Simon Says: "Send Money"

Patrick N. Conrad
Independent Researcher
Fort Smith, Arkansas 72903, USA

Luay A. Wahsheh
Department of Computer and Information Science
Arkansas Tech University
Russellville, Arkansas 72801, USA

ABSTRACT

Social engineering attacks have increased dramatically in the past few years. The case study that is described in this work involves the deception of a subordinate by someone posing as his or her superior. The attacker assumes the identity of a high-level person in the company, usually a Chief Executive Officer (CEO) whose actions are rarely questioned. The attacker poses as the CEO through a spoofed email address or even one that looks similar to the correct one, and then sends a message to his or her assistant or another person in the company that fields the CEO's requests. The message requests funds to be transferred through various methods ranging from wire transfers, credit card payments, and even the purchase of store gift cards. We believe that social engineering attacks that threaten personal and organizational information can be prevented by creating a cyber security awareness culture. Increasing awareness by drawing attention to the social engineering case that is discussed in this work is a step towards achieving this goal.

Keywords: Fraud, Phishing, Scam.

1. INTRODUCTION

This case study involves a phishing attack that convinced an employee to purchase gift cards, and then send the access codes and authorizations to the instigator via email.

2. INTERNET CRIME

A recent twist to phishing attacks is where the attacker spoofs a CEO's email address and convinces an employee to quickly purchase a set number of gift cards and send the information to him or her so he or she can distribute the information to any number of members of any group. The emails are convincing, and the employee is used to performing whatever the CEO wants. Without question, the employee makes the purchase and sends the information. By the time he or she figure out what happened, it is too late. The numbers have already been transferred to the culprit's account, and the company is out several hundred if not thousands of dollars.

Adamek [1] describes this new trend of attacks as "These scams have one thing in common: the use of fear, confusion, and desperation to separate vulnerable people from their money. A new class of international cybercriminal, adept at exploiting security flaws and legal loopholes, is finding creative ways to pilfer and launder money".

3. FBI TAKES NOTICE

This activity has caught the eye of the FBI's Internet Crime Center and became one of the hot topics of their 2017 Internet Crime Report [2]. The crime report lumps the gift card scams in with the larger wire transfers into a group categorized as Business Email Compromise / Email Account Compromise. Even though the number of complaints was only 1% of all complaints received, the losses were reported as 12% of the overall Internet crime statistics.

Foreman [3] states that this type of crime has cost companies over two billion dollars from October 2013 to February 2016. The FBI calls these scams Business Email Compromise Scams (BEC). Figure 1 shows Internet crime complaints and losses from 2013 to 2017 as reported to the FBI's Internet Crime Complaint Center [2]. Foreman believes that open platforms such as WhatsApp open doorways for the attackers as they do not follow normal corporate security protocols and there is no way to police them. Users love them for their flexibility, but IT professionals despise them in a corporate setting because of their security inadequacies.

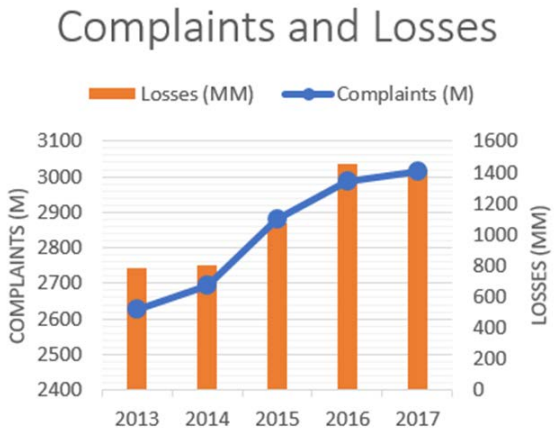

Figure 1. Internet crime complaints and losses from 2013 to 2017 as reported to the FBI's Internet Crime Complaint Center [2]. Gift card scams are virtually non-existent prior to 2018.

4. MORE EXAMPLES

The problem is becoming rampant as is evidenced by the following statement: "Email provides a particularly lucrative opportunity for social engineers – according to a 2014 study by McAfee, 97 percent of people globally were unable to correctly

identify phishing emails. And the FBI reports that in the U.S. alone, there have been more than 7,000 victims and $747 million in losses as a result of business email compromise – a specific type of social engineering fraud – since 2013." [4]. Meinert [4] defines the problem and provides specifics of the CEO impersonating attack. "In other cases, crooks will impersonate corporate CEOs, creating fake email addresses or hacking existing email accounts. From there, Syrop, Director of Fraud and Loss, says, they typically reach out to a lower-level employee with wire origination authority and request a transfer of funds, often stressing confidentially. The employee naturally wants to comply with their boss' wishes as quickly and efficiently as possible – which is exactly what fraudsters are counting on." [4].

This example of another case study identifies repeat attacks on the same victims. "Two months later, yet another fake email went from me to the CFO. The reply-to address was a Gmail account and again it asked if Tim could confirm that he would be able to handle the transfer prior to sending along the details of the recipient, a supposed client." [5]. Luckily though, this attack was identified and stopped before any damage could be done.

5. THE SCAM IN ACTION

Here is a typical scenario for this type of scam:

- The scammer starts by sending an email to a subordinate employee. These messages are targeted because they usually are sent to those who have common interaction with the CEO.
- The messages have an artificial time limit. This triggers a sense of urgency that the recipient should act quickly.
- The recipient recognizes the name of the sender and begins to process the request.
- If the recipient stops long enough to decipher the message, he or she should be able to determine if it is a valid request.
- If the recipient acts without question, he or she provides what was requested which results in losses to the company.

6. MITIGATION

One way to identify if it is a real or fake request is to look at the sender's email address. This is usually an address that has some similarities to the CEO, but it is from a different domain. All users in the company should be familiar with their corporate email structure to identify outside addresses.

The user should also verify the request by contacting the CEO over other channels, preferably a phone call. The CEO might feel bothered by a call from a subordinate, but will appreciate the call to verify the transaction if it is actually a fake request.
Some companies have insurance policies that protect against crime, but because the employees are scammed into performing a voluntary act to provide the scammers with the funds, the courts can find that there was no crime. In light of this finding, many insurance companies are including endorsements to cover this new type of fraud [6].

While the problem is rampant, there is hope in sight. In order to curb these attacks, all persons that interact with others need to be aware of the threats and learn how to recognize them. Kaila and Nyman [7] outline best practices to identify the threats and hopefully eliminate them from becoming successful. Several of these practices include learning how to recognize phishing by identifying fake email addresses and websites. Artificial intelligence is getting better at identifying the threats, but it is not totally foolproof. "It is very important for all employees to have a basic grasp of such tricks and how to spot them." [7].

7. CONCLUSIONS

Scammers continue to improve their game by inventing new ways to gather information and funds. The employees need to be diligent in verifying the request to ensure they do not fall prey to this sort of scam. No matter how legitimate the request sounds, it is always a good idea to verify before sending any funds out via a nontraditional channel.

8. REFERENCES

[1] D. Adamek, "Spotting Fraud Victims", Journal of Accountancy, vol. 226, no. 3, pp. 22, 2018.

[2] S. S. Smith, "2017 Internet Crime Report", Federal Bureau of Investigation, Washington, D.C., 2018.

[3] M. Foreman, "CEOs Under Fire from Email Fraud", Credit Control, vol. 37, no. 5/6, pp. 19-21, 2016.

[4] M. C. Meinert, "Social Engineering: The Art of Human Hacking", ABA Banking Journal, vol. 108, no. 3, pp. 49, 2016.

[5] T. Kemp, "Social Engineering Fraud: A Case Study", Risk Management, vol. 63, no. 6, pp. 8-9, 2016.

[6] A. Selarnick and E. Kandel, "Insuring Against Social Engineering Attacks", Risk Management, vol. 64, no. 5, pp. 12-14, 2017.

[7] U. Kaila and L. Nyman, "Information Security Best Practices: First Steps for Startups and SMEs", Technology Innovation Management Review, vol. 8, no. 11, pp. 32-42, 2018.