MindPoint GROUP℠

We Specialize in One Thing:
Cybersecurity. Period.

Social Engineering

A Proactive Security

PRESENTED BY:
Stephanie Carruthers
Team Lead

MindPoint Group, LLC
1330 Braddock Place, Suite 600, Alexandria VA 22314
(o) 703.636.2033 | **(f)** 866.761.7457 | **www.mindpointgroup.com**

Part One – A Dirty Old Trick

TABLE OF CONTENTS

WHAT IS SOCIAL ENGINEERING?

Social engineering has become a household name in the cybersecurity industry, but what exactly does it mean? Social engineering is the use of techniques to influence a target to perform an action or to divulge information which may not be in their best interest. In other words, what the average person might call a 'con' is known in the security world as social engineering.

"43% of company data breaches occur using Social Engineering"

Social engineering is not a new concept. Stories of these exploits are littered throughout history. Yet while zero-day exploits, machine learning cyber solutions, and nation-state actors dominate the news, social engineering still remains a core weapon in the attacker's arsenal in successful breaches. After all, technology is constantly changing, getting more sophisticated and complex, but people are still susceptible to the same tricks that have been used by con men for decades. This is why the human element of an organization is such a common attack vector as cybercriminals target the easiest point of entry. According to the 2017 Verizon Data Breach Investigations Report, *43% of company data breaches occur using social engineering*. (Verizon Enterprise, 2017)

This paper will explore the concept of social engineering by dissecting select examples of use cases throughout history and today. This exploration aims to demonstrate the effectiveness of various social engineering manipulation techniques used to motivate victims into divulging information that attackers can exploit for various forms of gain.

SOCIAL ENGINEERING – A DIRTY OLD TRICK

It's a different day, but it's still the same old trick. Elements of many of the popular and successful "cons" throughout history have been adapted for use today. While the cybersecurity world may refer to these "cons" as social engineering, examples of the same techniques used by modern day cybercriminals go back decades, if not centuries. This longevity of success is based on the fact that they rely on the consistency of human psychology. In this section, we will explore three examples of social engineering throughout history and why each was effective.

THE DOUBLE SWITCH – "ALL SALES ARE FINAL"

Sometime in the late Middle Ages, the sale of pigs in pokes was quite common. For those not familiar with the vernacular of the middle ages, a bag or sack was referred to as a poke back then. Suckling pig was a popular, though expensive meat and was commonly sold in a poke. Hence the name "pig in a poke." When the pig in a poke was sold, the poke was always closed shut to keep the pig from escaping. Most people never checked the poke to confirm there was indeed a pig inside because there was an understanding or belief that the pig was actually in the poke, that is until the con men arrived.

Image 1 – Pig in a Poke (Ereads, 2011)

Meat from pigs was hard to come by during the late Middle Ages. However, there was no shortage of dogs and cats, which made them the perfect substitutes for a small pig. An unsuspecting buyer would purchase the pig in a poke, not verifying that there was a pig inside, and upon returning home they would realize the bag contained another animal, typically a cat. Some also believe this is the origin of the phrase "the cat's out of the bag."

Also referred to as the "Double Switch", this con has been modernized and is used today with the selling of electronics (laptops, iPads, cell phones, gaming consoles, etc.). The attacker has two items which appear to be identical that they intend on selling to the target. These two items are typically in their boxes and packaged, appearing to be brand new. The attacker will open one box (the real item) to show the target and let the unsuspecting victim review and inspect it. Once the target likes what they see and wishes to buy the item, the attacker hands over the other box that appears to be unopened, making it seem as if they were getting a perfectly packaged item. Most of the time the box the target has purchased is something of equal weight to the real item but is commonly filled with tiles, bricks, etc.

WHY WAS IT EFFECTIVE?

People are creatures of habit. This con was successful because it relied on the consistency of the targets' actions. The social engineers understood that their targets had consistent patterns of behavior (not verifying the pig was actually in the poke) and used that behavior to exploit them. This consistent behavior pattern can be attributed to two of Dr. Robert Cialdini's six (6) Principles of Influence, Commitment and Consistency as well as another called Social Proof where he posits that people will do things that they see other people are doing. (Wikipedia, 2017)

Dr. Robert Cialdini's six (6) Principles of Influence: Social Proof, Authority, Scarcity, Reciprocity, Liking, Commitment & Consistency.

P.T. BARNUM - "THERE'S A SUCKER BORN EVERY MINUTE"

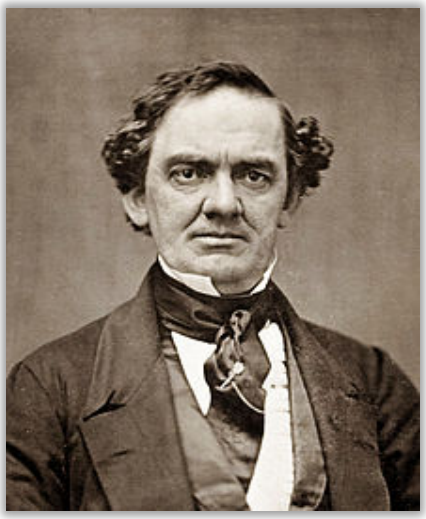

Image 2 - P.T. Barnum (Wikipedia, n.d.)

Born in 1810, P.T. Barnum was a man of many talents and interests. While he's mainly known for his role as one of the founders in the Barnum & Bailey Circus, Barnum was also the self-proclaimed "Prince of Humbugs." A humbug is something designed to deceive and mislead. While in the entertainment business, Barnum used a wide array of humbugs to captivate visitors to his freakish attractions. In addition to false advertisement, most of his attractions were some type of hoax, which is in part why he is widely credited with stating "there's a sucker born every minute."

Below is an example of one of Barnum's many humbugs.

"The Cardiff Giant"

A gentleman by the name of George Hall commissioned a statue of a gigantic, 10-foot tall, petrified man. He then had the statue transported to his cousin William Newell's farm in Cardiff, New York. Around a year later, in 1869, Newell hired some workers to dig a well on the spot where he had previously buried the statue. After a bit of digging, the workers reported that they discovered an ancient petrified giant, which would be dubbed "the Cardiff Giant". When the reports of the discovery garnered interest in seeing this rarity, Newell set up a tent over the giant and charged people an entrance fee to see his discovery. The admission price started at 25 cents, but was quickly raised to 50 cents due to demand.

Over time, rumors spread that the giant was not real while others claimed they had discovered giants of their own. This led Hall to sell the statue to a few men who then put the giant on display in New York. Barnum viewed the statue in Syracuse and attempted to buy it. Despite offering the men a considerable sum, they refused Barnum's offer. Not willing to pass up an opportunity to make a buck, Barnum commissioned a replica of the Cardiff Giant.

Barnum had several newspaper editors on his payroll, enabling him to influence many of their stories and decide what ultimately went to print. Once stories were released claiming Barnum's giant was the "only real one," it eventually made Barnum's giant more popular where it outsold the original "Cardiff Giant."

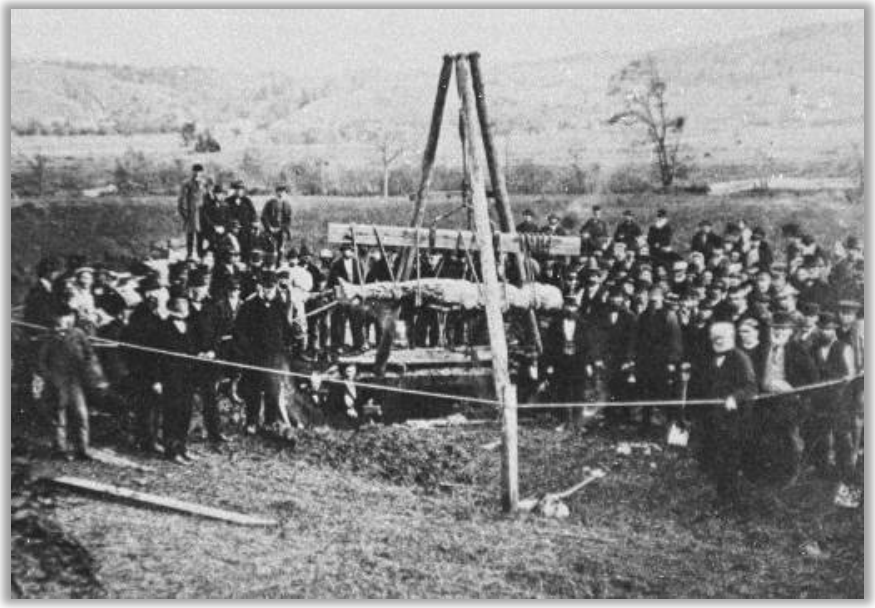

Image 3 – Cardiff Giant (Wikipedia, n.d.)

WHY WAS IT EFFECTIVE?

In both above examples, the scams used a variety of influence factors to persuade potential victims into believing the authenticity of the giants. This in turn created demand to view said giants which led to financial benefit for the scam artists. During the 1800s, modes of communication were limited. This limitation allowed "eye witnesses" and newspapers to exude a higher degree of influence as the distributors and authority (Wikipedia, 2017) of information. In the Cardiff Giant case, Newell used his hired diggers as "eye witnesses" to help spread the word about the discovery of his giant. By using several different newspapers to state the authenticity of his giant, Barnum was able to do the same. In both cases, the scam artists successfully invoked the Multiple Source Effect (Wikipedia, 2017) where people give more credence to ideas that are stated by multiple sources. The successful application of the authority effect and multiple source effect (a subset of the Social Proof effect) created the Scarcity Effect (Wikipedia, 2017), as people wanted to see the '*one true' giant* over other phonies. In other words, it created a perception that the object was rare and viewing time was possibly limited, therefore, people saw it as more valuable, leading to increasing interest and demand for the giants. While both scams used the same principles, Barnum's was more effective because he cast a wider net to a larger audience and used a medium with higher authority (newspapers).

GEORGE C. PARKER - "AND IF YOU BELIEVE THAT, I HAVE A BRIDGE TO SELL YOU"

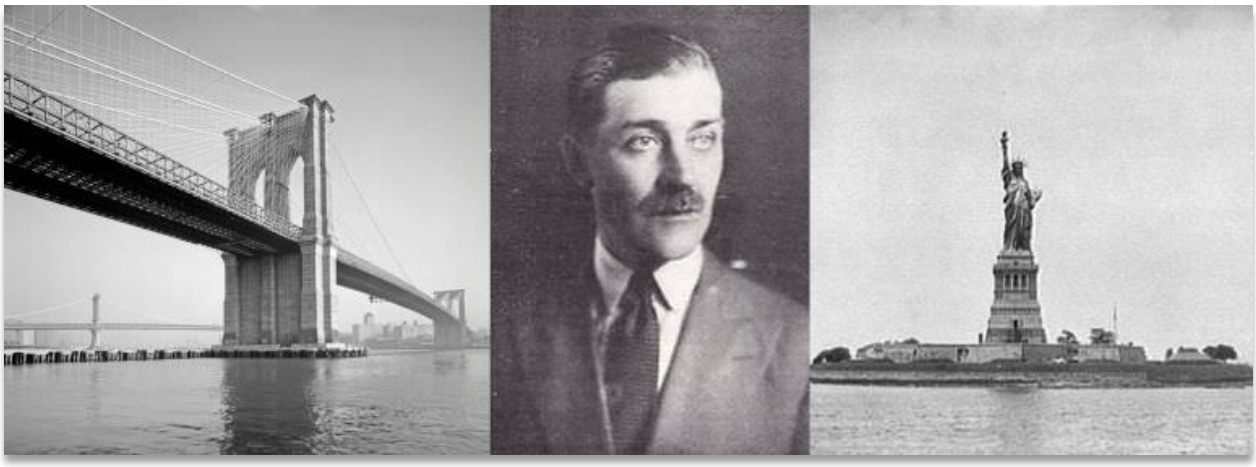

Image 4 – George C. Parker and Landmarks Targeted By His Scam (Lost At E Minor, 2014)

One of the most well-known confidence men (con men) in US history was George C. Parker. He was known for scamming people into buying famous New York landmarks. The landmarks include Madison Square Garden, the Statue of Liberty, and The Metropolitan Museum of Art. Parker targeted visitors and immigrants who did not know New York well. He was also known to do a lot of intelligence gathering before conducting his cons, making himself look more legitimate. Parker knew the more credible he appeared (even with forged documents), the more trust he would build with his targets.

Parker was most known for selling the Brooklyn Bridge not just once, but on average twice a week for decades. The price sold ranged anywhere from $50 to as high as $50,000. Parker ran these scams from 1883 to 1928, when his third arrest put him away for life in prison.

WHY IT'S EFFECTIVE?

Parker's main tactic was applying the Scarcity Effect (Wikipedia, 2017). The landmarks that he was selling were "one of a kind" high value items with large potential for generating income via tolls etc. Since there was a limited quantity of such landmarks that Parker was selling, he was able to successfully utilize the Scarcity Effect to persuade his victims to fall for his con.

To ensure his scarcity tactic was successful, Parker conducted a great deal of Open-Source Intelligence (Wikipedia, 2017) gathering to prepare for his con. Once he had the information he needed, he used an Authority approach (Wikipedia, 2017) with his targets, wherein he would claim legitimacy in order to provide the justification and right to exercise the sale of the landmarks. For example, Parker would "have a fake office set up, with plenty of official documents and impressively forged ownership deeds lining his desk, which he would sign over to the Mark after the money had exchanged hands." (RUA, 2014)

SOCIAL ENGINEERING – THE CON OF TODAY

So how is Social Engineering used today? While the basic tactic (manipulation) is the same, the environment in which social engineering is utilized has moved from the tangible world to the cyber world. In the cybersecurity world, there are three methods of delivery email (phishing); phone calls (vishing or voice-phishing); and in-person. The following are examples of each.

NIGERIAN 419 SCAMS (PHISHING)

The Nigerian 419 Scams are believed to be based off the Spanish Prisoner scam which was "a confidence trick originating in the late 18th century. In its original form, the confidence trickster tells his victim (the mark) that he is (or is in correspondence with) a wealthy person of high estate who has been imprisoned in Spain under a false identity." (Wikipedia, 2017)

Many of the 419 scams are written with poor grammar and bad English because they are targeting a specific demographic.

The 419 scam gets its name from the actual section of Nigeria's Criminal Code Act, Part 6, Division 1, Chapter 38, Section 419, which states "Any person who by any false pretense, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years." (International Center for Nigerian Law, n.d.)

While there are many variations of this email scam, one of the most popular is where a "member of the Nigerian royal family" sends an email asking the target to send a small amount of money to release another royal family member from prison with a promise of paying back a very large amount for their help. This does two things, it makes the target feel as if they are being helpful and gives them the impression they will be rewarded with a greater sum of money.

An alternative version of this scam targets older people. This is called the Grandparent Scam (Fraud.org, n.d.). This happens when the attacker impersonates the target's grandchild asking the grandparent to wire money, typically with a sense of urgency by using scarcity tactics.

WHY IT'S EFFECTIVE?

Nigerian 419 scams typically work due to two reasons. The first reason is by applying Reciprocity (Wikipedia, 2017). Since the victim is going to send over an amount of money, they are being promised by the attacker that they will reciprocate (with a larger sum). The second reason utilizes the Scarcity Effect (Wikipedia, 2017). The email is written to invoke a sense of urgency to perform an action – "because time is running out." When people are put under pressure to perform an action with urgency, there is a higher probability to act on emotion rather than logic.

MICROSOFT SUPPORT PHONE SCAM (VISHING)

There are many vishing scams, however some of the most popular ones currently trending are the technical support scams which exploit via the impersonation of Microsoft employees. The scam is performed via phone calls. Most of the attackers originate from organized call centers in India and focus on people who live in America, Australia, and the United Kingdom.

The attacker calls their target (mainly through cold calling) and explains that the target's computer has a virus and they need access to help resolve it. The attacker then walks the target through giving them remote access to their computer. Once the attacker gains access, they run a fake detection tool and try to show that the computer is infected. The attacker explains that they can fix the target's infected computer for a fee. Usually, the attacker collects the fee and often uses the credit card information for later fraud use.

WHY IT'S EFFECTIVE?

The attacker uses many tactics when performing this scam. First, to establish legitimacy, the attacker takes advantage of the Authority Effect (Wikipedia, 2017), by impersonating a Microsoft employee. To persuade the victim to agree to the request, the attacker also uses urgency to distract the target and not give the victim any time to think. Oftentimes when people are worried and need to act urgently, they do not think rationally or logically. The other tactic used here is Reciprocity (Wikipedia, 2017). Since the attacker called, located a bad virus, and "helped" to fix the issue by pretending to run a detection tool, the target feels obligated to pay them back.

SHORT CHANGE (IN-PERSON)

Short change or short count scams happen many times a day, typically at retail locations, depending on how experienced the attacker is and how susceptible the target.

While there are many variations, typically the scam works like this:

1. The attacker buys a low value item with a large bill, in this case a $20. This action is done to get the cashier to open the register, start the transition of money, and have the cashier count large values.
2. At this point, it is important to note that the attacker is completely done with this transaction. As such, they pocket the change and pull out a preset wad of nine single dollar bills. Once change from the purchase is received, the attacker then asks the cashier if they can get a $10 bill in exchange for pre-staged nine singles.
3. The attacker hands off nine singles, and while the cashier counts the money, the attacker takes the $10.
4. At this point the cashier notices it is only $9 and points it out to the attacker.
5. The attacker reaches into their pocket and pulls out another single AND the $10 bill that the cashier had just handed over and then just asks for a $20 bill to make things easy.

If you are confused, you should be because that's the point. However, consider that in the steps described above, the attacker has only given the target nine $1 bills, then another $1 bill, and the $10 bill that the target gave them in the first place. The attacker gives $10, and gets $20.

WHY IT'S EFFECTIVE?

Short change scams are effective with employees who do not know how to identify it (due to lack of training and exposure). Some retailers have policies requiring employees to complete one transaction at a time. These types of policy are an effective preventative measure so long as the employee follows the policy.

While it was not outlined in the above scenario, the technique often used to facilitate this scam is the Liking Effect (Wikipedia, 2017) which is essentially the concept that "People are easily persuaded by other people that they like." The more the attacker uses tricks to build rapport with the target, the higher their likelihood of not getting caught, as their target is distracted and more willing to comply. In other words, if the attacker is likeable, the victim is less inclined to believe ulterior motives are at hand. If you have ever seen the 1973 movie Paper Moon, there is a scene which portrays the short change con in real time. The attacker, in this scenario, built significant rapport with his victim. In short, he suspended his ego by asking his target personal questions and bestowing flattery, all in an effort to distract her from the con. These rapport tricks are well documented in Robin Dreeke's 2011 book "It's Not All About 'Me': The Top Ten Techniques for Building Quick Rapport with Anyone." (Dreeke, 2011)

NOW WHAT?

Now that we have established a basic understanding of social engineering attacks, future whitepapers in this series will provide a deep dive understanding of the various types of social engineering attacks as well as tips on how you can lower your organizational risks to these types of attacks. The full series will include:

- Part Two: Open-Source Intelligence
- Part Three: Phishing
- Part Four: Vishing
- Part Five: Physical Security
- Part Six: How to Lower Your Risks to Social Engineering Attacks

ABOUT MINDPOINT GROUP

MindPoint Group is a cybersecurity firm focused on providing innovative cybersecurity solutions that include:

- *Cloud Security*
- *Security Operations*
- *FedRAMP 3PAO Services*
- *Governance, Risk & Compliance*
- *Proactive Security*
- *Managed Security Services*
- *Security Architecture & Engineering*

MindPoint Group's Proactive Security Services offer Social Engineering solutions lead by Subject Matter Experts. Our methodology is focused on providing customizable White Box (Insider Threat Simulation) and Black Box (Adversarial Simulation) assessments to meet the unique requirements of our clients. Our Social Engineering assessment and audit services range from Open Source Intelligence, Phishing, Vishing, Physical Security Assessment, and Physical Security Audit.

ABOUT THE AUTHOR

After winning a black badge at DEF CON 22 for the Social Engineering Capture The Flag (SECTF), Stephanie Carruthers pursued her career as a full time Social Engineer. Stephanie focuses on services such as Open-Source Intelligence (OSINT) gathering, Phishing, Vishing, and Physical security assessments. Stephanie has taught courses and presented at numerous security conferences including BSidesSLC, CircleCityCon, SAINTCON, ISACA (Salt Lake City), Hackfest Canada, and NolaCon - as well as guest webcasts for SANS. In her free time, she enjoys going to theme parks and playing table top games. Stephanie currently resides in Salt Lake City, Utah with her family.

LEARN MORE

For additional information about our cybersecurity services, please visit our website and social media:

- mindpointgroup.com
- GitHib
- LinkedIn
- Glassdoor
- Twitter
- Facebook

To learn more about MindPoint Group's Social Engineering services, please email Stephanie and the Proactive Security team at: pss@mindpointgroup.com

REFERENCES

Dreeke, R. (2011). It's Not All About "Me": the Top Tem Techniques for Building Quick Rapport with Anyone. In R. Dreeke, *It's Not All About "Me": the Top Tem Techniques for Building Quick Rapport with Anyone* (p. 98).

Ereads. (2011, July). *Poke*. Retrieved from ereads.com: http://ereads.com/wp-content/uploads/2011/07/Poke.jpg

Fraud.org. (n.d.). *Parent Scam*. Retrieved from fraud.org: http://www.fraud.org/grandparent_scams

International Center for Nigerian Law. (n.d.). *Criminal Code*. Retrieved from nigeria-law.org: http://www.nigeria-law.org/Criminal%20Code%20Act-Part%20VI%20%20to%20the%20end.htm

Lost At E Minor. (2014, May). Retrieved from lostateminor.com: http://cdn0.lostateminor.com/wp-content/uploads/2014/05/clipboard_01_.jpg

RUA. (2014, February 14). *Ive-got-a-bridge-to-sell-you*. Retrieved from iamrua.com: http://iamrua.com/index.php/ruas-blog/ive-got-a-bridge-to-sell-you/

Verizon Enterprise. (2017). *Verizon Insights Lab.* Retrieved from Verizon Enterprise: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Wikipedia. (2017, June 13). *Open Source Intelligence*. Retrieved from Wikipedia.com: https://en.wikipedia.org/wiki/Open-source_intelligence

Wikipedia. (2017, June 1). *Robert Cialdini.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Robert_Cialdini

Wikipedia. (2017, August 8). *Social Proof*. Retrieved from wikipedia.com: https://en.wikipedia.org/wiki/Social_proof

Wikipedia. (2017, May 25). *Spanish Prisoner*. Retrieved from Wikipedia.com: https://en.wikipedia.org/wiki/Spanish_Prisoner

Wikipedia. (n.d.). *Cardiff Giant*. Retrieved from Wikipedia: https://upload.wikimedia.org/wikipedia/commons/f/fd/Cardiff_giant_exhumed_1869.jpg

Wikipedia. (n.d.). *PT Barnum*. Retrieved from Wikipedia: https://upload.wikimedia.org/wikipedia/commons/thumb/8/8b/PT_Barnum_1851-crop.jpg/220px-PT_Barnum_1851-crop.jpg