JUNE 30, 2019

SOCIAL ENGINEERING AND REAL-WORLD MEASURES EMPLOYED IN DEFENSE OF THEM

MASON CARNES, JONAH OLIVER, KELLY WOODWORTH

CIS 481-50 : INTRODUCTION TO INFORMATION SECURITY

Executive Summary

Social engineering attacks are one of the most common threats to a business, as the target of these attacks seek to exploit the number one vulnerability to companies today – their own employees. In this paper we discuss the most commonly seen forms of social engineering attacks and their effects on businesses in the past several years. We report findings from two Louisville businesses – Humana and KFC – that make clear that businesses are realizing that more must be done to educate employees about these types of attacks and stress that they are often the first line of defense between sensitive information and those that wish to gain access to it through nefarious means. Businesses that invest in their employees will do well to strengthen their defense against attacks, and the amount of effort invested in employee training is reflective in how often a breach occurs.

Regardless of how much time and money an organization spends on security systems, without proper education and training of employees on how to recognize and react to security threats, the organization remains extremely vulnerable. Because employees inherently require access to an organizations information and systems, they remain one of the greatest security threats to their own organization – one careless action from one employee could result in a major security breach. Because of this, many organizations are recognizing the importance of ensuring their employees are informed about and invested in how to keep information and systems secure in order to close the gap of this unmistakable liability. Because threats come in many forms, we will first focus the discussion of this paper on the nature and history of some of the most common social engineering threats that employees can fall prey to, and then address some of the techniques used to educate and engage employees about these threats, and how companies go about keeping the conversation about security with employees' active.

Businesses spent nearly $100 billion was spent in 2017 on cybersecurity, yet most businesses will report being the victim of some type of security attack. A 2017 survey revealed that 30% of employees surveyed did not know what phishing was, and nearly two-thirds of those surveyed did not know what ransomware was (Hernandez). This is a major problem, and one that companies need to address in a big way, or risk spending more money on security products that may not reduce risk in any significant way.

Not all security threats are directly related to technology. Organizations must prepare and educate their employees for other risks that could compromise the integrity of their systems. One of these types of threats is called social engineering. According to the Cybersecurity and Infrastructure Agency (CISA), an attacker using social engineering utilizes their social skills to obtain the information they are after from an organization or their systems. One viable option

attackers use in an attempt to get what they want is to pose as someone respectable and trustworthy, like a fellow employee or a contracted repair person for example (CISA, 2009). You don't need to be an expert in the realm of IT to pose a threat to organizations. Social engineering takes advantage of one of the weakest links of any institution, its people.

Social engineering takes many forms because there are many ways to trick and manipulate people. Some of the more common are phishing and spear phishing, baiting or quid pro quo, pretexting, and tailgating. Phishing involves the attacker using a combination of a form of trusted communication, such as email, and websites meant to look like those of a trustworthy organization but are actually malicious in nature. An attacker would send an email to a victim that looks like it was sent from a trustworthy source (CISA, 2009). The contents of the email will encourage the victim to click on a link that is provided and give up critical information, such as a username and password combination. While the website may look genuine at first glance, its purpose is to steal any information the victim is willing to give up. A more targeted approach to phishing that attackers might use is known as "spear phishing." These attacks target specific employees of an organization – often those that might have more access than others, rather than the more general approach of normal phishing. To make these attacks more believable, attackers will likely incorporate personal information from the victim or seem to be sent from an organization that the victim is personally associated with.

Phishing may well be the most common social engineering threat, basically because of how simple it is to deploy. An attacker can set up a system to mass email employees in an organization, and just getting one to fall victim to the attack could result in a huge payload for the attacker. Campaigns are not limited solely to email, attackers are also using social media and phone calls to attempt to garner information from victims. In 2018, 83% of businesses reported

being victims of phishing attacks, with over 50% of those attacks being via business emails. 95% of attacks on business networks are the result of successful phishing. And this risk is on the rise – the numbers reported on 2018 phishing attacks show a 13% increase from 2017 in businesses reporting they have fallen victim to some type of phishing attack. The most common methods used HTTPS encryption and web page redirects (Jentzen).

CISA offers up some suggestions to avoid becoming a victim of phishing and many organizations are taking the time to train their employees on these matters as well. Some of the suggestions are fairly evident, like not to give information to people unless you are absolutely sure of their identity and to be wary of any forms of unsolicited communication. Another not so obvious tip is to double check the URL of any website you find suspicious. When attackers try to make an untrustworthy site look authentic, there will be slight variations in the URL when compared to the actual websites (CISA, 2009). If you think you have fallen victim to a phishing attack, there are some important steps you may need to take.

Report the incident to the appropriate staff members of your organization if you believe you have revealed any sensitive information regarding you or your organization. This could be a manager, someone in the information security department, or other administrators. In the meantime, change any sensitive account information you believe the attacker might have gotten ahold of, such as your password. If the situation calls for it, consider reporting the attack to the law enforcement. As a final step, ensure that you stay alert for any signs of further attack or damage (CISA, 2009). Of course, it is always best to avoid giving away sensitive information to begin with. Organizations should take it upon themselves to protect their employees from phishing attempts by never letting them reach their inbox in the first place. They can do this by keeping their email filtering and anti-malware tools up to date. As stated before, the weakest link

in an organization is often its people. The best way for an organization to ensure the integrity of its information is to not give its employees the opportunity to make mistakes. Stopping phishing attempts before they reach their intended target is the best way to accomplish this. However, if you have compromised sensitive information in some way you should perform some or all of these steps to mitigate the damage as much as possible.

Another common form of social engineering is called "baiting." Baiting is often confused with other kinds of social engineering attacks. The main distinguishing characteristic of baiting is the promise of a good that attackers use to deceive their victims (Paganini, 2019). Baiting relies on the curiosity of the victim and that the victim will want whatever the attacker is offering. It is common for attackers to offer free music or movie downloads to their potential victims. Baiting can also incorporate the use of physical media. If an employee sees a lone USB drive located in or near their office, they may become curious of its contents and plug it into their computer. Unbeknownst to them, however, the drive was infected with a virus and placed there deliberately in hopes that a curious employee would snag it. After plugging it into their computer, the attacker is able to access confidential information about the organization.

A popular variation of baiting is called "quid pro quo." Instead of tempting a victim with the promise of a certain good, quid pro quo promises a service or benefit in exchange for information or the completion of a certain act. For this reason, it is also known as the "something for something" attack (Paganini, 2019). Quid pro quo attackers like to impersonate IT service people to gain the trust of their victims. They may even go so far as to actually help potential victims with their technology problems. Attackers will attempt to manipulate people into disabling their antivirus software or to install malware, claiming it will be a quick fix for their

problems. Infecting the computer with malicious software is easy if the attackers are successful in this way.

The best way to protect yourself and your organization against baiting and quid pro quo is the same as with phishing. Educating yourself is key if you want to recognize and avoid baiting and quid pro quo attacks. Organizations should take the time to educate and train their employees as well. In addition to training an education, organizations should make it a point to make their culture one of strong security and security awareness. There are still other forms of social engineering that individuals and organizations should be aware of.

Yet another scheme used in social engineering is called "pretexting." Pretexting involves the attacker devising a believable made-up scenario they can use in an attempt to steal confidential information (Bisson, 2015). The more credible the pretext of the attacker, the more likely the victim will trust them and give up their private information. Especially helpful in the creation of this pretext is for the attacker to build a new identity and to take on the role of someone else. Experienced social engineers may have many identities that they use in order to obtain the information they are after. Much like phishing and baiting, individuals should avoid giving up private information to anyone unless they are absolutely certain of their identity. Even if this is the case individuals should provide their password to no one. Individuals and organizations to be trusted should never ask for a user's password.

The last common form of social engineering to mention is tailgating. Much like the name implies, the tactic involves tailing closely behind someone. The attacker is not authorized to enter the restricted area they want access to. Without someone else to let them through, they would be stuck outside. Their plan is to follow a person who has authorized access into the facility they are trying to infiltrate. Of course, they don't want to look suspicious waiting for

someone to open the door for them. They may wait in their car until someone starts walking toward the door or even dress up in a delivery person's uniform (Bisson, 2015). If the attacker appears respectable and strikes up a friendly conversation, the authorized person may be more willing to hold open the door for them.

With all the various forms of attacks that social engineering can provide, there are plenty of opportunities for attackers to manipulate people into allowing them access to information they should not have. A few famous social engineering attacks have occurred fairly recently and it's not always information attackers are after. In 2015 Ubiquiti, a manufacturer of Wi-Fi hardware and software, had their accounting apartment attacked by hackers using social engineering techniques. The attackers used phishing, sending employees emails in which they claimed to be from the organization's Hong Kong subsidiary. Ubiquiti didn't give the exact details of the exchange, but it is believed that the attackers simply informed the employees of changing payment account details and gave them instructions for where to deposit money. The accounting department followed the instructions of the email without verifying with company administration or the credibility of the email. Ubiquiti lost nearly $47 million to the hackers from the blunder made by the accounting department (CSMD, 2017). One of the largest information breaches of all time occurred in 2013 and was the result of social engineering. An engineer employed at Yahoo received a spear phishing email and took the bait, comprising all Yahoo customer accounts. The public wasn't aware of the true extent of the attack until 2017 when word got out that roughly 3 billion accounts were compromised. The customer information went up for sale on the dark web shortly after the attack occurred (CSMD, 2017). With the frequency and severity of social engineering attacks that have occurred, it is no surprise that many organizations place a

large emphasis on educating and training employees to recognize and react appropriately to attacks.

There are some general guidelines individuals should be aware of and that organizations should be teaching their employees that work to combat many forms of social engineering. They are good rules for general computer safety as well. The first is to not open emails from any source you do not recognize. If you do recognize the source, say a friend or family member, but they are communicating in a way that seems unlike them, confirm via a different medium whether they sent the message (Bisson, 2015). Often times attackers will spoof the from field to act as though the message was sent from someone else. Another good tip is appropriate for any aspect of life. If it seems too good to be true, it probably is. A low effort attack from a social engineer is to make offers that are unrealistic. People need to recognize these cursory attempts of manipulation so that they do not fall victim. Keeping all of your devices locked down is also a good idea. Even better if you can keep them with you at all times. If your devices are in sight, you know that no one is going to use them as a tool in their next attack. Next is to make sure that your devices have antivirus software installed and to keep that software up to date. Hackers devising new methods of attack all the time. There is little use in having antivirus protection if it cannot guard against the latest forms of attack. It is important to note though that antivirus software cannot protect your devices against everything. There are still ways attackers can work around that protection so individuals should guard their systems in more than one way. Regarding organizations specifically, employees should know when it is appropriate to let a stranger into the building by understanding their company's privacy policy (Bisson, 2015). It would be unreasonable to restrict access to every stranger trying to enter the building. By

following the standard procedures of their organization, employees should repel attackers while still allowing access to those who truly need it.

Programs aimed at helping businesses develop comprehensive and effective training programs for employees have several recommendations when it comes to what companies should consider. Frontloading employees from the day they begin working generally sets a precedent and an expectation that the business requires the employee to be knowledgeable about information security threats and outlines the official company policies that the employee must follow in order to successfully protect themselves and the company's information. Because threats are constantly changing, it is recommended to have ongoing information sessions for employees, and continually update them with information that can help them recognize an attack attempt. Allowing employees to see or react to threats as they may be encountered in real life can further help employees recognize when they may be encountering a threat. Additionally, making sure employees are aware of the reasons why it is so important to be educated and vigilant when it comes to security can help them understand the emphasis on security. Lastly, fixing problems with weak or ineffective password rules should not be overlooked as a great way to bolster security on the employee level (Hernandez).

We had the opportunity to survey two of the more prominent corporations located in Louisville about their Information Security departments and programs. Both Yum and Humana were able to help us get a good idea of what a developed corporation uses to protect itself from social engineering attacks and to lay the foundation of keeping employees informed of threats and procedures to protect the company. The discussions we had with the security professionals we spoke with helped to make it clear that most companies see poorly trained employees and phishing attacks as the biggest threats that affect companies of all sizes.

Humana

Those interviewed from the Humana Information Security department all had one thing to say when asked what they believed to be the easiest, most effective, or most important way to protect secure information from social engineering attacks like phishing: Training. Humana stresses to its employees from day one that they are the first line of defense when it comes to protecting not only secure company information, but the employee's personal information as well. The belief is that if the employee is informed and aware of threats that might expose sensitive information in their personal life, that vigilance will spill over to their work life as well, and vise-versa.

"Delivering training allows us to be proactive when it comes to cybersecurity threats. Through training, we're able to give associates necessary knowledge and skills to protect Humana along with mitigating the human factors of cybersecurity." Says Alan Vo, Cyber Training and Awareness Engineer with Humana.

But how does a company with over 50,000 employees manage to reach and teach each employee about current threats? There are several programs in place that are aimed at educating employees, engaging them to actively think about information security, and rewards vigilance when reporting potential security threats. The key to getting employees to attend these events and continue engaging with information security is through incentivization – free food, rewards programs, and recognition.

One program sets up a monthly optional lunch series where employees can sign up to attend and learn about different topics that are relevant to information security in the workplace. These "Lunch and Learn" sessions are led by security experts who share their knowledge on a

topic and engage employees about how the topic impacts people in work or everyday life. Recent topics include social media, passwords, identity theft, penetration testing, cloud computing, mobile device safety and security, and social engineering. Employees who sign up to attend the sessions are treated to lunch and points in an incentive program. Employees that may not have been able to make it to the session, or those that work remotely, can view the event replay and presentation slides after the presentation if they so choose, in order to keep up-to-date on the topics that have been discussed.

There is also a week dedicated to cyber security awareness at the organization, where employees are incentivized through a points program for attending information sessions aimed at educating employees about information security topics. The week is heavily advertised to employees so they are aware of the week-long event and can make plans in their schedules to attend events throughout the week as they are able.

Outside of the dedicated awareness week, employees can elect to invest time educating themselves about security by earning badges through a program launched in partnership with IT Learning Services called the Learning and Development Driven Employee Recognition (LADDER) program.

"We created badges on different cybersecurity topics or threats such as identity theft, Internet of things, and social engineering." Says Vo, "After earning a certain of badges, associates are able to claim rewards. Though I noticed some associates just enjoy completing the badges for the sake of including the badge icons in their email signatures. Some associates even make the completion of badges part of their Workday goals."

Another program rewards employees that successfully report phishing attempts to the information security department with a pack of Swedish fish. Phishing campaigns are launched

by the information security department with the goal of determining which employees do fall prey to the attempts and which ones do successfully report the incidents to the information security department. Those who are tricked by the campaign can be reached out to separately and educated about the error, with the goal of heightening the employee's awareness of these types of attacks and reducing the chance of future errors.

"I think an effective strategy is by applying real world examples/threats to our training." Vo explains, "For the phishing campaigns my team conducts, we model our emails off real attacks reaching Humana's associates. In addition, my team strives to empower associates into remaining vigilant."

As a way to engage employees through multiple platforms, employees can also join the Information Security group on the company's internal social media app. Employees can post, share, and read about emerging threats, recently spotted vulnerabilities, or general articles on topics that might be interesting for someone looking to learn a bit more about information security. Keeping the conversation going about information security is a key tactic to keeping the subject at the forefront of an employee's mind.

Focusing on everyday actions, Humana aims to make employees aware that things that may not be apparent security risks are brought to focus. Like other companies, policies about identification, badging in and out of secure areas and buildings, secure document shredding, and navigating through the network on company devices are in place. Because the information Humana protects can be very sensitive health information, there are many safeguards in place regarding when and how employees can access the network. However, due to the company size, a large number of employees are remote workers, or are able to work from home a number of days a week, which definitely does complicate the systems in place to keep connections secure.

Because of the complicated nature of having employees so spread out, the number of technologies employed by the company, the level of security required to keep health information safe, as well as the requirements put in place by the government regarding the protection of health information, Humana has grown its information security department into one independent from the rest of information technology, allowing it to focus solely on its mission.

With all of the safeguards in place, we can ask how effective it is by looking at how often Humana finds itself in the news in regard to breaches of security and unintended exposure of member data. Just a simple search in Google shows that Humana certainly isn't immune to falling prey to breaches that expose member information. However, because only the first few results relate to recent breaches – the most recent being from earlier this year – one can conclude that Humana's efforts have been relatively successful, considering the company is nearly 60 years old. Digging into the pages of results reveals that this isn't just the result of careful search engine optimization and that large breaches aren't being hidden from the public for the sake of protecting the company's reputation.

As for the news article found regarding the reporting of a 2018 breach, it revealed that Humana notified 684 members of the breach, which was determined to have been the result of a hacker gaining access via an employee's credentials [Spitzer]. Though Humana covers tens of thousands of members, just because the number of individuals the breach may have affected feels small in comparison doesn't negate that it was an incident to be taken seriously, because next time the effect may be much more impactful.

KFC YUM

When posed with the question of what an organization can due to reduce the threat of social engineering, Director of Restaurant Technology at KFC US, Patrick Coty gave the following response:

> It starts with the weakest link. In security, the weakest link is the end users. It starts with education. How much can you prepare people for the potential attack? We have security awareness campaigns on phishing, tailgating (people following you through the door), the types of questions they [social engineers] ask. We try to educate people as much as possible. We go through an annual compliance training where people get educated on what are the dos the don'ts, what are the things we need to consider as far as leaving things lying around or what do I post on social media that may expose us…. today we have a phishing tool and it sends out periodically a phishing campaign and we won't tell anybody when its going out, if you fall for it, we let you know, 'hey you should have recognized this, this and this.' But if you correctly click on the tool bar and you click report phishing, it goes 'hey, good job on recognizing this threat!'

The importance of education and awareness regarding social engineering cannot be understated. An organization could have multiple layers of security in place, but it only takes one person within an organization to mishandle their credentials to put the business at risk. Therefore, the idea that Coty expressed in our interview regarding the end user being the weakest link is an important realization. In operations management, the idea is "a chain is only as strong as its weakest link," which also holds true in the case of information security. In short, an organization

should continuously focus on educating its employees on the threat of social engineering as it can be equally as impactful as other existing methods of attack. As well as utilizing phishing campaigns, compliance training and incentives as methods of raising awareness.

While a business is responsible for providing its employees with education on how to prevent social engineering, the question amongst security leadership, states Coty, is how do you get people to care about security? He discusses an approach slightly similar to Humana's, but with less emphasis on incentives in his following response:

> I care if it causes me to do something I don't want to have to do. It's a little bit of shaming, but it's also something that will lead to people caring more. So, what happens if you get a speeding ticket? You can pay the bill or go to traffic school. So, in our case, first times a warning, second time you go to traffic school. Not an online class, a sit-down class that last 30 minutes. And a third time, it gets escalated up the chain. Someone falling for one of these phishing attempts can be a really big deal.

Of course, Coty reminded me that they also attempt to make it fun, but they are more focused on getting people to care. This starts with getting people to invest their energy in educating themselves on the different types of attacks that exist. Whether it be through incentives or the fear of repercussions for failing to meet expectations set out by leadership.

It is no surprise that credentials are coveted by attackers, because in a sense, they are the like keys to the car (car representing an organization's proprietary data). Without password protection and data encryption, it would be hard to sustain any business model in today's world. There seems to be a split in thinking when it comes to password policies across security leadership. One advocating for scheduled password changes and the other in favor of minimizing

frequency of changes and increased password complexity. When asked his thoughts on the matter, Coty had strong feelings. According to Coty, people are more likely to forget their password and utilize tools such as password reset when they are forced to change their password on a regular basis. This is where it becomes dangerous says Coty, “If somebody can get into password reset and initiate that process, if they can clone your phone and intercept your SMS. They can clone your phone and reset your password by sending a push to that clone.” These are the type of attacks that worry Coty.

As more and more organizations are implementing 2-factor authentication, hackers are being forced to adapt. The focus shifts from stealing credentials to gaining access to the keys that allow you to reset those credentials. Coty reiterates that it is always defense in depth, but at the end of the day, an attack is going to be successful and an organization must be ready to respond. “When that attack happens and we don’t block it 100%, we have must have the ability to contain it. Identify it as quickly as possible, contain it and remediate it as quickly as we can.” This is where organizations should have incident response, disaster recovery and business continuity plans in place were an attack of varying impact to be successful.

But how does an organization determine what is worth protecting and what is not worth protecting? More precisely, how does an organization determine its risk appetite? In our interview, I asked Coty exactly this. Firstly, you have to ask, “what are you trying to protect?” states Coty. He discusses the tendency of people to want to over engineer as if “we’re [those within the organization] securing the crown jewel”. Coty reiterates that there is always risk in business and that if we wanted to be completely secure, organizations would disconnect from the internet and not accept credit cards as a form of payment. But in today’s world, that would not be a very sustainable business model. Getting to the point, Coty advised me that, “it’s not security’s

job to accept risk, it's security's job to *assess* risk. The businesses job is to *accept* risk." Those within the information security team present the risk to upper level management and they decide what they are willing to accept.

After further analyzing and comparing the responses from our interviews with both Humana's and KFC US's information security team members, we've found that there are more similarities in the way these organizations operate than we initially may have thought. Both organizations clearly emphasized that before anything else, organizational wide awareness through training and education is the most important counter measure any organization can implement to protect itself from the risk of social engineering.

How do they go about spreading awareness though? Both of these organizations have implemented phishing campaigns to simulate real world threats, that help them analyze where they need to improve and where their weakness exist. One question that we felt was important to ask the information security leadership members of each respective organization was how do you get people to care about security? While they both expressed similar answers, there was a slight difference in the emphasis on positive reinforcement versus punishment. In KFC US's case, the emphasis was on punishment. If an employee were to fall victim to one of the organization's phishing campaign, they'd initially get a warning. Now if it happened a second time, they'd be forced to take a 30-minute sit-in class on the topic. Although, there is an emphasis on making it fun, they didn't put quite as much emphasis on positive reinforcement, unlike Humana. In Humana's case, while punishment surely exists if an employee were to fall victim to a phishing campaign, they place a high value on incentivizing through positive reinforcement. They do this by offering free food, reward programs and through employee recognition. We believe that a mix of both positive reinforcement and punishment is the best way to go about getting people to care

about information security, but it also depends on what amount of risk an organization is willing to accept.

In the case of Humana, they cannot afford for a breach to occur as they are likely carrying important medical information regarding its customers. Allowing this information to fall into the wrong hands could be a violation of HIPAA (Health Insurance Portability and Accountability Act of 1996). KFC US, on the other hand, does not carry information that is equally as sensitive. As Patrick Coty stated in our interview, “people want to over engineer as if were securing the crown jewel. We’re securing data that if it went public, it’s not that big of deal.” Not to argue that it wouldn’t be a big deal, but there are different levels of risk associated with the data that these two organizations are carrying.

In regard to password policies, we recommend ditching the enforcement of password expirations in favor of an overall increase in password complexity. The idea is that the more often an end user has to change their password, the more likely they are to forget it. Not only that, but frequent changes influence end users to make slight deviations to their old passwords by adding a few characters or by reusing a password from their own personal dictionary. The less a user has to reset their password and/or update their password the better. We also recommend the implementation of single-sign on and password managers such as LastPass whenever possible. LastPass is a password manager that allows a user to store credentials for multiple accounts with the use of one master password and dual factor authentication. It allows you to create passwords for any account with scaling complexity and the best part is, the user only has to remember the single master password. We feel this is a superior alternative to having multiple passwords stored in places that are unencrypted and that do not use dual factor authentication.

Following our interviews, another realization we came to with these organizations is that it is inevitable that an attack will land in some shape or form. The important thing is how quickly you can respond, contain and remediate any impact the attack had on the organizations ability to operate. We feel that it is necessary for every organization to at the least, have an incident response plan that helps to standardize how an organization goes about responding to these attacks. Although, it is important to understand that there is a lot of variability between methods and techniques in which attackers can use to target an organization and there is not a sure-fire way to respond to every potential threat. We came away from these interviews with the knowledge that in the world of information security, there are no absolutes. Information security is a process and the field is ever changing. New techniques will take form that will cause organizations to reconsider their current policies and technologies. It is the job of information security analyst to stay up to date with current technologies and threats that arise and to present these risks to their organization for assessment of what is considered acceptable versus unacceptable. It is the job of each employee in the organization to stay educated on these threats that the organization has deemed worthy of protecting against. If both of these focuses can be consistently maintained, an organization will greatly reduce its likelihood of falling victim to attacks and more specifically, those in the realm of social engineering.

References

Bisson, D. (2015, March 23). 5 Social Engineering Attacks to Watch Out For. Retrieved June 26, 2019, from https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

CISA. (2009, October 22). Avoiding Social Engineering and Phishing Attacks | CISA. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-014

Coty, Patrick – KFC US (2019, June 26). Personal Interview.

CSMD. (2017, November 2). Top 5 Social Engineering Attacks of All Time. Retrieved from https://www.cybersecuritymastersdegree.org/2017/11/top-5-social-engineering-attacks-of-all-time/

Hernandez, Pedro. "Designing Employee Security Awareness Training that Works." *Effective IT Security Awareness Training for Employees*, 6 July 2018, www.esecurityplanet.com/threats/employee-security-awareness-training-that-works.html.

Jentzen, Aaron. "The Latest in Phishing: First of 2019." *Security Awareness Training Software,* 2019, www.wombatsecurity.com/blog/the-latest-in-phishing-first-of-2019.

Paganini, P. (2019, February 06). The Most Common Social Engineering Attacks. Retrieved June 26, 2019, from https://resources.infosecinstitute.com/common-social-engineering-attacks/

Spitzer, Julie. “Humana Notifies Members of 2018 Security Breach.” *Becker’s Hospital Review*, 7 January, 2019. www.beckershospitalreview.com/payer-issues/humana-notifies-members-of-2018-security-breach.html.

Vo, Alan - Humana (2019, June 17). Email Questionnaire/Interview.