Psychology in Phishing

Jonathan Dolan

IASP 470 System Security Capstone

March 17th, 2020

Abstract

Phishing is a common security issue for organizations and personal computer users worldwide. Malicious attackers have access to so much information and skills today, that crafting specialized emails to trick users into giving their credentials is the easiest key when picking the lock of security. The techniques and styles used by these attackers are limitless. But what is it about these emails that make people click? How is the human psychology wired when it comes to decision making and can we use this insight to improve the security of the front lines. This paper intends to analyze these aspects as well as provide elaborations on the mitigation of this risk through user education and gamification.

Table of Contents

Introduction

Communication as we know it today has seen a rapid evolution in a short space, culminating in constant accessibility. Due to advancements in technology people are able to communicate through multiple mediums across geography and time zones. However, this evolution has come at the expense of privacy and security. We are now in charge of more online accounts, apps and platforms than ever before with protection for them lacking. Due to the accessibility of the internet, malicious agents from around the world can target unsuspecting users through the very communication tools that have enhanced everyday living. A common attack in this domain is known as 'phishing'. The National Institute of Standards and Technology (NIST) describes phishing as: "Tricking individuals into disclosing sensitive personal information through deceptive computer-based means."[1] This can come in the form of bogus emails where the attacker manipulates the user into clicking links and entering sensitive data into forged webpages. Further techniques and styles will be discussed later in this paper.

Phishing is an enormous problem in the world of cyber and information security. Preventing such an attack, not only depends on technological sophistication but also human characteristics. Vishwanath details that "phishers engineer attacks to take advantage of individuals' high in affective commitment by personalizing [emails] and invoking brand familiarity, using fear appeals in the form of threats and warnings, appealing to individuals' sense of patriotism…[The] emphasis is on peripheral route persuasion where images and symbolic cues distract attention away from detailed and thoughtful cognition."[2] This is a common problem for private users as well as organizations worldwide, with the cost of such attacks having devastating impacts. According to Proofpoint's *2020 State of the Phish*, "More than half (55%) of respondents (of a survey of more

than 600 IT professionals across seven countries) said their organization fell victim to at least one successful phishing attack in 2019 […] 65% of U.S. organizations experienced a successful phishing attack last year, well above the 55% global average."[3]

Phishing emails are commonly used to harvest credentials but are also be used to deliver more malicious payloads. Common payloads include ransomware, which lockdown a host's device by encrypting all files and demanding ransom in the form of bitcoin or other cryptocurrency. Last year (2019), "GandCrab, a ransomware-as-a-service offering, plagued many organizations[…] It reportedly generated $2 billion in ransom payments before going off the market in June."[3] Also, as Vishwanath points out, "in addition to being used by criminals, such phishing type attacks have been implicated in cyber-espionage attacks. For instance, in a recent case (2012) that has been attributed to the Chinese government, a phony Facebook profile of a high-ranking U.S. navy commander was used to friend military personnel in the U.S. and U.K. in order to monitor their movements […] " [2]. To further this, as Schenkman points out "[in] the infamous case of John Podesta, Hilary Clinton's campaign chairman for the 2016 presidential election, his clicking on a phishing email allowed a foreign nation to steal politically sensitive emails" [4]. Phishing is not only just used for petty theft but also nation state espionage.

With these threats in mind, why hasn't technology been able to stop this criminal activity. The problem is that no matter what protections are put in place in the form of hardware, software or artificial intelligence, these malicious agents find new ways to infiltrate and expand their techniques. Boyd describes three common techniques being used today:

- "[Open] source software such as 'PHP Mailer' allows threat actors to manually type in both 'To' and 'From' addresses. Once the email is delivered, the recipient will be

viewing an email that looks very much as though it's from the email account listed in the 'From' field, regardless of where it *actually* came from."

- "[Threat] actors often hijack mail servers and use them until the provider cottons on to their game. At that point, they'll simply hijack a different mail server and keep on keeping on."
- "By far the simplest way for threat actors to send convincing emails is to use throw-away email domains, free email addresses, and ISP access accounts, all with fake, forged, or stolen IDs. Once again, even when the provider catches on, all they have to do is move to a new account" [5]

With all this in mind, how do we mitigate these attacks? What can organizations do to limit the risk and cost that these threats provoke? This paper aims to investigate these questions and provide solutions. The aim of this paper will be to analyze common phishing emails seen in the wild and understand the techniques and styles used to trick unsuspecting users. It will investigate the psychology into why people click on phishing emails, giving us an insight into the mind of the end user. This paper will then finish by examining risk mitigations to these issues through the means of user education and by reviewing an example of a company that utilized gamification in order to achieve these means.

Analysis of Common Phishing Emails

Phishing emails come in many shapes and forms. There are event different types known as ‘Spear Fishing’ and ‘Whaling’. NIST describes spear phishing as: “A colloquial term that can be used to describe any highly targeted phishing attack” [1] and whaling as: “A specific kind of phishing that targets high-ranking members of organizations” [1]. With these specifics in mind, malicious agents craft their bogus emails depending on the user. To get a foothold and trust worthiness with the individual they are attempting to deceive, they need to customize their email to achieve their goal. Here are some examples that have been seen in the wild:

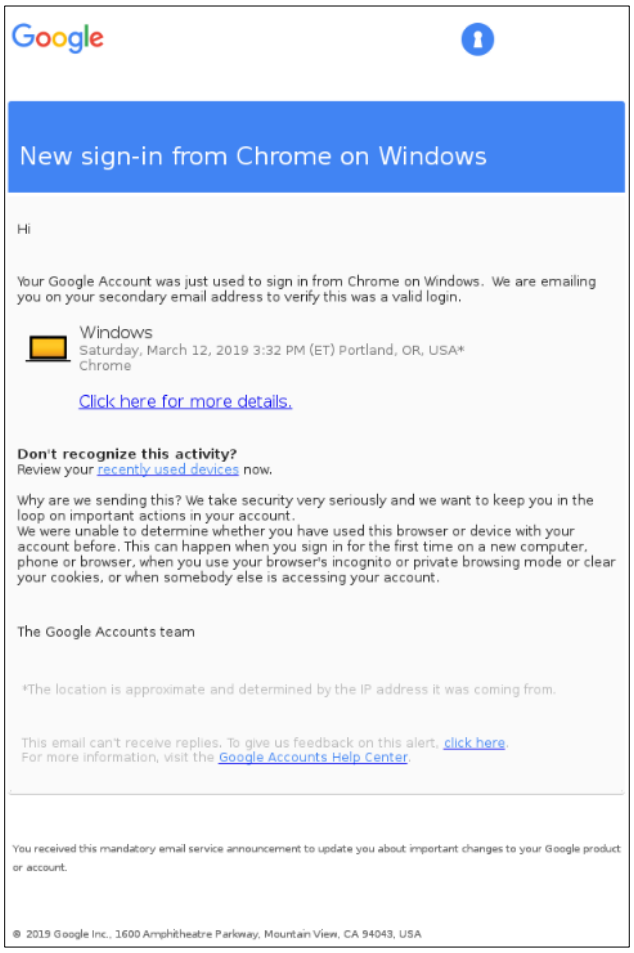
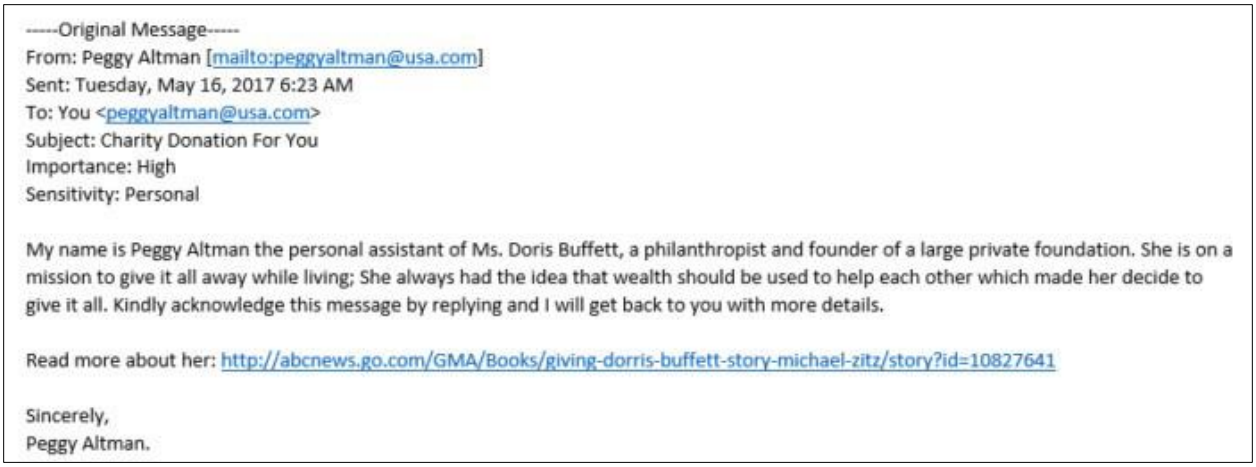


Figure 1. Google Security Notification. [6]



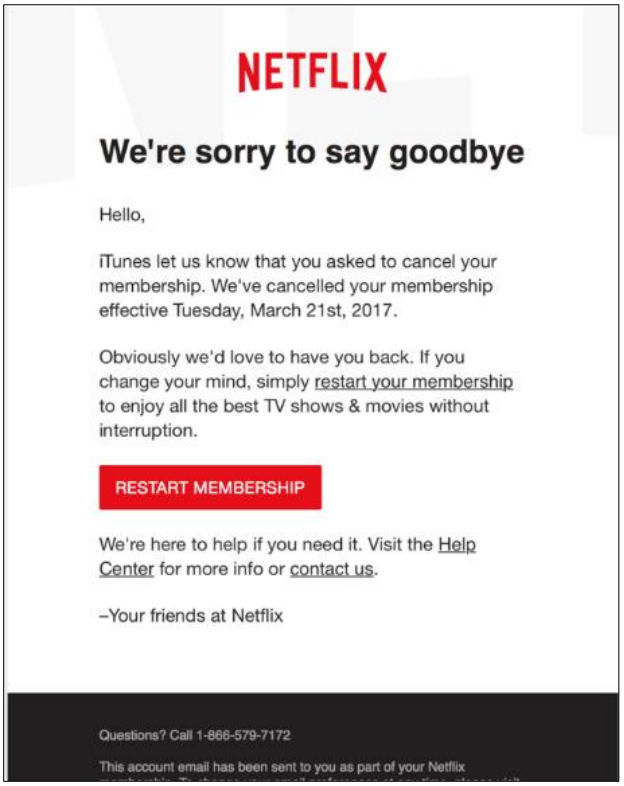
-----Original Message-----
From: Peggy Altman [mailto:peggyaltman@usa.com]
Sent: Tuesday, May 16, 2017 6:23 AM
To: You <peggyaltman@usa.com>
Subject: Charity Donation For You
Importance: High
Sensitivity: Personal

My name is Peggy Altman the personal assistant of Ms. Doris Buffett, a philanthropist and founder of a large private foundation. She is on a mission to give it all away while living; She always had the idea that wealth should be used to help each other which made her decide to give it all. Kindly acknowledge this message by replying and I will get back to you with more details.

Read more about her: http://abcnews.go.com/GMA/Books/giving-dorris-buffett-story-michael-zitz/story?id=10827641

Sincerely,
Peggy Altman.

Figure 2. Charity Donation. [6]



NETFLIX

We're sorry to say goodbye

Hello,

iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we'd love to have you back. If you change your mind, simply restart your membership to enjoy all the best TV shows & movies without interruption.

RESTART MEMBERSHIP

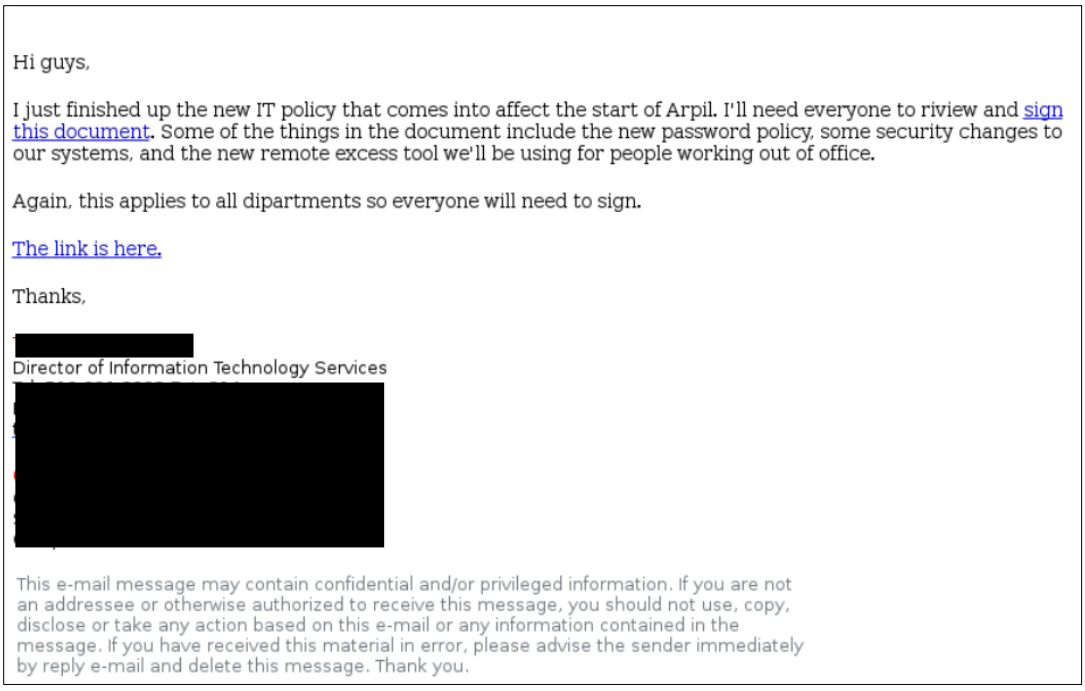
We're here to help if you need it. Visit the Help Center for more info or contact us.

–Your friends at Netflix

Questions? Call 1-866-579-7172

This account email has been sent to you as part of your Netflix

Figure 3. Netflix. [6]



Hi guys,

I just finished up the new IT policy that comes into affect the start of Arpil. I'll need everyone to riview and sign this document. Some of the things in the document include the new password policy, some security changes to our systems, and the new remote excess tool we'll be using for people working out of office.

Again, this applies to all dipartments so everyone will need to sign.

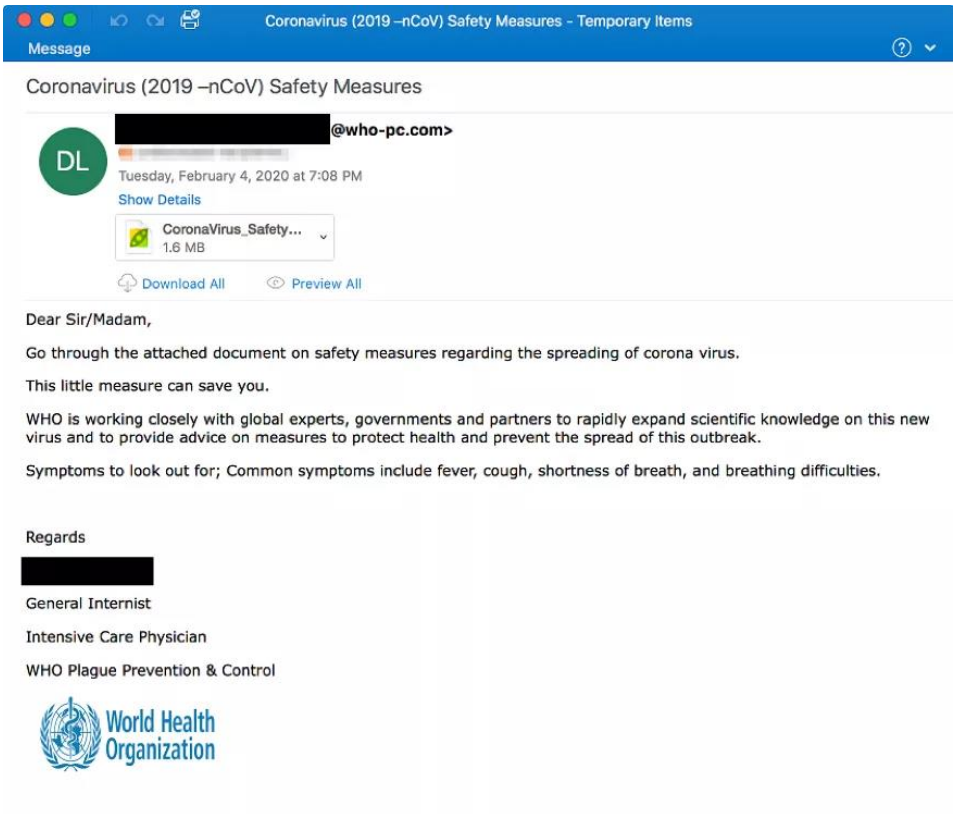
The link is here.

Thanks,

[redacted]
Director of Information Technology Services
[redacted]

This e-mail message may contain confidential and/or privileged information. If you are not an addressee or otherwise authorized to receive this message, you should not use, copy, disclose or take any action based on this e-mail or any information contained in the message. If you have received this material in error, please advise the sender immediately by reply e-mail and delete this message. Thank you.

Figure 4. IT Manager. [6]



Coronavirus (2019 –nCoV) Safety Measures - Temporary Items

Message

Coronavirus (2019 –nCoV) Safety Measures

DL [redacted]@who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

Show Details

CoronaVirus_Safety... 1.6 MB

Download All Preview All

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[redacted]

General Internist

Intensive Care Physician

WHO Plague Prevention & Control

World Health Organization

Figure 5. COVID-19. [7]

As we can see from the examples from Figure 1-5, the general form of phishing emails is to mimic brands, organizations, and people to convince the user that the content of the message is real. In four of the above cases we see the use of URL hyperlinks, which prompt users to clicking. These hyperlinks, while displaying an address or keyword, will hijack the action and redirect the user to a webpage where the attacker can harvest credentials (see Figure 6 below) or download a malicious executable.

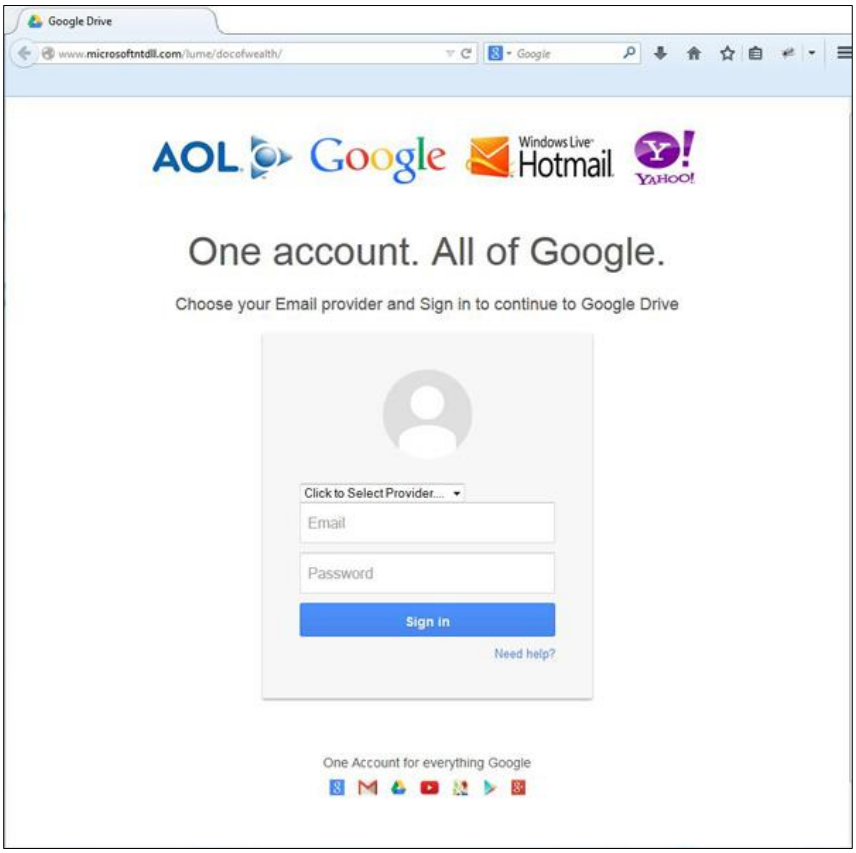


Figure 6. Fake Login Page. [8]

In Figure 5 we see an email with an attachment. Clever attackers know that, for the most part, email spam filters can analyze emails and see malicious links placed inside, quarantining the email. However, attachments can be used to bypass this protection. The attacker can choose to place a

hyperlink in a word document or excel workbook and instruct the user to click through this method. Another technique more commonly seen is the use of macros. This is when the user opens the word document, and the document says that it contains macros that need to be enabled. If the user clicks to enable a macro, malicious code may be executed, and the user's device will be compromised. Infamous malicious malware such as 'Ransomware' and 'Emotet' have successfully propagated through this form.

In the creation of these emails, sending addresses are often spoofed to appear more believable, i.e. Figure 5, the sender's domain address is listed as "@who-pc.com" to mimic the World Health Organization. However, the most significant aspect of phishing emails is in the content. Manipulation by means of familiarity, urgency or empathy are some of the tools used to trick users into following the commands given. As pointed out by the Federal Trade Commission (FTC) consumer website [9]:

"Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may:

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a government refund
- offer a coupon for free stuff"

These common, curiosity-inducing techniques are tried and tested methods in tricking the psychology of users, which will be explored more in the next section.

Why do People Click?

With all the information that is out there, and the vast amount of money put into research and development of anti-phishing products, how are phishing emails still effective? As mentioned previously, regardless of the technological sophistication, there is still a human sitting behind the screen making decisions. Where there are humans making critical decisions, there is an exploration into human psychology. Goel [10], Schenkman [4] and Jones et al. [11], discuss at least two psychological processes humans make when it comes to critical decision making. Schenkman summarizes this school of thought:

> "System 1 is fast, intuitive, and emotional — "like when you come to a doctor's appointment and you decide where to sit," she says. System 2, on the other hand, is slow and deliberate. Because we have to make thousands of decisions per minute, we need System 1, which depends on mental shortcuts to help us move through life efficiently. For instance, we have a truth bias, a belief that others are more likely to tell the truth than to lie; to assume otherwise would be exhausting. But biases like this can also leave us open to unwise decisions, by, say, making us predisposed to assume that an email which says it's from our bank updating our password is really from our bank." [4]

From this we see that because human thinking has different processes for dealing with different tasks, email being a mundane task of everyday work life falls into the category of "System 1" thinking. Depending on the position of employment and workload, email inboxes can be overwhelming with mental fatigue setting in when trying to process each message. As Goel puts

it, “people often process email messages quickly by using mental models or heuristics and, hence, overlook cues that indicate deception […]” [10]. Goel further elaborates on the psychology of phishing emails by stating, “[when] processing information peripherally, people do not think carefully about the content of the message; instead, they are influenced by superficial factors surrounding the communication. Phishing attempts often capitalize on peripheral routes to persuasion by incorporating cues that provoke action without careful deliberation.” [10]. This is then taken advantage of when “[a] carefully constructed phishing email may activate basic emotions that nudge people to comply with the disguised malicious request. For example, fear stems from the perception of threat to one’s wellbeing and acts as a warning signal for forthcoming harm […]” [10]. So, the evolution of our thinking when it comes to mundane communication or tasks highlights that we can be deceived by playing on this peripheral processing of information. By tweaking emails with deceiving information and mimicking real people and brands and without fully processing and deliberating in a “System 2” level of thinking, users will get caught out. As Schenkman reports, “While technology adapts and shifts quickly and frequently, humans don’t, [Daniela Oliveira (Cyber Security Expert)] says — and anti-phishing strategies should take that into account: “Evolution has hardwired us to operate the way we do. We’re not going to change that fast” [4].

The most crucial aspect to this is the sensitivity we have to time. In everyday work tasks, we are held and measured by the constant of time. Urgency and prioritizing of tasks becomes a common theme and normalizes the way we think. With that sensitivity to time, however, we are susceptible to making mistakes. The less we use the “System 2” thinking by deliberating on where emails are coming from and the context of the message, the more prone we are to attacks. Jones et al. describes this in a study: “Time pressure represents a situational factor that is shown to impair decision

accuracy, undoubtedly just one of many such factors in our daily environment. Individual differences are substantial, and at least partially explicable, here in terms of sensation seeking and cognitive reflection. Moreover, error rates are quite consistent with the argument that message persuasiveness reflects content such as sender familiarity and consistency" [11] and confirmed as much in their study of 224 university students and staff. On the other side of this, Jones et al. elaborated on the more deliberate thinking:

> "Participants were told to either give rapid responses upon a first look at an email (intuitive), or told to take their time, and read the email carefully before deciding on their final response (rational). In the rational decision-making condition, participants correctly identified more emails as fraudulent. Further to this, research based on self-reports regarding the use of rational and intuitive decision-making strategies after receiving a simulated phishing email demonstrated that higher reliance on rational processing predicted lower trust in the legitimacy of the email" [11]

This leads us into the next realm of psychology and phishing emails. How do we program the users to be more deliberate and equip them with the tools to identify and report malicious emails?

Awareness and Education

To combat this ever-present threat for organizations, Jansson informs, “most researchers and information security specialists agree that the key countermeasure to mitigate or prevent phishing attacks is security training” [12]. This is further backed up by Proofpoint’s 2020 report, in the survey of IT professionals, of which, “78% [say] security awareness training reduces phishing susceptibility” [3]. The idea of user education is widely accepted to reduce the threat of phishing across organizations because as Janseen further deliberates, “[although] technical tools can protect a user from falling prey to phishing attacks to a certain extent, it is important that the user does not become too reliant on technology. Thus, it is critical to combine the technical tools with phishing training” [12]. This goes back to the point that the most successful way to mitigate this risk is not relying on the technological sophistication but investing into changing the human characteristics that stand between a malicious attacker and the integrity of business security. The focus is not just on whether we educate users or not but how to educate them as best as we can. Going back to Proofpoint’s survey in the report, it is said that “63% of organizations punish users who regularly fall for phishing attacks” [3]. This would mean that 37% of businesses do not address the seriousness of phishing and input very little to no user education.

The idea of punishment for repeat offenders appears to be something of differing opinions. There is no ‘one-size-fits-all’ approach to dealing with the severity of this common vulnerability. Whatever the approach, Silic & Lowry argue that:

> "Although threats, fear, sanctions, and costs/benefits may have an appropriate place in organizations [e.g., 11, 27, 52], these approaches also run the risk of backfiring, causing reactance, a sense of injustice, or employee engagement in 'malicious compliance' or other microaggressions [63, 65]. Most employees prefer to work in an enjoyable and supportive work environment rather than one laden with rules, regulations, fear, and punishments." [13]

When it comes to training such a sensitive area of cyber security within a business there is a need for such penalties or else the motivation to participate is nonexistent. And if users are not participating then they are not learning. The use-case in this study comes from firsthand experience shared by this author at a medium sized business with more than 350 employees. To protect the identity of the business no names will be discussed, just training metrics. Information Security training was regularly implemented through online quizzes and simulated phishing attacks on a monthly schedule. The simulations were measured in 'clicks' and 'data entries' and users were recorded for each. Depending on how many 'clicks' or 'data entries' a user accumulated the penalty increased. Responses to infringements were quick, with Information Security staff, including myself, talking to users and informing them of the severity. Reactions to the simulations were not welcoming and reactions to meetings, post-infringement, were met with disdain. It is fair to say, the perception of the Information Security team was that of annoyance and aggravation. This reaction that we received reinforced Silic & Lowry's view of a backfire met with microaggressions. The phishing simulation test numbers also reflected the trend with wild fluctuations in 2018 ranging from a 10 % phish prone rate (calculation based on how likely a user is to be phished) to 22 % by the end if year. A high rate, but what was also concerning was the

lack of reporting of said emails with the Information Security team. Our issue was the approach to training.

Silic & Lowry [13], in the article, *Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance*, became an enlightening source for helping to think differently about changing the behaviors of users in regards phishing safety. They state that:

> "Employees [have] difficulty focusing on lengthy training sessions, especially when they are concerned about their actual work tasks. This is especially true in the context of security, in which most employees are not experts and lack efficacy. Most employees do not recognize the importance of caring about security in the context of everyday work. Thus, changing users' security-related behaviors through training is highly complex and prone to failure" [13]

To address this, a refocusing of the energy of the user group needs to happen. An idea to make something as trivial and unimportant, to the vast majority of users in an organization, more appealing. The method was to utilize gamification of the user learning experience. This "is an effective approach for improving intrinsic motivation, learning, coping skills, and subsequent security compliance. People are more motivated and conscientious when they have an enjoyable, immersive experience" [13]. As Tchakounté et al. describes, "it engages users at the emotional level for attitudes and behavior change, as well as knowledge acquisition" [14].

To draw on the ideas of gamification and user learning, Winkler & Manke lay out 4 principles: "1) Goal establishment, 2) Rules, 3) Feedback, and 4) Participation is voluntary" [15]. The goal establishment was to bring the 'phish prone' percentage as low as we can to minimize the risk. The rules were set so that all users knew how to participate and win. This was set up by tracking

users' performance in phishing simulations and whether they could report on real phishing emails received by distinguishing them from general spam. The early drawbacks of this were that not all departments or users got the same influx of email, however, to start the process this was temporarily overlooked. Once a monthly total of tracking was taken, a 'Phish Master of the Month' award was given to the winner and public recognition was received. This method of positive reinforcement is backed by Karl Kapp, a professor of instructional technology at Bloomsburg University and author of The Gamification of Learning and Instruction [16]. Interviewed by Crystal Bedell for InfoSecurity Professional, he describes the psychology of this method, "Rather than feedback around the game, give feedback messages around the behavior. That way when the employee is rewarded, it's aligned with the behavior you want to occur". He furthers this adding, "It's also important to have direct-line supervisors on board [...] They should be monitoring user behavior and providing verbal feedback whenever possible to reinforce the program. If positive feedback can be given within a group setting, that's even better." This too was added to the new program, with awards given to a senior manager once every quarter. The involvement of senior management propelling the seriousness of the training and setting an example. To loosen the restrictions on the game, as Winkler & Manke suggest, participation was voluntary. The idea of winning a tangible prize and recognition of their peers made participation desirable. Feedback for the program was overwhelmingly positive. After a couple of monthly winners had been presented, users became very engaged in the processes of the training and participation. A culture of competitiveness emboldened the learning aspect of what we were trying to achieve. Spencer Wilcox, the executive director of technology and security at PNM Resources in Albuquerque, N.M., is quoted by Bedell, framing the program "[the] more playful you make the environment, the more incentivizing and rewarding people will find the environment. You need to find the right

balance of play and entertainment that the culture requires to build awareness, to reward good behavior and disincentivize poor behavior" [16]. This was the balance we, the Information Security team, had hoped to find. After implementing this we noticed the 'phish prone %' had stabilized and only breached 10% on two occasions over the next year, with reporting of phishing emails drastically improving.

Bedell describes this shared profit from Masha Sedova, a former cyber analyst for the government and Salesforce. "During her tenure at Salesforce, she sent a phishing attack to two groups of people—those who had participated in her gamified training and those who had not. Alumni of her program were 50% less likely to click on a malicious link and 82% more likely to report the link." [16]. Sedova summarizes these findings adequately: "Gamification helps with the motivation factor. It doesn't necessarily change the mindset. The thing I've realized is that people still might not care about security—that comes from a different place. It might not mean anything to me to be secure, but competition or winning or a sense of accomplishment might mean something to me" [16]. We cannot expect all users to be fully cognizant of security threats and how severe they can be to an organization, but by implementing small ways to appeal to their behaviors could give cyber security an advantage. As Winkler & Manke conclude, "fundamentally any security measure is measured not in participation or perfection, but in the amount of loss mitigated by the measure compared to the cost of implementing the program" [15].

Conclusion

In understanding the psychology of phishing, we analyzed the concept in two ways. How users get manipulated by bogus emails set up by malicious attackers to harvest credentials or execute malware and how users' psychology can be positively manipulated to help them learn and engage with their peers in mitigating the risks that phishing emails pose. We analyzed common phishing emails and the techniques that are used in the art of deception. Elaborating on this, one needs to be aware of the sending address, the context of the message and whether there are suspicious attachments involved. Understanding that technological sophistication can only barricade so much, users need to be fully equipped with the tools and education needed to increase security. We understood what psychological flaws humans have when it comes to decision making and how it is used against us. We see that the common ground for mitigation of this risk is user education but also, with the aim of this paper, to prove that engaged learning through gamification can pave the way forward in a more universal acceptance of training by users in organizations.

References

1. NIST. Computer Security Resource Center (CSRC), csrc.nist.gov.

2. Vishwanath, Arun. “Habitual Facebook Use and Its Impact on Getting Deceived on Social Media.” Journal of Computer-Mediated Communication, vol. 20, no. 1, 2014, pp. 83–98., doi:10.1111/jcc4.12100.

3. Proofpoint Inc., *2020 State of the Phish*. Sunnyvale, CA: Proofpoint, Inc., 2020. *Proofpoint, Inc.* Web. 02 March 2020.

4. Schenkman, Lauren. “Why We Fall for Phishing Emails - and How We Can Protect Ourselves.” Ideas.ted.com, Ideas.ted.com, 30 Jan. 2020, ideas.ted.com/why-we-fall-for-phishing-emails-and-how-we-can-protect-ourselves/.

5. Boyd, Dane. “Why Some Phishing Emails Will Always Get Through Your Spam Filter.” Why Some Phishing Emails Will Always Get Through Your Spam Filter, 15 Sept. 2016, info.phishlabs.com/blog/why-some-phishing-emails-will-always-get-through-your-spam-filter.

6. E-Tech. “6 Sophisticated Phishing Email Examples and Why They’ll Trick You.” E-Tech Computing, 11 Sept. 2019, www.etechcomputing.com/6-sophisticated-phishing-email-examples-and-why-theyll-trick-you/.

7. Morrison, Sara. “Coronavirus Email Scams Are Trying to Cash in on Your Fear.” Vox, Vox, 5 Mar. 2020, www.vox.com/recode/2020/3/5/21164745/coronavirus-phishing-email-scams.

8. Gudkova, Darya, and Nadezhda Demidova. “Spam and Phishing in Q2 2014.” Securelist English, 12 Aug. 2014, securelist.com/spam-and-phishing-in-q2-2014/65755/.

9. “How to Recognize and Avoid Phishing Scams.” Consumer Information, 20 Feb. 2020, www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

10. Goel, Sanjay, et al. “Got Phished? Internet Security and Human Vulnerability.” Journal of the Association for Information Systems, vol. 18, no. 1, 2017, pp. 22–44., doi:10.17705/1jais.00447.

11. Jones, Helen S., et al. “Email Fraud: The Search for Psychological Predictors of Susceptibility.” PLoS ONE, vol. 14, no. 1, Jan. 2019, pp. 1–15. EBSCOhost, doi:10.1371/journal.pone.0209684.

12. Jansson, K., and R. von Solms. “Phishing for Phishing Awareness.” Behaviour & Information Technology, vol. 32, no. 6, June 2013, pp. 584–593. EBSCOhost, doi:10.1080/0144929X.2011.632650.

13. Silic, Mario, and Paul Benjamin Lowry. “Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance.” Journal of Management Information Systems, vol. 37, no. 1, 2020, pp. 129–161., doi:10.1080/07421222.2019.1705512.

14. Tchakounté, F.; Kanmogne Wabo, L.; Atemkeng, M. “A Review of Gamification Applied to Phishing.” Preprints 2020, 2020030139 (doi: 10.20944/preprints202003.0139.v1).

15. Winkler, Ira, and Samantha Manke. “How to Create Security Awareness with Incentives.” CSO Online, CSO, 2 Dec. 2013, www.csoonline.com/article/2134189/how-to-create-security-awareness-with-incentives.html.

16. Bedell, Crystal. “Play On.” InfoSecurity Professional, 2019, pp. 16–18.