Winter 1-15-2019

Social Engineering in Call Centers and Ways to Reduce It

Maureen York
La Salle University, yorkm1@student.lasalle.edu

Social Engineering in Call Centers and Ways to Reduce It

Maureen York

Executive Summary

Social engineering is the use of trickery, deception, persuasion, emotional manipulation, impersonation, and abuse of trust to gain information or access through the use of a human interface (Thompson, 2006). Social engineering relies on the human behavior in order to gain information or access. The technique of social engineering can be performed in numerous ways and has been proven to be an effective way for perpetrators to obtain valuable information.

This capstone project, I will focus on social engineering of call centers and the steps organizations can take to reduce it. For most organizations, the call centers or customer support are there to provide assistance to others in a friendly and polite manner. They also have access to a great deal of information available to them which makes them an easy target for social engineers. Call centers are also the weakest link within an organization as they have few defenses in place. Attackers are usually armed with information that they have obtained from other means about the person they are impersonating. With the growing number of security breaches involving personally identifiable information, attackers have more information available to use at their disposal. For these reasons, when attackers call in to these centers, they are usually able to answer the necessary authentication questions and are able to gain access to the desired information.

Social Engineering Defined

Social engineering is the use of trickery, deception, persuasion, emotional manipulation, impersonation, and abuse of trust to gain information or access through the use of a human interface (Thompson, 2006). It relies on expected human behavior in order to gain information or access. The technique of social engineering can be performed in numerous ways and has been proven to be an effective way for perpetrators to obtain valuable information. Social engineering poses information security risks as it bypasses most information security measures put into place including intrusion detection systems, firewalls, and access control systems (Bullée, Montoya, Pieters, Junger & Hartel, 2018). Social engineering relies on the weakest link in information security: humans. One of the biggest dangers of social engineering attacks is the fact that they can go unnoticed and appear to be legitimate on the surface. Social engineering can be devastating to its victims and can have long-term effects that are felt by its victims for years to come (Potter, 2018).

Social engineers can use various techniques to gain the information or access they are seeking. One technique that is used by social engineers is baiting. Baiting is a form of social engineering that relies on exploiting human curiosity. Social engineers make a promise of an item or goods to entice the victim. Baiting involves the use of physical media. For example, a social engineer will leave a USB drive with malicious software that the target will plug into their computer out of curiosity to see what is stored on it. This will then infect the user's computer with the malicious software, giving the social engineer access to the victim's computer (Whiteman, 2017). Steve Stasiukonis, Vice President and founder of Secure Network Technologies used a baiting attack to assess the security of his clients. Dozens of USB drives infected with a Trojan virus were distributed in the target organization's parking lot. The infected

USBs activated a keylogger when the drives were plugged in to a computer. This allowed Steve and his team to gain access to a number of employees' log in credentials (Bisson, 2015).

Phishing is another form of social engineering that seeks to gather sensitive information from a victim to gain access to a system or network. Phishing is the most common form of social engineering (Whiteman, 2017). It uses malicious websites or emails to pose as a legitimate person or organization in order to solicit information. An example of phishing is an email that appears to be from a person's bank telling them their account was blocked for suspicious logins. The email then directs the customer to a website to change their credentials, but first they have to enter their current credentials (Whiteman, 2017). Phishing emails often look like they are from a legitimate source, but some may be very poorly constructed making it obvious they are not legitimate. These emails make the victim feel a sense of urgency to act and victims often overlook the obvious errors that would tip them off that the email is not legitimate.

Quid pro quo is another common form of social engineering that relies on reciprocity. In a quid pro quo attack, the attacker promises something in return if the victim complies with the attacker's request. Most people are willing to give up sensitive information if they think they are getting something in return (Whiteman, 2017). An example of a common quid pro quo attack is an attacker posing as IT personnel, requesting access to their computer in order to fix an issue. Thinking that they are getting something in return, the victim allows the attacker access to their computer. In this example, the attacker then installs malicious software on the victim's device and gains the information they are looking for (Whiteman, 2017). Colin Greenless, a consultant for Siemens Enterprise Communications, tested this approach with his clients to see how vulnerable they would be to this type of attack, Greenless posed as an IT engineer, made phone calls to the organization's employees from his personal phone. Greenless advised the employees

that he noticed there was an issue with their emails and he needed their usernames and passwords to fix the issue. Greenless was able to obtain credentials from eighty-five percent of the employees he targeted (Wakefield, 2009).

Pretexting is another form of social engineering in which the attackers fabricate a story or a pretext in order to gain access to someone's personal information. Pretexting persuades the victim to give up some pieces of personal information and opens the door to allow the victim to gain trust in the attacker. Pretexting focuses on gaining both personal and nonpersonal information. This form of social engineering relies heavily on the ability of the attacker to gain the victim's trust (Whiteman, 2017). By gaining the victim's trust, the attacker is able to get the information they are after much easier. A key to gaining the victim's trust in these types of attacks is to have a solid pretext, making sure that that there are not holes in one's alias, story, or identity. In the example above, Greenless' pretext was that he was an IT engineer for the target company. By using this false identity, he was able to gain access to employees' login credentials because the employees believed the story his was telling them (Wakefield, 2009).

Another common form of social engineering is tailgating, also known as piggybacking. This is when an unauthorized person follows an authorized employee in to a restricted area in order to gain access to information, computers or networks. In order to go unnoticed by other employees the attack will have to make it appear as if they are supposed to be there. An example of this can be performed by the attacker pretending to make a delivery and asks an authorized employee to hold the door so that they could bring in the packages. The attacker is then able to bypass security measures that have been put in place (Whiteman, 2017). In Greenless' attempt to assess his client's vulnerability, he also tested his tailgating abilities and was successful in gaining access to not only the building, but sensitive information. Greenless was able to access

the building because the swipe-card operated lift was held open for him, he was not challenged by security and was able to walk right in. Greenless was able to access multiple floors in the building and actually set up in a meeting room where he worked from for three days. In his three days, Geenless was able to gain access to human resources information, information pertaining to mergers and acquisitions, and even the phone numbers of senior management. Greenless even brought in a second consultant who was able to gain access to the building as well (Wakefield, 2009).

How Social Engineers Work

Social engineers rely on the different aspects of human nature and personality traits to trick others into giving them the information that they are requesting. Social engineers often find it easier to rely on the weaknesses in people to obtain the information they desire rather than trying to hack in to a system to obtain the information. It is much easier for a social engineer to manipulate a person rather than trying to bypass firewalls and intrusion detection systems (Peltier, 2006).

Social engineers prey on human nature in order to get what they want. Social engineers rely on peoples' willingness to help. Companies train their employees that the customers' needs are the most important thing and the goal is to have a satisfied customer. This often can lead to employees giving away too much information in an attempt to please the customer (Peltier, 2006). Another aspect that the social engineer relies on is that human nature has a tendency to trust others until they have a reason not to. People are usually taken at face-value and believed to be who they say they are. Social engineers rely on this tendency to trust believing that they will seldom be asked proof of who they are. Another aspect that social engineers rely on is that

people act out of fear of getting in trouble. Employees may also take someone's word at face-value because they fear repercussions if someone complains about them. Lastly, social engineers rely on the fact that people cut corners. Employees may not follow procedures for a number of reasons which can often lead to the social engineer obtaining the information they set out to obtain (Peltier, 2006).

Another trait that social engineers rely on is the diffusion of responsibility. Social engineers will make the targets believe that they are not solely responsible for their actions by creating complex factors that will distract the target from their personal responsibility to make a decision (Peltier, 2006). Another trait that social engineers exploit is the chance for ingratiation. Targets are conned into believing that by complying with the social engineers they will be getting something in return. Social engineers also rely on guilt to get what they want. Social engineers will make the target believe that not doing what they ask will have significant consequences to the social engineer. Most people will comply with the request in order to avoid feeling guilty for not complying (Peltier, 2006). For example, a social engineer may make a request for information from an employee. The social engineer can give a reason to the employee of why they need the information immediately, maybe they made a mistake and are facing losing their job if the employee does not help them. Many employees may not want the guilty feeling that the person making the request may lost their job and often complies with the request rather than dealing with what could be an uncomfortable situation (Peltier, 2006).

Why Call Centers are Vulnerable

The employees in an organization's call center are most vulnerable to a social engineering attack because their job is to help the customer in a polite and friendly way. Call

center representatives are most focused on the satisfying the needs of the person who has called in. This, combined with the fact that call centers usually have access to the most customer information, make call centers the perfect target for social engineers looking to gain access to information (Aoki, 2018). Katherine Thompson, Founder and Chair of the Cyber Council at the Canadian Advanced Technology Alliance and Co-founder of the Security Culture Institute, stated "The fastest way to breach a company's security is through customer service. The more companies want to please customers, the more that can be exploited by con artists, hackers and other cybercriminals through social engineering. (Aoki, 2018,)" Call centers are also a viable target for social engineers due to the amount of personal and financial information that is usually shared within a short phone conversation (Chang, 2017).

Many companies have decided to outsource their call centers as they have expanded, and often rely on their call center agents to use scripts when assisting customers. While scripts can help call center agents to quickly respond to customer inquiries quickly, scripts also make it easy for a social engineer to be able to navigate their way through the answers to get to more information. Social engineers are able to call in repeatedly to learn the methods used by an organization and prepare themselves for future calls in to the call center. This also allows the social engineer to be able to gain a better understanding of a company's internal structure. Social engineers may be able to gain information related to an organization's network or key employees to target them in a future attack (Chang, 2007). A call center's main focus is to process the calls and to process them concisely; the social engineer can rely on the fact that the agent on the other end of the phone wants to process the call as quickly as possible in order to keep their metrics up (Chang, 2007). Chris Roberts, chief security strategist at Acalvio a provider of advanced threat

detection and defense solutions, stated that the "confused" caller is often handled with little security due to the call center agent working through the calls so quickly (Chang, 2007).

Another reason why call centers are a viable option for social engineers to obtain information can be attributed to the lack of vested interest in maintaining security from the employees. If the call center is not outsourced, the call center employees are often the lowest paid employees within an organization and have little interest in the company. If the call center is outsourced, the employees working there are not even employees of the company. Companies focus much of security efforts around cybersecurity, leaving the call center wide open for a social engineer to get through. Mark Lazar, CEO of call center security company Victrio, stated that "Fraudsters are shifting attacks into call centers. (McGarvey, 2013)" Shirley Inscoe, a fraud expert with Aite Group, reported that there is a rise in call center attacks by organized criminal organizations (McGarvey, 2013.) Companies also do not provide the call center employees with ongoing training to being awareness to the problem (Chang, 2007).

Call centers are also targeted due to their weak authentication processes. Call centers usually rely on a PIN to access an account. Based on a 2011 survey of United States consumers, Gartner Inc. believes that about 60 percent of consumers would use the same PIN to access an account through the phone as the one used for an ATM card. These PINs can be skimmed from an ATM attack and allow a fraud caller to gain access to an account. Another authentication method that is commonly used by a call center is caller ID. Organizations may rely on the phone number showing on the caller ID to identify a caller and authenticate the caller. Social engineers can circumvent this by manipulating the caller ID, hiding the true phone number that originated the call (Litan, 2014).

Many call centers rely on knowledge-based authentication procedures in order to allow a caller access to information. Knowledge-based authentication is the process of asking a caller questions that only the true customer should know in order to identify if the correct person is on the other end of the phone. Knowledge-based authentication can be questions that the customer set up themselves, or can be based on the customer's life history, found in public records databases (Litan, 2014). Examples of knowledge-based authentication questions can be: What is the name of the customer's high school? What is the customer's previous address? What is the make or model of the customer's current vehicle? With the rising trend of data breaches involving personally identifiable information and the use of social media, social engineers are able to obtain this information needed to be able to successfully authenticate with knowledge-based questions. According to the Identity Theft Resource Center, from January 1, 2005 to September 30, 2018 there were 9,463 breaches reported with over 1.1 Billion records exposed. These breaches are defined as incidents in which an individual's name in combination with a Social Security number, driver's license number, medical or financial records are potentially at risk of being exposed as a result of the breach (Data Breaches, n.d). The Identity Theft Resource Center also noted that in 2017, the number of incidents reported reached a record high of 1,579 incidents. This was a 44.7 percent increase over the reported incidents from 2016 (2017 Data Breaches, 2018).

Call Center Fraud Cost is on the Rise

Call center fraud is growing at alarming rates and the cost to companies is growing. Pindrop Labs analyzed over 10 million calls to a major organization's call centers between 2011 and 2016. Pindrop found that in 2013 the average call center had 1 fraud call for every 2,900 calls that it received. By 2017, the rate of fraud calls received increased 45 percent to 1 in every

2,000 calls. The rate is even higher for financial institutions, with 1 in every 1,700 calls being fraudulent and can be even higher for credit card companies (Dewey, 2017). Pindrop has attributed the growth of call center fraud to the rollout of EMV chip credit card technology in the United States, increases in data breaches worldwide, and advancements in online and mobile security. The financial costs of call center fraud also increased from $.57 per call in 2013 to $.65 per call in 2015. The increased losses are contributed to attackers being more sophisticated with even more information at their disposal then they have had in the past. It is estimated that call centers who are receiving about 40 million calls per year are losing 25 million dollars annually to call center fraud (Dewey, 2017).

In addition to the obvious costs of call center fraud, there are hidden costs to organizations that are not as obvious. Call centers will need to establish the caller's identity prior to offering assistance which can be more time consuming. This can create a negative customer experience and cause customers to become easily frustrated with the call center employees. When call center agents cannot quickly discern the legitimacy of the caller, agents typically spend much more time trying to authenticate the caller which can ultimately make a legitimate customer feel like they are being treated like a criminal (Dewey, 2017). Longer call times associated with establishing the caller's identity also contributes to higher operational costs for the call center. Attacks on call centers can also lead to data breaches and compromising customers' personal information. These types of attacks can severely damage an organization's reputation. The Aite Group surveyed twenty-five executives at eighteen of the forty largest U.S. based financial institutions from August 2015 to February 2016. The survey asked the executives to rate the social engineering fraud trend their organizations were seeing in their contact centers. Twenty-eight percent surveyed reported a minor issue, half reported it was a major issue and

twenty-two percent reported it to be a critical issue in their institution. Of the executives surveyed, only one reported that contact center fraud losses have trended downward due to process overhauls related to authentication, fraud prevention, policy changes and training. Seventeen percent of the respondents claimed that the trend was flat but admitted that they have a lack of insight to contact center fraud as they do not perform root cause analysis (Inscoe, 2016). Seventy-two percent of the executives surveyed also reported that they forecasted that the fraud trends in the contact center would increase over the next one to two years.

Tools Used in Call Center Social Engineering

Burner phones are widely used when perpetrating social engineering through phone calls. Burner phones are convenient for the social engineers to use because they are generally untraceable, purchased normally with cash or a gift card and discarded after use. There are also applications available that serve the same purpose as a burner phone as well. While the applications that provide burner phone service are used because a social engineer can quickly get access to a new number, they are not as secure as having the actual phone (The Social Engineering Framework, n.d.). Burner phones allow the social engineer to perpetrate the fraud with virtually no way of tracing the calls back to them.

Voice over Internet Protocol (VoIP) is another tool that social engineers have to use to perpetrate fraud. VoIP uses broadband internet to make voice calls rather than a traditional landline or cell phone (Voice Over Internet Protocol, 2015). VoIP calls are also widely used in call center fraud and social engineering. Pindrop Labs identified that 7.8 percent of the general public uses VoIP as there means for phone communication. Bad actors used VoIP for 53 percent of their calls (Urrico, 2015). VoIP is frequently used by social engineers because VoIP is

inexpensive and allows users from all over the world to call wherever they would like while concealing their true identity.

Social engineers have also made use of the caller ID that so many people and organizations rely on to identify who is calling. Social engineers make it appear as if they are calling from a specific phone number by using caller ID spoofing. By spoofing a caller ID display, the social engineer can make it appear as if the call is coming from within the organization, from a partner organization, or even from the customer. Spoofing the caller ID to show that the call is coming from who they are impersonating can often falsely add to the social engineer's credibility. One popular way to spoof the caller ID is with the use of Spoofcard. Spoofcard allows someone to purchase a card, call a 1-800 number and provide the PIN number associated with the purchased card. The purchaser then enters the phone number they want displayed followed by the phone number they want to call. Spoofcard does come with a cost but is easy to use and works just as described (The Social Engineering Framework, n.d.). Spoofcard also allows users to record conversations. Spoofcard also allows the caller to change their voice to sound like a woman or a male, as well as adding in background noises that the user wishes. Another spoofing tool is SpoofApp, which works relatively the same as Spoofcard. SpoofApp allows users to download an application on their cell phone to allow the same features through an application on a cell phone as the Spoofcard. Caller ID spoofing can also be done with VoIP calls using services from companies such as Asterisk. Companies like Spoofcard and Asterisk promote that their intended services are to protect the identity of legitimate users, but social engineers have found that these services offer them a great tool to be able to perpetrate fraud (The Social Engineering Framework, n.d.)

How to Prevent or Mitigate Fraud

In order to prevent or mitigate social engineering attacks on call centers, an organization needs to ensure that they have proper internal controls in place. Having strong policies and procedures in place will help a call center representative when being challenged with a social engineering call. Ensuring that there are strong authentication procedures in place to being able to identify the caller on the other end of the phone is essential in fighting social engineering through the call center. Another way to prevent or deter fraud in a call center is to provide ongoing training to call center agents (Aoki, 2018). Agents need to be aware of social engineering, have an understanding of what it is and how to identify when it is happening. Agents also need to be trained on how to escalate when they think there is an issue. Call center agents need to be empowered to safeguard customer information and know that the customer's privacy comes first (Aoki, 2018). Agents should also be trained to trust their gut, instead of just going through the motions. Proper training of call center staff will allow an organization to balance security and customer service so that important information is protected without jeopardizing customer experience (Aoki, 2018). Agents should also be trained on the red-flags to look for when it comes to social engineering. For example, were there multiple calls from the customer in a short time period? Is this typical activity for a customer? Were there a number of profile changes before the current call? By training agents on what to look for, organizations can combat fraud at the front door. Call center agents need to be made aware of the risk of social engineering, how to identify it and what to do when it is identified. If an organization fails to do this, there is little organizations can do to prevent the dangers to the may follow (Potter, 2018).

Training employees is a vital part of preventing social engineering in the call center, but it is recommended that organizations also implement strong authentication tools that will assist

agents in identifying a fraudulent caller. There are a number of authentication methods that organizations can implement from technology-based to knowledge-based methods. By implementing these authentication methods, organizations can take the decision making out of the call center agents' hands, relying on the tools to decide if the caller is legitimate. Each method has its own benefits and drawbacks. In Lexis Nexis' report *Confronting Fraud at the Call Center*, the risk solution company recommends a multi-layered authentication approach to preventing call center fraud rather than using just one method. The use of knowledge-based authentication integrated with phone or voice analytics or one-time passcodes is the best way to ensure secure authentication while not impacting customer experience (Confronting Fraud at the Call Center, 2016).

Authentication Tools Available

While knowledge-based authentication is not an ideal method to authenticate callers, it is something that is still frequently used as some still believe it to be effective. Changes to current knowledge-based authenticators could make this method more secure and more effective. Instead of relying on questions found in public records, social media, or even compromised through data breaches, companies should start to look for information that only the company and the customer should know. Avivah Litan stated "knowledge-based authenticators based on internal records that the criminals haven't stolen yet is a good option (Crosman, 2016)." Using knowledge-based authenticators based on internal records could slow the criminals down and make it harder to gain access.

The issue that still surrounds knowledge-based authentication is that a skilled social engineer may still be able to get this information from a call center representative. If a social

engineer calls in to a call center and is unable to answer the questions being asked, organizations run the risk that the caller will hang up and call back repeatedly until they are able to get someone on the phone who is willing allow them access (Crosman, 2016). Another issue with knowledge-based authentication is that it is estimated between 10 and 20 percent of callers are unable to answer authentication questions are legitimate callers. It seems as though the fraud caller can answer authentication questions quicker than some legitimate callers (Litan, 2014). Litan believes that knowledge-based authentication is practical when it is deployed in the right way, but it does not offer 100 percent prevention (Crosman, 2016).

One-time passcodes (OTP) are also used by call centers to authenticate the caller on the other end. OTP are just that, a single-use code that is sent to a customer in an attempt to authenticate a customer. OTP can be sent by SMS to a mobile phone, phone or email. Due to the fact that OTP is a single-use method, this eliminates the risk associated with shoulder-surfing or overhearing the code to gain access at the later time (Potter, 2018). The method of OTP has been used for over ten years and is convenient for users as the majority of people have access to a smartphone. According to a study conducted by Pew Research Center, only 5 percent of Americans reported that they did not have a mobile phone and 77 percent of Americans had a smart phone (Potter, 2018).

This method was once cutting-edge but has since been diminished over the years. The use of OTP requires an organization to have the correct information on file for the customer they are attempting to authenticate (Brand, 2015). Another disadvantage of OTP is that it is sent to a phone number and relies on the security of the mobile carrier. A mobile phone account takeover (ATO) will result in OTP as an authentication unreliable. In a mobile phone ATO, SIM cards can be swapped, and phone numbers can be ported. This would result in the OTP being sent to a bad

actor instead of the legitimate customer (Potter, 2018). Mobile devices are also susceptible to malware and viruses, which means that the OTP can be intercepted by someone other than the customer (Potter, 2018). Another disadvantage to OTP is that applications allow users the ability to synchronize applications across multiple platforms and devices. This means that if a one of the user's devices is compromised, the fraudster can intercept the OTP through an application on another device (Potter, 2018).

Voice biometrics, also known as a voice printing, is another way to prevent social engineers from manipulating their way through a phone call. Biometrics is derived from the Greek words bio and metric; bio meaning life and metric meaning to measure (Voice Biometrics, 2017). Voice biometrics uses physiological and behavioral features in a person's voice that can be used to identify and verify the caller. Voice biometric technology allows an organization to create a voiceprint of their customer who is calling in. When a customer calls in later, a quick search of the voiceprint database allows the caller to be identified and thus authenticated (Voice Biometrics, 2017). Voiceprinting can eliminate the need for the caller to answer security questions or provide personal information.

In addition to authenticating a legitimate caller, voiceprinting can also help to catch the fraud caller who is calling in. Voiceprints can be blacklisted when a fraud caller has been identified. It is estimated that about 70 percent of call center fraud is being done by the same bad actors, so being able to blacklist a voiceprint will help an organization to identify when a known bad actor is calling back in (Litan, 2014). This database of blacklisted voiceprints will take away the need for call center representatives to have to make a difficult decision of whether or not to proceed with assisting a suspicious caller on the end of the line (McGarvey, 2013). One challenge with blacklisting a voiceprint is that fraud callers can distort their voice and use voice

synthesizers (Litan, 2014.) The voice biometrics industry is expected to grow to $4.7 billion by 2020. In 2015, the banking industry spent over $750 on voice biometrics as many financial institutions believe that this best way to secure customer information (Voice Biometrics, 2017). Voice biometrics not only can enhance security, but also allows the call to be quicker as it eliminates the need to authenticate a caller. Voice biometrics is expected to be adopted by more industries, including mobile carriers, airlines and credit card companies. Visa is also planning to adopt the technology by requiring customer's making online purchases to speak into a microphone during the transaction to authenticate (Voice Biometrics, 2017).

Barclays implemented voiceprint in 2012 and 57,000 of their customers are enrolled in the service. On average, sixty-five percent of their calls are authenticated using voiceprint. Barclays is reporting that voiceprint has made their authentication more secure for the customers and has reduced fraud through the phone channel. One limitation in the research is the amount of savings to Barclays due to the implementation of voiceprint. Barclays is also reporting other added benefits in addition to the fraud savings. Since the implementation of voiceprint, Barclays' call center has reduced call times by fifteen percent and they have a ninety percent reduction in complaints regarding their security (Customer Service Solutions, 2014).

Banco Santander also implemented voiceprint technology in their organization and is seeing many benefits from using the service. Banco Santander chose voiceprint technology because it was reasonably priced, was also convenient for their customers and provided a high level of security. Banco Santander was the first bank in Mexico to rollout voiceprint technology. By September 2014, the bank had over 2.1 million customers enrolled in voiceprint and used the voiceprint authentication in over 4.1 million calls. While there is no information on the savings of the use of voiceprint related identifying fraud, Banco Santander has reported a savings in

operational costs. Banco Santander saw a savings of one million dollars the first year after implementing this technology and were anticipating that their investment in voiceprint technology would be paid back by the savings within three years. Banco Santander's call handling times dropped because the time spent on authenticating customer was reduced from 72 seconds to 30 seconds. Banco Santander was able to shift the focus of 53 agents to allow them to work on other tasks. Banco Santander's survey of its customers also shows that customers are more satisfied with the ease of use of voiceprint and the ability to conduct transactions quicker and more efficiently (Nuance Communications Inc., 2014).

While voice biometrics seems like a promising way to fight fraud through a call center, there are some issues with voice biometrics that could complicate a call. For instance, if a caller is sick or there is bad connection with the call voice biometrics may be unreliable. Background noise during a call may also cause voice biometrics to be unreliable. It is estimated that between the corporate and government use of voice biometrics, there are over 90 million voice prints stored in databases (Satter, 2014).

The American Civil Liberties Union believes that the use of voiceprints raises privacy issues. Jay Stanley, an analyst for the ACLU, stated that "reducing fraud is a good thing, but we can't anticipate what bright new uses this database will be put to in the future," referring to the blacklists of voice prints (Satter, 2014). Another issue arising from the use of voice biometrics is consent. Bank who are using this technology are assuming consent, at best, by playing a message that the call may be monitored or recorded. Companies could possibly run into legal issues as some states restrict collecting and sharing of biometric data (Satter, 2014). While an argument can be made that the collection of biometric data is to protect customers. Stanley argues that the original intent nobody objects to often broadens and leads to different uses of collected

information (Satter, 2014). For example, a caller may anonymously call in to a radio station to give their opinion on a topic without being identified. Someone in possession a voiceprint database may run the voice through the database and be able to find the true identity of the person on the radio (Stanley, 2015). Stanley also argued that the voiceprint technology does not report the false-positive or false-negative rates, making it possible that a legitimate caller may be treated unfairly if they falsely match to the voice of a fraud caller (Stanley, 2015). Another issue that Stanley brings up is that the danger of spoofing voiceprints is unknown. As with most technology, fraudsters find ways around it. It is still unclear if or how easily fraudsters can find a way to get around voiceprinting to gain access to the information or accounts that they are targeting (Stanley, 2015).

Another possible method to identify call center fraud is the use of phone printing. Phone printing analyzes multiple factors from the phone call to detect and identify a fraudulent call. Phone printing creates a unique telephony profile by analyzing audio features. Some of the features that are analyzed include the spectrum of the call including the quantization, and frequency filters; packet loss and noise clarity. Phone printing analyzes the caller's metadata and compares it to the caller's geo-location to determine if there is discrepancy between the two, indicating a suspicious caller (Phoneprinting Technology, n.d.). Like voice printing, fraudulent phone prints can be blacklisted so that if a bad actor uses the same phone print in the future, call center agents will be able to identify the fraud caller quickly to mitigate any fraud attempts (Litan, 2014). Phone printing can also identify anomalies in calls, track calls, and detect the origination of the call. Phone printing can tell if the call is a coming from a landline, mobile phone or voice over IP phone. Phone printing can also detect if the phone number on the caller ID is being spoofed (Litan, 2014). Phone printing has proven to be an effective method in

fighting social engineering of call centers. Payment Systems for Credit Unions, Inc. (PSCU) became the first credit union service provider to adopt phone printing technology through Pindrop Security in their call centers in the fourth quarter of 2014 (PSCU, pindrop partnership, 2018). Phone printing technology allowed PSCU to identify and confirm over 300 fraudulent calls within the first month of implementation, leading to an estimated savings of $1 million in the first month.

Conclusion

In conclusion, social engineering in call centers is a growing problem that organizations are facing and are expected to continue facing. While organizations are focusing on their fraud prevention efforts on cybersecurity, they are failing to protect their weakest leak-the call center. Social engineers are relying on manipulating people as it is easier to bypass than other security measures in place like firewalls and intrusion detection systems. Social engineers rely on expected human behavior in order to gain access to the information they seek. Social engineers rely on people's willingness to help and play on their targets' emotions in order to manipulate the person in to doing what they want.

An organization's call center usually has access to a great deal of information. This combined with their willingness to help and weak authentication methods make them popular targets for social engineers. Organizations need to put some focus back on their call center by giving their employees the training and tools they need to survive these type of attacks. By training call center employees the red flags to look for when it comes to social engineering, call center agents will be able to identify these attacks and take control of the situation. Organizations should also invest in better authentication methods in order to give their call center employees

the necessary tools to combat social engineers. Using knowledge-based authentication based on the organizations internal records allows call center agents to ask questions that only the organization and their customer should know the answer to. This method is more secure than traditional knowledge-based authentication that is traditionally based on the customer's life history and public records. With the increase of data breaches on PII and the use of social media, the questions used in traditional knowledge-based authentication can be easily found by the social engineers.

In addition to strengthening knowledge-based authentication, it is recommended that organizations invest in technology-based authentication methods. Technology-based authentication methods include OTP, phone printing, and voiceprint. OTP has been around for at least ten years and allows customers to receive a single-use code by email, phone, or SMS to verify their identity. Phone printing created a telephony profile by analyzing the voice audio. It analyzes the spectrum and frequency filters as well as the metadata to determine the true origination of the call. Voice printing analyzes physiological and behavioral features of the caller's voice to identify and authenticate the caller. Voice printing also allows for voices to be blacklisted to easily identify when a fraudulent caller is calling in. Voice printing not only adds to an organization's security but has also cut the operational costs of those who have implemented the technology. The voice biometrics industry is expected to continue to grow and be adapted by more industries over the next few years.

Organizations continue to implement the authentication methods above in an attempt to prevent fraud in their call centers. PSCU did report that within the first month of implementing phone printing they were able to identify over 300 fraudulent calls with an estimated savings of $1 million. There is not much information available about the organizations that have

implemented the recommended authentication methods and how the methods have reduced their fraud. This could be due to the fact that they do not want to tip off the fraudsters by sharing what fraud prevention methods they have in place. While most organizations are not reporting their fraud reduction, Banco Santander and Barlcays have both reported benefits not related to fraud reduction. After the implementation voice biometrics both organizations have increased their customer satisfaction and reduced their operational costs. It is clear that there are benefits to the organizations that implement these authentication methods. Organizations that are implementing these authentication methods will be in a better position to prevent social engineering in their call centers than those organizations who are not focusing on their call centers.

Bibliography

2017 Data Breaches. (2018). Retrieved from https://www.idtheftcenter.org/2017-data-breaches/

Aoki, M. (2018, May 19). Are You Protected? Why Every Contact Center Needs Social Engineering Training. Retrieved from https://blog.contactcenterpipeline.com/2018/03/are-you-protected-why-every-contact-center-needs-social-engineering-training/

ATMmarketplace.com: PSCU, pindrop partnership thwarts $1M in fraud in 1st month (2018). Chatham: Newstex. Retrieved from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/1999783568?accountid=11999

Bisson, David. "5 Social Engineering Attacks to Watch Out For." The State of Security, 23 Mar. 2015, www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/.

Brand, C. (2015, October 21). So long to one time passwords. Retrieved from https://www.bai.org/banking-strategies/article-detail/so-long-to-one-time-passwords

Chang, E. (2017, January 28). Clever hackers love call centers to tap into sensitive information. Retrieved from https://www.thestreet.com/story/13964029/1/clever-hackers-love-call-centers-to-tap-into-sensitive-information.html

Confronting Fraud at the Call Center: New Tactics and the Tools to Defend Your Business. [White Paper] (August, 2016). Retrieved from https://risk.lexisnexis.com/-/media/files/financial-services/white-paper/ln-call-center-fraud-wp-pdf.pdf

Crosman, P. (2013, Nov 22). Phone fraud is a growing risk for bank call centers: Pindrop security. American Banker Retrieved from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/1460532166?accountid=11999

Crosman, P. (2016). The case for knowledge-based authentication. *American Banker, 1*(58)

Customer Service. (n.d.). Retrieved from https://www.social-engineer.org/framework/general-discussion/common-attacks/customer-service/

Data Breaches. (n.d.). Retrieved from https://www.idtheftcenter.org/data-breaches/

Dewey, D. (2017, April 26). When Fraudsters Attack the Call Center… What Are the Costs? Retrieved from http://www.callcentertimes.com/Articles/tabid/59/ctl/NewsArticle/mid/407/CategoryID/1/NewsID/1227/Default.aspx

Inscoe, S. (2016). *Contact Centers: The Fraud Enablement Channel* [White Paper] Retrieved from https://www.pindropsecurity.com/wp-content/uploads/2016/08/Contact-Centers_The-Fraud-Enablement-Channel_Report-2-2.pdf?mkt_tok=eyJpIjoiWkdSa09ETTFOV1ZtWkRreiIsInQiOiJ2VTBSSTFia0pwT0o5OTE4SDRZTFllVVwvamlRNjlrdHFwYWFNaHI5K3FpaEVmT1VjenZrNjRpSXdOWmdXYXdhdXVcL1NIQlZ1NUpaUVhyaUdjT05GZUgxMFlNZVQzRmJ5UExlYWd3aFhKS0p3aEFIRE5MVThDcHZibDlzaEVuTFg5In0%3D

Litan, A. (2014, July 03). Preventing Fraud in the Call Center with Phone Printing and Voice Biometrics. Retrieved from https://www.forbes.com/sites/gartnergroup/2014/06/18/preventing-fraud-in-the-call-center-with-phone-printing-and-voice-biometrics/#c99f4df7b388

McGarvey, R. (2013). Threat of the week: Call centers under attack. Credit Union Times.Breaking News, Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1448400722?accountid=11999

Nuance Communications, Inc. Adiós to PINs, Passwords, and Security Questions. Adiós to PINs, Passwords, and Security Questions., 2014, images.marketing.nuance.com/Web/Nuance/{b8cd0636-deb5-40f7-85ea-e024b821f401}_Nuance_Banco_Santander_CS_10-14.pdf?elqTrackId=96db776e09eb4fd584fc3fd84ea40c12&elqaid=3774&elqat=2.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. Information Systems Security, 15(5), 13-21. Retrieved from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/229581839?accountid=11999

Phoneprinting™ Technology | Voice Recognition Biometrics. (n.d.). Retrieved from https://www.pindrop.com/technologies/phoneprinting/

Potter, K. (2018). Increased use of two-factor authentication force new social engineering tactics (Order No. 10789454). Available from ProQuest Dissertations & Theses Global. (2037183631). Retrieved from

https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/2037183631?accountid=11999

Satter, R. (2014, October 13). Banks harvest callers' voiceprints to fight fraud. Retrieved from http://www.sandiegouniontribune.com/sdut-banks-harvest-callers-voiceprints-to-fight-fraud-2014oct13-story.html

Stanley, Jay. “On the Creation of Giant Voiceprint Databases.” American Civil Liberties Union, Aclu, 26 Apr. 2015, www.aclu.org/blog/privacy-technology/medical-and-genetic-privacy/creation-giant-voiceprint-databases.

The Social Engineering Framework. (n.d.). Retrieved from https://www.social-engineer.org/framework/se-tools/phone/burner-phones/

Urrico, R. (2015). Call center fraud rises: Pindrop security. Credit Union Times.Breaking News, Retrieved from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/1689986020?accountid=11999

Voice Biometrics. (2017). In Encyclopedia of Emerging Industries (7th ed., pp. 651-654). Farmington Hills, MI: Gale. Retrieved from http://dbproxy.lasalle.edu:5066/apps/doc/CX3664200140/GVRL?u=phil31439&sid=GVRL&xid=ca6f0927

Voice Over Internet Protocol (VoIP). (2015, November 01). Retrieved from https://www.fcc.gov/general/voice-over-internet-protocol-voip

Wakefield, Jane. “Office Intruder 'Steals' Data.” BBC News, BBC, 6 May 2009, news.bbc.co.uk/2/hi/technology/7843206.stm.

Whiteman,Jack R., I.,II. (2017). Social engineering: Humans are the prominent reason for the continuance of these types of attacks (Order No. 10684196). Available from ProQuest Dissertations & Theses Global. (2007620740). Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/2007620740?accountid=11999