# PHISHING OUR CLIENTS: A STEP TOWARD IMPROVING TRAINING VIA SOCIAL ENGINEERING

**Kevin J. Slonka, Sc.D., Pennsylvania Highlands Community College, kslonka@pennhighlands.edu**
**Brian F. Shrift, CISSP, Precision Business Solutions, brian.shrift@precisionbs.com**

## ABSTRACT

*It has been over 20 years since the first phishing attack was executed, yet anecdotal evidence suggests that employees of small businesses are unable to detect and appropriately deal with phishing emails. In an effort to improve their security and awareness training, the researchers conducted a study whereby their own clients were subjected to a phishing attack. The results of this study will determine certain differences between the business sectors that were attacked.*

**Keywords**: Phishing, Social Engineering, Security, Training, Credentials, Spear Phishing

## INTRODUCTION

Privacy issues have plagued the Internet for many years. What once was a means for academia and the military to share information, the Internet has been adopted by most of the developed world. The ease of access to the Internet and the ease of publishing content to the Internet, especially by those untrained in its proper use, can lead to private and devastating information ending up in the wrong hands. Most people with an email account can recount times when random emails have appeared in their inbox claiming that their PayPal account has been locked, their bank is offering free money for opening a new account, or a Nigerian prince happens to have a small fortune with their name on it. Each of these seemingly random emails have one thing in common, they are phishing emails.

The attacker's goal is to craft an email that will appeal to the victim in such a way that they will voluntarily divulge information, such as usernames and passwords. Because of how critical this information can be, especially if the usernames and passwords are to systems that contain financial, medical, or other important data, organizations need to ensure that their employees are competent enough with their usage of the Internet so as not to fall victim to these attacks. Much research has been done into phishing attacks but few researchers are willing to launch so-called deception attacks against others due to the ethical implications. Although launching an in-the-wild phishing attack for research purposes is classified as deception research, many in the field argue that it is necessary in order to study the actual attributes of such an attack. Deception research, when conducted properly, has minimal harm (no more than any person is submitted to in their normal life) and is completely legal (El-Din, 2012; Finn & Jakobsson, 2007; Lenz, 2007).

Previous research has suggested that demographics have no statistically significant correlation with vulnerability to phishing (Dhamija, Tygar, & Hearst, 2006). Because of these results this research will not focus on demographics; instead, this research will assess the depth to which persons fall victim to phishing attacks as a means to suggest alterations to current security training.

In order to achieve this goal, the spear phishing campaign that will be executed as part of this research will target clients of the Managed Service Provider (MSP) Precision Business Solutions (PrecisionBS). The executors of this research and the spear phishing campaign (herein known as the researchers) are PrecisionBS's president and his senior systems engineer. The researchers will attempt to socially engineer their own clients, acting as outsiders with no internal knowledge of the company so as to execute a campaign with all attributes of a campaign executed by malicious attackers.

## LITERATURE REVIEW

### Social Engineering

Social engineering is not a new concept. Though the concept has received greater attention due to the Internet and on-line scams, Baron and Sanders (1975) speak of social engineering as early as the mid-seventies. In their study,

social engineering was spoken of in terms of people being "manipulated to ignore their own interest if it conflicts with the requested activity" (p. 283). The main idea was that people will cooperate with the decision of the group despite their conscience guiding them in a different direction.

Weinberg (1967), almost a decade earlier, introduced the same issue. In order to solve any social problem "one must persuade many people to behave differently than they have behaved in the past" (p. 7). Weinberg's goal was to offer technological fixes for social problems in an effort to curb the need for social engineers. A difference of definition arises with this notion. Baron and Sanders (1975) are using, or at least referring to, the term social engineer pejoratively. Weinberg (1967), however, uses the term in the laudative sense. For Weinberg, a social engineer is a person who can, literally, engineer social situations in order to solve problems.

It is clear that a dichotomy exists. Social engineering has both positive and negative connotations depending on the rhetor. In the post-2000 world, literature suggests that the separation is based on content area. On one side, when the term social engineering appears in literature relating to information technology, the term is pejorative (Balzarotti, et al., 2010; Elohor, Emamuzo, Folake, & Fasiku, 2011; Lakshmi & Vijaya, 2011). Conversely, in other areas, such as biology and the social sciences, the term social engineer can assume a laudative connotation (Feng, Ljungwall, & Guo, 2011; Kitano, Ghosh, & Matsuoka, 2011; Wehmeier, 2009). For the purposes of this research, due to the technology aspect, social engineering will be used in its pejorative sense.

**Psychological Engineering**

"Psychoanalysis is almost wholly absent from the persuasive computing literature" (Blythe, Petrie, and Clark, 2011, p. 3476); however, due to phishers utilizing the same persuasive methods as advertisers (one of which being direct instead of general addressing), attacks can be aimed at one's "hidden desires" (p. 3476) instead of their rational thoughts. This opens the door for the work of Freud and Bernays to be applied to social engineering, specifically phishing (2011).

Bernays, the nephew of Freud, utilized his uncle's psychoanalytic theories in order to become the father of public relations. As Philbin (2012) succinctly summarizes, "[...] Bernays substituted the idea he desired for current ideas, fabricating dramatic 'high spot' events and contrived circumstances that translated these ideas into effective and dramatic communications" (p. 24). Knowingly or not, this is the same principle that Mitnick used in his, now infamous, social engineering attacks. Eliciting private information from the human mind is like playing a "chess game" (Mitnick & Simon, 2002, p. 41). Bernays used these tactics to convince people into believing whatever idea he had during a specific campaign; likewise, social engineers use the same tactics to trick their victims into giving up valuable information. Because this is an unexplored area in information security literature, just as Jesus taught his Disciples to be "fishers of men" (Matthew 4:19, New American Standard Bible), future research into the works of Freud and Bernays can teach social engineers to be phishers of men.

**General Privacy**

Internet websites have seen a rise in an area of security issues previously foreign: privacy. Though one may categorize privacy issues as foreign, they have been on the minds of legal scholars for hundreds of years. Warren and Brandeis (1890) advocated for new laws to cover rights of privacy, which weren't taken into consideration in the late 1800's in the United States. There was a clear distinction between that which arbitrarily existed in one's mind or on one's countenance and that which had been preserved in writing or some other, more permanent, medium. The former was argued to "receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression" (p. 206). These rights, though not explicitly afforded to citizens of the United States, had been afforded to French citizens since legislation enacted on the 11th of May, 1868. Part of this legislation, "Toute publication dans un écrit periodique relative à un fait de la vie priveé constitue une contravention punie d'un amende de cinq cent francs" (as cited in Warren & Brandeis, 1890, p. 214), specifically sets a fine for items published that are considered a matter of privacy.

Warren and Brandeis (1890) argue that even though matters of privacy are not explicitly stated in the laws of the United States they are covered (both laws and punishments) under the laws of libel and defamation and the law of literary and artistic property. These issues existed long before the advent of the Internet and mass communication as known in 2016. Godkin (1890) took a fatalistic approach to protecting one's privacy, arguing that as long as one

can make money by invading the privacy of others the invasions never will stop. These issues discussed over a century ago are the same issues currently being discussed in regard to one's right to privacy on Internet websites.

### Phishing

Phishing is an email attack usually purported by mass mailing fraudulent emails to many people in the hopes of divesting those who are untrained in this type of fraud detection of their personal property (Krejčiřová & Dvořák, 2013). These types of attacks begin with a fraudulent email that tricks a person, utilizing some of the previously covered psychological engineering techniques, into divulging their personal information to the attacker via some means: replying to the email, a phone call, a visit to a fraudulent website, etc. Once the attacker has gained enough personal information havoc can be wreaked on the victim's digital life. The successful attacker gathers enough information to login to the victim's email account(s) and, via further means of social engineering, makes his way into other, more important, accounts, such as banks, credit unions, healthcare, etc. Not only can phishing attacks be used to defraud individuals or companies, the money stolen from victims can be routed to organized crime syndicates or terrorist organizations and used to fund illegal operations, even implicating the victim as a terrorist supporter (Jensen, 2011).

Although phishing on a massive scale can be successful from the attacker's perspective, Jagatic, Johnson, Jakobsson, & Menczer (2007) found that phishing attacks are four times more successful when the victim is solicited by a known acquaintance. This kind of phishing, known as spear phishing, requires more preparation and crafting of the attack to ensure that the phishing email delivered to the victim appears extremely legitimate by offering "inside information" typically not known by outsiders (Ashenden, 2016; "Spear phishers", 2009).

## METHODOLOGY

### Research Questions

R1. To what depth of compromise do targets of spear phishing attacks descend?
R2. What are the differences in compromise between compromised company types?

### Population and Timeframe

This spear phishing exercise studied multiple clients of the MSP PrecisionBS. Since the purpose of this exercise was to execute an attack as an outsider, victim email addresses were gathered via means available to any person with an Internet connection: websites, social networks, available databases, etc. Victims were only selected if they showed some connection to the MSP via those means. The number of email addresses collected totaled 1199; however, due to some emails being undeliverable, the total population that received the spear phishing email was 1174.

The spear phishing campaign began on Thursday, March 31, 2016 with all phishing emails being sent and ended on Saturday, April 16, 2016 with the fraudulent website linked within the emails becoming unavailable. The electronic nature of the campaign allowed for completion at the participants' convenience. This ensured that specific days or times were not targeted, which would have been contrary to the nature of this research.

### Planning the Campaign

In order to answer the research questions, the objectives needed to be explicitly defined (Dodge, Carver, & Ferguson, 2007). The campaign measured three items:

1. Clicks on the email's spear phishing hyperlink
2. Submissions of the website form that asks for personal information
3. Clicks on other hyperlinks after accessing the website form

Measuring these three items allowed the researchers to determine on how many levels the spear phishing campaign succeeded. By measuring objective 1 the number of victims were separated from the total population. This objective was critical due to the existence of drive-by infections that can occur simply by visiting a malicious website. Objective

2 was the ultimate purpose of this study. By submitting personal information via the malicious website form the victims exhibited not only an inability to detect a phishing email but also an inability to detect fraudulent websites asking for information that normally should not be provided over the public Internet. Measuring objective 3 determined any further interaction with the malicious website by logging when a victim clicked other hyperlinks. Similarly to objective 1, following hyperlinks from a malicious website can lead to drive-by infections as well as other issues, such as cookie stealing and session hijacking.

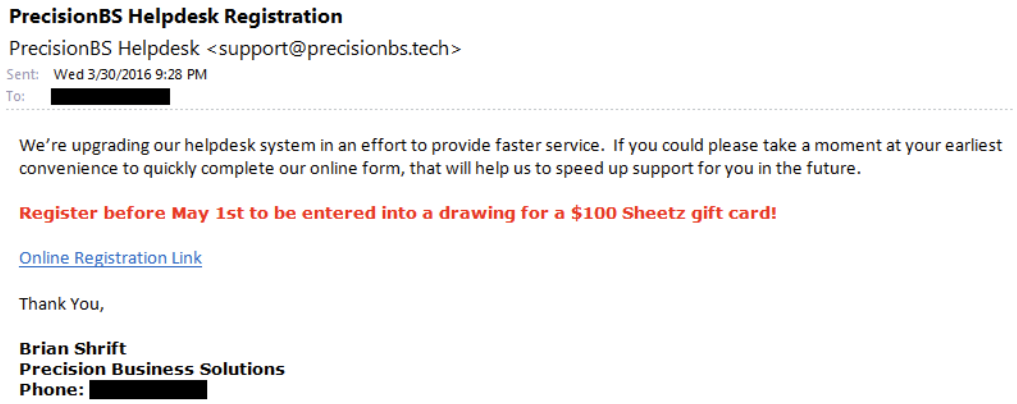
**Crafting the Phishing Spear**

To preserve authenticity and limit suspicion of the phishing email, the design of the phishing email followed the work of Wright, Chakraborty, Basoglu, & Marett (2010), who exposed a list of cues that lead people to believe that an email is malicious. Some of the cues avoided by this study were not giving substantiated reasons for requesting the personal information, the urgency implied in the email not matching the perceived urgency of the situation, and the appearance of the email being unauthentic.

The potential victim's initial encounter with the phishing email was the appearance of the email in the victim's inbox. If the victim was to open the email its appearance in their inbox must be authentic. It is reasonable to assume that an attacker could have acquired any number of random emails sent by PrecisionBS. Simply by acquiring a random group of emails the attacker could have gathered many crucial pieces of information, such as the From Address, the From Name, typical Subject lines, and typical message contents for mass emails. Using this information, the researchers constructed an email header that would cause the least amount of suspicion (2010).

Since this attack did not simulate a compromise of the PrecisionBS primary domain, the researchers registered a similar domain, precisionbs.tech, with GoDaddy Operating Company, LLC. This gave the researchers the ability to house a website and database in the GoDaddy datacenter and utilize a GoDaddy email server to send the phishing email. From the gathered data, the researchers chose "PrecisionBS Support" as the From Name on the email and "PrecisionBS Helpdesk Registration" as the Subject line (the content of the email included a request to register for their new helpdesk system, a reasonable request). The most common From Address of the gathered emails was "support@precisionbs.com". While it would have been technologically simple to spoof the From Address of the phishing email so that it appeared like it was sent from the precisionbs.com domain, many email servers have spam filters that flag messages where the From Address does not match the domain of the originating email (recall, the phishing email was sent through a precisionbs.tech mail server). In order to ensure that the phishing email had the lowest chance of being flagged by a spam filter the researchers set the From Address to "support@precisionbs.tech". While the victim could have noticed that the .tech domain differed from the normal .com domain, this cue is was a small price to pay for ensuring that the most amount of phishing emails were correctly delivered to the victims' inboxes.

Just as important as crafting an authentic email header is crafting an authentic email body (2010). Previous research has exposed three main goals for which to strive when attempting to create an authentic and actionable email body: the body must include clear and explicit instructions detailing what the attacker wants the victim to do upon reading the email (Perloff, 2007; Trenholm, 1989), provoking emotional arousal, such as by adding time pressures, will help elicit a quick, careless action on the part of the victim (Verplanken, 1993), and other internal staff should not be referenced in order to preserve trust in the company (Dodge, Carver, & Ferguson, 2007; Kumaraguru et al., 2009). Figure 1 depicts the body of the phishing email that was constructed to abide by the aforementioned goals.



**PrecisionBS Helpdesk Registration**

PrecisionBS Helpdesk <support@precisionbs.tech>

Sent: Wed 3/30/2016 9:28 PM

To: [redacted]

We're upgrading our helpdesk system in an effort to provide faster service. If you could please take a moment at your earliest convenience to quickly complete our online form, that will help us to speed up support for you in the future.

**Register before May 1st to be entered into a drawing for a $100 Sheetz gift card!**

Online Registration Link

Thank You,

**Brian Shrift**
**Precision Business Solutions**
**Phone:** [redacted]

*Figure 1*. Body of the phishing email.

The body of the phishing email refrained from mentioning any other staff of PrecisionBS, added a sense of urgency by offering a chance at a gift card for completing the malicious form before a certain date, and gave clear instructions to the victim. In addition to these three goals, the researchers added additional elements to ensure that the email's authenticity was at its maximum. Nothing was misspelled or used improper grammar (a common cue seen in mass phishing attempts), the hyperlink to the malicious form (hosted at the precisionbs.tech website) was disguised by the words "Online Registration Link", and the exact email signature of the PrecisionBS president was added to the bottom. This signature was one of the elements gathered via the same means as the email header information and could have been obtained by anyone able to access a legitimate email from PrecisionBS.

Other than the different domain cue, advanced users may have realized that the SMTP headers of a suspicious email could be examined for IP Address information, which could be used to generally locate the geographical source of the email. The phishing emails originated from the IP address 50.248.75.209. Were one to execute a WHOIS query on that IP, the results would show that the IP Address is owned by Comcast Cable Communications Holdings, Inc. in Pennsylvania, thus allaying any suspicion of an offshore attack.

The SMTP headers also would have made the use of the .tech domain more prevalent, possibly piquing the interest of savvy victims. Were one to execute a WHOIS query on the precisionbs.tech domain an error would occur due to the majority of WHOIS servers not being able to answer queries for the .tech TLD. As a last resort, the savvy victim could have determined the IP Address for the precisionbs.tech domain and executed a WHOIS query using that IP Address, which would have given them information on the hosting provider of the precisionbs.tech website. The website was hosted by GoDaddy, a trusted website hosting company and reasonable provider for PrecisionBS.

The researchers exerted maximum effort in the crafting of the phishing email and limited the suspicious cues to a single oddity, the use of the non-standard, but plausible, precisionbs.tech domain.

**Crafting the Attack Website**

To exhibit the same authenticity for the website as the email the researchers crafted the website to be identical to a publicly available precisionbs.com form that asked for similar information. This allowed for all aforementioned authenticity goals to be met. To ensure that this website was created in the same manner as an outsider, the researchers did not utilize their internal access to precisionbs.com servers to copy code for the website. Instead, the precisionbs.com form website was scraped using the "wget" utility and the code and resources were modified so they functioned under the new precisionbs.tech domain name. The result of this process was a perfect replica of the precisionbs.com website with modified wording to fit the spear phishing campaign.

Although the website front-end could be argued to be the most crucial of the campaign since it would bear the most interaction time by the victims the back-end code could be argued to be even more critical. Without proper back-end code to control how the website functioned the objectives of this campaign could not have been met. Sections critical to the satisfying of the campaign objectives will be discussed in detail.

The first section of code enabled the ability to track who clicked the hyperlink in the email and accessed the website. As will be explained in a future section, the email address was encoded into the hyperlink so that each victim had a unique hyperlink in their email. Upon clicking the hyperlink and accessing the website the back-end code created an entry in the database to log that particular website access. Upon a normal page access (clicking on the hyperlink from the email), the code in Table 1 looked for a GET variable named "form", which contained the encoded email address for each user. It then decoded it and determined the IP address of the victim. Finally, this information was logged in the database with "access" entered in the column used to delineate the type of log entry. This allowed the researchers to find all website accesses and determine by whom the website was accessed. In addition, all log entries were automatically timestamped by the database.

The next critical section of code was the researchers' answer to the suggestions of Dodge, Carver, & Ferguson (2007) and Kumaraguru et al. (2009), who suggested that when conducting deception research, such as a phishing campaign, it is of paramount importance to maintain the victim's privacy. Steps should be taken to ensure that no data is leaked outside of the company. Since this study's purpose was to simulate credential stealing the researchers ensured that any usernames and passwords entered by the victims were deleted in the client browser before any data began to transmit across the Internet to the web server hosting the malicious website. Even though the researchers secured the website with a valid SSL certificate through GoDaddy to ensure all communications between the victim and the web server were encrypted, this further step was taken to ensure that no credentials were ever transmitted across the Internet. A Javascript function was called when the victim clicked the Submit button on the form. Both username and password textboxes were checked to see if they contained values and, if so, the values were rewritten to a series of asterisks: eight asterisks to signify that the victim entered a value and nine asterisks to signify that the textbox was left blank. Once the sensitive values were removed the form was submitted and the data transmitted to the web server.

It is important to note that the victim would see the values of these two textboxes update to asterisks when they clicked the Submit button (a common occurrence on some web forms with sensitive information). Because of this, the sequences of eight and nine asterisks were chosen so that it was unlikely that the victim would have detected a difference.

The third critical piece of code handled the form submission. Upon the victim clicking the Submit button, which created an HTTP POST request to the web server instead of the normal HTTP GET request, the code read all values supplied by the user via the form and saved them for later processing. These values included the series of asterisks for the username and password, which were converted to "yes" or "no" to be saved in the database. Once the values were stored in the database, the victim was redirected to the legitimate precisionbs.com website. It was the researchers' hope that the victim failed to notice that the malicious form was hosted on a precisionbs.tech website instead of precisionbs.com.

The last critical piece of code allowed the researchers to measure if a victim accessed the malicious website but clicked any of the other links rather than submitting the form. Every hyperlink on the web page was altered so that the HREF attribute of the anchor tag was "#", which usually would precede a reference to an anchor on the same page but in this case would do nothing due to the lack of a reference after the symbol. Instead, Javascript was added to the anchor tag using the onClick method to execute the "redir" function. The "redir" function took a valid URL as an argument, encoded it in base64, and sent it along with the encoded victim email address in an HTTP GET request to a PHP script on the web server, redirect.php. This PHP script acted as a middle man in the hyperlink process by logging the click to the database before redirecting the victim's browser to the intended web page. These four critical pieces of code allowed the researchers' spear phishing campaign to meet their three objectives and have a database full of data on which to run statistical analyses in order to answer the research questions.

**Throwing the Spears**

With the phishing email constructed and the attack website ready to divest victims of their personal information, the last puzzle piece was the ability to send the phishing emails to every user in the previously constructed email list in an automated fashion. Because the sending of emails needed to be executable by either of the researchers, a script that could have been executed on the Windows operating system was required. Powershell was selected as the language of choice for the script due to its built-in methods for sending email. After setting the required

information for the email header, the script looped through each email address in the file that contained the entire list of email addresses. For every email address in the file the script constructed an email message as previously described, sent the email, and waited a random number of seconds before continuing to prevent the GoDaddy email server from becoming overwhelmed with requests and possibly flagging our system as spam, which would have halted the entire campaign.

**After the Attack**

A critical part of deception research conducted for the purposes of training is to notify those who were a part of the study of the execution and findings of the study (Kumaraguru et al., 2009). As part of keeping participants from more harm than they'd encounter during a normal day the researchers created a plan for making all participants aware of the study. The plan involved two parts: a security and awareness training video was produced that, among other items, included details on phishing and the current study and a larger, in-person, presentation was given by the researchers at a public event sponsored by the local chamber of commerce's Small Business Council, which any member of the public could have attended.

## DATA ANALYSIS

Answering the research questions required the addition of several columns of data. The first column was a nominal data type column for the normalized company name. Part of the data cleaning process was to ensure that every page access was attributed to the appropriate company and that name needed to be consistent in order for the statistics to calculate the correct results. The next column was a nominal data type column for company type. Each company was categorized into their business area (e.g., healthcare, finance, etc.) based on the North American Industry Classification System ("2012 NAICS", 2011) and that category was stored in the company type column. The additional columns enabled the researchers to run the appropriate statistical analyses in order to answer the second research question.

Those statistical analyses were dependent on the data itself, however. Descriptive statistics and frequencies were run on the data to check for bad data and outliers, of which there were none. In addition, whether or not the parametric statistical analyses were run depended on the normality of the data. The Skewness and Kurtosis values of the scale variables indicated that the data was non-normal; only the non-parametric tests were used.

**Research Question Analysis**

**R1. To what depth of compromise do targets of spear phishing attacks descend?** Of the 1174 targets, the phishing website was accessed by 240 distinct people (a 20.4% success rate) accounting for 493 total interactions. Of those interactions, 167 were form submissions, meaning that the victim not only clicked the email hyperlink to access the website but also clicked the submit button on the form. It is also interesting to note that four of the interactions were page clicks, meaning that the victim visited the website and clicked on a different hyperlink on the page rather than submitting the form.

71 distinct companies were represented in the sub-population of interactions. The top five interacting companies represented almost 30% of the total interactions. In addition, since the companies were categorized into 14 groups based on their business area, the website interactions were grouped based on those categories. Employees in the healthcare industry comprised the largest group of victims interacting with the phishing website at 33.3% (164 interactions), 20.5% more than the next largest group. From the total interaction population of 493, 30.8% (152) submitted the form providing both their username and password.

While looking at the data in terms of the total interaction population is helpful, better conclusions can be made by narrowing the population to only those interactions that resulted in the sending of credentials. The top four compromised companies were, together, 30.9% of all compromised companies. Once again, healthcare companies were the largest group with 49 unique credentials phished (32.2%) with the next closest group of compromised companies at 25 (16.4%).

Of the entire population that received the phishing email (1149), 12.9% descended through multiple layers of compromise and divulged their credentials.

**R2. What are the differences in compromise between compromised company types?** A Kruskal-Wallis test was run on the company types and whether or not each victim submitted his credentials by first using the password column and second by using a calculated index (e.g., 0=no credentials, 1=username or password, 2=username and password). Both findings were not significant, p=.433 and p=.365 and respectively, suggesting that there was no significant difference between company types.

## DISCUSSION

Companies' level of compromise due to a spear phishing campaign has been documented throughout this study. Little academic research currently exists on this topic due to its classification as "deception research". The purpose of this study was two-fold: to add to the limited body of knowledge on spear phishing attacks and to gain insight into improving security and awareness training methods so that compromise due to phishing attacks can be minimized.

Though R1 was answered strictly using descriptive statistics and frequencies, it allowed the researchers to gain critical insight into their client base. While the 20.4% success rate of victims being deceived by the attack may seem low, the result is truly staggering. Clients from 71 different companies representing 14 different business sectors fell victim to this attack on some level, with 152 clients willingly divulging their usernames and passwords. While many may scoff at the idea that giving away their credentials to a system behind a firewall is a serious issue, this feeling cannot be further from the truth.

Were this attack to be conducted by a malicious actor, the information submitted using the phishing website would be a gold mine. Names, companies, and email addresses can be used in social engineering attacks. With many companies offering some sort of remote access to company resources, the divulged information could help attackers reset passwords and gain access to email accounts or even systems behind a firewall. Once an attacker has access to these items, it's game over for the company. The attacker can exfiltrate electronic health records, financial records, and worse, now that critical care devices are connected to hospital networks attackers now have inside access that can allow them to access ventilators, IVs, and other devices. Serious harm to patients, even death, can be brought about because a single physician working out of his small office in the middle of nowhere, Pennsylvania was tricked into submitting his credentials to a malicious website.

Although a 12.9% rate of credential stealing seems low, four of the top five compromised industries are those with critical information about everyone in their service area, from school-children to CEOs. The results of R1 cut to the core of the issue: something needs to be done about peoples' lack of understanding of information security issues.

The results of R2 initially seemed disheartening, but negative results are still results. In this case, the results will help the researchers in future endeavors training their clients on the dangers of the Internet. While R1 showed that many people are still vulnerable to phishing attacks, R2 suggests that one's vulnerability is not affected by the business sector in which one works. This is critical information. The researchers are now able to create security and awareness trainings that are generic (i.e., specific trainings on phishing attacks per business sector are unnecessary). Because PrecisionBS is a MSP for many business sectors, the researchers can devote their time to creating a single, all-encompassing training rather than develop 14+ different trainings.

### Limitations and Recommendations

Various items could have been executed differently in order to produce better results. While this study measured three objectives, a fourth objective could have provided more intricate results. As was previously explained, the population consisted of all who received the email. The researchers' measuring began with the victim clicking on the email hyperlink; however, the compromise process actually began with the victim opening the email. A method of tracking whether or not a victim opened the email, such as adding a transparent GIF image in the email that, when loaded, would have logged an entry in the database, would have given the researchers the ability to calculate better results about the population by adding the "read but didn't click" dimension to the data.

Furthermore, a more regimented attack could have been crafted such that the number of phishing emails sent per business sector were near even. The current research was conducted from the perspective of a would-be attacker,

with no knowledge of the victims other than they had a connection to PrecisionBS. A follow-up study could be conducted where the attackers have inside knowledge (i.e., a typical corporate security exercise). Such a study could validate the results of this study ensuring that all business sectors are on equal grounds.

In addition to the aforementioned future study, further studies should be conducted to determine why people are vulnerable to these types of attacks. The literature review revealed that no data currently exists about malicious social engineering in the realm of psychoanalysis. Completely answering "why" would entail a more thorough analysis of the human mind. An expert in the field of psychology should be contracted to participate in the conducting of this research.

**Conclusion**

The purpose of this study was to analyze PrecisionBS's clients' susceptibility to phishing attacks. Overall, as of 2016, a significant portion of industry is still vulnerable to phishing attacks. These results were assumed but are now backed by research and, as such, more reliable.

The results of this study can be used by a wide array of parties. First, as previously mentioned, this study can serve as a base on which future researchers can create new, improved studies. Second, educational institutions should heed the warnings of this research. Some sort of awareness training needs to be integrated into post-secondary curricula. Last, businesses who offer Internet access to their employees must also offer awareness training, as the integrity of their corporate infrastructure lies in the ability of their employees to detect and ignore malicious email.

This study adds to the limited body of knowledge in this domain and creates a base on which to conduct future studies in order to better understand this problem and make substantial strides in mitigation of the risks. People are the weakest link. We can train them; we have the technology.

**REFERENCES**

(2009, April 1). *Spear phishers: Angling to steal your financial info*. Retrieved from https://www.fbi.gov/news/stories/2009/april/spearphishing_040109

(2011, Nov 7). *2012 NAICS*. Retrieved from http://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012

Ashenden, D. (2016). The Human Shield. *The Chemical Engineer*, (896), 22-25.

Balzarotti, D., Banks, G., Cova, M., Felmetsger, V., Kemmerer, R., Robertson, W., ... Vigna, G. (2010). An experience in testing the security of real-world electronic voting systems. *IEEE Transactions on Software Engineering, 36*(4), 453-473.

Baron, R. S. & Sanders, G. (1975). Group decision as a technique for obtaining compliance: Some added considerations concerning how altruism leads to callousness. *Journal of Applied Social Psychology, 5*(4), 281-295.

Blythe, M., Petrie, H., & Clark, J. A. (2011). Proceedings of the 2011 annual conference on human factors in computing systems: *F for fake: Four studies on how we fall for phish*. New York, NY: ACM.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Proceedings of the Conference on Human Factors in Computing Systems: *Why phishing works*. Montreal, Quebec, Canada: CHI.

Dodge, J., Carver, C., and Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73–80.

El-Din, R. S. (2012). Proceedings of BCS HCI 2012 Workshops: *To deceive or not to deceive! Ethical questions in phishing research*. Edgbaston, Birmingham, UK: HCI.

Elohor, O. O., Emamuzo, O., Folake, A., & Fasiku, A. I. (2011). A secured chat system with authentication technique as RSA digital signature. *International Journal of Computer Science and Information Security, 9*(10), 123-130.

Feng, X., Ljungwall, C., & Guo, S. (2011). Re-interpreting the "Chinese Miracle." *International Journal on World Peace, 28*(1), 7-40.

Finn, P. & Jakobson, M. (2007). Designing and Conducting Phishing Experiments. *IEEE Technology and Society, Special Issue on Usability and Security*. 1-21.

Godkin, E. L. (1890, July). The rights of the citizen. IV. To his own reputation. *Scribner's Magazine, 8*(1), 58-67.

Jensen, K. (2011). A Matter of Concern: Kenneth Burke, Phishing, and the Rhetoric of National Insecurity. *Rhetoric Review, 30*(2), 170–190

Kitano, H., Ghosh, S., & Matsuoka, Y. (2011). Social engineering for virtual 'big science' in systems biology. *Nature Chemical Biology, 7*(6), 323-326.

Krejčiřová, L., & Dvořák, J. (2013). PHISHING -- THE THREAT OF INTERNET BANKING. *Scientific Papers Of The University Of Pardubice. Series D, Faculty Of Economics & Administration, 18*(26), 51-65.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). Proceedings of the 5th symposium on usable privacy and security SOUPS '09: *School of phish: a real-world evaluation of anti-phishing training*. New York, NY: ACM.

Lakshmi, S. V. & Vijaya, M. S. (2011). The SVM based interactive tool for predicting phishing websites. *International Journal of Computer Science and Information Security, 9*(10), 58-66.

Lenz, R. (2007). School Conducts Anti-Phishing Research. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/07/22/AR2007072200439.html

Mitnick, K., & Simon, W. (2002). *The art of deception: Controlling the human element of security*. New York, NY: John Wiley & Sons.

Perloff, R. M. (2007). *The dynamics of persuasion: Communication and attitudes in the 21st century*. Hillsdale, NJ: Lawrence Erlbaum.

Philbin, G. (2012). *Edward Bernays and the art of public persuasion: A case study of his work for the American Nurses Association*. (Unpublished doctoral dissertation). Robert Morris University, Pittsburgh, PA.

Trenholm, S. (1989). *Persuasion and social influence*. Englewood Cliffs, NJ: Prentice Hall.

Verplanken, B. (1993). Need for cognition and external information search: Responses to time pressure during decision-making. *Journal of Research in Personality, 27*(3), 238 - 252.

Warren, S. D. & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220.

Wehmeier, S. (2009). Out of the fog and into the future: Directions of public relations, theory building, research, and practice. *Canadian Journal of Communication, 34*(2), 265-282.

Weinberg, A. M. (1967). Can technology replace social engineering? *The American Behavioral Scientist (pre-1986). 10*(9), 7-10.

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where Did They Go Right? Understanding the Deception in Phishing Communications. *Group Decision & Negotiation, 19*(4), 391-416.