2018

Security awareness training in a corporate setting

Nichole Dugan
Iowa State University

Security awareness training in a corporate setting

by

Nichole Dugan

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Information Assurance

Program of Study Committee:
Douglas Jacobson, Major Professor
Mani Mina
Diane Rover

The student author, whose presentation of the scholarship herein was approved by the program of study committee, is solely responsible for the content of this thesis. The Graduate College will ensure this thesis is globally accessible and will not permit alterations after a degree is conferred.

Iowa State University

Ames, Iowa

2018

DEDICATION

This thesis is dedicated to my wonderful husband, Darin Dugan. His support throughout my entire career and especially my master's program has made this entire process possible. He has been an amazing father to our son, and has spent countless hours reviewing papers, giving feedback, and helping me study. None of this would have been possible without him.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

NOMENCLATURE

MFA	Multifactor Authentication
ARIN	American Registry for Internet Numbers
DNS	Domain Name System
AI	Artificial Intelligence
CSC	Critical Security Controls
IDPH	Iowa Department of Public Health

ACKNOWLEDGMENTS

I would like to thank my committee chair, Dr. Douglas Jacobson, and my committee members, Dr. Diane Rover, Dr. Mani Mina, for their support of my work as an off-campus student. I would also like to thank Dr. Thomas Daniels for substituting for Dr. Mina during my final oral exam.

In addition, I would also like to thank Benjamin Holland for his assistance navigating the thesis process and help testing with his students. I want to also offer my appreciation to those who were willing to participate in my surveys and tests doing the escape rooms, without whom this thesis would not have been possible.

ABSTRACT

The 2018 Verizon Data Breach Investigation report indicates that over 90% of common breaches start with a social engineering attack. While organizations are adding security awareness training programs, it is clear these programs are not working. Diverse workforces call for a variety of training options, and different ways to engage users. Programs must ensure users know how they will be contacted by IT staff, and what to do in different scenarios. Users may need to learn the fundamentals of computers and the Internet in order to understand and retain security awareness training. In this work, we propose an interactive security education training aimed at students and industry professionals. In order to reduce barriers to learning we implement our security training in the form of a recent and familiar entertainment form called an "escape room".

CHAPTER 1. INTRODUCTION: THE SOCIAL PROBLEM

Data security is a growing problem as computers have become a necessity in day to day life and business. It is important for security professionals to understand how attackers are targeting their organizations and determine ways to counter their attempts to breach security.

Attackers tend to follow specific patterns when organizing a targeted hack. They perform reconnaissance, scan the external network for vulnerabilities in systems, gain access to resources, try to maintain access, and cover their tracks. Many of the attacker's first steps may be thwarted by diligent IT staff, including quickly applying patches to operating systems and applications, shutting off unused services, and changing default passwords on networking equipment. But even the best IT departments have users in their organizations, and this human component can let an attacker through the front door. The Verizon Data Breach Report indicates that over 90% of all attacks start with a social engineering attack. [1]

An obvious answer to the human problem is to provide training for the users. Users in corporate environments can be diverse, ranging in age from teenagers to near retirement, with many different backgrounds and skillsets. [2] Selecting one training method to suit all employees of an organization would be nearly impossible as different users respond to information in different ways. These differences are highlighted in "Going Spear Phishing: Exploring Embedded Training and Awareness", published by IEEE, users surveyed after clicking on spear phishing emails, responded to training in many different manners. [3] In addition to finding the correct type of training, the amount of time spent on training must be considered. Similarly, the frequency of the training is a concern. Once a year, while a frequent minimum standard, doesn't keep the issue in most people's minds. At the other

extreme once a week might be unnecessary and overwhelming. Additionally, management may be reluctant to have their employees spend an excessive amount of time on security training, as day to day tasks still need to be performed.

Most companies are quick to attempt replacing training with technology, as technology can be purchased and implemented without involvement of the entire organization's staff. While technology has come a long way in helping users protect themselves, including intrusion detection and prevention systems, antivirus software, monitoring tools, and email filtering, human intervention will still be required until machine learning or artificial intelligence can reliably outsmart any attacker. This human intervention often fails, for example, when users are prompted with unfamiliar or repetitive warning messages. Users may often click yes without reading the message, as they have become habituated to the warnings. [3]

While most organizations today have a security awareness training program, they tend to be compliance-based, focused on checking a box to say the organization has security training. In these cases, there is still a large concern with how users are being trained. Training programs may be purchased and implemented in an organization without much thought of how the users will react to the training, or what the users are learning from the training. If the organization and security team haven't considered the training's objectives, and users aren't aware of what they should get out of the training, the likelihood of the program being successful is small. Security awareness programs also tend to focus on telling users what to do without context or explanation. For example, telling users to hover over links in emails is a typical recommendation for training, but this advice may not make sense to a person who doesn't understand how URLs are structured or what they mean. They may

comply with the request, hovering over the link before clicking it, but aren't aware if the URL they are reading is a legitimate one or not.

This paper seeks to find a way to move past compliance-based security awareness training for an organization, explaining how to build a security awareness program that engages users. Research done on this topic focused on how attackers can use social engineering to find ways into a network, common tools designed to help users mitigate an attack, why those tools fail, why typical security awareness training fails, and how to create a better program. The organization studied for this research is the Iowa Department of Public Health (IDPH), a state agency with approximately 400 employees of varying educational levels, ages, and backgrounds with technology. The agency had many security controls in place but was lacking a defined communication strategy between the IT staff and users. A documented standard communication strategy is important because without one it is more likely an attacker can short circuit or work around other security processes.

IDPH employees were required to take a yearly security awareness training done online and split into modules. Each module was ten minutes or less, with a question at the end to determine understanding of the previous module. Different modules were assigned to members of business units to align with their job functionality. Users reported ignoring the training and letting it run in the background. The training had not changed for several years, and the questions at the end of the modules were trivial and allowed the users to answer the question several times until they got the answer correct. Training amongst staff was considered an annoyance and it had outlived its usefulness.

CHAPTER 2. INSIDE THE ATTACK

The first step to understanding what training to focus on, is to learn how hackers determine the best way into a system. Targeted attacks against organizations tend to follow the same pattern of reconnaissance, scanning the external network, gaining access to resources, and covering tracks. [4] This chapter will focus on the first three steps an attacker takes, how these attacks can be mitigated in part by IT, and how attackers can use humans to circumvent these controls.

Reconnaissance

In targeted attacks, hackers will spend time researching everything they can about the organization they are attempting to breach. They will review the victim's website searching for phone numbers, email addresses, employee names, and physical addresses to be used. They will use search engines to find news stories detailing mergers or acquisitions of the company. Using Domain Name System (DNS) tools such as dig and nslookup on the URL of the main website attackers can learn IP addresses, DNS servers and hosting information for the organization. They can then use the American Registry for Internet Numbers (ARIN) to find contact information for the company. Attackers will also review social media sites for the organization to learn about technologies used by the company. For example, an employee posts on LinkedIn that they work for the organization, and the employee lists a proficiency in IIS web servers, or Cisco networking equipment. This can give a hacker insight into the technologies being used at the company. Additionally, attackers can find public social media posts from employees sharing personal information commonly used to answer security questions, such as their first car or first pet, family names or birth dates, etc.

To limit some of the available information, security departments may recommend to business members and executives that information be removed from public facing websites, or prohibit employees' mentioning organization details in resumes and on social media, but this strategy often isn't feasible or enforceable. Additionally, some companies may have a requirement to keep information such as phone numbers and email addresses accessible to the public. It is always important for the security department of companies to be aware of the information that is available and to know how an attacker could use that information against them.

Scanning

After the hacker finishes their reconnaissance stage, they generally move on to the scanning phase of an attack. This scanning phase usually involves doing TCP/UDP scans against a range of IP addresses known to be associated with the target organization. The scan will show active hosts and ports. The attacker can use this information to look for vulnerabilities in systems and attempt to exploit them.

Security departments can do their best to minimize the number of hosts accessible to the internet and remove unused services running on machines, but some things still need to be allowed through, or business may not function. Most current organizations, even small companies, tend to have strategies in place for patching workstations. As Microsoft moved towards creating a monthly release of patches for its Windows operating system, organizations have created programs to ensure workstations and servers in their environments are patched. Many organizations also have vulnerability scanning programs in place, using tools such as Nessus or Tripwire, to find problems before an attacker can.

Although organizations may have addressed the effectiveness of malicious scanning by timely patching, properly configured firewalls, no use of default credentials, and few

exposed services, it is important for an organization to have a mature model for tracking software and hardware on their own network. Without an ongoing inventory, users may introduce security holes without the security department's knowledge by adding unknown and unauthorized hardware or software.

Gaining Access to Resources

In the third stage of an attack, the hacker gains access to resources on the company's network. This can be done by exploiting vulnerabilities, or as shown in most data breach reports, by carrying out social engineering attacks against users of a system. Once the attacker has accumulated email addresses, for example, they can send targeted emails to individual users. If they are aware of the employee's job function and relationship to other employees, they can further customize communications to appear more legitimate.

CHAPTER 3. TECHNOLOGY TO HELP USERS

Technology professionals tend to want to solve all problems with technology, finding it interesting to install new tools and easier than dealing with people. Historically, security departments have grown through the networking teams, as the first line of defense tends to be firewalls and networking equipment. While this is an important first step, networking specialists don't tend to focus on individuals in the organization. Artificial Intelligence (AI) seems like the best solution to help users determine legitimate communications, but AI is still far from where it needs to be to provide proper assistance. Some technology companies have begun adding AI into their antivirus and intrusion detection systems, but user training will be necessary in the near future.

Network Tools

Almost all organizations support a suite of networking tools to dissuade attackers from attempting to break into their networks. Firewalls exist to block access to internal resources, as well as monitor when attackers are targeting them. Intrusion detection and prevention systems also stop or report attacks. Antivirus and antimalware programs are employed to stop malicious software from infecting a host. As network administrators have gotten better at protecting their networks, attackers have changed their methods to breach sensitive resources.

Password Attacks

Passwords are a critical weakness commonly targeted by hackers. Humans who create passwords tend to have a difficult time remembering them, so they tend to use a few common strategies that are easily exploitable. People often use dictionary words, adding a few special characters or numbers to meet password complexity requirements based on the system they

are using. Attackers, using a combination of dictionary lists, rule-based substitution, and brute force can often crack these passwords within a few minutes. Also, as systems are breached, such as LinkedIn in 2012, attackers will post previously cracked passwords online for other hackers to use. Corporate systems attempt to mitigate these issues by forcing users to create longer or more complex passwords, requiring users to change passwords frequently and writing policies that users are not allowed to reuse a password for multiple services. This can be painful for users because it is difficult to come up with long, secure, and memorable passwords, which may lead to poor security practices, such as writing down passwords in simple text files or on paper near their computers.

Password Managers

One technological mitigation to password attacks and complex password policies is for companies to promote a password manager. A password manager program can securely generate, store and retrieve passwords on behalf of the user, protected by one master password or credential. If an organization wishes to implement a password manager enterprise wide, it must determine a product that fits with their goals and user base so it will be widely adopted. A review of ten popular password managers was done, comparing different feature sets. Three were determined to be the easiest to use, and most likely to obtain adoption from the company's users.

Dashlane [5]

- Scans email for known services for which it can store passwords
- Password generator to create strong passwords
- Secure notes storage

- Storage of credit card information and IDs such as driver's licenses and passports
- Emergency contact. If you are incapacitated a predefined trusted contact can gain access to your passwords. The system will warn you first, providing the opportunity to deny access in non-emergency situations.
- Multifactor authentication setup by default

LastPass [6]

- Security Challenge to assess the security of a password
- Notification if email addresses have been involved in security breaches
- Secure notes storage
- Auto form completion
- Emergency contact and allow the trusted individuals access to your accounts. The system gives you time to respond to refuse access, allowing you to deny illegitimate requests.

1Password [7]

- Travel Mode setting. Wipe all secure information from your device when traveling.
- Storage of credit cards
- Secure notes storage
- Sharing of data on devices through generated 34 alpha-numeric secret key

Selecting a password manager for an organization is important for a few different reasons. If the organization provides the password manager for its users, it will need to choose the best fit for the organization based on price and feature set. IT helpdesk staff will

need to be trained on the selected software, as users will likely need assistance at some point. Policies will need to be created around the recommended and supported use of the password manager, including if users will be allowed to store personal passwords in a company provided password manager, and the company's access to or responsibility to provide them in the event of employee separation. Communication would need to be crafted to the users explaining how to use the software, along with ongoing updates to functionality and policy. Without an organization-sanctioned password manager companies may still need to develop a policy on storing work related passwords in a personal password manager. If no recommended password manager is chosen, the help desk may be inundated with questions about many different personal password managers they may not be familiar with or have any ability to support.

Multifactor Authentication

Another technology solution to weak passwords is to implement multifactor authentication (MFA) for the user's work accounts. This adds a second layer into the authentication process, combining something the employee knows, the password, with something the person has, like a cell phone. This helps stop attacks because even if the attacker manages to steal or crack a weak password, they would still need to obtain the second factor required for authentication.

Implementing this in organizations may present different challenges. For example, users may be reluctant to use personal cell phones for organizational multifactor, whether that is an app to install, receiving text messages, or receiving phone calls. Some alternatives may include providing a hardware token for the user, allowing the employee to use their desk phone as a second stage authentication mechanism, providing a company-owned mobile device, and printing one-time codes that can be used.

As with all the solutions mentioned previously, communication would need to be developed to inform employees of how to use MFA, the various options available to provide the second layer of authentication, and what to do if they need assistance. Helpdesk staff would need to be trained on the options available to staff, timelines for rolling out the new features, and any factor reset or temporary bypass options that may exist.

While a promising technological solution to help with lost credentials, multifactor authentication will not prevent users from installing malicious software. MFA also requires user input; the user will need to enter a one-time use code or approve an MFA challenge on their mobile device.

Social Engineering Attacks

Social Engineering attacks comprise the largest vector attackers use to target users. These can be done in several ways, including spear phishing attacks, a targeted email to a specific user, designed gain access to the network or sensitive information the user may possesses. Using an employee's phone number to call them and get information from them is a social engineering attack called vishing.

Many technologies have been implemented into email trying to cut down on bulk spam, but it can be more difficult to identify targeted spear phishing attacks where the email may look legitimate. There are also few technology solutions to vishing, as attackers can spoof phone numbers to make their calls look legitimate.

Technology Conclusions

There are many technological solutions available to help users maintain security. However, implementing these solutions effectively in an organization is more complicated than just buying a product and installing it on the user's machines. Organizational policies may need to be developed to deal with the new technologies, helpdesk staff may need to be

trained on new products, and communications to users will need to be written explaining why the organization is introducing the new technology, how to use the product, and what to do if they have issues.

It has also been found that many users have been habituated to warning messages, clicking through warnings without reading them. [4] Some research has been done in creating polymorphic warning messages, messages that change to look or act differently, which can help, but users still tend to click through them with little comprehension. [3]

Technology limitations are further evidenced in a recent study by Barkly, who found 90% of successful phishing attacks completely bypassed the victim's antivirus and email filtering. 83% of successful attacks bypassed the victim's firewalls, and 55% were successful despite user having previous security awareness training. [9]

It is encouraging to see many technological solutions available, but organizations must understand how to implement these technologies in their environments to have a successful program. While technology is an important component of a company's defense in depth strategy, a solid security awareness training program is also critical.

CHAPTER 4. TRAINING PREPARATION

As mentioned previously, employees in organizations naturally vary in age, race, religion, and economic background, which impacts their learning style. For example, a millennial may respond to playing a game that has lessons, while others may prefer reading case studies on breaches and lessons learned.

Executive level support is vital for any security awareness training that will occur at the organization, as well as determining how much time will realistically be available for training employees. It is also important to consider the culture of the organization before creating training.

Another important item to consider when crafting a security awareness training program is to avoid shaming users who fall victim to attacks or make mistakes. Management may be quick to punish users who fail phishing tests or download malware, but fear rarely leads to positive outcomes. Users may quickly start to fear opening any emails, which could impede their day to day activities.

Survey

Before launching a training program, it may be helpful to do a baseline survey of the organization, trying to determine weaknesses in users' computer literacy. In an example survey, 10 questions were created gauging users' understanding of security basics and attacker approaches. Users should be asked about the following:

- Knowing if they were a target
- Knowing what information about them is publicly available
- Knowing if information posted on social media can be used by attackers
- Understanding physical security

- What to look for in phishing emails
- Knowing how to unshorten URLs
- Understanding URL structure

The survey questions are listed in Appendix A. The survey should be given prior to training and sent to a wide base of users to ensure the organization's diversity has been captured.

Data Breach Report

Another place to gather information about where users need more training is the Verizon Data Breach Investigations Report. The report studies 53,308 security incidents, 2,216 data breaches in 65 countries with 67 organizations reporting to Verizon. [1]

Phishing Emails

According to the report, 4% of people in an organization will click on a link in a phishing email. [1] While this number doesn't seem high, it only takes one person to give an attacker entry into the network where they can do more damage. The report also indicates that once a person has clicked on a link once, they are more likely to be a repeat offender. In the average organization, a user will click on a link in a phishing email within 16 minutes, however, the first person will report the email within 28 minutes. [1] This is a 12 minute lag between the time the malware could enter your system and when it is reported. If the organization's monitoring systems don't capture the infection, many machines could be infected before anyone is made aware of the breach.

The data breach report indicates that 98% of social engineering incidents are from phishing attempts, or pretexting, where the attacker pretends to be someone else. These attacks compromise 93% of breaches and the most common way the attacker starts these attacks is through email. [1]

Creating training for users to understand what emails from the organization look like, how the help desk will contact them, and how to determine legitimate and non-legitimate emails should be the primary focus of any security awareness training program. Employees tend to want to be helpful, but they should be trained to be suspicious as well. Staff who work in human resources and finance are targeted more often than other employees of the organization, so extra training may need to be done with these users.

In addition to having users be aware of phishing emails, they need to be trained on how to report phishing emails. Reporting the emails allows the IT department a chance to do more monitoring or create methods of blocking malicious emails. IT department staff needs to be trained on how to respond to phishing emails as well.

Internal Threats

Another large method of breaches include user error, people sharing data with the wrong recipient, or allowing access to data incorrectly. Another internal threat is misuse of credentials to gather data not intended for them. [1]

Employees should be trained on sending emails and verifying recipient before sending sensitive information. Alternatives to using email to share data may also require training.

Policies regarding privileged account use may also need to be created and shared with employees to ensure awareness of proper use of credentials. All users should be trained on consequences of access data improperly.

Physical Threats

According to the Verizon Data Breach Report, the most common physical threats associated with an organization are the loss of paper documents and laptops. The report also states that the most common place of theft are the employee's work areas.[1] It is important

to train employees about keeping a clean desk and not leaving passwords next to their computers. Employees should also be trained on proper procedures for reporting lost and stolen equipment. 36% of theft of property included the victim's work area. [1]

Of the threats most organizations face, responding to phishing or pretexting emails, misuse of credentials, and loss of equipment are the most common. Procedures should be in place for how employees should respond to these instances and they should be trained on the threats these attacks can cause.

CHAPTER 5. DEVELOPING TRAINING

After preparing the organization for training by gaining executive support, understanding learning styles and culture, and establishing a baseline competency, training development can occur. There are several different types of training that should be considered for an organization, keeping in mind the primary focus of the training is to be as minimally invasive into the employees' lives as possible. There are several types of training that can be considered, such as emails that are sent on a weekly or monthly basis, labs that can be given once a year or so, and games that teach security principles. This chapter reviews some sample emails that could be sent to users, a sample lab dealing with a phishing email, and an escape room game that teaches participants about physical security.

Emails

Email can be an effective way to disseminate information to the organization quickly and easily. Email can be sent on a more frequent basis than most training can be given and provides a mechanism to keep security awareness in users' minds. The text should be short, but memorable, and cover many different topics.

The sample emails in Appendix B cover a few topics that are important for users to comprehend. The first set of emails introduce the concept that that any person in an organization is a target. Other topics include password length and password managers, understanding links, using free wireless, sharing information on social media, and common traits of phishing emails.

The emails were sent to IDPH employees in small sections on Thursday of each week. Additionally, when cyber security breaches made the news, a short email outlining the issue and what employees should do if they were affected was sent.

Hands-on Labs

While email can be a quick way to send information to users, many may ignore the messages. It is beneficial for an organization to have several different ways to engage and train users. A second way to train users is to create hands-on labs that employ real world scenarios a user may encounter.

The hands-on lab shown in Appendix C was created by setting up email accounts using Gmail. As more organizations offload their email to services like Gmail and Office 365, it is easy to set up free accounts to be used for labs and training. The software used to send the test phishing email was GoPhish, https://getgophish.com. The template was found at https://github.com/rfdevere/templates, [4] and was modified to seem more realistic. Appendix C shows the step by step directions for users in the lab setting.

While this lab was not tested at IDPH, it will be considered as part of a larger effort to modify security awareness training. If the survey shown in Chapter 4 is given to a wider audience, and results indicate difficulty identifying the characteristics of a phishing email, this lab would give employees the opportunity to practice and improve those skills with hands-on experience and being walked through traits to look for.

Games to Engage Users

While labs are great hands-on experiences for users, and when performed in a classroom setting participants can ask questions, engaging users with games is often a positive and memory approach. Escape rooms are popular today, and they provide the ability teach users a few important lessons about physical security as it relates to technology. The original idea for the escape room came from an article about FedEx developing an escape room [12], as well as Linda Ludwig's presentation on creating an escape rooms to engage

users. [13] This section will walk an instructor through setting up an escape room and how to teach participants about security by reviewing a takeaway at the end of game.

Game Setup

A computer lab may be the most practical environment for this escape room. It allows the instructor to have different workstations that are easily broken into and allow the users to see how an attacker would gain information from their workstation. The following walks through how to set up three computers with a profile on each computer representing a hacker on each computer. A local Windows profile was set up and logged in and locked when participants entered the room.

Darlene's computer has the password, "3efv$RGB", taped under keyboard. Once the participants get logged into the account, they see Darlene has images of the organization's structure showing an employee in finance and their supervisor. This image is shown in Figure 5.1. Another image has Darlene's email that shows a phishing chain with Darlene pretending to be the employee's supervisor by spoofing the supervisor's email address. Darlene, pretending to be the supervisor, asks for the user's password and the employee responds with their password. Other images on the desktop show Darlene using an IDPH website to determine the employee's username. Also on Darlene's desktop is a password protected zip file. Inside the zip file is an icon and a number that the icon represents. Escape room attendees were asked to find three icons and the numbers they represented to find the code to "escape" the room.

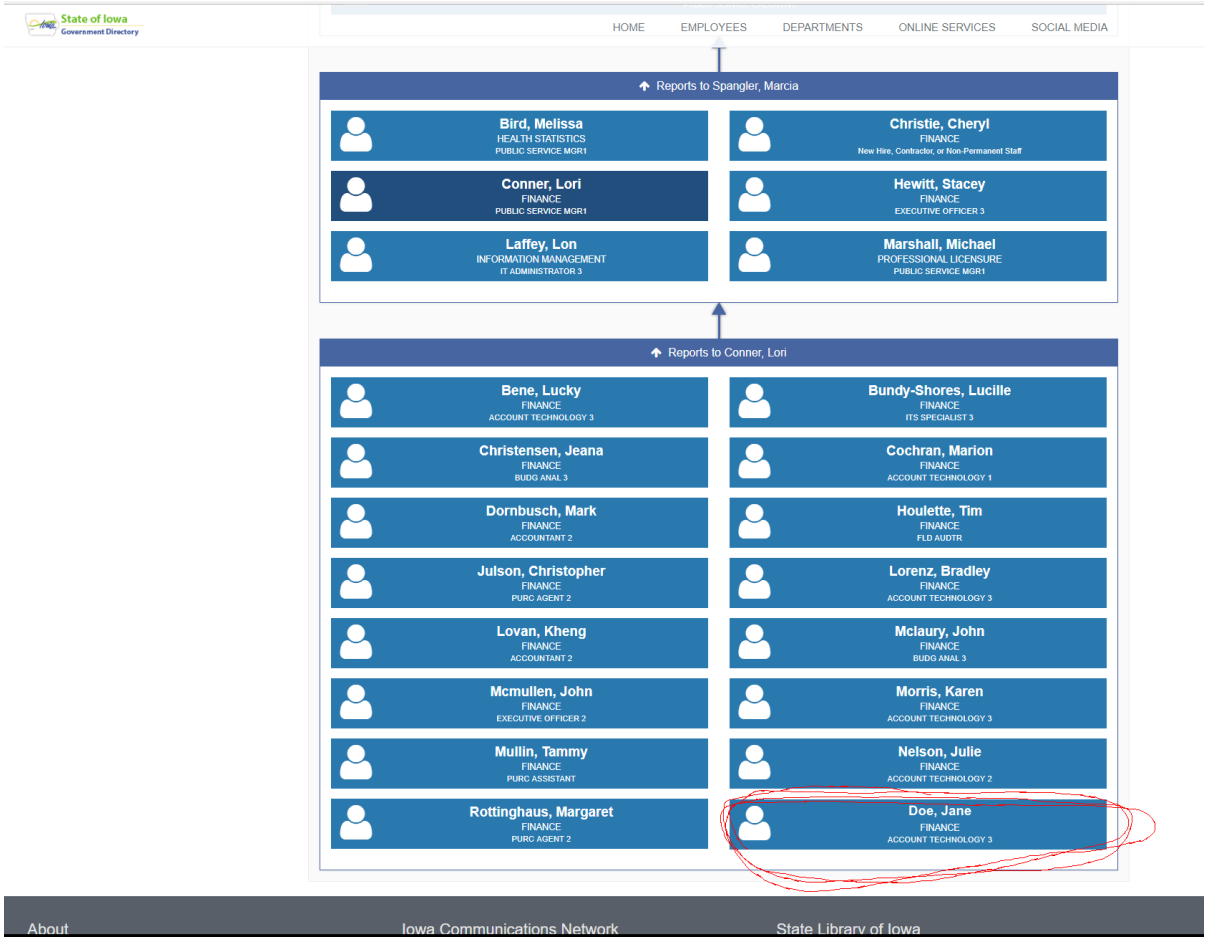

Figure 5.1 *Image on Darlene's desktop showing reconnaissance.*

Angela's mousepad was a Chicago Cubs baseball logo and taped to the monitor was a graphic stating I Love The Cubbies, this graphic is shown in Figure 5.2. Angela's password was "Cubbies!" Once logged into Angela's account, the participants were able to find Angela's reconnaissance, searching the directory for a user and retrieving their phone number. Angela's desktop contains an MP3 recording of a phone call between herself and the targeted user, where Angela pretends to be an IDPH helpdesk technician and informs the employee their computer has been infected and she needs his password immediately to help him save his documents on his computer. Angela uses the same method as Darlene to find the employee's username, and reuses her system password to secure the icon on her desktop.

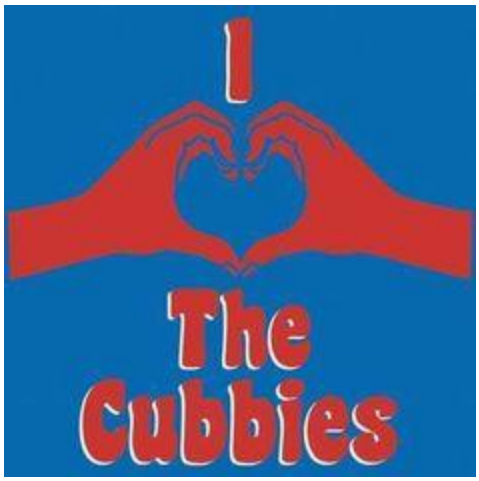

Figure 5.2 *Image taped to Angela's computer.*

Next to Elliot's computer, a file with a stack of papers contained a highlighted number, 511, and a book safe shaped like a dictionary. The book safe's PIN was 511, and once the safe was opened, Elliot's password was revealed, "Mr.R0b0t". On Elliot's desktop, images containing his reconnaissance, similar to Angela's and Darlene's desktops. Elliot's next step for his target included research on social media. Elliot finds the employee on Facebook and determines answers to some of her security questions through a public post, as shown in Figure 5.3. The files also included Elliot determining a user account using a website that had different responses for a valid and invalid account in the system. This is shown in Figures 5.4 and 5.5.

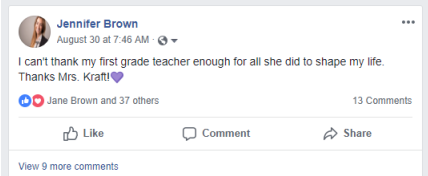

Figure 5.3 *Elliot's social media reconnaissance.*

Figure 5.4 *Website response for invalid user account.*

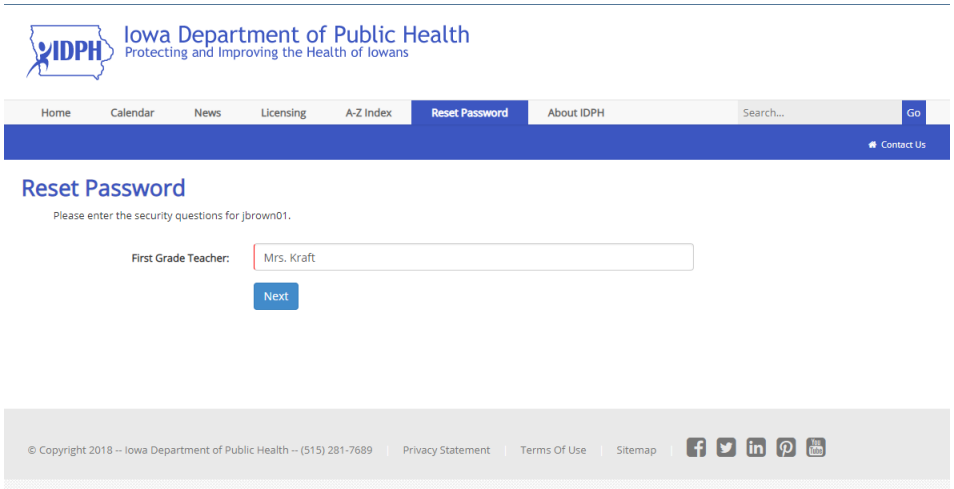

Figure 5.5 *Website response for valid user account.*

The data for each of the hackers was generated by using the organization website and modifying the content of webpages using Chrome's developer tools. This allowed the instructor to obfuscate information and not appear that a real employee had been hacked. Each piece of information in the hacker's profile corresponds to a real-life attack vector. Darlene's computer is an example of a spear phishing email and using a website's bad user management functions to determine usernames. Angela's computer is an example of vishing, using phone calls to social engineer a user to gain information. Elliot's computer is an

example of using publicly accessible information on social media to use an organization's password reset functions to reset a user's password and gain access to their accounts.

Game Introduction

The following is an introduction to the game to give the participants an idea of what is going to happen during the game.

Elliot and his band of hackers have decided to break into the IDPH network. They know IDPH has millions of records of identity data that could be sold for a profit. You have found their lair, and while you were watching them, the group ran off to the store to grab some energy drinks and snacks before finishing their mission. Your goal is to determine what data they already have and escape before they return in 30 minutes. Luckily for you, despite being a group of hackers, they have some poor security habits as well, so breaking in may be easier than you expect.

Participants should be asked to find three icons which represented a number. Finding all of the icons and adding them together yield a "code" to use to exit the room. A sheet should be given to participants to track usernames and passwords retrieved along with the numbers associated with each icon. This tracking sheet is shown in Appendix D.

Recap

After the time has elapsed, the instructor should take the time to go over the different lessons that from the game.

- How many usernames and passwords did the group get?
- What were some of the bad habits the hackers had?
    - Elliot – Stored password in safe, PIN was next to book, reused password

    - Angela – Password was favorite team, computer decorated with personal items
    - Darlene – Password was taped under the computer
- How did they get information from employees?
    - Phishing
    - Vishing
    - Social media profiles
    - Password reset on website different for known and unknown users

At the end of each session, 10-15 minutes at the end of the game should be given to recap the security awareness concepts from the game. Participants should be reminded that all contact information that is publicly available can be used by an attacker to target them in phishing and vishing campaigns. Participants should be informed that vishing attacks were on the rise, and to be aware that phone numbers could be spoofed, so caller ID is not a reliable method of authenticating someone. Discussion should include why everyone could be a target, as the attacker's primary goal is to get into the network and move from their initial victim to new computers. A discussion about Darlene's password, which uses keyboard walking, and Angela's password, could lead to conversations about how attacker's crack user's passwords using wordlists available on the internet.

If the session is provided to a more technical audience, for example programmers, an additional focus could be made on the website functioning differently for existing accounts and non-existent accounts. As software engineers, they will write websites, and it is important for them to understand how attackers can use information from those websites to gain access to systems.

Additionally, participants should be reminded of the following lessons:

- Anyone is a target.
- Don't leave passwords taped under your keyboard. (Or anywhere else near your computer.)
- Don't leave papers next to your desk with sensitive information.
- Be suspicious of emails and phone calls you receive asking for your information. Carefully review any emails you receive asking for financial information.
- Be aware of data posted publicly on social media.

Continuing Training

The training could be used as part of an ongoing security awareness program. This would provide more employees a chance to try the escape room and have discussions about security awareness. The game would likely need to be modified as more users take the training, as employees may share the secrets of the escape room. The hacker's passwords could be changed without much effort, and the images used to represent Angela's password may be changed. The overall lessons of the game can remain the same or be enhanced to include additional topics.

CHAPTER 6. CONCLUSION

Over the past few years, networks have become more difficult to breach as system and network administrators have done a better job of securing their networks and systems. This has led attackers to switch to new tactics, primarily focusing on social engineering attacks. Organizations are finding technology solutions inadequate to mitigate these attacks, particularly in smaller or less mature companies where the security team may be formed primarily from the networking team or other individuals who may not have training in security awareness. Immature security awareness programs tend to focus on compliance-based training, perhaps buying software and implementing it without concern that the training is effective. Employees of the company may not understand what they are supposed to learn from the training, leading them to feel frustrated and annoyed with the training, rendering the training useless.

This paper focused on ways for an organization to move past compliance-based training and engage users as active training participants. Many smaller companies lack the budget for security awareness software that can cost thousands of dollars, so the trainings suggested by this paper are inexpensive. Organizations should be able to use the practices from this paper to grow their security awareness programs.

The first step to creating a more robust security awareness program is to understand how attackers can target an organization. When the SANS Institute helped create their Top 20 Critical Security Controls (CSC), one of the guiding principles was “offense informs defense”. [14] The same principle should be applied to any security awareness training. Attackers generally follow the same steps in each attack: reconnaissance, scanning, and gaining access. Educating employees how attackers may target them helps them understand

what to be aware of in their daily activities. Training created for the organization should focus on how hackers actually work.

Another factor to consider in creating training is how much time an organization is willing to spend. Some compliance-based training may require users to complete hours' worth of training in a few days. Dividing large trainings into smaller activities completed more frequently keeps the idea of security awareness fresh in users' minds and stops from overwhelming them once a year.

A baseline of users' understanding about different security topics can be beneficial when developing or delivering training and provides a basis for comparison to measure effectiveness. Technology professionals who have been working with computers for years may not understand how poorly they are communicating with their less technical users. It is likely the employees of an organization have been told, "Do not click on links before hovering over them", but if the individual does not understand how a URL is structured, or doesn't know how to unshorten a URL, the advice is lost on them or they may get frustrated and click on the link anyway.

It is also important for the technology division of an organization to be transparent in how they work, especially with the helpdesk. Users should understand how to contact the helpdesk, how the helpdesk will contact them, and how to report things they find suspicious. Without that communication, an attacker may be able to contact employees and request their password or other information because the individual may think the email or phone call is legitimate.

Different types of training should be available to users. Different individuals will respond to different types of training, so sending the same message in several ways can help

reach more of the organization. For this paper, emails were created to give tips on a weekly basis. The emails should be short and cover various topics affecting normal users. Hands-on labs were created, demonstrating a phishing email and explaining to users different items to look for in suspicious emails. Lastly, a game was created to teach physical security and illustrate attackers perform research and carry out social engineering attacks.

Hackers breaching networks through users has been the trend for the last few years as networks and systems have become harder to penetrate. Security awareness training programs do not appear to be working currently, and security teams need to do a better job understanding what is going wrong. A cross-domain research study between psychology and information assurance could help understand this problem further. In the absence of such a study, training should focus on the individuals, teaching them how attackers do their jobs, learning where gaps exist in current knowledge, avoiding shaming the users, and learning how to engage them effectively.

REFERENCES

[1] Verizon, "2018 Data Breach Investigations Report," Verizon, 2018.

[2] D. Seiler, "Age and Learning Style in the Adult Learner," *The Journal of Human Resource and Adult Learning*, vol. 7, no. 2, p. 6, 2011.

[3] D. D. Caputo, S. L. Pfleeger, J. D. Freeman and M. E. Johnson, "Going Spear Phishing: Exploring Embedded Training and Awareness," *IEEE*, pp. 28-38, January 2014.

[4] A. Vance, J. L. Jenkins, B. B. Anderson, D. K. Bjornn and C. B. Kirwan, "Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiements," *MIS Quarterly*, vol. 42, no. 2, p. 41, 2018.

[5] Cybrary, "Summarizing The Five Phases of Penetration Testing," Cybrary, 6 May 2015. [Online]. Available: https://www.cybrary.it/2015/05/summarizing-the-five-phases-of-penetration-testing/. [Accessed 24 September 2018].

[6] Dashlane, "Features," Dashlane, [Online]. Available: https://www.dashlane.com/features. [Accessed 29 July 2018].

[7] LastPass, "How LastPass Works," LastPass, [Online]. Available: https://www.lastpass.com/how-lastpass-works. [Accessed 29 July 2018].

[8] 1Password, "Families," 1Password, [Online]. Available: https://1password.com/families/. [Accessed 29 July 2018].

[9] J. L. Jenkins, B. B. Anderson, A. Vance, C. B. Kirwan and D. Eargle, "More Harm Than Good? How Messages That Interrupt Can Make Us Vulnerable," December 2016. [Online]. Available: https://pubsonline.informs.org/doi/pdf/10.1287/isre.2016.0644. [Accessed 24 September 2018].

[10] R. Harnedy, "The State of Phishing 2016: What IT Pros are Seeing In the Real World," Barkly, August 2016. [Online]. Available: https://blog.barkly.com/state-of-phishing-2016-survey-statistics. [Accessed 25 September 2018].

[11] R. DeVere, "Templates," 24 April 2017. [Online]. Available: https://github.com/rfdevere/templates. [Accessed 26 June 2018].

[12] M. House and S. Fackler, "Security Awareness Escape Rooms," December 2017. [Online]. Available: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1513173289.pdf. [Accessed 9 September 2018].

[13] L. Ludwig, "Escape Rooms: Capturing Their Attention While Sharing Your Message," 11 April 2018. [Online]. Available: https://events.educause.edu/special-topic-events/security-professionals-conference/2018/agenda/escape-rooms-capturing-their-attention-while-sharing-your-message. [Accessed 9 September 2018].

[14] SANS, "CIS Critical Security Controls: Guidelines," SANS, [Online]. Available: https://www.sans.org/critical-security-controls/guidelines. [Accessed 18 October 2018].

[15] D. Grauman and D. Jacobson, "Lesson 11: Creating Strong Passwords," Iowa State University, Ames, 2016.

[16] D. Grauman and D. Jacobson, "Lesson 29: Reading URLs," Iowa State University, Ames, 2016.

[17] D. Perret, "Phishing Awareness Training: 8 Things Your Employee Should Understand," VadeSecure, 7 October 2016. [Online]. Available: https://www.vadesecure.com/en/phishing-awareness-training-8-things-employees-understand/. [Accessed 19 July 2018].

APPENDIX A. SECURITY AWARENESS SURVEY

1. Are you aware that information can be gathered from the internet including your name, job title, phone number, address, and reporting structure?
    a. Yes
    b. No
2. Are you aware that any person at IDPH could be a target for a social engineering attack?
    a. Yes
    b. No
3. Which of the following are things you should review when checking to see if an email is legitimate or not?
    a. Sender
    b. Subject
    c. Spelling/Grammar
    d. Links
    e. All of the above
4. Should you give your password out via email or over the phone?
    a. Yes
    b. No
5. Are you aware of the XXXX@idph.iowa.gov email address and that you can forward suspicious emails for review?
    a. Yes
    b. No
6. Can you determine where this URL goes without typing it in or clicking the link? http://bit.ly/2xNBEjW
    a. Yes
    b. No
7. Are you aware posting things on social media such as first grade teacher, favorite pet, etc, can be used as security questions and found by attackers to reset your password?
    a. Yes
    b. No
8. Are you aware leaving your password near your computer, or using a password based on your favorite things could make you a target for an attacker?
    a. Yes
    b. No
9. Are you aware that the owner of a URL is usually the word before the ., directly before the first / after http(s)://, for example, http://www.google.com/ is owned by Google.
    a. Yes
    b. No

10. Did this escape room help you learn something about security awareness you didn't know before?
    a. Yes
    b. No

APPENDIX B. SAMPLE EMAILS

You Are a Target

You might think no one would want to target you to steal your data, but the reality is that as an <<organization>> employee, you might have access to information an attacker wants. Even if you don't have access to the data, you might be an entry point into the corporate network, which contains sensitive data.

As a state agency, all our information is available online, including our phone numbers, email addresses, and organization structure. If you've never been to the state directory, https://directory.iowa.gov, take a few minutes to review the data listed there. Most attackers start by doing reconnaissance on the company they would like to target. Be aware of emails you receive out of the blue without prior communications with an individual.

Hacking Is Easy!

TV and movies portray hackers as young men in hoodies hunched over their computers in their parents' basements. In reality, hackers come in many forms, including novice hackers using tools, information security experts trained to help secure organizations, and hackers who work for nation states. Many tools exist for hackers to try to compromise individuals and networks, and they are easy to use. Some require very minimal time to learn to use. So be aware, there are a lot more people trying to break into networks than you'd expect.

Password Length

The most important factor in whether a password is able to be cracked is the length. This is the reason the Information Management (IM) department will be implementing a 16-character minimum length password policy later this year. Here is a short video explaining

how to use a passphrase to implement longer passwords. https://www.youtube.com/watch?v=wHY2WQsmMzM&index=11&list=PLzQX06Oo2BXS4JsXtPuy6tmKyApQlAuS1 [5]

Additionally, consider using a password manager to store your passwords. LastPass and Dashlane are excellent options that allow you to store passwords, credit card information, and secure notes. Both offer free versions and the ability to test the paid version for 30 days. Both of the paid versions for these pieces of software are relatively inexpensive, and if it saves you from losing your banking information from an attacker, it's definitely worth it!

Understanding Links

It is important to review links before clicking them in an email. URLs are structured in a particular way, and if you'd like to understand how they work in more detail, watch the video at the following link. https://www.youtube.com/watch?v=ouKPcYJM96k&index=29&list=PLzQX06Oo2BXS4JsXtPuy6tmKyApQlAuS1 [6]

Attackers can use tools called URL shorteners, you might have seen URLs that look like: http://bit.ly/1dk39ak, that is a URL that has been generated from a URL shortener tool. This makes it difficult to determine where the URL will actually take you, so you can go to an unshortening tool, like https://www.unshorten.it before clicking the link.

Once you have learned about URLs, you can take quick quiz determining whether links are legitimate or fake, by following this link. https://www.opendns.com/phishing-quiz/

Free WiFi

Be careful when you connect to WiFi networks. An attacker can set up a WiFi network and intercept all your internet traffic. Even using https secured websites can be

intercepted, as the WiFi network can give you a fake certificate and you might not realize they are watching your traffic. These types of attacks are called "man-in-the-middle" attacks. Be aware of the WiFi networks you are connecting to, and turn off your Bluetooth on your computer if you are not using it. Attackers can sometimes connect to Bluetooth and steal data from your devices.

Sharing on Social Media

Be careful of the data you share on social media. It's great to want to share your vacation photos but be aware this can alert people to the fact that you are not home. Also be aware of commenting on posts with things like, "What was the name of your first pet?". These questions are often security questions and sharing on these posts can make your information available online.

Check your social media settings and make sure you are not sharing things with the public you don't intend to. Log out of your accounts and view them as if you were a complete stranger.

Traits of Phishing Emails

When reviewing an email, there are a few things to look for. [7]

- Look at the sender of the email. Make sure the part after the @ sign corresponds to who you are expecting the email to be from.
- Hover over links in the emails and make sure they are going to a location you trust.
- Be aware of spelling mistakes in the emails. Most emails from legitimate companies will be spelled correctly.

- Be aware of grammar that doesn't fit your normal communications. Some attackers are from other countries and have a hard time translating to English.
- Review the greeting. Is it personalized to you, or does it say, "Dear Sir/Madam".
- Review the ending of the email. Similar to the grammar point, does the signature seem legitimate.
- If the email is asking you for personal information, or your password, the odds of it being a phishing email drastically increase.
- Be aware of emails that have urgency to them. "I need this right away!". The attacker is hoping you will be willing to help them without taking the time to review their email.
- Do not open attachments to emails you were not expecting. Attachments can contain viruses or malware that can infect your computer. While Gmail, Office 365 and other providers do a great job of filtering out many bad attachments, they can't catch everything.

Remember attackers can easily steal images from the internet, so even if the logos and text appear legitimate, remember to hover over links before clicking them.

APPENDIX C. PHISHING LAB

Step 1

Log into Gmail by going to http://www.gmail.com.

Step 2

On the Sign in screen, type in idph.training<number> where <number> is the number assigned to your computer. In the screen shot in Figure A.1, the <number> is 1.

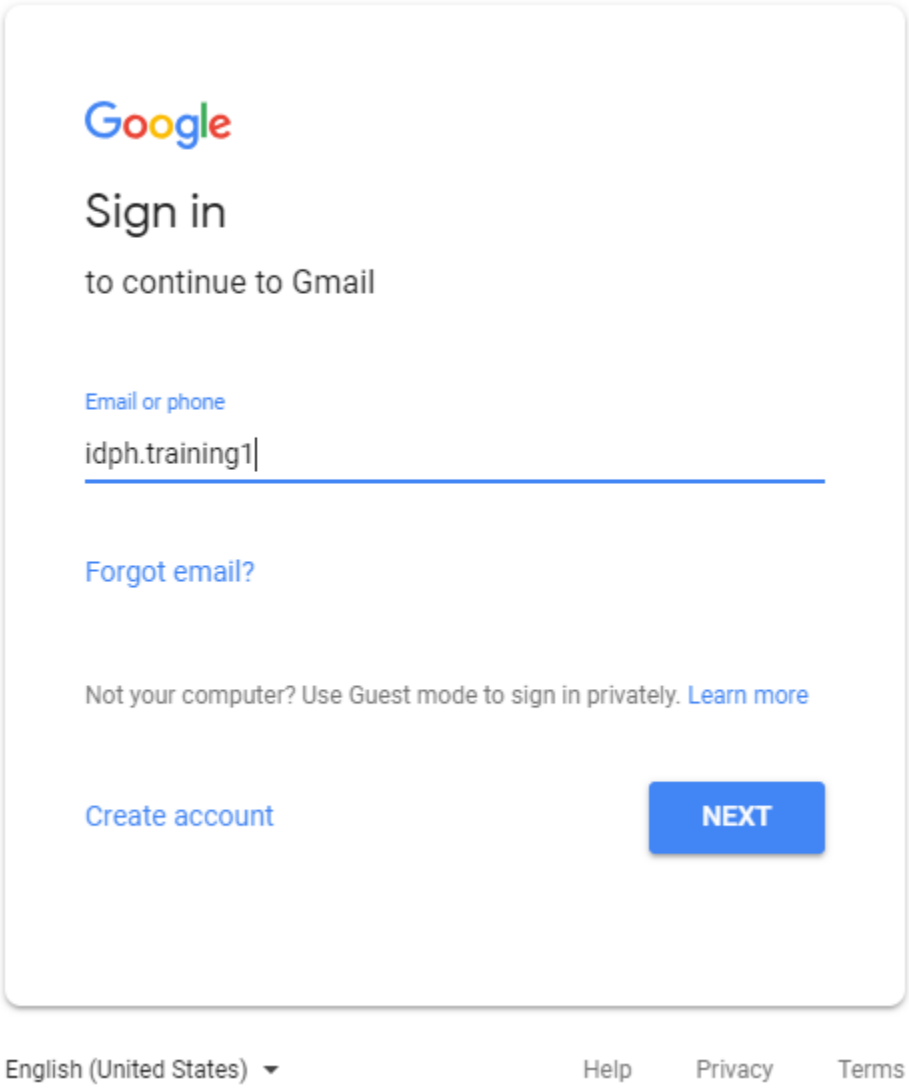

Figure C.1 *The Gmail login screen shows the username.*

Step 3

On the Welcome screen, enter the password, <<password>>, where <number> is the number assigned to your computer. In the screen shot in Figure A.2, the <number> is 1.

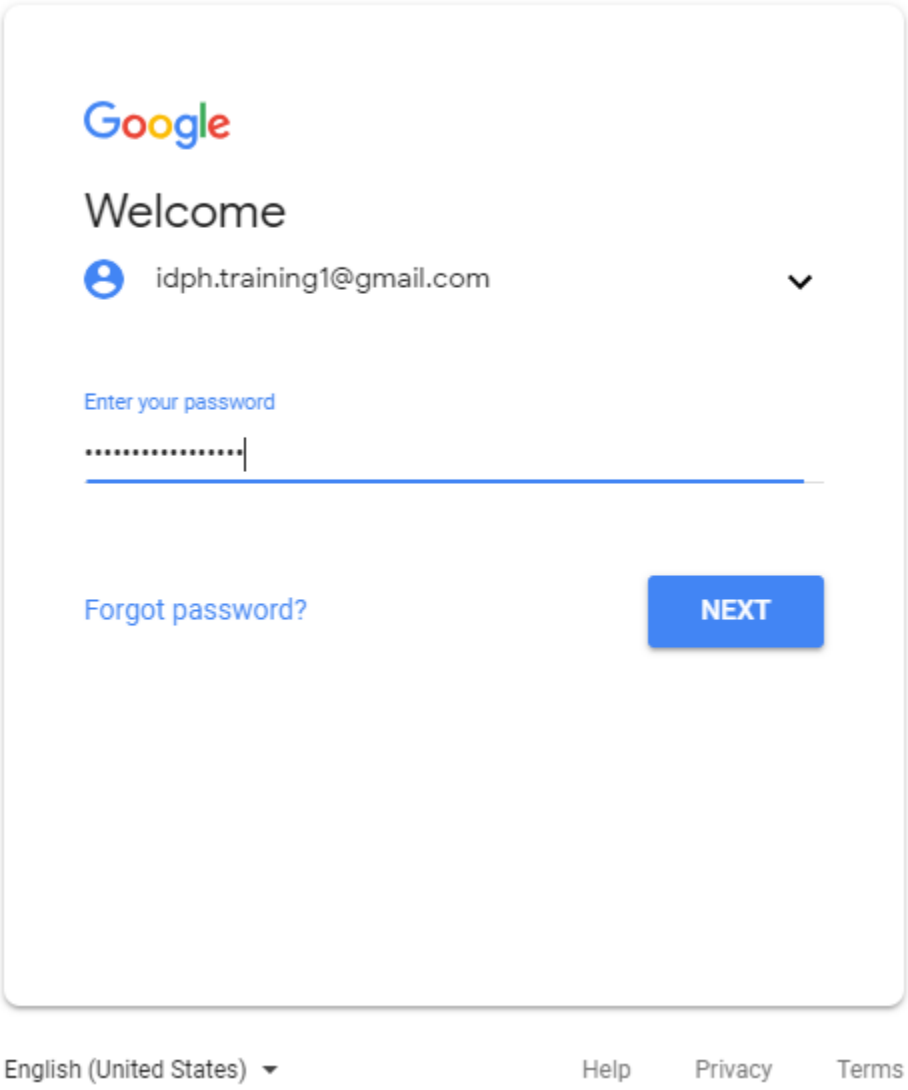

Figure C.2 *The Gmail password screen*

Step 4

Once you are signed in, you will see there is an email with the subject "Google – Account Sign In". Open the email and take a minute to review the email to see if you can

find any indicators that the email is fake. Review the following steps to see the areas to review in the email.

Step 5

There are several indicators that the email is not a legitimate email. First, look at the from address. It is displayed as cam@idph.iowa.gov.

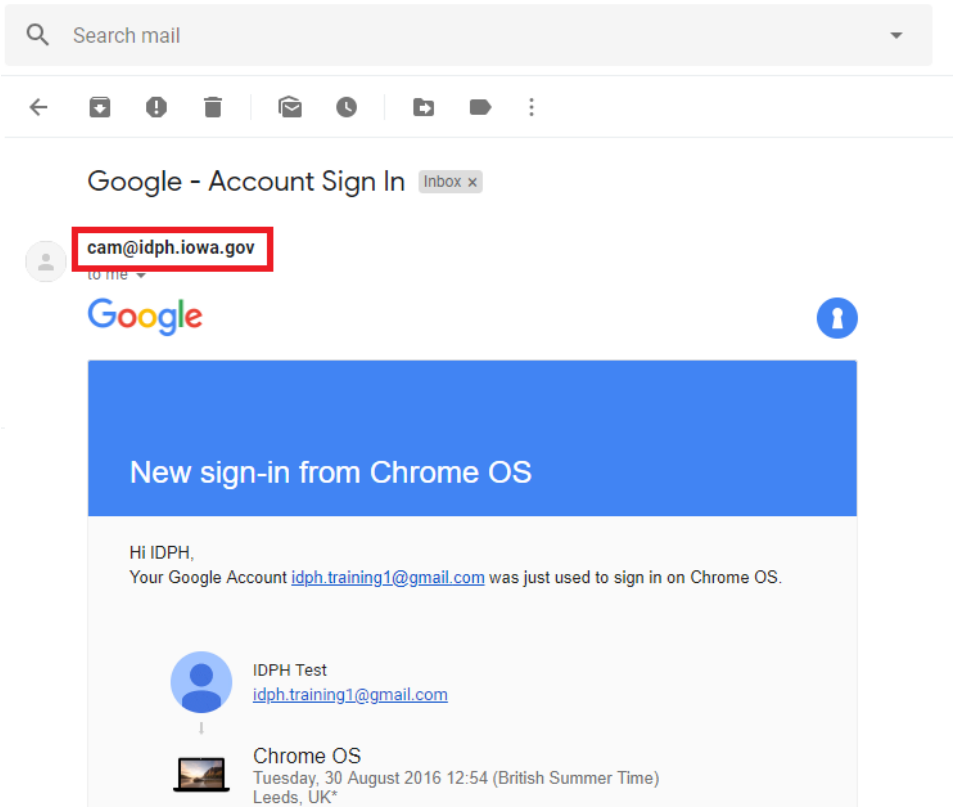

Figure C.3 *This figure illustrates the phishing email in Gmail.*

There are several grammatical errors in this email, including "recognise", the lack of capitalization of "if" in the second sentence, and the misspelling of the word "pleace".

Figure C.4 *This figure illustrates the spelling errors in the phishing email.*

Hovering over the links in the email, and viewing where the link takes us in the bottom right hand corner of Chrome, we see the links point to “192.168.1.1/?rid=rwFtetM”, which is not the expected URL of, http://www.google.com.

Figure C.5 *This figure illustrates the IP address instead of a URL in the email.*

APPENDIX D. USER TRACKING SHEET

Username	Password
elliot	
angela	
darlene