Phishing Attacks: Preying on Human Psychology to Beat the System and Developing Cybersecurity Protections to Reduce the Risks

Natasha M. Wojcicki

Dominican University

Abstract

The evolution of technology over the years has allowed people to more easily store, access, and share information on the Internet. People can bank online, shop, and post their latest life news. Unfortunately, all this available information has attracted the attention of cybercriminals who want to use this personal information for fraudulent purposes. A common technique used by cybercriminals to obtain sensitive information is a scam called phishing. Criminals pose as a trusted entity in order to trick victims into revealing sensitive information that they will later use to commit illegal money transfers, identity theft, or other fraud. The consequences of phishing scams may lead to the loss of data, money, identity, reputation, and trust. As a result, organizations and individuals need to familiarize themselves with the process of a phishing attack and how to protect their systems and information. Organizations and individuals not only need the proper hardware and software to protect their information, but they also need to understand that cybercriminals prey on human psychology. Cybercriminals often use social engineering tactics to persuade people to willingly share their personal information. Therefore, cybersecurity policies and security prevention tips should address technical elements, as well as human behavioral factors that use the CIA (Confidentiality, Integrity, and Availability) model as a guide.

Keywords: Phishing; Cybersecurity; Information Security; Cyber Fraud; Social Engineering; Social Influence Framework; Data Breach; Data Protection; Cybersecurity Policy; CIA Model; Cybersecurity Awareness

About the Author

Natasha M. Wojcicki is a current graduate student of the MSIM program at Dominican University in River Forest, Illinois. In 2006, Natasha graduated from Dominican University with her B.A. in Criminology and Sociology. In 2008, she graduated with her M.A. in Sociology at Loyola University of Chicago. Natasha is currently working towards her Master of Science degree in Information Management with a specialization in cybersecurity.

The Internet and advancement of technology has made it possible for people to easily store, access, and share information from anywhere and on a variety of different devices. From their desktop computers, tablets, or mobile phones, people can simply look up the latest news, shop, pay bills, check e-mail, or post current life events to their social media accounts. Unfortunately, the ease of accessing and sharing information online has attracted the attention of cybercriminals who want to exploit this information for financial gain. A common technique employed by cybercriminals to obtain sensitive information from victims is called phishing. The term "phishing" originates from the analogy of "fishing" for victim's personal or financial information (Gupta, Tewari, Jain, & Agrawal, 2017). Typically, phishers will send a malicious e-mail by impersonating "a trusted entity with the intention of convincing the recipient to share sensitive information, transfer funds, or connect to a fraudulent website" (SonicWall Inc., 2018). The method that phishers frequently use to collect this information from victims is through social engineering tactics that prey on human nature.

Phishing attacks are a serious threat and a growing concern for individuals, businesses, and governments. Trend reports substantiate these concerns as phishing attacks continue to rise each year and the methods used by phishers advances along with technology. The ramifications of being a victim of a phishing attack may mean the loss of money, identity, reputation, trust, and intellectual property. As a result, individuals and organizations need to stay current on the latest phishing schemes and prevention tips. Additionally, it is important that organizations develop policies and procedures to act as a line of defense against cybercriminals. They need to implement a cybersecurity policy to address security prevention and detection of its systems, as well as user training.

Literature Review

Phishing attacks are rapidly growing and posing a serious threat to Internet security. According to Elliot Volkman of PhishLabs, "phishing attack volume grew 40.9% in 2018 and 83.9% of attacks targeted credentials for financial, e-mail, cloud, payment, and SaaS services" (Volkman, 2019). Additionally, "the use of free website infrastructure to stage and launch attacks grew substantially" (Volkman, 2019). Some types of phishing attack methods include spear phishing, whale phishing, session hijacking, e-mail/spam, keyloggers, malware, and ransomware.

The prevalence of phishing schemes among cybercriminals is due to the low risk and high reward involved. Unfortunately, phishers are rarely apprehended and prosecuted because of jurisdiction issues, as many live outside of the victim's area, and it is often difficult to trace their whereabouts. Furthermore, a successful phishing scam can mean a lucrative financial reward. In 2018, the financial loss to victims was reported to be $48,251,748.00 (FBI, 2019).

Due to the growing awareness of phishing scams and the liability they pose, many institutions have taken steps to secure their infrastructure by implementing phishing detecting technology and security awareness training programs. Technical countermeasures include e-mail filtering and anti-phishing toolbars, which "successfully detect phishing attempts in about 35 percent of cases" (Wright & Marett, 2010). However, it is important that fraud definitions are continually updated and that bogus websites are flagged. Unfortunately, "preventing false alarms from occurring continues to challenge individual users and IT departments," as well as an up-to-date registry of valid and invalid websites (Wright & Marett, 2010). Since anti-phishing technology tools are not always reliable, end users are the last line of defense against phishing attacks. It is critical then that users receive proper security awareness training because phishers often use social engineering tactics on their victims. In fact, "98% of attacks that made it past enterprise e-mail security controls and into user inboxes contained no malware" (Volkman, 2019). This means that phishers are relying on social engineering to exploit victims to gain access to sensitive information.

Social engineering on the Internet "is a means of gaining access to systems or data by exploiting human psychology" (Muscanell, Guadagno, & Murphy, 2014). It is a common tactic among phishers because it has proven to be successful. It has been argued that easy access to the Internet and people's reliance on it in everyday life has made them more complacent and susceptible to social influence tactics (Muscanell et. al, 2014). Robert Cialdini, a social psychologist, developed a social influence framework that explains the nature of social engineering techniques and why they are so effective. He lists six social influence principles that can be misused as "weapons of influence," which is explained further in Figure 1 below. (Muscanell et. al, 2014).

Figure 1. Social Influence Principles and Phishing Tactics

Social Influence Principles and Phishing Tactics	
LIKING	People tend to believe that likeable people are more honest and trustworthy. This works well for a phishing scam known as the "The Stranded Traveler" in which an individual receives an e-mail from a friend, family member, or acquaintance stating that they need money to return home from a foreign country (Muscanell et. al, 2014). People are more inclined to help someone that they like and consider trustworthy.
AUTHORITY	People often view someone in a position of authority as credible and honorable. This was used to the advantage of phishers in 2012 when military members at the U.S. Department of Defense received an e-mail from someone claiming to be from Defense Finance and Accounting Services. Victims were asked to e-mail VA and IRS documents that contained personal information in order to receive compensation (Muscanell et. al, 2014).
SCARCITY	People attach more value to an object or opportunity if it is perceived to be limited in supply or hard to acquire (Muscanell et. al, 2014). An example is the popular phishing scam in 2011 when people received a "limited time offer" opportunity to collect a $100.00 Walmart gift card via e-mail and Facebook (Muscanell et. al, 2014).

SOCIAL PROOF	People tend to take social cues from the behavior of others around them. An example is when Facebook users download an application that they see is popular with their friends. Unfortunately, these apps may contain malware to harvest their personal data (Muscanell et. al, 2014).
RECIPROCITY	People are more likely to comply with a request when they feel obligated to help someone in return. An example of this is the "Nigerian Prince" phishing scam (Muscanell et. al, 2014). An individual receives an e-mail stating that they are receiving a check for a sum of money. The victim receives the bogus check and then receives an e-mail from the phisher requesting that the victim wire funds. The victim in this case feels indebted because they received money from the phisher.
COMMITMENT & CONSISTENCY	People are thought to be more reliable, stable, and dependable if they show that they are committed and consistent (Muscanell et. al, 2014). This principle fits well with online dating phishing scams. The phisher builds a relationship with the victim showing commitment and consistency. As things progress and the victim is more invested in the relationship, the phisher persuades the victim to send money or personal information.

The social influence framework provides insight as to why phishing scams work at the end user level. It also helps security experts design cybersecurity policies and procedures by examining the human element of protecting systems rather than just the technical side.

Methodology

Phishing scams continue to be a growing threat to a variety of industries because it is a successful technique for cybercriminals. The reward is high and the risk is low. Phishers prey on the weaknesses of human behavior to achieve their goals. They have developed tactics to influence people into disclosing confidential information by posing as a trusted entity. The consequences to victims may be the loss of money, identity, reputation, trust, and intellectual property.

How do phishing attacks work? Why are people so susceptible to phishing scams? How can organizations and individuals reduce their risks of being victims of such scams? To find answers to these questions, an exploratory case study was performed by gathering the data of other research studies conducted on the topic, as well as real-life security breach incidents.

The research revealed that phishing scams are evolving due to the advancement and mobility of technology. While the medium may be changing, the stages of a phishing attack remains the same. Real-life security breach incidents show that cybercriminals rely on end users to either provide them access into an organization's network or into revealing sensitive information. Cybercriminals then use that information to obtain illegal funds or commit other fraud. The consequences can have a devastating effect on organizations and individuals. As a result, cybersecurity policies and user awareness/training programs need to be designed to reduce the security risks of cyber threats, particularly, phishing attacks.

Current Phishing Trends

Social Media. Phishing attacks are evolving based on the advancement of technology. The traditional mode of phishing by e-mail is still predominant, but the use of social media to perpetrate attacks is on the rise. Popular social media platforms that are a target of cybercriminals include Facebook, Instagram, Twitter, LinkedIn, and Snapchat. Phishers "lure victims to impersonation web sites by incorporating phishing URLs into posts or comments" (Piscitello, 2019). This new attack vector demonstrates "that phishers have adapted to society's increased mobility and today's diversity of messaging platforms" (Piscitello, 2019).

Business E-mail Compromise (BEC). Phishers looking for a bigger financial reward are using a sophisticated scam called Business E-mail Compromise (BEC). Phishers target both businesses and individuals in order to trick victims into wiring funds to the phisher's bank account. In 2013, the common method was to hack or spoof the e-mail account of the CEO or CFO of a corporation and instruct an employee to wire funds to pay an invoice or transfer money to a new account (FBI, 2019). The scam has evolved over the years to include compromised e-mail accounts of individuals, vendors, lawyers, and real estate agents (FBI, 2019). In 2018, the IC3 received an increase in complaints requesting victims to purchase gift cards. In these instances, "victims received a spoofed e-mail, a spoofed phone call or a spoofed text from a person in authority requesting the victim purchase multiple gift cards for either personal or business reasons" (FBI, 2019). According to the FBI, the total loss to victims of BEC scams in 2018 was $1,297,803,489.00 (2019).

Encrypted Websites. As mentioned previously, "the use of free website infrastructure to stage and launch attacks grew substantially" in 2018 (Volkman, 2019). It appears that there is a trend among some phishers to use digital certificates on their fraudulent websites. "Nearly half of phishing sites use digital certificates," which gives the appearance to unsuspecting victims that they are on a legitimate webpage and ignore browser warnings (APWG, 2019). Unfortunately, consumers are under the misconception that "HTTPS" means that the website is secure (Newman, 2017). Rather, HTTPS signifies that the communication between the server and the user's browser is encrypted and protected against interception (Newman, 2017). If this trend continues, more Internet users will fall victim to this type of phishing attack. Therefore, more user education is needed and maybe even changes to web browser features.

Stages of a Phishing Attack

The stages of a phishing attack include: 1. Plan, 2. Setup, 3. Attack, 4. Collect, and 5. Fraud. The process model of a phishing attack is pictured in Figure 2.

Stage 1 – Plan: Phishers identify a target, such as an individual or organization, and acquire information on the specific target. They can obtain this information from websites, telephone calls, physically visiting the organization, or monitoring network traffic.

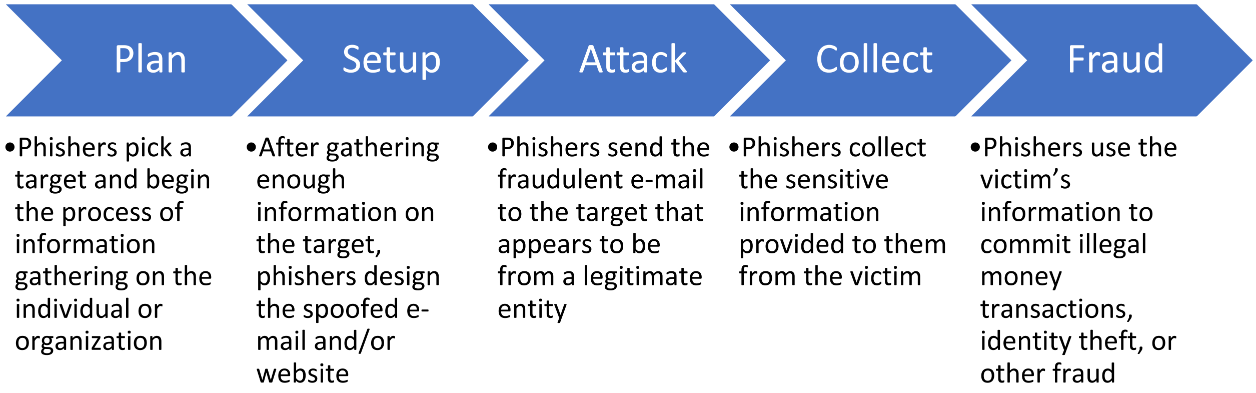
Stage 2 – Setup: Phishers may develop a fraudulent website that is identical to a legitimate business or create malware that will execute on the victim's device like a computer or mobile phone. The malware can be designed to capture keystrokes or used to lock down the victim's computer files in order to ask for ransom (a.k.a ransomware).

Stage 3 – Attack: The spoofed e-mail is sent to the target and it appears to be from a trusted entity such as a bank, customer, vendor, friend, etc. The e-mail is usually written with a sense of urgency and requires the target to update information, reset a password, wire funds to a different bank account, or provide other sensitive information.

Stage 4 – Collect: Phishers collect the information that the victim provided to them via the fraudulent website, e-mail, or captured keystrokes from installed malware.

Stage 5 – Fraud: Phishers now have the victim's personal information such as credit card numbers, website credentials, and bank account information to commit illegal transactions, identity theft, or other type of fraud.

Figure 2. Process Model of a Phishing Attack



Plan

- Phishers pick a target and begin the process of information gathering on the individual or organization

Setup

- After gathering enough information on the target, phishers design the spoofed e-mail and/or website

Attack

- Phishers send the fraudulent e-mail to the target that appears to be from a legitimate entity

Collect

- Phishers collect the sensitive information provided to them from the victim

Fraud

- Phishers use the victim’s information to commit illegal money transactions, identity theft, or other fraud

Security Incidents

Despite efforts by organizations and individuals to protect their information and systems, there will always be security risks associated with phishing. This is because as security practices evolve with the advancement of technology, phishers are also developing their attack techniques in order to find loopholes in the new technology or organizational procedures. Therefore, individuals and organizations must continually be vigilant on the latest phishing schemes. Unfortunately, people sometimes miss the red flags of a phishing scam or the e-mail bypasses security protocols. Below are some examples of security incidents from phishing scams.

Memorial Hospital. On December 6, 2018, an employee at Memorial Hospital in Gulfport, Mississippi, fell victim to a phishing attack that allowed an unauthorized party to gain access to the employee's e-mail account (Davis, 2019). The data breach was discovered by hospital officials more than a week later on December 17. The employee's account was immediately secured and an investigation was opened to determine the extent of the incident

(Davis, 2019). Officials found that 30,000 patient records were exposed. The patient information contained within the e-mails "included names, dates of birth, health data, and information about services received at MHG. For a limited number of patients, Social Security numbers were included in the breached data" (Davis, 2019). In response, the hospital offered patients with compromised social security numbers to receive free credit report monitoring and identity protection services for one year.

Facebook and Google. In March 2017, the Department of Justice apprehended Evaldas Rimasauskas from Lithuania and extradited him to New York in August of the same year. He was charged with defrauding Facebook and Google of more than $100 million over a two-year period. According to an unnamed source, Google lost $23 million in 2013 and Facebook lost $98 million in 2015 (Dolmetsch, 2019). Rimasauskas and unidentified co-conspirators operated a phishing scheme against the two U.S. tech giants by posing as Quanta Computer, a computer supplier that regularly did business with both companies. They e-mailed invoices to employees of Facebook and Google using fake e-mail addresses. Rimasauskas created "fake bank accounts in Latvia and Cyprus to receive the scammed proceeds," and signed "fake contracts and documents that were submitted to banks to support the wire transfers" (Dolmetsch, 2019). On March 20, 2019, Rimasauskas pleaded guilty to one count of wire fraud and agreed to forfeit $49 million. His sentencing will be held on July 24, 2019 and Rimasauskas could receive a sentence of up to 30 years in prison.

According to a spokesperson from Google, they alerted authorities to the fraud as soon as it was discovered and they recouped all funds (Huddleston, Jr., 2019). A spokesperson from Facebook stated that they have been working with law enforcement and have received the "bulk of the funds shortly after the incident occurred" (Huddleston, Jr., 2019).

Target. In early 2014, Target announced a data breach that exposed credit card numbers and personal data on more than 110 million consumers (Krebs, 2014b). An investigation revealed that a third-party vendor, Fazio Mechanical, an HVAC firm, fell victim to an e-mail phishing scheme in which malware captured the network credentials the firm used to access a Target vendor portal. It appears that cybercriminals were somehow able to hack their way from the vendor portal to Target's cash registers within stores. A couple of days later, the hackers were able to push "their malware to a majority of Target's point-of-sale devices, and were actively collecting card records from live customer transactions" (Krebs, 2014a).

It was discovered by an investigative reporter, Brian Krebs, that Target and Fazio Mechanical were not using cybersecurity best practices (2014b). Fazio Mechanical did not have a proper anti-malware program running on their system. Rather, it was a free version of Malwarebytes that did not run real-time protection and was not meant for corporate use (Krebs, 2014b). Additionally, Target systems were not properly segmented from the third-party vendor portal (Krebs, 2014b). Unidentified sources at Target admitted that the company's security practices need improvement. The sources stated that third-party vendors are rarely required to use two-factor authentication or a one-time token (Krebs, 2014b). They added that Target is also lax when it comes to doing security assessments of its vendors (Krebs, 2014b). Target may have developed better security policies and procedures in response to this data breach. However, if not, then an overhaul of their cybersecurity policy is needed to address flaws and weaknesses.

Cybersecurity Policy

Successful phishing attacks can have severe consequences to an organization. The potential outcome may be the loss of data, money, reputation, and consumer trust. It could also put some businesses out of commission because the damage is too great to repair. As a result, organizations need to develop and implement a cybersecurity policy that effectively protects them against cyber threats like phishing.

The purpose of a cybersecurity policy is to protect and preserve the security of an organization's data and technology infrastructure. Therefore, instructions and security measures should be documented to reduce security risks such as human error and attacks by cybercriminals. The scope of the policy should apply to all employees, vendors, contractors, and others who have access to the organization's network and hardware. The elements of a policy should be guided by the CIA (Confidentiality, Integrity, Availability) model, which addresses information security within an organization. *Confidentiality* restricts access to information to authorized users only; *integrity* is maintaining the accuracy and trustworthiness of data throughout its entire life cycle; and *availability* is ensuring that authorized users have reliable access to information by rigorously maintaining system hardware and software for full functionality (Haughn & Gibilisco, 2014).

Since phishing attacks are a dangerous threat to organizations due to the value of the sensitive information that they store, policy elements addressing phishing attacks should be incorporated to avoid potential security breaches. It should be emphasized that data is confidential, and employees are obligated to protect it. Examples include information on finances, employees, business partners, customers, and vendors. IT administrators also need to set permissions that either allow or restrict users to access this information. To further protect the confidentiality of information, employees should be trained on how to safeguard data and be informed about the security risks. Common methods to ensure the confidentiality of data include complex passwords, data encryption, two-factor authentication, and security tokens. It is crucial that employees do not share passwords or document them without some form of encryption or password management tool.

In addition, transferring data introduces security risks, so it is imperative to implement security measures that protect the integrity of the data. The security risks should be communicated to employees, as well as how to securely transfer confidential data. To protect the integrity of data, confidential information should not be transferred to unauthorized devices or recipients. Furthermore, sensitive information should not be transferred over public Wi-Fi or other private connection that is not within the company network. When e-mailing sensitive information, the recipient should be verified as an authorized receiver and data encryption should be used.

Since phishing attacks commonly come through e-mail, the cybersecurity policy should specifically address how to spot potential scams. For example, employees should be trained to carefully review all e-mails from known and unknown senders. Employees should check the sender's e-mail address, as well as look for inconsistencies like grammar mistakes, spelling errors, and formatting issues. Employees should also avoid opening attachments or clicking on links when the content is not satisfactorily explained, and the URL leads to a different location. Doing so may lead to the installation of malicious software onto the employee's computer and company network. Any e-mails requesting money or business procedural changes should be verified with the sender by phone or in-person. The IT Department should also be informed of any potential phishing scams for further investigation.

Lastly, it is important to protect an organization's technology infrastructure to ensure the availability of information to authorized users. Unfortunately, phishing attacks threaten this availability. Successful phishing attacks could potentially lock or shut down an organization's systems. Consequently, authorized users will not be able to access data.

Therefore, IT specialists of an organization need to properly maintain all hardware and software, keep current with the latest operating system and appliance upgrades (like firewalls, routers, etc.), apply access controls, utilize data monitoring and redundancy, and create a disaster recovery plan.

Recommended Security Steps

Knowing how phishing attacks work and the motivation behind them is key to spotting potential scams. As a best course of action, it is recommended that individuals and organizations follow the security steps outlined below to avoid being a victim of a phishing scam:

1. Be suspicious of e-mails, text messages, social media posts, and other communication that requests personal or financial information.
2. Be cautious of communication that is marked urgent or has a threatening tone.
3. Do not open e-mail attachments or click links from unknown senders. You may inadvertently download malware or be taken to a fraudulent website. It is good practice to only open attachments when you are expecting them, as well as open a web browser and type in the URL rather than click a link in the e-mail.
4. Review e-mails carefully to check the sender's e-mail address, grammar mistakes, spelling errors, and incorrect formatting.
5. Do not divulge personal information over the phone unless you initiate the call.
6. Beware of sudden changes to wiring instructions or business procedures. Be sure to verify any change requests by phone or in-person. Do not use the phone number or other contact information contained in the e-mail.
7. Keep your operating system, firewall, and other security appliances up-to-date.
8. Make sure the security definitions of your anti-malware and anti-virus programs are current.
9. Use two-factor authentication, security tokens, and/or complex pass phrases.
10. Report scam incidents to office management, IT, and/or the IC3.

This is not a full list of security steps to avoid phishing scams, but it is a good start. It is important to stay current on the latest phishing attacks from security experts in order to learn how the scam works and what security steps they recommend to avoid such scams.

Conclusion

As more confidential information is being stored online, access to it needs to be protected from cybercriminals who want to misuse that information for fraudulent purposes. A common technique that cybercriminals use to obtain personal and financial information from victims is through phishing. Phishing is when a cybercriminal poses as trusted and legitimate entity in order to trick victims into revealing personal and financial information like credit card numbers, passwords, and social security numbers. Typically, phishing scams involve the use of e-mail, but phishers are turning to social media and messaging services to execute their scams.

The process of a phishing attack starts with a plan by cybercriminals. Phishers pick a target and gather information on the individual or organization. Next, is the setup in which phishers design a malicious e-mail and/or website. Third, phishers initiate the attack by sending the e-mail to the target. Fourth, is the collection of data supplied by the victim. Lastly, phishers use the information to commit illegal transactions, identity theft, or other fraud.

Phishers use social engineering tactics that prey on human nature to illicit private information from victims. The social influence framework introduced by social psychologist, Robert Cialdini, explains why people are so susceptible to phishing scams. He states that six social influence principles are often misused as "weapons of influence" (Muscanell et. al, 2014). These principles include: 1. Liking, 2. Authority, 3. Scarcity, 4. Social Proof, 5. Reciprocity, and 6. Commitment and consistency. As a result, security experts need to consider both the technical and human elements when designing a cybersecurity policy and user training.

It is essential that institutions develop and implement a cybersecurity policy that addresses threats like phishing. The damage posed by phishing attacks can mean the loss of data, money, identity, reputation, consumer trust, and intellectual property. No organization is too big or too small to have a cybersecurity policy. Everyone is a target. The goal of a cybersecurity policy should be to protect and preserve its information and technology infrastructure. The scope of the policy should include anyone with access to a company's network such as employees, vendors, contractors, etc. Policymakers should use the CIA model as a guide for developing a comprehensive information security policy. It should focus on how to keep data confidential, list security measures to safeguard the integrity of data, and ensure availability of information to authorized users.

Individuals, businesses, and governments need to remain vigilant against phishing attacks and other cyber threats. Cybersecurity policies and security awareness programs are ways to defend against cyber-attacks. However, it is important that people do not become overconfident with these methods and become complacent. As technology advances, so do the strategies of cybercriminals. They are always planning new strategies of attack and looking for loopholes in technology. Therefore, individuals and organizations need to keep up with the changing landscape of cyber threats like phishing and technology.

References

APWG. (2019). Phishing Activity Trends Report, 4th Quarter 2018. *APWG*. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q4_2018.pdf

Davis, Jessica. (2019). Phishing Attack Breaches Data of 30,000 Memorial Hospital Patients. *HealthITSecurity*. Retrieved from https://healthitsecurity.com/news/phishing-attack-breaches-data-of-30000-memorial-hospital-patients

Dolmetsch, Chris. (2019). Facebook-Google Scammer Pleads Guilty in $121 Million Theft. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2019-03-20/man-pleads-guilty-in-100-million-scam-of-facebook-and-google

FBI. (2019). 2018 Internet Crime Report. *IC3*. Retrieved from https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf

Gupta, B., Tewari, A., Jain, A., & Agrawal, D. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing & Applications*, *28*(12), 3629–3654. Retrieved from https://dom.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=125580514&site=ehost-live&scope=site

Haughn, Matthew & Gibilisco, Stan. (2014). Confidentiality, Integrity, and Availability (CIA triad). *WhatIs-TechTarget*. Retrieved from https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Huddleston, Jr., Tom. (2019). How this scammer used phishing emails to steal over $100 million from Google and Facebook. *CNBC Make It*. Retrieved from https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html

Krebs, Brian. (2014a). Target Hackers Broke in Via HVAC Company. *KrebsonSecurity*. Retrieved from https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Krebs, Brian. (2014b). Email Attack on Vendor Set Up Breach at Target. *KrebsonSecurity*. Retrieved from https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

McGee, Marianne Kolbasuk. (2016). L.A. County: Major Breach Stemmed from Phishing Attack. *Bank Info Security*. Retrieved from https://www.bankinfosecurity.com/la-county-major-breach-stemmed-from-phishing-attack-a-9595

Muscanell, N. L., Guadagno, R. E., & Murphy, S. (2014). Weapons of Influence Misused: A Social Influence Analysis of Why People Fall Prey to Internet Scams. *Social & Personality Psychology Compass*, *8*(7), 388–396. Retrieved from https://doi-org.dom.idm.oclc.org/10.1111/spc3.12115

Newman, Lily Hay. (2017). Phishing Schemes Are Using Encrypted Sites to Seem Legit. *Wired*. Retrieved from https://www.wired.com/story/phishing-schemes-use-encrypted-sites-to-seem-legit/

Piscitello, Dave. (2019). The New Face of Phishing. *APWG*. Retrieved from https://www.antiphishing.org/apwg-news-center/newfaceofphishing

Roberts, Jeff John. (2017). Exclusive: Facebook and Google Were Victims of $100M Payment Scam. *Fortune*. Retrieved from http://fortune.com/2017/04/27/facebook-google-rimasauskas/

SonicWall Inc. (2018). Phishing in the Age of SaaS: The Essential Guide for Businesses and Users. *SonicWall Inc*. Retrieved from https://www.sonicwall.com/resources/ebook/phishing-in-the-age-of-saas/

Volkman, Elliot. (2019). 2019 Phishing Trends & Intelligence Report: The Growing Social Engineering Threat. *PhishLabs*. Retrieved from https://info.phishlabs.com/blog/2019-phishing-trends-intelligence-report-the-evolving-threat

Wright, R. T., & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems*, *27*(1), 273–303. Retrieved from https://doi-org.dom.idm.oclc.org/10.2753/MIS0742-1222270111