Digital Social Engineering Attacks

10/10/18

Christopher Hovis

East Carolina University

ABSTRACT

This paper will look at how social engineers exploit human vulnerabilities through digital social engineering attacks and how those attacks can affect the confidentiality, integrity, and accessibility of information and computer systems. Social engineering attacks are propagated by malicious links, spoofing websites, SMS text, or pop-up windows that ask for sensitive information or infect the target's computer with malware for use in a later attack. This paper will define the types of human vulnerabilities that are exploited during a social engineering attack and define and discuss the most used attack techniques that are carried out by social engineers in the attempt to collect a target's information, gain access to their systems, or prevent them from accessing their systems or devices.

INTRODUCTION

Cyber-attacks have been increasing rapidly over the past decade (Conteh & Schmick, 2016). The impact of cyber-attacks and cyber-crime have reached the point that in 2013, the then director of the FBI James Comey, testified to the Senate Homeland Security Committee that cyber-attacks have surpassed terrorism as the leading domestic threat to the United States (Conteh & Schmick, 2016). One of the most used cyber-attacks is social engineering. According to the website social-engineer.org, roughly 66% of all cyber-attacks use some form of social engineering to execute the attack (Social-Engineer.Org, 2014).

So, what is social engineering? According to Christopher Hadnagy, a professional social engineer and author, social engineering is “any act that influences a person to take an action that may or may not be in their best interest” (Hadnagy, 2014). So, how can a social engineer influence a target to perform an action? The answer is, by exploiting the target’s vulnerabilities. Yes, just like an unpatched web server, we humans have vulnerabilities. Vulnerabilities are linked to feelings and emotions. They can sometimes blind us to what is really going on and cause us to, like Hadnagy said, take an action that might not be in the target’s best interest.

The goal of this white paper is to define the human vulnerabilities that are exploited that allow social engineering attacks to succeed. Additionally, the paper will highlight the most popular techniques used to persuade unsuspecting victims into providing money, information, or access to computer systems. Examples of each

technique will be discussed as well as how they affected the confidentiality, integrity, and availability of the target's data and information systems.

HUMAN VULNERABILITIES

Social engineering attacks are designed to exploit feelings and emotions. These attacks are successful because unlike other cogs of a system that may have vulnerabilities, patches or countermeasures for users are not implemented, like awareness and education classes, on a consistent basis to lessen the likelihood or consequences of an attack. Researchers have pointed to curiosity, fear, greed, sympathy, respect for authority, and trustworthiness as possible human vulnerabilities that malicious actors can exploit to achieve their objective.

Curiosity - In the article "Which phish get caught? An exploratory study of individuals' susceptibility to phishing", curiosity is defined as "excitement about the possibilities made possible by a technology" (Moody, Galletta, & Dunn, 2018). Social engineers use the curiosity about technology to their advantage. This curiosity influences the target to find out more about the technology, which social engineers use to achieve their goal.

Fear / Anxiety - Fear is one of the most powerful motivators and because of that, it is one of the most commonly abused emotion when it comes to social engineering (Whipple, 2016). Fear is the emotional feeling we get when we perceive that we are threatened. Social engineers are good at creating situations where the target feels

anxious. That anxiety is what social engineers are looking for to influence a target to perform an irrational action.

Greed - Austin Whipple in his article “Hacker psychology: Understanding the 4 emotions of social engineering “on networkworld.com defined greed as “an intense and selfish desire for something, especially wealth or power” (Whipple, 2016). Social engineers use this desire to further their attacks. This is done by convincing the target that a monetary gain or something for free is available if they perform a simple action or pay a small fee.

Sympathy - Social engineers can exploit a target’s overall goodness (Social-Engineer, 2013). These attacks try to pull at the heartstrings of the target to collect money and information. They can craft stories to entice potential victims into either clicking a malicious link in an email or perhaps donating money to a fake charity.

Respect for authority - According to social-engineer.org, there are three types of authority that malicious actors try to use in the attempt to persuade a target to comply with their request. They are legal, organizational, and social authority (social-engineer.org, n.d.). All three of these use the perception of authority to influence the target into performing an action.

Trustworthiness and Helpfulness - Malicious actors can use a target’s trustworthiness and helpfulness against them. A good example of this is in Christopher

Hadnagy's book "Social Engineering: The Art of Hacking". In the book, he tells the story of an Interviewee asking the receptionist if he could print a new copy of her resume from a USB stick since the original copy had coffee spilled on it. Unknowingly, the helpful receptionist infected his computer and possibly compromised the company's network because he was trying to be helpful (Hadnagy & Wilson, Social Engineering: The Art of Human Hacking, 2010).

Social engineers can select one of these emotions to attempt to persuade the target into complying with the request. However, when they combine several of these exploits, they can attack the target on multiple fronts. So, instead of only preying on the targets fear and anxiety, a social engineer can use trust as well. This is apparent in attacks that use a target's bank as their pretext. The target's trustworthy nature leads them to believe the communication from their bank is legitimate, and the anxiety they feel after being notified that their account has been closed or suspended creates a very powerful motivator to comply with the communication to rectify the issue.

ATTACK TECHNIQUES AND EXAMPLES

There are several ways that malicious actors can use social engineering to influence the target into complying with their requested action. These techniques, in combination with the selected attack vector and targeted human vulnerabilities, will be used to maximize the effectiveness of the attack and to cause the loss of confidentiality, integrity, and availability of the target's information and systems.

The most popular attack technique that utilizes social engineering is a phishing attack. According to the Infosec Institute, phishing is defined as “a method of sending a user (or many users) digital correspondence that appears legitimate but is actually meant to lure a potential victim into providing some level of personal information for nefarious purposes, including identity or monetary theft” (Phishing Definition, Prevention, And Examples, 2018). Social engineers can use several attack vectors to carry out phishing attacks. They can use email, websites, or SMS texting, to deliver their attack to the target(s) in hopes that they will comply with the malicious actor’s request (Chiew, Yong, & Tan, 2018).

The most common form of phishing uses email as the attack vector (Phishing Definition, Prevention, And Examples, 2018). An example of an email phishing attack is the Nigerian email scam. This scam mass emails thousands of users in an attempt to find users that have the correct vulnerabilities to fall for the hoax. In some cases that might be greed and trustworthiness, in others, it may be curiosity and helpfulness. In either case, the outcome is the same. The target will be scammed out of their hard-earned money.

Fred Haines, a handyman from Kansas, was scammed out of $110,000 from the Nigerian Prince scam between 2005 and 2008. Mr. Haines was quoted saying “I thought, man, $580 million — yeah, I should be able to get a little bit of that" (McKinley, 2018). Mr. Haines was curious and eventually blinded by the financial benefits if he cooperated. Below is an example of a Nigerian prince phishing email.

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost $ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost $ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

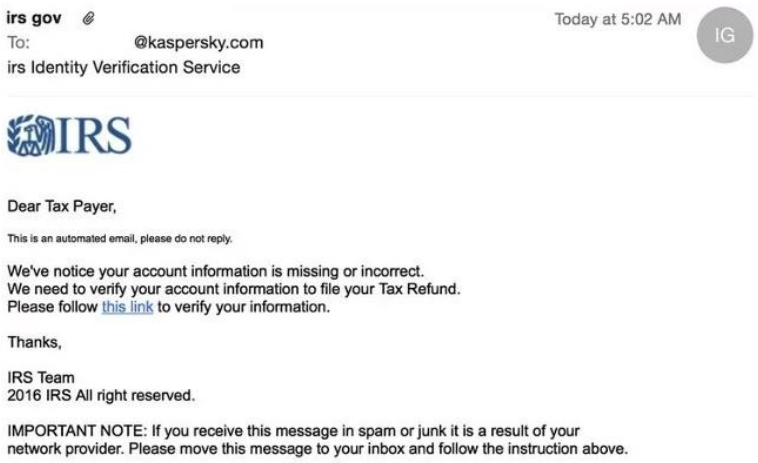
Please acknowledge the receipt of this message via my direct number [redacted] only.

Yours Sincerely, Dr. Bakare Tunde
Astronautics Project Manager

Figure 1.0 Nigerian prince email (kaspersky, 2016)

In the Nigerian Prince phishing example, Mr. Haines lost money, but he did not lose the confidentiality, integrity, or availability of his data or system. That is not the case in all phishing attacks. Below is a phishing attack that can affect these pillars of information security.

In an attack like the below IRS phishing email. The confidentiality, integrity, and availability of the target's information and systems could be compromised. The provided link could lead to a spoofed web page where sensitive information, such as usernames and passwords, could be collected. Additionally, the link could install malware that could cause the loss of availability.



irs gov
To: @kaspersky.com
irs Identity Verification Service
Today at 5:02 AM
IG

IRS

Dear Tax Payer,

This is an automated email, please do not reply.

We've notice your account information is missing or incorrect.
We need to verify your account information to file your Tax Refund.
Please follow this link to verify your information.

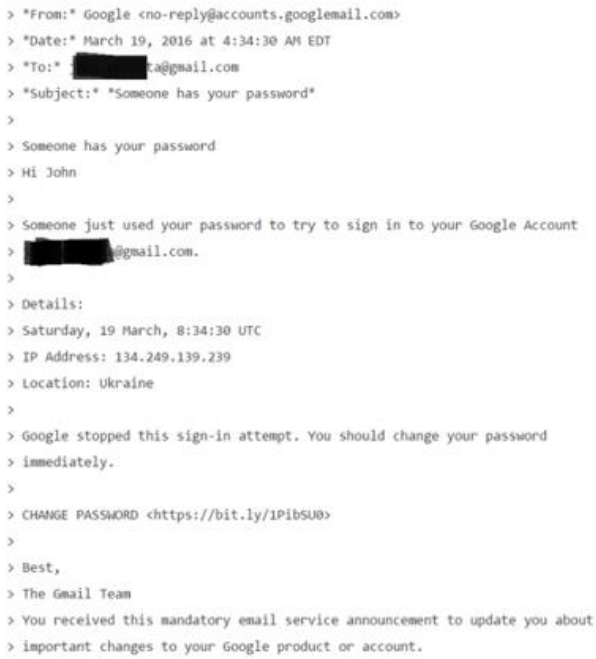
Thanks,

IRS Team
2016 IRS All right reserved.

IMPORTANT NOTE: If you receive this message in spam or junk it is a result of your network provider. Please move this message to your inbox and follow the instruction above.

Figure 2.0 IRS phishing email (Johnson, 2017)

Spear phishing is a phishing attack that can target a specific person, group, or organization (Chiew, Yong, & Tan, 2018). This type of attack has seen an increase in popularity due to its superior success rate over the typical phishing attack. This is due to the relevant nature of the content that is used in the attack. The target may have used the site before, or the communication appears to be from a known source (Chiew, Yong, & Tan, 2018). Social Media, like Facebook, Twitter, and Linkedin, have made spear phishing easier since so many people and organizations post personal and professional information. Social engineers can collect and use this information to further their attack.



> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [redacted]a@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.

Figure 3.0 John Podesta email from Wikileaks (CBS News, 2016)

An example of a spear phishing attack is the hacking of John Podesta's (the chairman of the Hillary Clinton campaign for President in 2016) emails. CBS News reported that in mid-March of 2016, Mr. Podesta received an email stating that his Gmail password had been used from someone in Ukraine and they suggested that he change his password (CBS News, 2016). Alarmed by this, Mr. Podesta, sought confirmation of the authenticity of the email. Charles Delavan, a staff aide, replied to Mr. Podesta, stating "This is a legitimate email. John needs to change his password immediately" (Lipton, Sanger, & Shane, 2016). Unfortunately for the Clinton campaign, Mr. Podesta took Mr. Delavan's advice, and the results of his action can now be found on the Wikileaks website.

In this example, the malicious actors involved, now known to be Russian hackers attempting to interfere with the 2016 Presidential election (Lipton, Sanger, & Shane,

2016), used email as their attack vector to deliver their spoofed email with a malicious link embedded to Mr. Podesta. The New York Times reported that Mr. Delavan commented that they were getting many of these types of email (Lipton, How We Identified the D.N.C. Hack's 'Patient Zero', 2016). This is an indication of a spear phishing attack, with the goal of infiltrating the Clinton campaign. The email used trustworthiness and fear to persuade Mr. Podesta or anyone else that received this email, to comply with the email's request. Google is a reputable company and the email presented to Mr. Podesta appeared to be authentic, and from personal experience, the notion that his email account had been compromised would have caused some anxiety.

When looking at this case from an information security standpoint, the confidentiality of Mr. Podesta's emails was compromised by the attack. But in a spear phishing attack such as this one, the attackers could have easily compromised the integrity of Mr. Podesta's emails, by sending unauthorized emails as the target or compromised the asset's availability by denying access to the account.

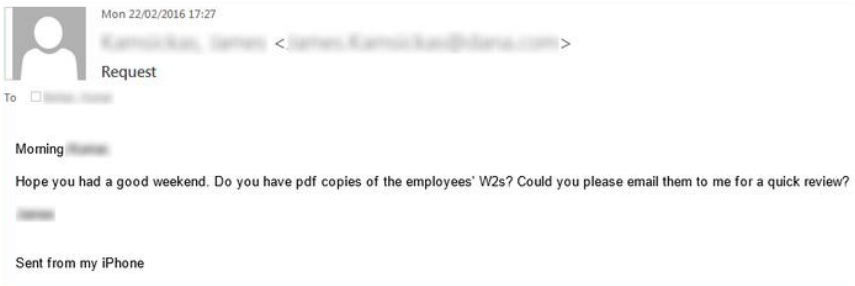
The social engineering attack called whaling is very similar to both phishing and spear phishing. The difference is that a whaling attack has a very specific target in its crosshairs (Chiew, Yong, & Tan, 2018). Whaling targets are typically an executive or someone in upper management of an organization. Malicious actors spend considerable amounts of time and resources gathering information about the target (Amro, 2018). Information available via social media helps these attackers gather vital information needed to carry out the attack.

Whaling has been linked with another type of attack called business email compromise. In a business email compromise attack, malicious actors send emails,

either spoofed or from a compromised account via a whaling attack (Shah, 2017), disguised as a high ranking official requesting money transfers, fake invoices be paid, or requesting sensitive data (FBI, 2017). According to the FBI, they have been tracking business email compromise attacks since 2013 and have seen a 1300% increase in BEC attacks since 2015, with three billion dollars in losses (FBI, 2017).

An example of a whaling and business email compromise attack is what happened to Leoni AG, Europe's largest wire and cabling manufacturer, in August of 2016. The perpetrators were able to pull off a whaling attack by infiltrating Leoni AG's network and gaining access to a high-ranking employee's email (Cluley, 2016). The malicious actors used this access to initiate a BEC attack on Leoni AG. According to Mary-Ann Russon of the International Business Times, the CFO at the Bistrita, Romanian plant received a spoofed email that was designed to appear as if it came from the compromised executive within the company. The email requested a $44.6 million transfer to the malicious actor's account. The thieves used the information they gathered beforehand to craft the email in a way that followed company procedures when dealing with money transfers (Samarati, 2016). This was done so no red flags were raised, and it worked. The CFO followed procedure and sent the transfer.

In this instance, the integrity of Leoni AG's data was lost. Data, in this case, an email, was being created that was not authentic to Leoni AG. But, Whaling and business email compromise attacks could also lead to the loss of confidentiality. Below is an example of a BEC attack that was used to steal Snapchat's payroll data in 2016 (CSO).


Mon 22/02/2016 17:27

Request

To

Morning

Hope you had a good weekend. Do you have pdf copies of the employees' W2s? Could you please email them to me for a quick review?

Sent from my iPhone

Figure 4.0 Snapchat BEC email (Tung, 2016)

Smishing is the same technique as a phishing attack, except smishing uses the attack vector of SMS texting instead of email. Smishing is very dangerous because people tend to be more trusting of a text message than an email (Symantec, n.d.). We have not yet been conditioned to view an SMS text as a threat like we have with email. Additionally, spotting a smishing message can be quite difficult as well. Since there are no pictures or colors in an SMS text, creating a fraudulent message is quite easy for the attackers. Furthermore, the delivery method also makes it difficult to detect a malicious message. Instead of an email address, SMS testing only has a phone number (Jakobsson, 2018), this makes detection more difficult.

Since the increase in popularity of mobile banking many social engineers have started spoofing text messages from financial institutions (social-engineer.org, n.d.). Below is an example of a Smishing attack that is using the bank Wells Fargo as its pretext. This smishing attack attempts to use the target's trusting nature along with their fear and anxiety of having an issue with their bank account to accomplish the social engineer's goal of stealing the target's login information. Additionally, the message has no distinguishing features that raise any red flags. The message is short and to the point. The lack of features makes it near impossible to determine if these types of text are malicious or not.

Figure 5 Smishing text message (social-engineer.org, n.d.)

Smishing is like phishing when it comes to the concerns of confidentiality, integrity, and availability of the target's information and computer systems. Depending on the goal of the attack, malicious actors can compromise the confidentiality of the target's information by setting up a spoofed website to collect financial or personal information to be used in later attacks.

Another digital social engineering attack that exploits human vulnerabilities is scareware. Scareware exploits a target's fear and anxiety by displaying a perceived threat that could affect the confidentiality, integrity, or availability of the target's data or computer systems (Malin, Gudaitis, Holt, & Kilger, 2017). These vulnerabilities are exploited to push the target into performing an action that, as Hadnagy said, may not be in their best interest. A scareware social engineering attack usually starts with a popup window with the claim that the user's computer has been infected with malware or a serious error has occurred.

The SystemSecurity malware from 2009 is an example of social engineers playing on the fears of their targets to extract money or information to be used for later malicious activities. The scareware SystemSecurity created a fake blue screen of death

screens to intimidate the target into purchasing the SystemSecurity software. This was a scam, the computer was never infected, other than the SystemSecurity software. The goal of the attack was to steal money from their targets (SPAMfighter, 2009).

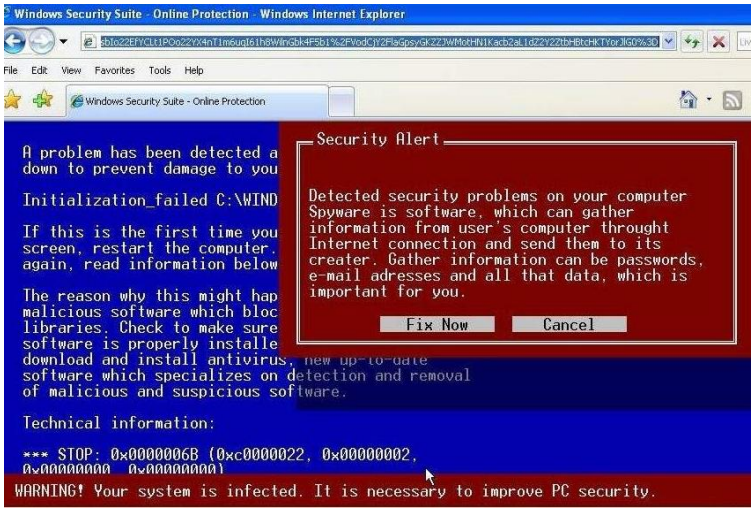


Figure 6 scareware blue screen of death (FraudWatch International, 2017)

The SystemSecurity scareware affected the target's data integrity. The authors of the SystemSecurity malware in effect compromised the integrity of the victim's bank account by causing a transaction under false pretenses. Additionally, the target's information was used for identity theft (pchubs, 2008) furthering the compromise of the integrity of the target's data.

CONCLUSION

Cyber-attacks have become a major issue within the United States and social engineering play a major role in its success, with around 66% of all attacks containing some form of social engineering component (Social-Engineer.Org, 2014). Digital social engineering

attacks are successful because they can exploit human vulnerabilities to persuade the target to carry out the attack for the malicious actor. Whether it is from some form of phishing, smishing, business email compromise, or scareware attacks, the consequences are the same. These attacks negatively affect the confidentiality, integrity, or availability of data or systems and cost the affected organization millions of dollars per incident.

Until an effective patch to these human vulnerabilities has been found, more and more of these attacks will be seen by email, websites, text messages, or any other form of communication that may be thought up in the years to come. To combat this digital epidemic, controls and countermeasures need to be implemented to reduce the likelihood of an attack reaching an end user, and to reduce the impact of an exploitation of the human vulnerabilities if it is successful.

References

Amro, B. (2018). Phishing Techniques in Mobile Devices. *Journal of Computer and Communications*, 27-35.

CBS News. (2016, October 28). *The phishing email that hacked the account of John Podesta*. Retrieved from cbsnews.com: https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/

Chiew, K. L., Yong, K. S., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, 1-20.

Cluley, G. (2016, September 1). *How one company lost $44 million through an email scam*. Retrieved from tripwire.com: https://www.tripwire.com/state-of-security/security-data-protection/44-million-email-scam/

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 31-38.

FBI. (2017, February 27). *Business E-Mail Compromise*. Retrieved from fbi.gov: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

FraudWatch International. (2017, March 8). *What is… Scareware?* Retrieved from What is… Scareware?: https://fraudwatchinternational.com/expert-explanations/what-is-scareware/

Hadnagy, C. (2014). *Unmasking the Social Engineer: The Human Element of Security.* John Wiley & Sons, Incorporated.

Hadnagy, C., & Wilson, P. (2010). *Social Engineering: The Art of Human Hacking.* John Wiley & Sons, Incorporated.

Jakobsson, M. (2018). Two-factor inauthentication – the rise in SMS phishing attacks. *Computer Fraud & Security*, 6-8.

Johnson, C. (2017, July 21). *15 Examples of Phishing Emails from 2016-2017*. Retrieved from edts.com: https://www.edts.com/edts-blog/15-examples-of-phishing-emails-from-2016-2017

kaspersky. (2016, June 30). *Sometimes Nigerian spam comes with near-constant belly laughs*. Retrieved from kaspersky.com: https://www.kaspersky.com/blog/funny-email-scam/12503/

Lipton, E. (2016, December 20). *How We Identified the D.N.C. Hack's 'Patient Zero'*. Retrieved from nytimes.com: https://www.nytimes.com/2016/12/20/insider/how-we-identified-the-dnc-hacks-patient-zero.html

Lipton, E., Sanger, D. E., & Shane, S. (2016, December 16). *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.* Retrieved from nytimes.com: https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Malin, C. H., Gudaitis, T., Holt, T. J., & Kilger, M. (2017). Phishing, Watering Holes, and Scareware. *Deception in the Digital Age*, 149-166.

McKinley, E. (2018, June 11). *Nigerian Prince Scam took $110K from Kansas man; 10 years later, he's getting it back*. Retrieved from kansascity.com: https://www.kansascity.com/news/state/kansas/article212657689.html

Moody, G. D., Galletta, D. F., & Dunn, B. K. (2018). Which phish get caught? An exploratory study of individuals' susceptibility to phishing. *European Journal of Information Systems*, 564-584.

pchubs. (2008, December 22). *System Security Removal Process*. Retrieved from pchubs.com: https://www.pchubs.com/blogs/system-security-removal-process-remove-systemsecurity

Phishing Definition, Prevention, And Examples. (2018, October 10). Retrieved from Infosec Institute: https://resources.infosecinstitute.com/category/enterprise/phishing/#gref

Samarati, M. (2016, September 5). *Leoni AG victim of business email compromise – €40 million lost*. Retrieved from itgovernance.eu: https://www.itgovernance.eu/blog/en/leoni-ag-victim-of-business-email-compromise-40-million-lost

Shah, N. (2017, July 24). *Worried About Business Email Compromise? Lacking Visibility into Advanced Attacks? Look No Further*. Retrieved from symantec.com: https://www.symantec.com/connect/blogs/worried-about-business-email-compromise-lacking-visibility-advanced-attacks-look-no-further

Social-Engineer. (2013, July 16). *Sympathy Used By Social Engineers*. Retrieved from social-engineer.com: https://www.social-engineer.com/sympathy-used-by-social-engineers/

Social-Engineer.Org. (2014, April 28). *The Social Engineering Infographic*. Retrieved from Social-Engineer.Org: https://www.social-engineer.org/social-engineering/social-engineering-infographic/

social-engineer.org. (n.d.). *The Social Engineering Framework*. Retrieved from www.social-engineer.org: https://www.social-engineer.org/framework/influencing-others/influence-tactics/authority/

social-engineer.org. (n.d.). *The Social Engineering Framework*. Retrieved from social-engineer.org: https://www.social-engineer.org/framework/attack-vectors/smishing/

SPAMfighter. (2009, August 28). *Malware Writers Develop Scareware Imitating Blue Screen of Death*. Retrieved from spamfighter.com: http://www.spamfighter.com/News-12982-Malware-Writers-Develop-Scareware-Imitating-Blue-Screen-of-Death.htm

Symantec. (n.d.). *What is smishing?* Retrieved from us.norton.com: https://us.norton.com/internetsecurity-emerging-threats-what-is-smishing.html

Tung, L. (2016, March 4). *This is what the CEO spoofing attack on Snapchat looked like*. Retrieved from cso.com.au: https://www.cso.com.au/article/595279/what-ceo-spoofing-attack-snapchat-looked-like/

Whipple, A. (2016, May 13). *Hacker psychology: Understanding the 4 emotions of social engineering*. Retrieved from Networkworld: https://www.networkworld.com/article/3070455/cloud-security/hacker-psychology-understanding-the-4-emotions-of-social-engineering.html