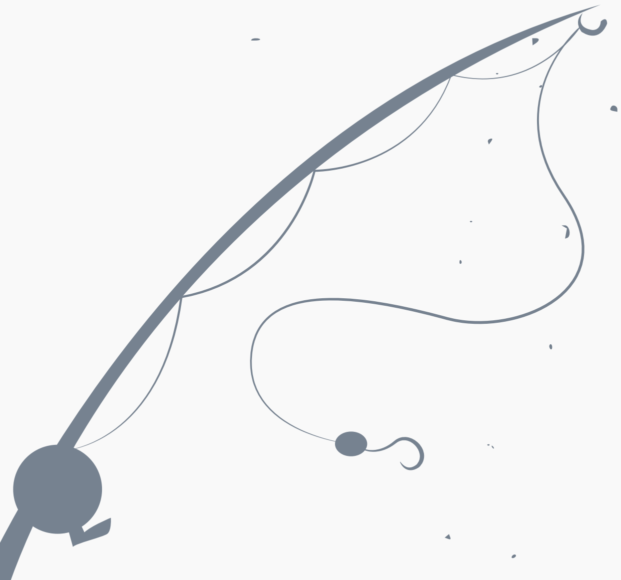
PHISHING SCAMS IN THE WORKPLACE

KEEP YOUR COMPANY SAFE



PROPOSED BY

ROBERT CRAGER

TABLE OF CONTENTS

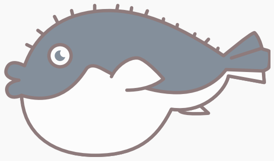


TABLE OF FIGURES

EXECUTIVE SUMMARY

DATE PROPOSED

8TH MAY 2020

With most businesses today, internet security is a major issue and a key aspect of any company. Whether the company is an I.T. firm that consults other companies on their internet security practices or the company is a basic brick and mortar coffee shop. They all need internet security to keep their customer and employees' information secure. One of the most threatening cyber attacks is any form of social engineering, which is the process of manipulating people or social situations for malicious gain. A form of this is phishing scams.

Phishing scams have taken a rise over the past 10 years and have now become a very serious threat to companies and their infrastructure. Phishing could cause a company to lose a client, employees, or even create lawsuits. Due to the recent 640% increase in phishing encounters, companies should start taking these incidents very seriously. Phishing has caused companies to lose over 20 billion dollars in 2012 alone. Additionally, there are around 6.5 million phishing emails sent per day.

The proposed solution is broken down into a three-phase plan. The first phase is to establish spam filtering on the company email system, using the most advanced spam filtering software for emails, Gmail. The second phase consists of email warning messages and other configuration settings for the employees to see when they view emails. The warning messages will appear when the sent from address is an address outside of the company domain and will not automatically download attachments, as they could be malicious. The third phase of the plan involves training the employees about phishing through regular weekly meetings. The meetings will take place on a Tuesday at 10 am and will regularly consist of examining fake emails, understanding the best practices in those scenarios. By successfully implementing this plan, the company will have a secure and nearly spam-less email experience with educated and trained employees to protect client data and save the company millions per year.

INTRODUCTION

The purpose of this proposal is to show the importance of internet security and teach companies about phishing scams by holding regular meetings with employees and establishing strict spam filters in company emails. Implementing the recommended solution will increase company profits, labor efficiency, and both client and employee security.

This solution is prompted by the 640% increase in phishing URL encounters in 2019.[1] This is likely because of the urbanization of offices in recent years. And as companies modernize their office equipment, they are not or do not inform their employees on how to securely use the equipment. As a result, people often fall victim to phishing scams in the workplace.

QUESTIONS THAT WILL BE ANSWERED

- What is Phishing?
- How does phishing affect companies?
- What are the companies options to combat phishing scams?
- What is the proposed solution to phishing?
- What about phishing and the solution will this proposal cover?

[1] Drew, Frey. "2020 Webroot Threat Report: Phishing Attempts Grew by 640% Last Year" *Webroot.com*, Webroot, March 2020, https://community.webroot.com/news-announcements-3/2020-webroot-threat-report-phishing-attempts-grew-by-640-last-year-342560, Accessed 30 April, 2020.

BACKGROUND

WHAT IS PHISHING?

Phishing is a recently coined term by the technology field and is defined by an attempt to impersonate someone to extort information from another, typically through means of email. A phishing email in a workplace environment could be catastrophic to the company's data, deeming the company unsafe and uninformed. An example of a phishing scam would be when you receive an email from someone claiming to be a higher up in the company. This person instructs you to release the information of a client, clearly going against any signed non-disclosure agreement, but you continue because it appears to be an official email from your higher up.

HOW DOES PHISHING AFFECT COMPANIES?

Phishing can create many problems in any environment, especially a work environment. Some problems include both employee and company data leaks leading to identity theft, financial credentials being compromised, or even lawsuits. Continuing from the example earlier, you have now leaked information of a client without rightful permissions to do so, causing that client to leave the company and potentially sue. This was all caused by one simple email, that could have been prevented with very simple steps. These situations will cost any company a tremendous amount of money to fix and will take countless hours trying to recover their reputation with their current or potential clients.

DONT TAKE THE BAIT!

LAWSUITS | DATA LEAKS | LOSS OF CLIENTS

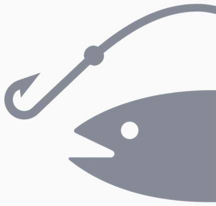
SOLUTIONS

WHAT ARE THE COMPANIES OPTIONS TO COMBAT PHISHING SCAMS?

When it comes to phishing, there are multiple ways to mitigate and virtually eliminate the threats. The first and most obvious method to eliminate phishing attacks is to simply delete emails from unknown sources. However, with this method, there must be some degree of training involved, which will be discussed later in the proposal. Another option to combat phishing attacks is to establish spam filters on the email server within the company, there are also complications with this that will be discussed later. Some other examples of prevention methods include (but not limited to): refraining from downloading, clicking, or opening any links or files in an email, sub-netting the company network to reduce potential damage, notifying financial institutions after a suspected attack, etc.

WHAT IS THE PROPOSED SOLUTION TO PHISHING?

The proposed solution to solve the multiple issues that phishing has caused over the recent years would be to combine various solutions. This solution involves combining a training program for employees to educate them on the effects of phishing and how to prevent it, with spam filters enabled on the company email servers. The training programs will be held regularly from either a certified professional that will be on-site or may be held by a current I.T. team lead. The specifics for how spam filtering and how the training programs will work, will be explained in further detail later in this proposal.



SCOPE

WHAT ABOUT PHISHING AND THE SOLUTION WILL THIS PROPOSAL COVER?

This proposal will cover everything from explaining how the solution will work, to breaking down the total cost (to include the certified professional). Scattered throughout this proposal will be various graphs and diagrams showing how effective these types of solutions have been in other company environments. This proposal will not cover the in-depth knowledge needed to educate employees on phishing. This proposal will also not display how to implement spam filtering on email servers or how to use set up email servers in any capacity.

If an in-depth knowledge of phishing is required, please refer to a book entitled the Essential Cyber Security Handbook In English. N.p. by Nam H Nguyen published in 2018. This book will provide many wonderful examples of how attackers use phishing to gain access to systems and other credentials, along with how to prevent such encounters from happening. With that being said, the remainder of this proposal will cover the following:

- How to efficiently implement regular meetings to teach employees,
- How implementing spam filters will reduce phishing emails,
- How to spot phishing emails in the average email inbox,
- What to do when a phishing email is found,
- What not to do when a phishing email is found,
- How to protect the company in the event of a breach,
- How companies can recover after a phishing attack,
- How much this solution will cost companies.

THE PROOF

The reason for this proposal is due to the recent increase in phishing emails and their catastrophic effect on companies and organizations. In 2019 alone, 94% of malware was delivered via email, which would be characterized as phishing. Also worth mentioning is that 32% of breaches involve phishing. This means implementing this simple solution can cut down data breaches by 32 percent. Furthermore, as indicated by the chart below (Fig. 1), phishing emails can be attributed to up to .85% of total emails analyzed worldwide. Even though less than 1% seems to be very small, considering that there are over 290 Billion emails sent in 2019 and over 300 Billion emails sent in 2020 per day (Fig. 2), it is not a meaningless percentage. That would equate to about 2.4 Billion phishing emails sent per year or over 6.7 Million phishing emails sent per day.

% PHISHING EMAILS OUT OF TOTAL EMAILS ANALYZED

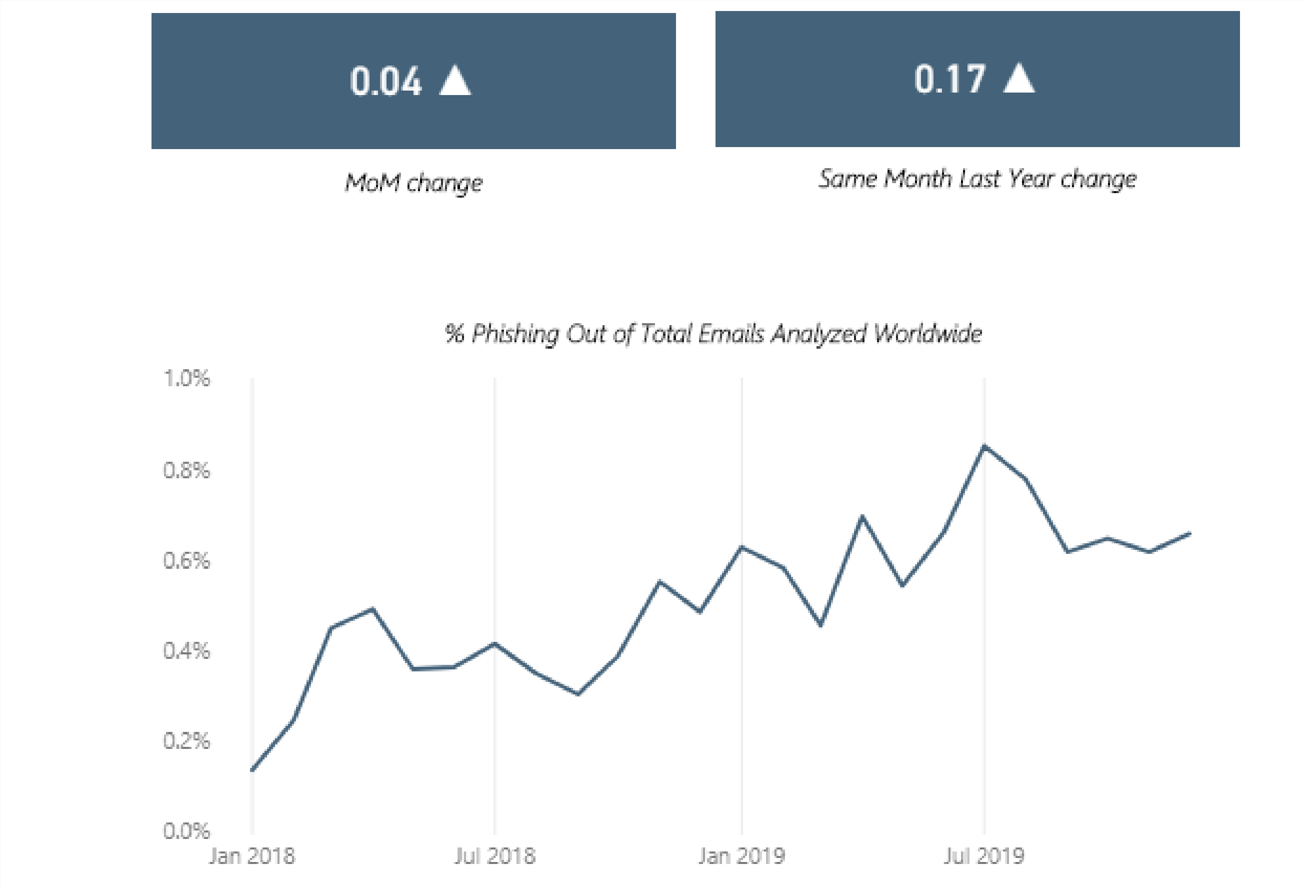


Figure 1 - Percentage of Phishing Emails Out of Total Emails Analyzed, Microsoft Security Intelligence Report, Microsoft, www.microsoft.com/securityinsights/Phishing.

EMAILS SENT AND RECEIVED PER DAY (BILLIONS)

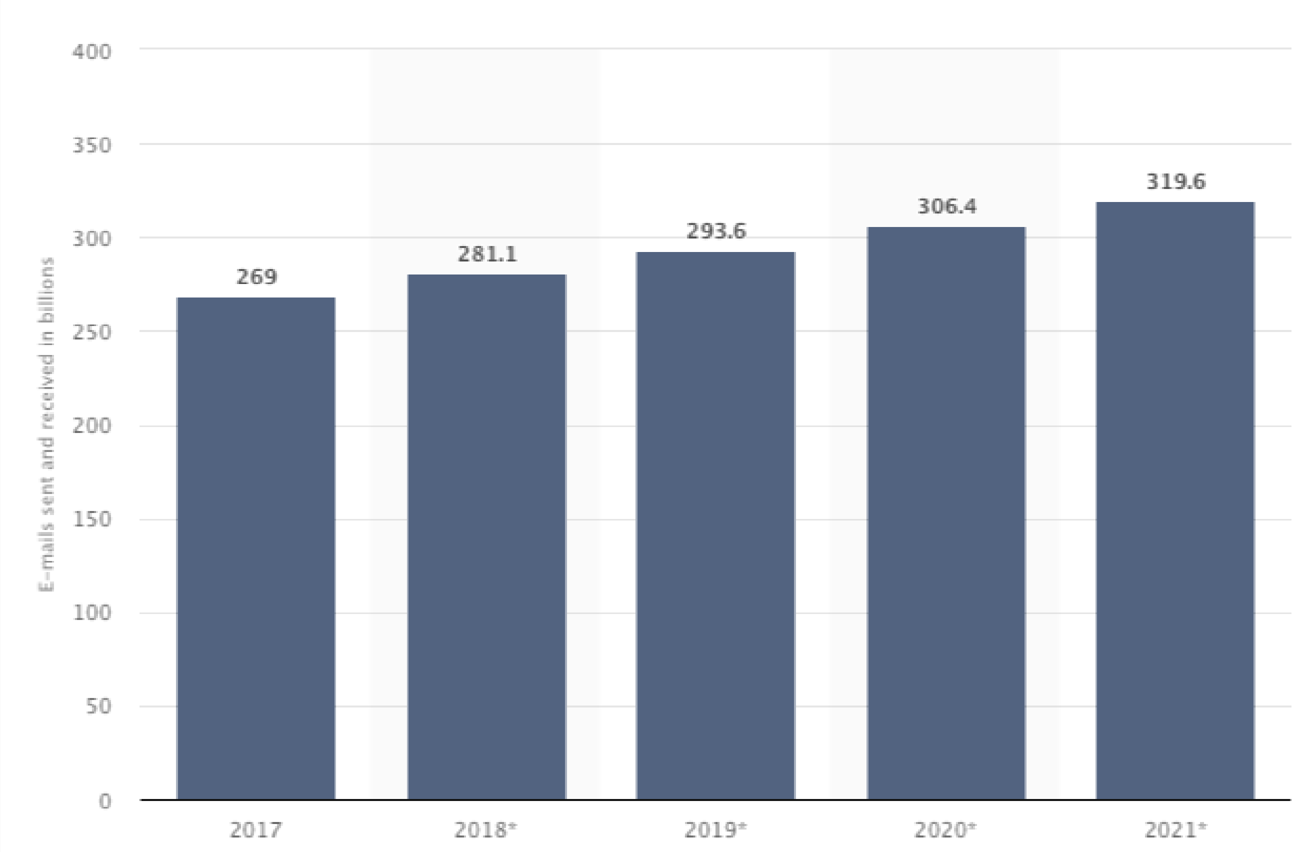


Figure 2 - Emails Sent and Received Per Day, “How Many Emails Are Sent Per Day.” Campaign Monitor, Campaign Monitor, Mar. 2019, www.campaignmonitor.com/blog/email-marketing/2019/05/shocking-truth-about-how-many-emails-sent/.

HOW TO IMPLEMENT REGULAR MEETINGS

Every successful company should be having regular meetings to discuss current and future projects with the team. Therefore, implementing regular meetings should be fairly simple so long as the company takes phishing seriously they will make time for the classes. The solution proposes that companies take around 10-15 minutes each week to talk about phishing and the effects of it. This 10-15 minute window will fit in perfectly to the 89% of employees that waste time throughout the day. It is recommended to implement the meetings on a Tuesday because this is the day of the week that most people are at the office. The meetings should also be implemented around 10 am, giving enough time for people to come into work and get settled in.

THE EFFECT OF REGULAR MEETINGS

By implementing regular meetings, the employees will adopt an attitude of constantly being reminded of these dangers in the workplace. This will cause them to think about what they are doing before they just start clicking on attachments in emails. The overall results of the meetings alone are as follows:

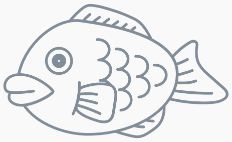
- better overall employee security and awareness
- better company security
- increase in labor efficiency

HOW IMPLEMENTING SPAM FILTERS WILL REDUCE PHISHING EMAILS

Any notable company has spam filters put in place to protect their company and their employees from spam and phishing emails. Spam filters are perfect for blocking known IP addresses of spam or phishing origins. With spam filters, the number of phishing emails is greatly reduced daily. Additionally, spam filters will block anything that looks suspicious or of a spam origin, so that any obviously phishing emails will be block and not visible to the employees. However, since spam filters have been in use for a couple years now, phishing emails have become more sophisticated and can slip past the filters often. Therefore, there is still a need to educate employees on the dangers of phishing emails.

EFFECTS OF IMPLEMENTING THE SOLUTION

Phishing and spam emails costed companies $20.5 billion in 2012 alone, averaging out to over $1,900 per employee. Additionally, 3 of every 4 companies fell victim to phishing scams in 2016. The statistic also mentions that most of those phishing emails are fake invoices, luring the victim to click the malicious attachment, which could infect the company network if proper precautions are not taken. However, by implementing this solution, companies will save billions per year and boost labor efficiency.



TIMELINE

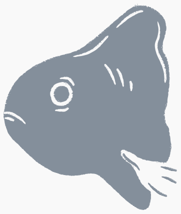
PHASE 1

In phase 1 of the solution, the company will begin by implementing a spam filtering system on their email systems and will be done through their I.T. department. There are multiple different spam filter methods to choose from, ranging from artificial intelligence to statistically measured ones. Although they are all great options, the spam filtering method that would be the best in this scenario would be an artificial intelligence one such as Google's Gmail spam filter. This spam filter has been proven to block multiple spam emails successfully. By implementing this spam filter, the company will see a massive drop in spam email encounters by blocking up to 99.9% of all spam emails. Other spam filters don't even compare when it comes to Gmail's spam filter. By only allowing only 0.1% of spam emails through the filter, Gmail will protect the company's employees and keep client data safe.

PHASE 2

Phase 2 will consist of adding more preventative measures against spam and phishing emails. These measures will essentially warn the employee that the email may be a phishing or spam email. The first implementation would be to include an additional filter on any emails that are sent from outside the company domain. This filter would disable the automatic downloading of email attachments in the email settings. Most companies have this setting disabled and have this filter put in place already by their I.T. department. Another almost mandatory aspect of preventing phishing emails is to subnet the company network - to separate the network into many small networks. Again, the I.T. department should have already done this, but if not, this will also prevent any further damage a malicious file can do to a company network.

By completing this phase the company will further reduce the risk that spam emails have on the employees by not downloading the attachments automatically. Additionally, if a malicious attachment were to be downloaded by an employee - because the network is segmented - the malicious file will have limited effects on the company and its employees.



PHASE 3

After the spam filters have been applied, it's time to move on to the phishing meetings. The meetings will take place every Tuesday at 10 am and will last around 10-15 minutes each week. As stated earlier, these 15 minutes will come from the 30 minutes that the average employee spends wasting time each day. The meetings will take place on Tuesdays at 10 am because that is the day and time when most people are in the office. Now, it is unrealistic to gather all the employees in one room at once, so instead of having a meeting for everyone every week, the meetings will cycle through each department. For example, one week the HR department will be meeting, then the next week the accounting department, and so on. By implementing this model, the company will still have recurring meetings with each department, they will just be more spread out.

Now, who will be conducting these meetings and where will the time and money come from for them? The meetings will be conducted by a trained cybersecurity professional or a member of the I.T. department at the company. In terms of cost, however, it would be most efficient to use an already existing I.T. department employee to conduct these meetings. The I.T. employee will prepare an initial presentation on phishing for the first week; this should be brief and simple - around 10 slides.

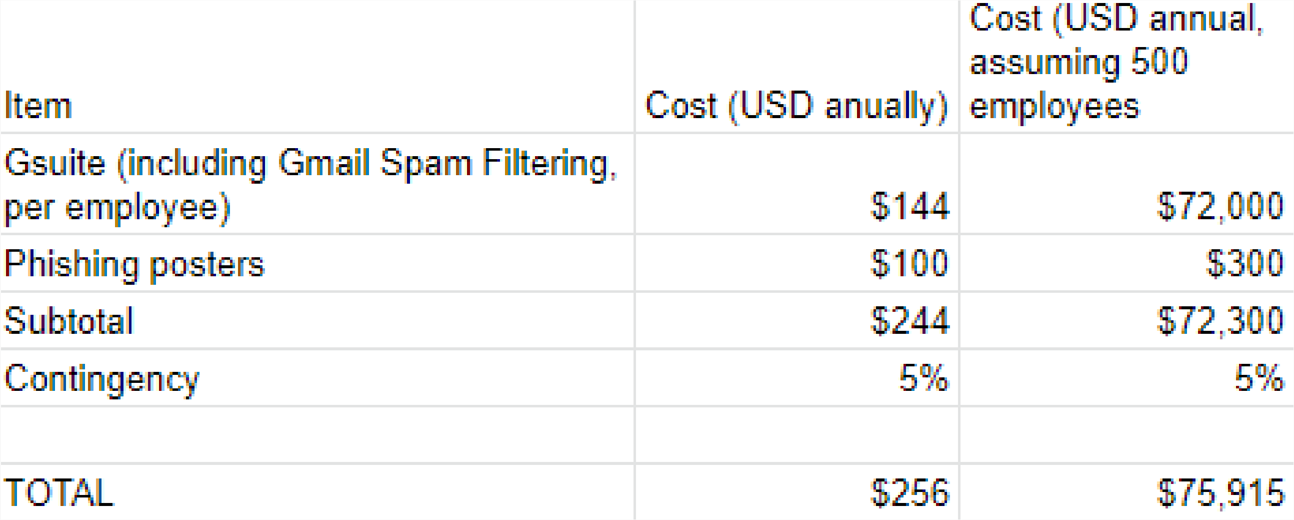
For the proceeding week's meetings, the conductor will prepare a brief report of the company phishing email statistics as a whole to analyze how the company is doing. They will gather this information from recording any phishing encounter that an employee has encountered. After the review, if time permits, the conductor will analyze a few of the phishing emails captured and show employees why it's a fake email.

PHASE 4 (OPTIONAL)

This phase is optional but highly encouraged. In this phase, the I.T. employee will occasionally go around the company office and post phishing awareness posters in visible locations. These posters will contain some form of a phishing definition followed by an example of a phishing email - presumably very visible text indicating this is a fake email.

COST BREAKDOWN

COST BREAKDOWN (USD, ANNUAL)



Item	Cost (USD anually)	Cost (USD annual, assuming 500 employees
Gsuite (including Gmail Spam Filtering, per employee)	$144	$72,000
Phishing posters	$100	$300
Subtotal	$244	$72,300
Contingency	5%	5%
TOTAL	$256	$75,915

Figure 3 - Cost Breakdown

In Figure 3, the cost breakdown is depicted. The Gsuite row is the price per employee, per year for a Gsuite subscription plan. This plan includes the Gmail email system and thus Gmail spam filtering. The Phishing posters row is to include the cost of poster material, research for poster and/or copyrights to posters. Finally, the Contingency row is to include any extra costs that may occur throughout the year (broken projector, more materials needed, etc). The total cost of this solution will be $256 per employee, and assuming the company is a medium-sized company with 500 employees, the cost annually will be $75,915. Considering the previously mentioned statistic that spam and phishing emails cost the average company $1,900 per employee, this solution is the most cost-effective solution to solve phishing and spam emails in the workplace.

CLOSING REMARKS

Overall, there is ample evidence that phishing has become a threat and will continue to threaten company and employee security. Phishing must be eliminated or mitigated to achieve the overall goal of company security. The proposed solution will allow for employees to browse their email safely and securely by implementing the following:

- Gmail spam filtering,
- Employee training,
- Email warning messages.

By using Gmail spam filtering and implementing employee training meetings, the company will save - on average - over $1,500 per employee and increase labor efficiency in the process. The overall cost of the proposal will be minimal and negligible to the amount of savings the company will gain. The proposed solution will not only save time and money at the company but, of course, improve company security and longevity.

WORKS CITED

Bauer, Emily. “15 Outrageous Email Spam Statistics That Still Ring True in 2018.” Propeller, Propeller, 1 Feb. 2018, www.propellercrm.com/blog/email-spam-statistics.

Essential Cyber Security Handbook In English. N.p., Nam H Nguyen, 2018.

Freydrew. “2020 Webroot Threat Report: Phishing Attempts Grew by 640% Last Year.” Webroot Community, Webroot Community, 25 Mar. 2020, community.webroot.com/news-announcements-3/2020-webroot-threat-report-phishing-attempts-grew-by-640-last-year-342560.

“How to Handle a Phishing Attack.” KashFlow, www.kashflow.com/handle-phishing-attack/.

Rampton, John. “Wasted Employee Time Adds Up: Here's How to Fix It.” Entrepreneur, Entrepreneur.com, 13 July 2018, www.entrepreneur.com/article/316450.

“The Mail You Want, Not the Spam You Don't.” Official Gmail Blog, 9 July 2015, gmail.googleblog.com/2015/07/the-mail-you-want-not-spam-you-dont.html.

“Verizon Data Breach Investigations Report (DBIR) - 2019.” Phishing Simulation & Awareness Training, Phishingbox, 28 Aug. 2019, www.phishingbox.com/news/phishing-news/verizon-data-breach-investigations-report-dbir-2019.

Workopolis. “Tuesday Is the Most Productive Day of the Week.” Workopolis Blog, 28 Jan. 2014, careers.workopolis.com/advice/tuesday-is-the-most-productive-day-of-the-week/.