Journal of Information Systems Education

Volume 34 | Issue 4 Article 1

12-15-2023

Teaching Tip: Hook, Line, and Sinker – The Development of a Phishing Exercise to Enhance Cybersecurity Awareness

Jacob A. Young
Bradley University, jayoung@fsmail.bradley.edu

Sahar Farshadkhah
University of Illinois Springfield, sfars2@uis.edu

Journal of Information Systems Education

Volume 34
Issue 4
Fall 2023

Teaching Tip

Hook, Line, and Sinker – The Development of a Phishing Exercise to Enhance Cybersecurity Awareness

Jacob A. Young and Sahar Farshadkhah

Recommended Citation: Young, J. A., & Farshadkhah, S. (2023). Teaching Tip: Hook, Line, and Sinker – The Development of a Phishing Exercise to Enhance Cybersecurity Awareness. *Journal of Information Systems Education*, 34(4), 347-359.

Article Link: https://jise.org/Volume34/n4/JISE2023v34n4pp347-359.html

Received: May 12, 2022
First Decision Made: August 9, 2022
Accepted: October 11, 2022
Published: December 15, 2023

Find archived papers, submission instructions, terms of use, and much more at the JISE website: https://jise.org

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Journal of Information Systems Education, 34(4), 347-359, Fall 2023

Teaching Tip
Hook, Line, and Sinker – The Development of a Phishing Exercise to Enhance Cybersecurity Awareness

Jacob A. Young
Department of Entrepreneurship, Technology & Law
Bradley University
Peoria, IL 61625, USA
jayoung@fsmail.bradley.edu

Sahar Farshadkhah
Department of Management Information Systems
University of Illinois Springfield
Springfield, IL 62703, USA
sfars2@uis.edu

ABSTRACT

In this paper, we describe the development of an in-class exercise designed to teach students how to craft social engineering attacks. Specifically, we focus on the development of phishing emails. Providing an opportunity to craft offensive attacks not only helps prepare students for a career in penetration testing but can also enhance their ability to detect and defend against similar methods. First, we discuss the relevant background. Second, we outline the requirements necessary to implement the exercise. Third, we describe how we implemented the exercise. Finally, we discuss our results and share student feedback.

Keywords: Phishing, Social engineering, Cybersecurity, Pedagogy

1. INTRODUCTION

The Federal Bureau of Investigation (FBI) has shared that email-based cyberattacks reported to the Internet Crime Complaint Center (IC3) in 2020 resulted in nearly $2 billion in financial losses in the United States (Federal Bureau of Investigation, 2020). The number of victims per year for the category that includes phishing has increased dramatically, from 26,379 in 2018 to 241,342 in 2020. Although an increase in cyberattacks can be attributed to the COVID-19 pandemic, these trends are expected to continue, especially with the sudden shift toward telework. The Identity Theft Resource Center (2022) reported that the most common attack vector from 2019 to 2021 was social engineering via electronic communication, such as phishing, smishing, and business email compromise. These attacks were responsible for over 41 percent of compromises over the three-year period.

To better address these costly, evolving, and growing cyber threats, we encourage cybersecurity instructors to find innovative ways to develop ethical hackers by teaching students how to craft social engineering attacks. Although this might sound counterintuitive to those outside of the cybersecurity field, providing an opportunity for students to craft offensive attacks not only helps prepare them for a career in penetration testing but can also enhance their ability to detect and defend against similar attack methods by developing an adversarial mindset (Hamman et al., 2017; Katz, 2019; O'Connor, 2022; Thompson et al., 2018). Further, refraining from teaching offensive concepts to students does not prevent them from learning such skills through other means. College courses can provide a controlled environment for students to safely develop ethical hacking skills. For example, Luse and Burkman (2021) described an exercise that exposed students to Gophish, a popular open-source phishing tool, and then allowed them to conduct a real-world phishing campaign against a client organization.

In this paper, we build upon Luse and Burkman's (2021) work by developing a less technically demanding exercise that does not require students to set up the phishing environment (e.g., purchasing a domain and configuring a web and email server). We also provide instructors with more detail on how to set up such an environment. In addition to increasing phishing awareness, we wanted to provide students with hands-on experience using a phishing platform to prepare them for subsequent courses on penetration testing and red teaming (Young, 2020). Ultimately, we believe that our exercise can introduce Gophish to all students, including those without a technical background.

In describing our exercise, we followed best practices for teaching tip articles (Lending & Vician, 2012). We discuss the relevant background on social engineering and then outline the requirements necessary to implement the exercise. We explain

how we delivered the exercise. This is followed by a discussion of our results and a presentation of student feedback. We also provide instructors with an example white hat agreement and our exercise instructions.

2. BACKGROUND

In this section, we provide an overview of the social engineering concepts that instructors can cover as part of our exercise that exposes students to the phishing process. We then discuss phishing from both offensive and defensive perspectives.

2.1 Social Engineering

Social engineering in information security refers to "incidents in which an information system is penetrated through the use of social methods" (Tetri & Vuorinen, 2013, p. 1014). More specifically, social engineering refers to social interactions that aim to acquire confidential information through manipulation or persuasion (Schaab et al., 2017). This persuasion could be any active attempt to change a person's mind (Petty & Cacioppo, 1996) and convince them to perform certain actions or disclose confidential information. Social engineering is effective largely because people are inherently optimistic and have yet to develop the healthy skepticism needed to identify social engineering threats (Junger et al., 2017; Rhee et al., 2012). Optimism bias leads many to hold the mistaken assumption that negative events will only happen to others (Weinstein, 1980), which leads them to believe that they will not be fooled and fall victim to social engineering attacks (Junger et al., 2017; Rhee et al., 2012).

Social engineers use various psychological techniques to achieve their goals. The techniques are rooted in Cialdini's (2006) principle of influence, Gragg's (2003) psychological triggers, and Stajano and Wilson's (2011) principle of scams, as discussed by Ferreira et al. (2015). Understanding the psychological principles that can be weaponized through social engineering helps to develop an effective, multi-level defense (Gragg, 2003). Examples of offensive social engineering techniques that an attacker might use include authority, social proof, liking, similarity, deception, scarcity, and distraction.

Since most people are reluctant to question authority, targets are usually willing to respond to requests that appear to come from someone in an authoritative position. Similarly, social proof refers to a situation in which people feel less suspicious and mimic the behaviors and risks that others seem to be exhibiting (Cialdini, 2006; Schaab et al., 2017). Moreover, social engineers recognize that people tend to stand by whom they like or to whom they are attracted, so attackers commonly attempt to develop a positive rapport with their target. Similarity refers to a situation in which attackers try to take advantage of the fact that people prefer to follow who they find or are similar to themselves (Ferreira et al., 2015).

Deception is another psychological technique that attackers use. In this strategy, attackers try to deceptively form a relationship with their target by sharing information with or talking to a common enemy (Ferreira et al., 2015). The scarcity principle can be used to create a situation in which the target is concerned about losing or missing out because of limited availability. In these situations, people usually focus on the lack of time, money, or goods, and ignore all other facts (Ferreira et al. 2015). Distraction is a psychological strategy rooted in the fact that individuals tend to focus on one thing and might not notice what is occurring in the periphery (Ferreira et al., 2015).

Social engineers can execute these techniques in various forms of attack. They could call a target or physically visit their office. One of the most common ways is to send an email that looks like one from a legitimate organization or person. However, the email is likely to contain a malicious attachment or link that asks the user to enter their credentials on a fake website. Although discussing each of the social engineering attack methods in a cybersecurity course is important, we focus our paper on crafting and defending against attacks delivered via email.

2.2 Phishing

Phishing refers to "the attempt to acquire sensitive information or to make somebody act in a desired way by masquerading as a trustworthy entity in an electronic communication medium" (Krombholz et al., 2015, p. 117). Threat actors primarily conduct phishing attacks using emails that might ask targets for information, instruct them to download a file, or lead them to websites where they share their credentials. Cybercriminals typically try to impersonate a trusted and legitimate party with deceptive email addresses and messages. When a phishing email looks like it is from a company, bank, or government-related agency, social engineers rely on the authority principle to ask the victim to perform an action. However, when social engineers use the social proof principle to persuade people, they may include information about how others think, feel, or act. Moreover, a phishing email may present false information as authentic. When attackers impersonate others by claiming that someone else sent the email, they rely on the principles of similarity and deception psychology. Therefore, phishing combines technical and social approaches.

Although most phishing campaigns tend to be generic, broad-based attacks, others target specific individuals, also known as spear phishing. When spear phishing targets a prominent individual, such as an executive or celebrity, it is known as whaling. For example, during the 2016 U.S. presidential campaign, Hillary Clinton's campaign manager, John Podesta, received an email appearing to be from Google claiming that the password to his account had been compromised and that he needed to click a link to change it (Ormeus, 2016; Stojnic et al., 2021). The email was forwarded to an information technology professional on the campaign's staff, who told Podesta that he should change his password. Unfortunately, Podesta's account was compromised when he attempted to change the password using the *bit.ly* shortened link provided in the phishing email instead of visiting Google directly. On October 7, 2016, shortly before the election, thousands of Podesta's emails were ultimately published on Wikileaks (Wikileaks, 2016).

Other categories of phishing emails include business email compromises and sextortion. Attackers commonly execute invoice scams, a specific form of business email compromise, with phishing emails that request payment for products or services that have never been delivered. For example, in 2015, Ubiquiti discovered that it had paid fraudulent invoices totaling $46.7 million (Hackett, 2015). Sextortion typically occurs when a victim receives an email threatening to publish embarrassing content, such as visits to pornographic websites or webcam footage, unless they make a payment in some form of cryptocurrency (Malwarebytes Labs, 2021). Although the

claims might be technically possible, most sextortion attempts rely entirely on intimidation and urgency to convince the victim that the threat is real. The hope is that the victim will be too embarrassed to seek technical assistance and will eventually submit the payment to prevent the supposed compromising content from being shared with family, friends, or colleagues.

Although it is impossible to prevent social engineering attempts, it is possible to mitigate harm to individuals and their organizations by employing a layered and diverse defense. First, organizations must understand the offensive strategies employed by attackers. Second, organizations must establish effective defenses to detect and respond to social engineering attacks. We will discuss phishing from both perspectives in the next two sections.

2.3 Offensive Strategies

In this section, we discuss offensive strategies that can increase the effectiveness of phishing attacks, such as open-source intelligence gathering, lookalike domains, typosquatting, and phishing platforms. Open-source intelligence (OSINT) has been defined by the United States Army as "intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement" (Headquarters, Department of the Army, 2023, p. 1-19). However, OSINT is not limited to military uses, and techniques can be employed to research any subject. The power of OSINT is evident in the Netflix documentary *Don't F**k with Cats: Hunting an Internet Killer* (Lewis, 2019), which tells the story of a crowdsourced group of volunteers who used OSINT techniques to identify and track down those responsible for killing kittens in a YouTube video. Cybercriminals will often conduct OSINT research on their targets to aid in crafting tailored attacks (Bazzell, 2021; Hayes & Cappa, 2018).

An excellent example of how OSINT complements social engineering is DEF CON's Social Engineering Capture the Flag competition (Social-Engineer LLC, 2019). Participants score points by obtaining flags, which consist of predetermined information about a target company. Participants first perform research using OSINT techniques over a three-week period. They can use the information they obtain to capture additional flags over the phone during a timed session at the conference where they perform vishing (i.e., voice phishing). Attackers can leverage the same information in phishing emails to make them more effective. The more the attacker understands their target, the more believable the social engineering attacks.

Another common technique used in phishing campaigns is to acquire a "lookalike" domain that victims could easily mistake for a legitimate website address. For example, if an attacker wants to pose as Twitter, they might replace the "W" with two lowercase Vs. Similarly, the "L" in Google and LinkedIn could be replaced by the uppercase "I." A more sophisticated approach to lookalike domains is the internationalized domain name homograph attack. This approach involves acquiring domains that use visually similar characters from different language sets, such as Unicode and Cyrillic. For example, since the Unicode "A" and Cyrillic "A" are visually indistinguishable from one another, the user would not recognize that they are not on the legitimate website without careful examination. Zheng (2017) provided an excellent example of this type of attack, as shown in the screenshot in Figure 1.

Although less common for phishing, since most victims click a link instead of type in a web address, typosquatting is another related method that is worth mentioning. This approach attempts to trick those who accidentally mistype an address for a legitimate website. If an attacker has already acquired a common misspelling of a particular domain, they can host a malicious replication of the real website. Unless the user recognizes their mistake by verifying the domain, they are unlikely to notice that they are on an illegitimate website before submitting their credentials or downloading malware. In Table 1, we provide example domains for popular services. Although most of these are unavailable, discussing each should help instructors explain how attackers can identify other believable domains for their intended targets.

Individuals who wish to conduct phishing have several platforms to consider, such as Gophish (https://getgophish.com) and *Phishing Frenzy* (https://www.phishingfrenzy.com). These platforms simplify the phishing process and provide anyone interested in phishing

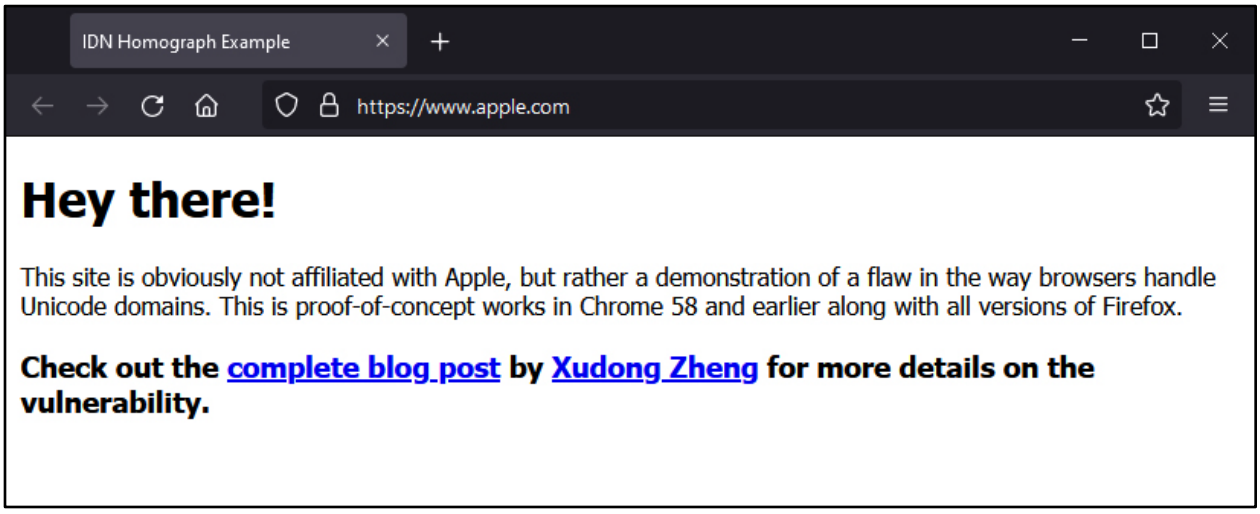


Figure 1. Internationalized Domain Name (IDN) Homograph Attacks Proof-of-Concept (Zheng, 2017)

Target Domain	Lookalike	Typosquatting	Alternate
Twitter.com	tvvitter.com	twiter.com	verify-twitter.com
Facebook.com	faccbook.com	faceboook.com	notify-facebook.com
Google.com	googIe.com	gooogle.com	no-reply-google.com
LinkedIn.com	linkeclin.com	linkedn.com	alert-linkedin.com
Dropbox.com	clropbox.com	dropbox.co	dropbox-share.com
Apple.com	appIe.com	applle.com	apple-store.com

Table 1. Example Domains

with the ability to quickly launch their campaigns. Regardless of the platform used, phishing emails and landing pages should be thoroughly tested prior to execution to increase deliverability and effectiveness. For example, emails should be evaluated to assess whether they are likely to be flagged as spam, and landing pages should be tested on multiple browsers and devices to ensure that they are rendered correctly.

2.4 Defensive Strategies

In this section, we will discuss various defensive methods that can help combat phishing threats, such as increasing user awareness, conducting internal phishing tests, implementing email filtering, performing domain authentication, and providing user warnings. We will also highlight how the adoption of password managers can help protect users against phishing attacks.

One of the best ways to protect against social engineering attacks is to improve security awareness among all users within an organization. Security Education and Awareness Training (SETA) "is a formal program with the goal of training users of the potential threats to an organization's information and how to avoid situations that might put the organization's data at risk" (Gardner & Thomas, 2014, p. 1). It is important that security awareness training programs provide a proper level of knowledge and impact user behavior.

SETA programs should focus considerable attention on social engineering attacks to raise awareness of the psychology principles mentioned earlier. Using psychological principles improves one's ability to manipulate another's attitudes, beliefs, and behavior (Schaab et al., 2017). Therefore, SETA programs should regularly inform employees about current tactics and provide knowledge about proper responses and coping behaviors (Schaab et al., 2017). Exposing people to persuasion attempts and arguments that social engineers might use is an effective way to improve individuals' decision-making processes. Unfortunately, only a small portion of organizations believe that their SETA programs are very effective (Hu et al., 2021). Therefore, we recommend complementing SETA programs with other strategies.

One method that organizations can use to assess their employees' awareness is to run simulated phishing tests. By whitelisting domains used in test campaigns, the organization can simulate a phishing attack that evades detection by email filters. This allows the organization to assess its last line of defense, the employee. The results of these tests provide valuable insights to help plan additional SETA sessions intended to mitigate insecure behaviors, such as clicking on links or sharing credentials. For example, Gordon et al. (2019) found that approximately 16.7% of healthcare workers were likely to click on links in phishing emails, but the rate decreased if employees were exposed to multiple simulated phishing emails.

Organizations should conduct OSINT research against their own assets. Gathering OSINT allows organizations to conduct an in-depth analysis of their own infrastructure and employees, all of which could be valuable inputs for strategic security planning. Hayes and Cappa (2018) demonstrated the efficacy of OSINT in improving an organization's security posture by performing a vulnerability assessment of a company's critical infrastructure.

Automated anti-phishing tools behave similarly to traditional spam filters and mail filters, also known as milters, by assessing email headers and contents according to various rules. Organizations can adopt rules from crowdsourced spam services as well as apply their own rules manually. Organizations should encourage employees to report suspicious emails so that they can review them and apply any necessary rules to prevent similar attempts from reaching other employees. There are several domain authentication methods with reliable criteria for assessing the legitimacy of an email. Domain authentication can be established for domains owned by the organization through domain name system (DNS) records, such as sender policy framework (SPF), DomainKeys identified mail (DKIM), and domain-based message authentication, reporting, and conformance (DMARC) (Nightingale, 2017). If the sending domain does not have these authentication measures in place, the recipient should view any email from the unauthenticated domain with skepticism.

However, domain authentication is not foolproof. For example, domain authentication can also make malicious domains appear legitimate. Therefore, we encourage organizations to purchase as many lookalike domains as possible and to redirect visitors to the authentic domain. This not only helps protect an organization's employees from phishing attacks but also limits the options available for attackers to target others who might communicate with the organization. Nevertheless, attackers might still find available lookalike domains that can spoof other organizations. Therefore, these efforts can only minimize the risk, not eliminate it.

Email clients should also provide employees with phishing warnings whenever the server receives emails from external domains. However, if every email is flagged as potentially malicious, employees will eventually ignore the warnings over time due to alert fatigue (Stojnic et al., 2021). Further, no rule is perfect, so there will always be false positives and false negatives. Therefore, organizations should carefully consider the rules that trigger phishing warnings to ensure that they do not desensitize employees or allow them to think that email filters can replace their sound judgment.

In addition to protecting account credentials, password managers can provide significant protection against lookalike and typosquatting domains because the credential is only associated with the legitimate domain. If the password manager

does not offer the expected credentials for a website, the user should question why that might be. It is likely that they clicked on a phishing link or accidentally mistyped the intended address. Organizations should train their users on the benefits of using a password manager and point out how it not only protects them from having their individual accounts compromised but also reduces risk for the organization.

3. EXERCISE SETUP

We do not expect students to have the technical skills to set up the proposed exercise. Our tutorial is meant to assist instructors in replicating our exercise and delivering the technical environment to students so that they can experience the phishing process from an attacker's point of view. We provide instructors with several options to consider before implementing this exercise. For example, instructors must decide how realistic they would like the exercise to be. Instructors should also determine the amount of preparation and class time they wish to allocate.

We recommend adhering to the following minimum requirements for the exercise. First, we encourage instructors to utilize white hat agreements. Second, instructors must install Gophish. Third, instructors must provide students with access to a mail server, such as Postfix. Lastly, instructors must acquire a domain to use for the exercise. If the goal is simply to expose students to a phishing platform, instructors can forego the optional domain authentication steps (Section 3.5), which would be necessary to conduct a real campaign. We discuss each requirement in more detail throughout the remainder of this section.

3.1 White Hat Agreement

If students have not already signed a white hat agreement as part of the course, we encourage instructors to have them sign one before beginning the exercise. We provide an example white hat agreement in Appendix A. This provides instructors with an opportunity to stress the ethical and legal implications of cybersecurity work. Instructors should explain to students that the difference between illegal hacking and authorized white hat activity is having permission to conduct penetration tests and security assessments. This distinction helps students realize that they can experience the fun and excitement of using offensive techniques but without fear of prosecution.

3.2 Gophish

Although there are several phishing platforms, we elected to use Gophish for this exercise. Gophish is an open-source phishing toolkit that anyone can download from a repository on GitHub (https://github.com/gophish/gophish/releases). We believe that Gophish strikes the best balance between usability and effectiveness. We recommend installing Gophish on a virtual machine (VM) by following the installation instructions in the Gophish User Guide (https://docs.getgophish.com/user-guide/). This allows for the creation of snapshots, which enable instructors to restore the VM to a clean instance of Gophish after each iteration of the exercise. Prior to facilitating the exercise, the instructor can add user accounts for each student. The instructor's administrator account will be able to assume the role of any regular user account, which can aid in troubleshooting.

3.3 Email Server

To send emails from Gophish, you must have access to an email server. There are a few options you could consider, but we recommend installing Postfix on an Ubuntu Server virtual machine. To ensure that our article remains useful, we encourage instructors to install Postfix by following Digital Ocean's guide (Drake & Jetha, 2022). We recommend this option because, although our reference points to the steps needed for Ubuntu 22.04, they regularly update their instructions upon the release of subsequent versions. Therefore, instructors will be able to select the latest release to obtain the most current installation guide.

3.4 Domain

Although it is possible to send email from existing accounts through Gophish, we also encourage instructors to purchase their own domains to use for phishing exercises. Instructors could purchase generic domains that do not mimic authentic domains, or they could search for available lookalike or typosquatting domains. Various DNS fuzzing tools, such as DNStwist (https://github.com/elceef/dnstwist), are also available to help identify lookalike domains. Once an instructor has acquired a domain, they will need to add mail exchange records that point the domain to their email server.

3.5 Domain Authentication (Optional)

The following requirements, although entirely optional, will not only enhance the realism of the phishing exercise but also increase the technical content that instructors can discuss. Enabling each domain authentication method decreases the likelihood of mail filters marking emails as spam. From a penetration testing or internal information security compliance perspective, these measures increase phishing campaign effectiveness when using lookalike domains. From an organization's perspective, employing these methods helps protect legitimate domains from spoofing attempts.

3.5.1 Sender Policy Framework. SPF records allow domain owners to specify the internet protocol (IP) addresses that are authorized to send email on their behalf. We reproduce Nightingale's (2017) example of an SPF record in Figure 2.

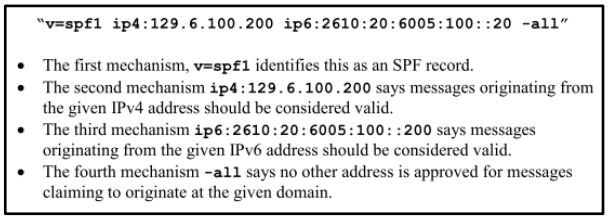


Figure 2. Example SPF Record (Nightingale, 2017)

3.5.2 DomainKeys Identified Mail. DKIM allows senders to digitally sign their email with an RSA signature, which is included in the message header. The recipient can then verify the signature by checking the public key stored in the domain's DNS record. This provides confidence that the message has not been modified in transit, such as through a man-in-the-middle attack. We reproduce Nightingale's (2017) example of a DKIM record in Figure 3.

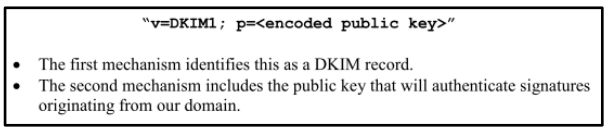


Figure 3. Example of a DomainKeys Identified Mail Record (DKIM) (Nightingale, 2017)

3.5.3 Domain-Based Message Authentication, Reporting and Conformance. DMARC not only provides authentication but also provides instructions to receiving email servers on what to do if an email fails to satisfy SPF and DKIM checks. Receivers can also share information with the sender regarding email messages that pass or fail. The use of DMARC allows e-mail services to coordinate their efforts more efficiently and effectively. The Global Cyber Alliance offers a helpful wizard for creating a DMARC record for a given domain (https://dmarcguide.globalcyberalliance.org). We reproduce Nightingale's (2017) example of a DMARC record in Figure 4.

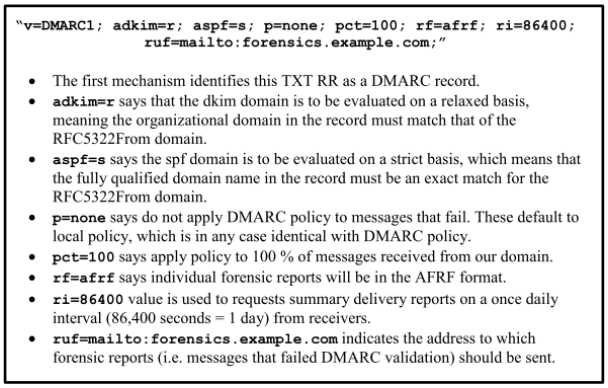


Figure 4. Example of a Domain-Based Message Authentication, Reporting and Conformance (DMARC) Record (Nightingale, 2017)

4. EXERCISE DELIVERY

Once instructors have implemented the infrastructure, they have the option of providing students with a specific target to clone or allow students to identify and select their own. Although students should be able to import most emails and landing pages into Gophish easily, we recommend providing students with preapproved options. This allows instructors to pretest the import process for various emails and landing pages to ensure that the initial exercise will run smoothly by eliminating complicated designs that can be frustrating and time-consuming for students to troubleshoot.

For our first campaign, we typically use a common email that all students are likely to have received before, such as one from their institution, Facebook, Twitter, Amazon, or Google. For this article, we will demonstrate how to create a campaign that impersonates Twitter. We have provided a copy of the instructions that we provide to students in Appendix B. Once students have demonstrated proficiency in creating and executing an effective phishing campaign, instructors can loosen restrictions to encourage further skill development.

4.1 Email Template

In our example, we replicate an email from Twitter that notifies a user when a login from a new device has been detected for their account. We obtained the source code from an authentic Twitter email, which we added to Gophish using the "Import Email" feature when creating a new email template. The only modification that we made was to replace the true Twitter username with "@ExampleAccount" for demonstration purposes. In addition to replicating the email content, Gophish automatically populates the subject and adds a tracking image to determine whether the target opened the email. We provide a side-by-side comparison of the authentic and fake emails in Figure 5, which demonstrates how attackers can easily create phishing emails that appear virtually identical to authentic emails.

4.2 Landing Page

The landing page that we replicated for this example is the Twitter login page (https://twitter.com/login). In Figure 6, we provide a comparison between the authentic Twitter login page and our landing page, which we replicated using the "Import Site" feature in Gophish. Again, the inability to distinguish between authentic and fake landing pages helps demonstrate to students just how easily attackers can execute effective phishing campaigns.

4.3 Spam Check

For a phishing campaign to be the most effective, it must be able to convince the receiving email server that it is a legitimate email. The spam check step provides an excellent opportunity for instructors to explain the importance of domain authentication measures, such as SPF, DKIM, and DMARC. The Global Cyber Alliance provides an infographic that demonstrates how all three work together to authenticate domains (https://dmarc.globalcyberalliance.org/how-it-works/).

We recommend that students assess their phishing campaigns using mail-tester.com (https://www.mail-tester.com). When students visit mail-tester.com, the service provides a random email address to use for the test. For the best results, students should enter this address into Gophish as a user target rather than using the Test Email feature located in the Email Template settings. Once students have the email and campaign configured, they can launch the campaign. After waiting a few seconds, students should refresh the mail-tester.com page. Once mail-tester.com has received the email, it will display a score and detailed analysis of the "spammyness" of the email, along with recommendations for each tested criterion. We encourage students to tweak their emails until they obtain at least a score of 8.0, but higher scores are more likely to pass through traditional spam filters.

4.4 Exercise Reset

If students are conducting the exercise through a virtual machine, instructors will be able to quickly restore the email server and Gophish instance to the snapshot. This allows for a quick reset without having to manually remove users and delete student content.

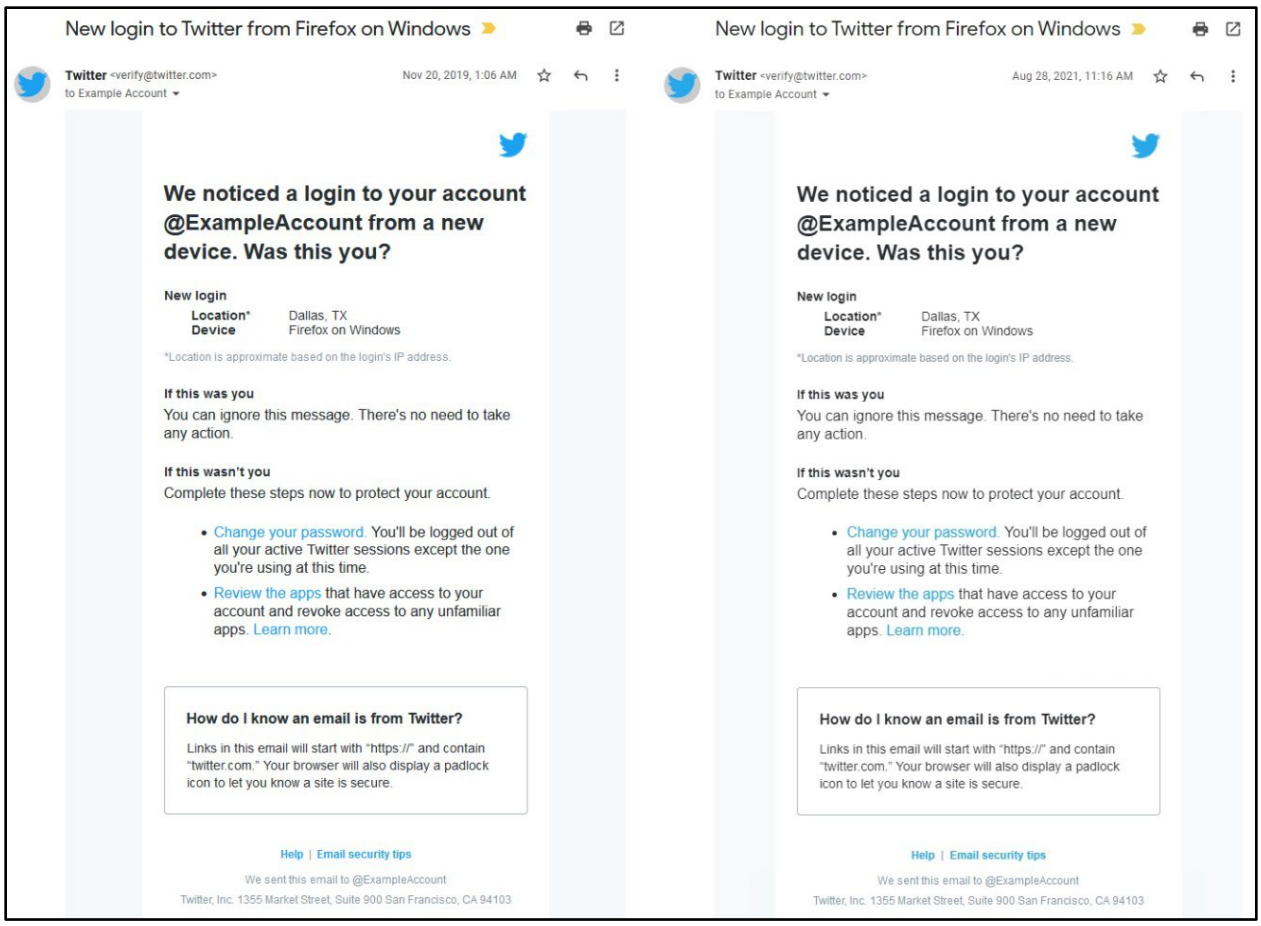


Figure 5. Comparison between Authentic (left) and Fake (right) Twitter Emails

5. RESULTS

We piloted this exercise in multiple sections of a junior-level information security course in 2021 and 2022. The active-learning portion of the exercise took approximately 30 minutes to complete. We walked students through importing an existing email and landing page, testing the phish using mail-tester.com, and then sending a phish to their own email address. To obtain credit for the exercise, the students forwarded their successful phishing email to the instructor.

After the students had successfully crafted and executed their first phishing campaign, we spent another 10 to 15 minutes discussing the security implications highlighted by the exercise. In addition to hearing feedback from students, the discussion focused primarily on the offensive and defensive strategies outlined earlier. Students also expressed how participating in the exercise opened their eyes to the phishing threat and that the experience was likely to make them more skeptical of emails in the future.

Following the in-class discussion, we also asked students to provide feedback on the exercise by completing a voluntary three-question survey. First, we asked the students what they enjoyed about the exercise. Second, we asked how the exercise enhanced their understanding of security concepts. Third, we asked how completing the exercise impacted their behavior. We received feedback from 58 students.

We identified four recurring themes in the student responses: awareness, ease, experiential, and tools. First, most student comments (62%) indicated that they benefited from an increased awareness of phishing techniques. One student believed that the exercise "*enhanced [their] understanding of security concepts by showing [them] how easy it is to click on digital things that are fake, like emails or websites. It also enhanced [their] understanding of how personal data can be stolen.*" Another student "*was able to conceptualize how easily people can be tricked into giving their credentials online without even knowing!*" The exercise showed "*that even when I thought I could tell the difference between legitimate messages and fake ones, I really cannot when using this tool. I'll have to be more careful.*" The awareness theme was also apparent in the following response: "*By completing this exercise, I am much more aware of the threat of phishing emails, and I will be much more cautious when following links. This has been an eye-opening experience, and I will need to slow down and check the email more thoroughly before proceeding.*"

In addition to increasing their own personal awareness, several students recognized the importance of educating all users on how to identify phishing attacks. One student shared that the exercise "*made me come to the realization that everyday people also need to be conscious of security breaches.*"

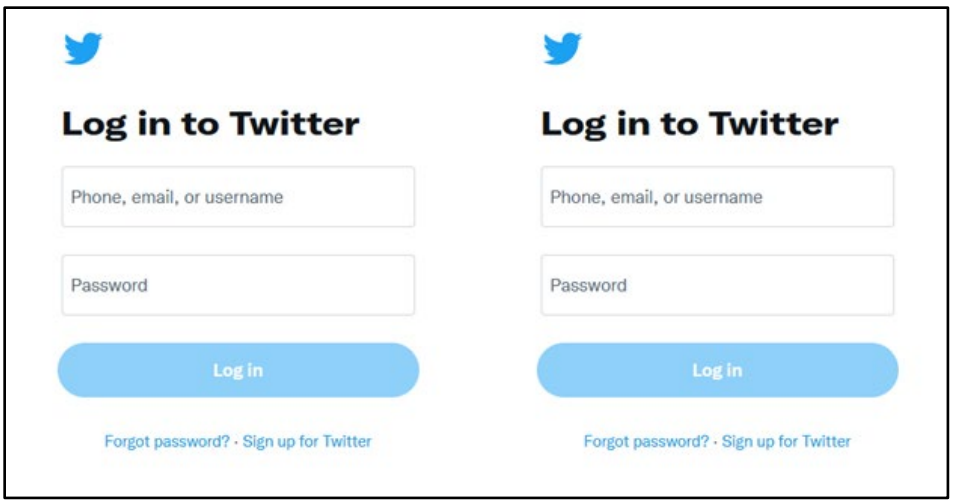


Figure 6. Comparison of Authentic (left) and Fake (right) Twitter Login Pages

Second, approximately 76% of students referenced how easy it is to develop and execute believable phishing campaigns, as is evident in the following response: "*I have received countless phishing emails in the past. I never understood how easy it was to send them until this exercise. I am an accounting major and have never really been taught what to watch out for regarding phishing emails, so I am happy I took this class!*"

Similarly, another student indicated that experiencing phishing from the perspective of a malicious hacker helped them realize how effective the technique can be: "*I really enjoy the opportunity to see how a hacker uses social engineering to distract people and manipulate receivers into doing what they want, such as clicking on the link from a phishing email. It's crazy how simple it is to create a fake email, but there is so much information that could be stolen from that.*"

Third, the students repeatedly indicated that they especially enjoyed the experiential nature of the exercise, as is evident in the following: "*As someone who learns best by doing things rather than reading about them in a textbook, the phishing exercise was very cool. It was cool both to see how easy it is to do and how phishing works outside of just 'someone steals your credentials by faking a website.*'"

Another student shared that the exercise was "*very relatable because everyone receives potentially dangerous emails, and it was insightful using a real tool to help create phishing emails. Approaching the topic from another perspective was interesting.*"

Fourth, approximately 22% of students mentioned that using a real phishing tool, such as Gophish, helped them realize the power of phishing. For example, one student shared, "*I was amazed to learn about the resources out there that can easily trick people into giving private credentials!*" Another shared the following: "*Seeing how easy it was to create a phishing email using the tool was very interesting to me during this exercise. I never realized how easy it could be to create such an email. How easy it was to use the tool made me realize that if someone understood the process, they could send hundreds of these a day and benefit quickly from a process like this.*"

Lastly, in the responses to our third question, students overwhelmingly (97%) indicated that participating in the exercise modified their behavioral intention regarding interacting with email. The two students who said the exercise would not impact their behavior explained that they were already employing best practices concerning recognizing and reporting suspected phishing emails. We summarize the frequency of student responses by theme in Table 2.

6. IMPLICATIONS AND FUTURE RESEARCH

Our proposed exercise can enhance student learning outcomes, increase phishing awareness within the community, and provide a foundation for the development of additional phishing exercises. First, instructors who teach courses involving penetration testing and security assessments can utilize our exercise to train students on phishing tools and techniques. Exposing students to our exercise can improve their personal cyber hygiene, which not only benefits the academic institution but also their future employers. Second, once students have refined their phishing skills, institutions could eventually offer local organizations a cost-effective way to conduct simulated phishing campaigns. This would not only provide students with experience in offensive techniques but also provide them with an opportunity to educate clients on phishing awareness.

Theme	Enjoyment	Understanding	Behavior	Total Frequency
Awareness	7 (12%)	45 (77%)	56 (97%)	108 (62%)
Ease	23 (40%)	31 (53%)	-	54 (31%)
Experiential	44 (76%)	-	-	44 (25%)
Tools	13 (22%)	-	-	13 (7%)
NOTE: We received a total of 174 responses from 58 students due to asking three questions.				

Table 2. Themes from Student Responses

Equipping students with these valuable skills allows them to better compete in the job market and will improve the quality of future security professionals. Third, given the rapid pace of technical development, we encourage instructors to publish similar research on in-class exercises to help others benefit from their experiences. For example, we welcome replications and extensions of our exercise, especially those that include a rigorous quantitative analysis of the pedagogical impact.

7. CONCLUSION

In this teaching tip article, we developed a detailed exercise, complete with step-by-step instructions, to help instructors provide students with an active learning phishing opportunity using Gophish. According to the in-class and survey feedback, the exercise was well received by the students. Although phishing is one of the most effective attack methods, we encourage researchers to develop exercises for other types of social engineering. For example, helping students recognize vishing attempts and the danger of USB-based attacks would also be extremely beneficial.

8. REFERENCES

Bazzell, M. (2021). *Open Source Intelligence Techniques: Resources for Searing and Analyzing Online Information* (8th ed.). CreateSpace Independent Publishing Platform.

Cialdini, R. B. (2006). *Influence: The Psychology of Persuasion.* William Morrow.

Drake, M., & Jetha, H. (2022). *How to Install and Configure Postfix on Ubuntu 22.04*. Digital Ocean. https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-postfix-on-ubuntu-22-04

Federal Bureau of Investigation. (2020). *2020 Internet Crime Report.* https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of Persuasion in Social Engineering and Their Use in Phishing. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9190*, 36-47. https://doi.org/10.1007/978-3-319-20376-8_4

Gardner, B., & Thomas, V. (2014). *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats.* Elsevier. https://doi.org/10.1016/C2013-0-12654-2

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open*, 2(3), e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

Gragg, D. (2003). A Multi-level Defense Against Social Engineering. *SANS Reading Room*, 13. https://sansorg.egnyte.com/dl/AbCFV3mA3o

Hackett, R. (2015, August 10). *Fraudsters Duped This Company into Handing over $40 Million*. Fortune. https://fortune.com/2015/08/10/ubiquiti-networks-email-scam-40-million/

Hamman, S. T., Hopkinson, K. M., Markham, R. L., Chaplik, A. M., & Metzler, G. E. (2017). Teaching Game Theory to Improve Adversarial Thinking in Cybersecurity Students. *IEEE Transactions on Education*, 60(3), 205-211. https://doi.org/10.1109/TE.2016.2636125

Hayes, D. R., & Cappa, F. (2018). Open-Source Intelligence for Risk Assessment. *Business Horizons*, 61(5), 689-697. https://doi.org/10.1016/j.bushor.2018.02.001

Headquarters, Department of the Army. (2023). *Intelligence (FM 2-0)*. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN39259-FM_2-0-000-WEB-2.pdf

Hu, S., Hsu, C., & Zhou, Z. (2021). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, 62(4), 752-764. https://doi.org/10.1080/08874417.2021.1913671

Identity Theft Resource Center. (2022). *2021 Annual Data Breach Report*. El Cajon, CA. https://www.idtheftcenter.org/wp-content/uploads/2022/04/ITRC_2021_Data_Breach_Report.pdf

Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and Warnings Are not Effective to Prevent Social Engineering Attacks. *Computers in Human Behavior*, 66, 75-87. https://doi.org/10.1016/j.chb.2016.09.012

Katz, F. (2019). Adversarial Thinking: Teaching Students to Think Like a Hacker. *KSU Proceedings on Cybersecurity Education, Research, and Practice*, 10, 55.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, 22(June), 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

Lending, D., & Vician, C. (2012). Writing IS Teaching Tips: Guidelines for *JISE* Submission. *Journal of Information Systems Education*, 23(1), 11-18.

Lewis, M. (2019). *Don't F**k with Cats: Hunting an Internet Killer* [TV Series]. Netflix.

Luse, A., & Burkman, J. (2021). Gophish: Implementing a Real-world Phishing Exercise to Teach Social Engineering. *Journal of Cybersecurity Education, Research and Practice*, 2020(2), 1-11. https://digitalcommons.kennesaw.edu/jcerp/vol2020/iss2/5

Malwarebytes Labs. (2021). *Sextortion Scam Rears Its Ugly Head in Time for 2021*. https://blog.malwarebytes.com/social-engineering/2021/01/new-sextortion-scam-in-time-for-the-new-year/

Nightingale, S. J. (2017). *Email Authentication Mechanisms: DMARC, SPF and DKIM*. https://doi.org/10.6028/NIST.TN.1945

O'Connor, T. J. (2022). HELO Darkside: Breaking Free From Katas and Embracing the Adversarial Mindset in Cybersecurity Education. *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education*, 1, 710-716. https://doi.org/10.1145/3478431.3499404

Ormeus, W. (2016). *"Is This Something That's Going to Haunt Me the Rest of My Life?"* Slate. https://slate.com/technology/2016/12/an-interview-with-charles-delavan-the-it-guy-whose-typo-led-to-the-podesta-email-hack.html

Petty, R. E., & Cacioppo, J. T. (1996). *Attitudes and Persuasion: Classic and Contemporary Approaches.* Westview Press.

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic Optimism on Information Security Management. *Computers & Security*, 31(2), 221-232. https://doi.org/10.1016/j.cose.2011.12.001

Schaab, P., Beckers, K., & Pape, S. (2017). Social Engineering Defense Mechanisms and Counteracting Training Strategies. *Information and Computer Security*, 25(2), 206-222. https://doi.org/10.1108/ICS-04-2017-0022

Social-Engineer LLC. (2019). *The 2019 Social Engineering Capture the Flag Report.* https://www.social-engineer.org/wp-content/uploads/2019/11/SECTF-DEFCON27-SECOM-2019.pdf

Stajano, F., & Wilson, P. (2011). Understanding Scam Victims: Seven Principles for Systems Security. *Communications of the ACM*, 54(3), 70-75. https://doi.org/10.1145/1897852.1897872

Stojnic, T., Vatsalan, D., & Arachchilage, N. A. G. (2021). Phishing Email Strategies: Understanding Cybercriminals' Strategies of Crafting Phishing Emails. *Security and Privacy*, 4(5), 1-17. https://doi.org/10.1002/spy2.165

Tetri, P., & Vuorinen, J. (2013). Dissecting Social Engineering. *Behaviour and Information Technology*, 32(10), 1014-1023. https://doi.org/10.1080/0144929X.2013.763860

Thompson, J., Herman, G., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., & Phatak, D. (2018). Student Misconceptions about Cybersecurity Concepts: Analysis of Think-Aloud Interviews. *Journal of Cybersecurity Education, Research, and Practice*, 1(5), 1-29.

Weinstein, N. D. (1980). Unrealistic Optimism about Future Life Events. *Journal of Personality and Social Psychology*, 39(5), 806-820.

Wikileaks. (2016). *Podesta Emails.* https://wikileaks.org/podesta-emails/

Young, J. A. (2020). Teaching Tip: The Development of a Red Teaming Service-learning Course. *Journal of Information Systems Education*, 31(3), 157-178.

Zheng, X. (2017). *Phishing with Unicode Domains*. https://www.xudongz.com/blog/2017/idn-phishing/

AUTHOR BIOGRAPHIES

Jacob A. Young is an associate professor of management information systems and the director of the Center for Cybersecurity at Bradley University. He focuses his research on privacy, security, and anonymity issues related to information systems. He serves as the Senior Advisor on Cybersecurity at the National Whistleblower Center in Washington, D.C. His research has been published in several journals, such as *Information Technology & People*, *Communications of the Association for Information Systems*, *AIS Transactions on Human-Computer Interaction*, *Journal of Information Systems Education*, *Journal of the Midwest Association for Information Systems*, *Cybersecurity Pedagogy & Practice Journal*, *DePaul Business & Commercial Law Journal*, and *Richmond Journal of Law and Technology*.

Sahar Farshadkhah is an assistant professor of management information systems at the College of Business and Management of the University of Illinois Springfield. Her main research interest is cybersecurity. Her research centers on understanding behavioral aspects of information security and helps organizations mitigate information security violations and increase employee's information security awareness and compliance. Her research has been published in several IS journals, such as *Computers & Security*, *Communications of the Association for Information Systems*, and the *Cybersecurity Pedagogy & Practice Journal*.

APPENDICES

Appendix A. White Hat Agreement

As part of this course, you will be exposed to systems, tools, and techniques related to information security. Used properly, these tools allow a security or network administrator to better understand vulnerabilities and security precautions. Misused (either intentionally or unintentionally), these tools can result in breaches of security, damage to data, or other undesirable results.

You must agree to the following before you can participate: If you are unwilling to sign this form, you cannot participate in this course.

I agree to:

- Examine only the areas outlined within the scope stated in the letter of engagement.
- Report any security vulnerabilities discovered to the course instructors immediately, and not disclose them to anyone else.
- Maintain the confidentiality of any client information learned through the course.
- Hold harmless the course instructors and _____ for any consequences of this course.
- Abide by the computing policies of _____ and by all laws governing the use of computer resources on campus.

I agree to NOT:

- Attempt to gain administrator access to any server, network hardware, or other network device to increase in privilege on any _____ workstation.
- Disclose any private information that I discover as a direct or indirect result of this course.
- Take actions that will modify or deny access to any data or services not owned by me.
- Attempt to perform any actions or use utilities in the course outside the confines and structure of authorized security assessment activities.
- Exploit any security vulnerabilities beyond the client's scope or beyond the duration authorized by the client.
- Pursue any legal action against the course instructors or _____ for consequences related to this course.

Executed as of the date and year below:

_____ _____

Student Date

Appendix B. Phishing Exercise Instructions

OVERVIEW

This exercise will introduce you to phishing. There are many phishing platforms, but we will focus on Gophish (https://getgophish.com). Gophish is an open-source tool that penetration testers and security professionals can use to assess employees' phishing awareness. You are prohibited from targeting anyone who has not agreed to receive a phishing email from you. Remember, you must always abide by the stipulations outlined in the White Hat Agreement.

ACCESSING GOPHISH

First, you will need to access Gophish. You do not need to install it on your own machine. Your device must be connected to the university network to access our instance of Gophish.

1. Visit [Gophish URL] and accept the warning for visiting a site with a self-signed certificate.
2. Sign in to Gophish using your university username and the password provided.

EMAIL TEMPLATE

Second, you will need to create an email template. Some emails will require more work than others, but Gophish does a solid job of converting existing emails into templates automatically. Knowledge of HTML, CSS, and JavaScript can come in handy.

3. Click "Email Templates" and click the "New Template" button.
4. Name your template, and then click the "Import Email" button.
5. Copy the source from your email account by clicking the three-dot button and then selecting "Show original" from the dropdown menu, as shown below. Then, click the "Copy to clipboard" button.
6. Paste the copied email into the "Import Email" textbox on Gophish.
7. Leave the "Change Links to Point to Landing Page" checked so that all links in the email will be automatically changed to our target landing page.

LANDING PAGE

Third, you will need to create a landing page that your targets will visit if they click on a link in your email.

8. Click Landing Pages and then click the "New Page" button.
9. Provide a name for your landing page, then click the "Import Site" button.
10. Paste the URL of the target website that you want to replicate for your landing page.
11. You will see a preview of the imported landing page. Clicking the "Source" button will display the imported code for your landing page, so you can make additional modifications to the landing page, if necessary.
12. Check the "Capture Submitted Data" checkbox so that you will receive your target's credentials when they enter them into the form on your landing page.
13. Once your landing page is ready, click the "Save Page" button.

SENDING PROFILE

The Sending Profile contains the email server information that Gophish will use to send the email.

14. Click on "Sending Profiles" and then click the "New Profile" button. Then, input the following values for the sending profile:
    - From: Your Name <youremail@domain.com>
    - Host: [mail server]
    - Username: [mail server username]
    - Password: [mail server password]
15. You can use the "Send Test Email" button to send yourself an email to make sure that the sending profile is configured correctly, but none of the links in the test email will resolve to a landing page. The links will only work once you have sent emails as a campaign.

SPAM TESTING

You should always thoroughly test your email and landing page before using them in a real campaign.

1. Click "Users & Groups" and click on the "New Group" button. Use "Mail Tester" as the group name.
2. In a separate browser tab, visit https://mail-tester.com and copy the email address displayed in the text box.
3. Paste the mail-tester email address into the "Email" field. Leave the remaining fields blank and click Save changes.
4. Click "Campaigns" and click the "New Campaign" button.
5. Name your campaign, then select your template, landing page, and sending profile from the drop-down lists.
6. Enter http://[DOMAIN] as the URL.
7. Select the "Mail Tester" group as the target for your campaign.
8. Click the "Launch Campaign" button.
9. After a minute or so, refresh your Mail Tester page to retrieve the results. The higher the score, the more likely your email will bypass most spam filters. At a minimum, we would like to see a score of 8.0 or above. You do not need to make any changes to your email for this demonstration, but we would want to address as many issues as possible for a real campaign.

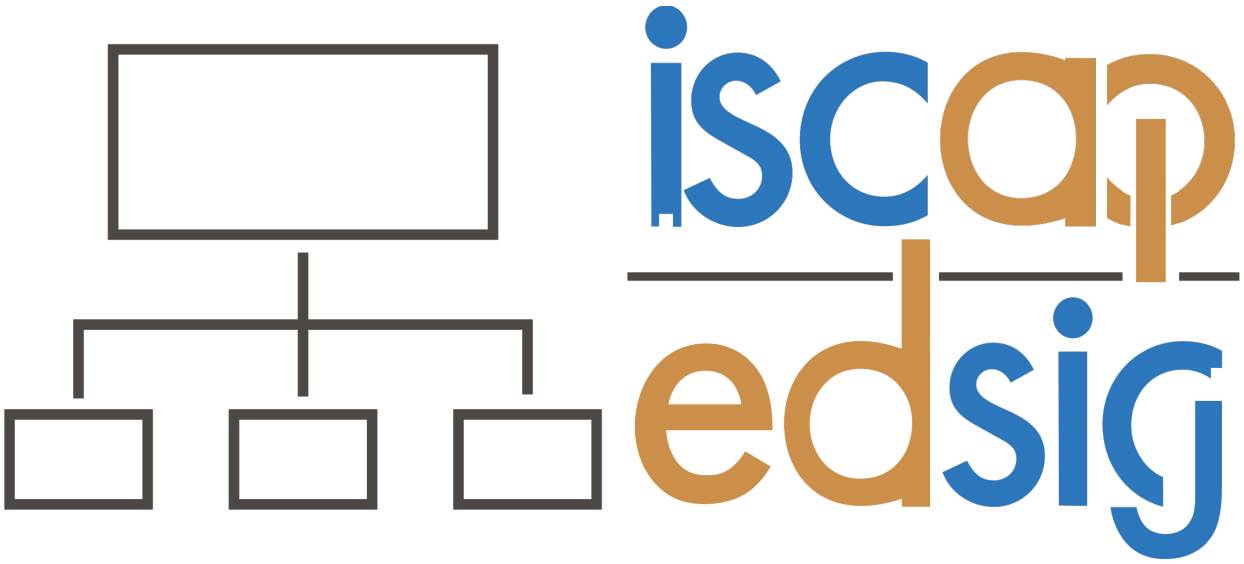
TEST CAMPAIGN

If everything worked to this point, you would want to add yourself to a campaign to test how everything would behave in a real campaign.

10. Click on "Users & Groups" and click on the "New Group" button. Use "Test Campaign" as the group name.
11. Fill in the fields with your name, email address, and position.
12. Click on "Campaigns" and click the "New Campaign" button.
13. Name your campaign "Test Campaign." Then select your template, landing page, and sending profile from the dropdown lists.
14. Enter [phishing domain URL] as the URL.
15. Select the "Test Campaign" group as the target for your campaign.
16. Click the "Launch Campaign" button.
17. Check your email to see if it made it to your inbox. If not, check your spam folder.

SUBMITTING YOUR WORK

Once you have received your "Test Campaign" email, forward the email to me at [instructor@university.edu] to receive credit for the exercise.



Information Systems & Computing Academic Professionals

Education Special Interest Group

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)