Text-mining and Visualizations of Phishing Attacks in the Education Sector

Mohamed Abdelhamid
California State University, Long Beach
Mohamed.Abdelhamid@csulb.edu

Ayush Vij
California State University, Long Beach
Ayush.Vij@student.csulb.edu

Madhur Ingle
California State University, Long Beach
Madhur.Ingle@student.csulb.edu

Ruben Cervantes
California State University, Long Beach
Ruben.Cervantes@student.csulb.edu

Abstract

Phishing is cybercrime in which the attackers usually impersonate a trusted source. The attackers usually send an email that contains a link that allows them to steal the receiver personal information. Phishing is among the top cybercrimes according the FBI IC3 2018 report. Several studies investigated ways increase awareness and improves employees' resistance to phishing attacks. However, in 2019, successful phishing attacks continued to raise at a higher rate. Phishing is all about the social tactics which attackers seem to get better at. In this preliminary research paper, we investigate trends in phishing attacks that targets the education sector. We apply text mining and data visualizations to reveal patterns. Utilizing eight years of phishing data from an education institution, we that recent general phishing reports and training do not completely apply to the education sector. Suggesting a need to move away from a one size fits all phishing awareness and training strategy. We, find that emails are getting more positive in sentiment, more objective, less wordy, and use less of time pressure tone. Thus, making it harder to detect a phishing email. However, the negative sentiment and time pressure strategy are utilized during the weekend using the deactivation theme when employees have no or limited access to staff. Unlike most recent reports state, November and December receive the lowest load of phishing attacks which makes applying an intensive phishing awareness strategy in the month of October (national cyber security awareness month) a misuse of resources.

Introduction

Phishing refers to the cybercrime where a normal computer/mobile phone user is targeted by a scammer. This is done when the scammers contact the user with a phone call, text message, IM chat or an email. This communication is most about luring the user to get their sensitive data like banking details, credentials to various account their own and more. The first time that the term phishing was used and documented was in 1996 in the United States and the first lawsuit was filed in California in 2004 (Gupta, Tewari, Jain, & Agrawal, 2017). The official website of *America Online* was imitated and the scammer was able to get sensitive data from a number of user who fell into the trap. Since then, there have been various means by which a scammer performs phishing digitally on a user. These methods are either calls, text messages, emails, or more. This helps them to get access to the target's private information unethically. This poses a great danger to digitalizing traditional paper based tasks. There are various terms that are used to define different means to phishing. If the phishing is done using voice calls, it is termed as *vishing,* in case the phishing is done using SMS or text messages, it is termed as *smishing* and there are many other terms that the scammers are coming up to define their method of stealing data.

According to various recent reports and research, the most common features of Phishing Emails are that they *are astonishingly true, sense of urgency (pushing to take an action as soon as possible), too many links, and unexpected attachments, anonymous or unknown sender.*

FBI released their annual IC3 report for 2018 (IC3, 2018). It said, there were about $2.7 billion in financial losses alone due to about 352K cases of theft, fraud and exploitation on the Internet. Donna Gregory, the Chief of IC3 quoted: *"The 2018 report shows how prevalent these crimes are. It also shows that the financial toll is substantial and a victim can be anyone who uses a connected device."* The report suggests the users who wish to recovery their financial losses to contact their bank immediately upon the discovery of a fraudulent transaction and report the crime to IC3.

Phishing does not only impact a user's monetary assets negatively but also builds a doubt on every single time there are contacted or notified via phone calls, texts or emails. This shatters all the reliability a user has on electronic media to carry out a variety of tasks. In a nutshell, it brings in a negative impact on electronic communication and hence wrecks the workflow in a larger aspect.

In this preliminary research, we explore changes in trends of phishing emails, specifically in education sector. Education sector is among the top 4 sectors by phishing attacks volume. We find that a one size fits all strategy does not work for the education sector. We find several changes in recent trends and many discrepancies between recent reports and our findings. We also apply text mining techniques and find changes in the structure and text characteristics of recent emails.

Examples of Recent Famous Phishing Attacks:

Some of the biggest and most famous phishing attacks are *Operation Phish Phry, the Walter Stephan scam, the Target / FMS scam, the attack on the Ukrainian Power Grid, the Moscow World Cup Vacation Rental scam (Brad, 2018).*

Hundreds of bank account credentials were phished by hackers when the users received an official looking email from their banks. These users were redirected to a fake website where they entered their account numbers and passwords on these fraudulent websites. FBI called this Operation Phish Phry the largest international phishing case.

The Austrian aerospace executive, Walter Stephan lost about $47 million on a single phishing scam. The cybercriminals created a realistic looking but fake email account of Stephan when he was the CEO of FACC and sent an email to a lower level employee to transfer the said amount to an unknown bank account calling this an acquisition project. This was a great game of hit and trail where the scammer actually reached his objectives. It is called as the Walter Stephan scam.

The Target data breach took place due to an indirect phishing attack. This affected 110 million users. The scammers attacked a third-party HVAC vendor named *Fazio Mechanical Services (FMS).* FMS had trusted access to the servers which Target owned. So, getting access FMS's servers led the scammers have access to Target's servers.

In December of 2015, three of the Ukrainian Power Grids were attacked where the attackers were able to take control of the information systems at three energy distribution companies and temporarily disrupt electricity supply to the consumers. The phishing emails sent to the computers at these electric grid companies contained the *BlackEnergy* malware that made this attack a success. The malware was automated and could receive scalable firmware updates to attack multiple sites with ease.

The Moscow World Cup Vacation Rental scam took place during the sale of FIFA Football game in Russia. Scammers sent a number of immutable emails to the fans of the game promising vacation packages, free tickets and what not. In another similar case, the attackers targeted the partner agency hotels of Bookings.com and extracted user data. And used this data to further contact the users of Booking.com using WhatsApp and SMS Messages asking them to verify their banking details to confirm their bookings.

Related Work

There have been many researches that have taken place to look for patterns in phishing emails exclusively using text mining. These patterns represent some of the similar things that a typical phishing email contains. There are many ways by which these patterns can be recognized. Jain and Richariya (2011) proposed that a web browser can also be trained and used to screen emails that arrived on a mailbox used to browse it. And with time as more and more emails arrive, the web browser can be trained to be more accurate in detecting fraudulent emails. The prototype web browser showed focuses on solving issues with banking frauds.

In addition, methods like Text clustering, text mining, topic modelling, and classification have been used to improve systems that detect and block phishing emails. For example, Basavaraju and Prabhakar (2010) used cluster analysis to detect spam emails. Jeeva and Rajsingh (2016) apply association rule mining techniques to detect phishing emails that contain malicious links.

Niakanlahiji, Chu, and Al-Shaer (2018) proposed a framework of Machine Learning has been proposed to detect Phishing webpages. It is dubbed as PhishMon**.** And it makes use of 15 novel features that can be used on a webpage effectively without relying on search engines or other services like Alexa or WHOIS. These results come with 95.4% of accurate output with a space of 1.3% of false positive rate for some unique phishing instances. Some researchers have focused on improving text mining and data extraction techniques which are then used as scripts to extract data from emails in a semiautomatic manner and analyze it to find patterns and other data (Zareapoor & Seeja, 2015).

However, in 2019, still about 30% of phishing emails bypass security detection measures (TheSSLstore, 2019). In addition, phishing volume has increased by approximately 41% in 2018 and the success rate of attacks has also increased. Although phishing detection technology is advancing, it cannot keep up with the advancement rate in phishing attacks. Therefore, many experts and researchers emphasize the importance of improving user awareness and training in regards to phishing. In fact, most expert agree that best way to defend against phishing attack is to train employees and individuals to detect phishing emails in addition to security measures that detects some of the attacks automatically.

Therefore, several studies have focused on the user side of the equation. User awareness for phishing emails stands to be one of the main prevention measures for phishing all around in the cyber space. Researchers have defined phishing as a social engineering where an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party. This brings in the scope for mental understanding of a normal user and the mentality loopholes that an attacker makes use of to execute their tasks. Hence, various awareness campaigns like public announcements, seminars, podcast and more help in make users aware of these attacks and hence preventing these phishing attacks in any forms (Jansson & von Solms, 2013). Miranda (2018) suggest that phishing training programs can increase employee resistance to phishing attacks. Various studies proposed a game design framework to prevent many phishing attacks (Chandrasekaran, Narayanan, & Upadhyaya, 2006; Goel & Jain, 2018). This framework enhances user avoidance behavior through motivation and hence results in preventing these phishing attacks. Other researchers looked at the characteristics of victims such as email habits, perception of risk, and self-efficacy (Arachchilage, Love, & Beznosov, 2016; Vishwanath, Harrison, & Ng, 2018).

The Problem

Efforts in awareness are yet to prove successful. As mentioned earlier the success rate of the attacks has increased globally. Further, about 35% of employees do not even know what phishing is (Wolinsky, 2019). In addition, many of the recent studies and current training are focused on recommendations that many attackers get around. For example, Jensen, Dinger, Wright, and Thatcher (2017) focus on training and recommendations that help individuals avoid phishing. One of the main recommendation is to look for HTTPS in in the address bar. Similarly many online material and articles list similar recommendations which also include unknown sender, generic greetings, and grammatical mistakes. However, according to the 2019 phishing trends and intelligent report, about 50% of phishing attacks utilize SSL making them harder to detect (PHISHLABS, 2019).

More importantly, attackers have constantly advanced and changed strategies. In fact, 2019 has been a year of phishing evolution. Microsoft released a report in December 2019 that talked about evolving methods of phishing and explained the three most notable attack techniques of phishing they observed with their Microsoft Threat Protection services in 2019 (Microsoft, 2019). The first one involved hijacking the links that appear in one's Google search results by adding an anchor tag in the HTML code of the webpage. The second one involved abusing the use of Error 404 pages. When online services like MTP scanned these websites, it would return a 404 error that the page was not found but when the real user surfed through the same link, it would detect a real user and redirect them to the main phishing page. The third attack makes use of the *man-in-the-middle (MitM) server*. Here, the attacker mimicked the sign-in or sign-up page of legitimate websites on their own custom domain and server. The user is invited to use the page to enter their sensitive information and then is the data is stored by the attacker and is passed to the legitimate server to give the user the results they expect. Hence, resulting in theft of sensitive data.

Phishing is ultimately a social tactic. According the Verizon data breach investigation report, 43% of cyber-attacks encompass social tactics and of those that utilize social tactics, 93% are phishing attacks. Therefore, constant efforts should be invested in understanding the trends and changes in the social tactics of attackers. Detection, awareness, and training strategies need to be constantly evolving. In addition, a one size fit all recommendations and strategies will not benefit most organizations. In this preliminary research, we show that trends in the education sector are different from most past and recent findings. We also show how the trend and social tactics are changing and improving in quality making current recommendations inadequate in some cases.

Methods

Data

The dataset comes from a large public university in California. About 84% of phishing attacks target the United Stated (PHISHLABS, 2019). In addition, California suffered the most financial losses from cybercrimes in 2018 in the United States (IC3, 2018). In fact, California's financial losses was more than the losses of 39 states combined making it the ultimate destination for cyber criminals. Thus, the findings coming from this data are generalizable.

The university cybersecurity team follows a specific process for reporting, recoding, and announcing phishing emails that targets the university employees. We received multiple pdf files of the data which contain 872 phishing emails recorded between 2012 and 2019. The emails represent high risk phishing emails that bypassed the system and were reported and/or discovered by employees. Only emails that were considered of high risk as per the judgment of the cybersecurity team were saved as an image and added to the public website that shows all unique phishing emails. University employees can visit the website to check the latest phishing emails.

Data Extraction

The emails were saved as picture and not in any structured way that allow analysis to be conducted right away. To structure the data, we used an optical character recognition (OCR) tool to convert images to text then extracted the data to an excel file. The initial excel file after the extraction contained the following

columns: Email date, Email Subject, From, Email Body, Summary of Email (written by the cybersecurity team), and Intent (written by the cybersecurity team).

Data Cleaning and Recoding

We then used python to clean, recode, text mine, cluster, and extract data then write to a new excel file. The following python libraries have been used: nltk, textblob, statistics, numpy, openpyxl, pandas, matplotlib, wordcloud, spellchecker, datetime, calendar, and wordcounter.

The subject line and body of the email is analyzed for sentiment polarity, sentiment subjectivity, sentence length, word length, and character length. From each row the code inserts a new column to collect the data of each entry {polarity, subjectivity, sentence length, word count, and character count}. Each row entry is analyzed and recorded onto the active sheet and recorded in its corresponding data cell.

From the extracted text the words were counted by frequency and a list of the top 20 words were created for subject line and email body. The body extracted text was run through a function that removed stopwords and other filtered words in order to produce a more meaningful wordcloud and frequent word list. Based on most frequent words were created different categories/types of emails such as deactivation, password, maintenance, update, other, etc. Each email was then assigned to one of those categories. The dates were split from a single 8 digit year/month/day to 3 separate columns year, date, month. This was done to facilitate analysis.

Analysis and Results

Phishing by Month

Most recent reports, indicate that the holiday season, specifically October, November and December, are the most popular for phishing scammers (Barracuda, 2019; F5, 2018). This makes the National Cybersecurity Awareness Month in October a perfect time for organizations to increase awareness of cybercrimes including the phishing attacks and increase phishing susceptibility activities such as phishing simulation. Educational institutions are no different, many universities hire third party companies to conduct phishing simulation, testing, and analysis during this month. Third party companies apply general knowledge of the bigger umbrella on a very unique setting. However, phishing data of eight years in an educational institution tells a different story. The months of November and December have the least volume of phishing attacks (see Figure 1). More importantly, this story is not a new one, the trend has been consistent since 2012. On the other hand, most attacks occur on August then September followed by February and January. These months represent the start of the fall and spring semesters. This means that many universities focus efforts against phishing a month after the worst attacks have occurred. Then, in ten month when all the knowledge gained in training is forgotten and when attackers have evolved their techniques even more, the universities are taking minimum actions.

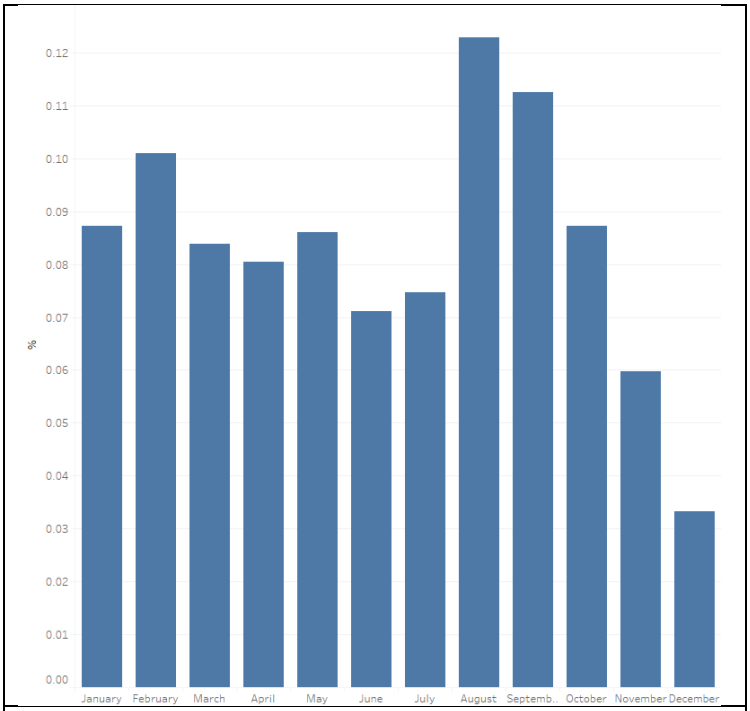

Figure 1. Phishing Emails by Month

Phishing by Weekday

Several reports presented statistics regarding the top phishing day of the week. However, there has been inconsistencies in the days. Some report that Friday is the top phishing day of the week (Sjouwerman, 2017). Others state that Tuesday is the top day for phishing attacks and Friday being the lowest of all work days (Barracuda, 2019). Most reports agree that the weekend has the lowest rate of phishing attacks. More interestingly, the 2018 State of Phish report indicate that only 1% of phishing emails are reported on a Saturday.

Our results show that the story might be different for the education sector. Figure 2 show the ratio emails by the day of the week. Overall, and in 2019, Wednesday is the top day followed by Tuesday then Monday. The results for Friday and the weekend are very similar to that of Barracuda (2019). However, this trend has not been the same in the past few years. Between 2014 and 2017, Monday was the most popular day for phishers. Then attackers shifted strategy in the last 2 years to midweek as they, probably, realized that faculty and staff are too busy to pay attention to emails in the first day of the week were prioritizing takes place.

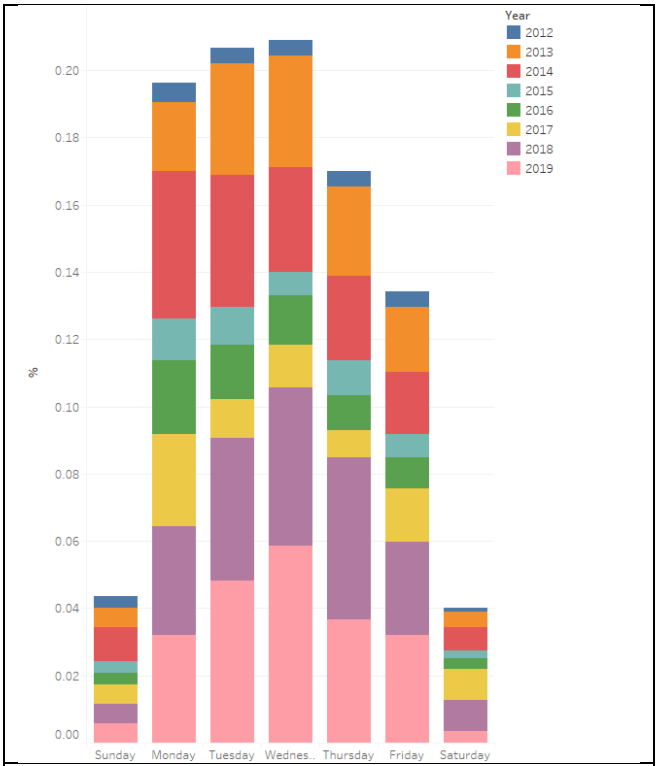

Figure 2. Phishing Emails by Weekday Trend

Text Mining

Sentiment by weekday

However, those statistics include all types of phishing emails. As mentioned earlier, phishing is all about the social tactics. As we explore the data closer, we find new trends that show how dangerous the weekend can be. Although the weekend have less volume of phishing emails, they have more negative sentiment polarity, on average (see Figure 3). The weekend is when employees do not have access to staff, employees, and colleagues to seek advice. Attackers take advantage of this fact by sending emails with a tone of warning that implants fear and pressures individuals to take actions as soon as possible. Emails of account deactivation and unusual sign in are popular in weekends. This was the old general tactic that has now been moved to the weekend. During the week, attackers started playing a different social tactic by making emails more realistic with less emphasis on time pressure and more positive sentiment (see Figure 4 for an example).

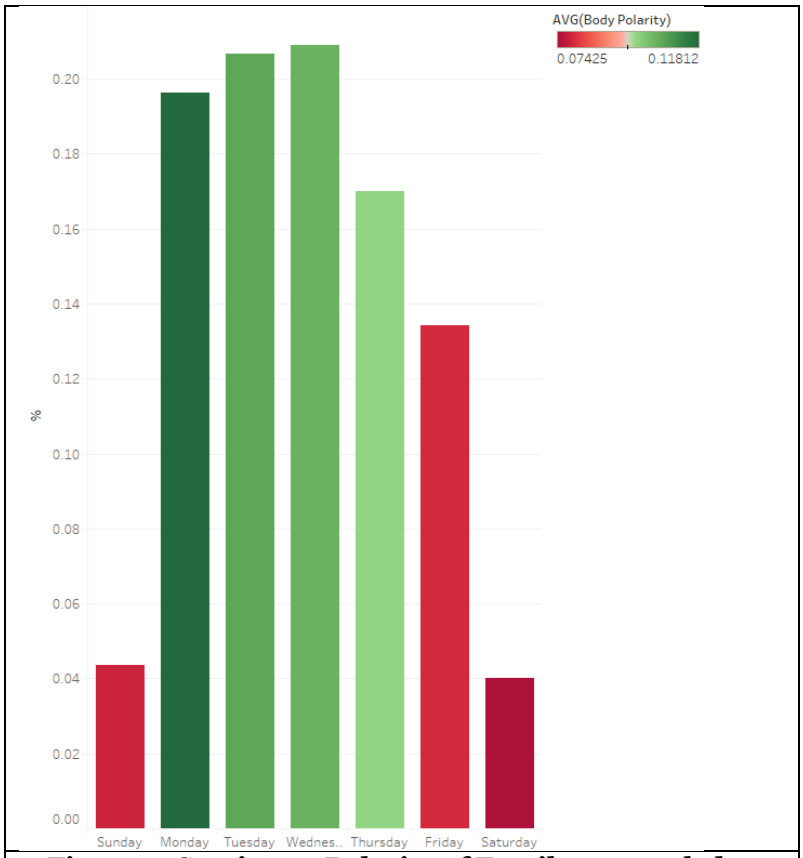

Figure 3. Sentiment Polarity of Emails per week day

Sent: Wednesday, March 22, 2017 10:45 AM
Subject: Mailbox Account Upgrade

Dear User

From the 20th March we are undergoing account maintenance please ensure to upgrade your account before March 24th or You'll not be able to read and send emails, you will no longer have access to many of the latest features for improved conversations, contacts and attachments.

Take a minute to update your ACCOUNT for a faster, safer and full-featured Mail experience VERIFY HERE
<https://webmailhelpdesk.typeform.com/to/oEAFEH>

Sincerely,
IT Help Desk

© 2017 Copyright. All rights reserved

Figure 4. Example of Positive Tone Emails

Sentiment Trend

Sentiment polarity measures the feeling and emotions in textual data. The values range from -1 (being very negative) to +1 (being very positive). In this study, we explore the trend in sentiment polarity in the all emails in the last eight years (see Figure 5). We find that attackers used to apply fear strategy to pressure victims to click on the link and possibly give personal information. However, the strategy is changing towards more use of positive words in the emails which work as method of persuasion. Many recent training, recommendations, and research emphasize on the on the negative tone and time pressure as being important factors in detecting a possible phishing attack. Thus, attackers are changing tactics to more positive tones. The example in Figure 4 illustrate the use of highlighting benefits that will be gained as result of clicking and complying with the messages as opposed to stressing losses that will occur if the user does not click.

Occasional negative sentiment emails are still being received. There could be several reasons for this. One reason might be that these emails represent low quality phishing attacks and attackers who have not advanced yet. Another reason could be completely strategic in which attackers' purposively send those types of emails to keep current recommendations and training unchanged. This will result in a higher success rate for higher quality emails that changed tone and sentiment.

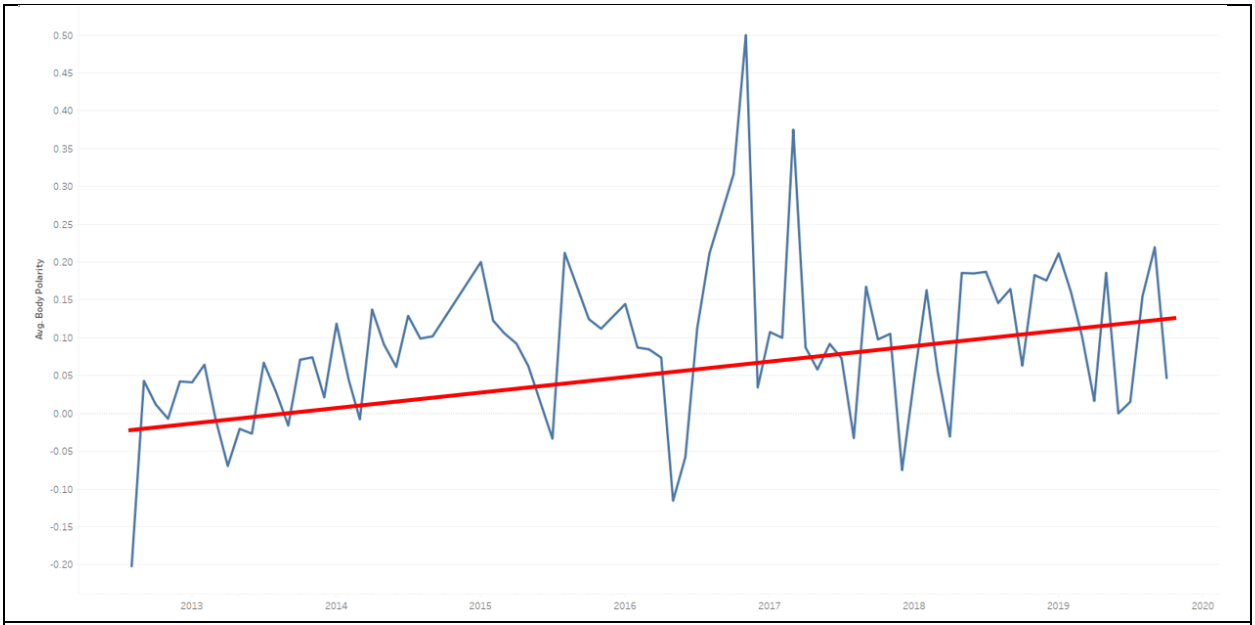

Figure 5. Email Sentiment Polarity Trend

In addition, we find that emails are getting much better in quality as they tend to be more and more objective making it extremely hard for the average person to detect a phishing emails. Sentiment subjectivity measures how subjective or objective the text is. Sentiment subjectivity can take any value between 0 and 1. Values between 0.5 and 1 indicate a subjective text with 1 being the very subjective. Values between 0 and 0.5 indicate an objective text with 0 being very objective. Figure 6 show that on average phishing emails seem to get more objective in recent years showing that the quality of phishing emails keeps getting better. Thus, current basic recommendation in detecting phishing emails need significant revamping.

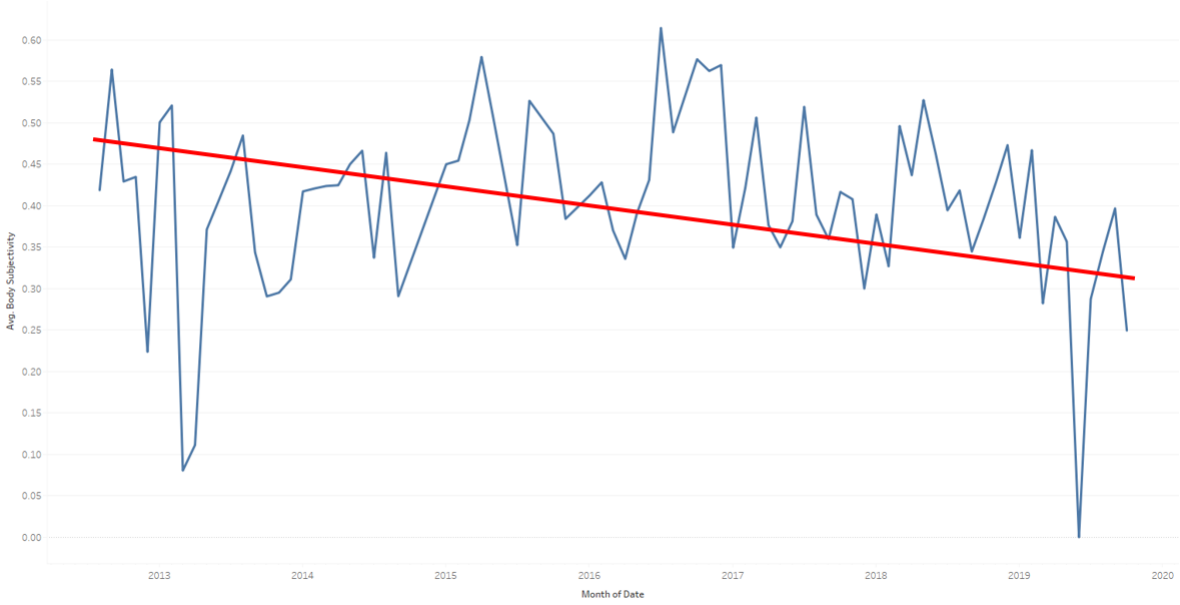

Figure 6. Email Sentiment Subjectivity Trend

Conclusion

Phishing remains a problem that continues to increase. While companies, experts, and researchers continue to develop new methods to detecting phishing attacks and improve resistance to falling a victim to phishing, attackers are advancing and improving phishing attacks at a higher and a more successful rate. 2019 has been named as a year phishing evolution by Microsoft as attackers' innovate in both technical and social tactics. The only way to mitigate phishing attacks is get ahead of the attackers. In this preliminary research, we focus on understanding trends in the social tactics that attackers use in the education sector. We find several differences between trends in recent reports and our findings. For instance, while most reports and experts state that holiday months (October, November, and December) are most dangerous, we find that November and December the least dangerous in the education sector. This proves that educational institutions put emphasis on phishing simulation, training, awareness in the month of October (National Cybersecurity Month) are investing resources in the wrong time. In fact, beginning of semester proved to be the most common for phishing attacks which requires changes of strategies in regards to awareness and training.

In addition, we apply text mining techniques to investigate characteristics and trend in the text of phishing emails. We find that in general, the quality and believability of phishing emails are getting better. For example, we find that emails have more positive sentiment and more objective compared to previous years. However, attackers understand that employees have less access to staff and experts during the weekend and thus send negative sentiment emails with time pressure and theme of fear such as account deactivation mostly during the weekend. These patterns could enable and motivate changes to internal business processes that mitigate such attacks. For example, specifying days for communications related to internal systems.

Moreover, there is less use of time pressure and more use of positive words which makes it even harder to distinguish between a legit and a phishing emails. We propose a more focused understanding of phishing attack for each organization and sector. A one size fits all training, simulations, and strategy might not benefit most organization.

References

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior, 60*, 185-197.

Barracuda. (2019). Spear Phishing: Top Threats and Trends. Retrieved from https://assets.barracuda.com/assets/docs/dms/Spear_Phishing_Top_Threats_and_Trends.pdf

Basavaraju, M., & Prabhakar, D. R. (2010). A novel method of spam mail detection using text based clustering approach. *International Journal of Computer Applications, 5*(4), 15-25.

Brad. (2018). The Top 5 Phishing Scams in History – What You Need to Know. Retrieved from https://www.phishprotection.com/blog/the-top-5-phishing-scams-in-history-what-you-need-to-know/

Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006). *Phishing email detection based on structural properties*. Paper presented at the NYS cyber security conference.

F5. (2018). 2018 Phishing and Fraud Report. Retrieved from https://www.f5.com/content/dam/f5-labs-v2/article/articles/reports/20181031_phishing_report/F5Labs_2018_Phishing_and_Fraud_Report.pdf

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & security, 73*, 519-544.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications, 28*(12), 3629-3654.

IC3. (2018). *2018 Internet Crime Report*. Retrieved from https://pdf.ic3.gov/2018_IC3Report.pdf

Jain, A., & Richariya, V. (2011). Implementing a web browser with phishing detection techniques. *arXiv preprint arXiv:1110.0360*.

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology, 32*(6), 584-593.

Jeeva, S. C., & Rajsingh, E. B. (2016). Intelligent phishing url detection using association rule mining. *Human-centric Computing and Information Sciences, 6*(1), 10.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of management information systems, 34*(2), 597-626.

Microsoft. (2019). The quiet evolution of phishing. Retrieved from https://www.microsoft.com/security/blog/2019/12/11/the-quiet-evolution-of-phishing/

Miranda, M. J. (2018). Enhancing cybersecurity awareness training: a comprehensive phishing exercise approach. *International Management Review, 14*(2), 5-10.

Niakanlahiji, A., Chu, B.-T., & Al-Shaer, E. (2018). *PhishMon: A Machine Learning Framework for Detecting Phishing Webpages*. Paper presented at the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI).

PHISHLABS. (2019). 2019 PHISHING TRENDS AND INTELLIGENCE REPORT. Retrieved from https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf

Sjouwerman, S. (2017). What Is The Top Phishing Day Of The Week? And Why?

TheSSLstore. (2019). 20 Phishing Statistics to Keep You from Getting Hooked in 2019.

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research, 45*(8), 1146-1166.

Wolinsky, J. (2019). The Cost Of Phishing Emails To Business Is Staggeringly High. Retrieved from https://www.valuewalk.com/2019/07/cost-phishing-emails-infographic/

Zareapoor, M., & Seeja, K. (2015). Text mining for phishing e-mail detection. In *Intelligent Computing, Communication and Devices* (pp. 65-71): Springer.