Gone Phishing: A Critical Analysis of Cybersecurity Awareness Policies in Practice at the University of Wisconsin-La Crosse

Student Author: Anatalia Radoc

Faculty Sponsor: Bryan Kopp, English Department

ABSTRACT

Higher education institutions are increasingly targeted by phishing scams due to their decentralized and complacent approach to data security, necessitating a comprehensive cybersecurity culture and awareness to protect sensitive information amidst the growing complexity and frequency of such attacks. This study uses the University of Wisconsin-La Crosse as a case study to compare university anti-phishing policies and practices with phishing messages, specifically emails, received by students to determine the efficacy of the university's information security awareness priorities. The policy analysis section used purposive sampling of UW System and UWL-specific information security policies and guidance to evaluate the university's obligations and effectiveness in protecting against phishing scams, while the message analysis section employed purposive sampling of phishing emails received by a student to assess typical scam characteristics and the efficacy of university policies in mitigating these threats. The policy analysis results indicate that UW System policies mandate annual information security awareness training for all users with digital access, including employees, students, and contractors, with specific protocols for phishing simulations targeting employees, but no equivalent requirements for students, highlighting a gap in comprehensive phishing prevention strategies across the university community. The textual analysis identifies key characteristics of UWL-specific internship phishing scams—such as sender domain spoofing, misleading subject lines, varying degrees of job description detail, and inconsistent use of logos, signatures, and formatting—highlighting significant gaps between the scam traits and UWL's current phishing prevention guidelines. Cybersecurity policy at UWL is inadequate for addressing phishing scams targeted at students, lacking necessary information security awareness training, a robust reporting system, and up-to-date guidance, necessitating bi-annual training and updated protocols to better protect students who are required to use university email accounts and are thus vulnerable to phishing scams.

INTRODUCTION

Higher education institutions (HEI) have become the latest target for phishing scams due to their decentralized nature, complacent attitude toward data security, and possession of hundreds, if not thousands, of individuals' personal information. One of the most widely accepted methods of protecting valuable personal data is creating a culture of cyber security throughout the institution via information security awareness education and reporting system. There is ample academic research to support the cybersecurity crisis in higher education. In his 2019 article titled *The Lease Secure Place in the Universe? A Systematic Literature Review on Information Security Management in Higher Education*, Ivano Bongiovanni identified several reasons why higher education institutions (HEIs) are vulnerable to attack:

> Students, academics, staff and visitors regularly access universities' IT infrastructures to consume and produce data, in a multi-modal fashion: from personal mobile phones and smart-watches (bring-your-own-device, BYOD), through corporate laptops and tablets, to laboratory sensors and swipe access card systems, the data exchange among universities as organizations and their different categories of end-users is continuous.

HEIs are places where the free exchange of ideas and connections to research, technology, and innovation are prevalent, meaning HEIs are responsible not only for securing student and faculty information, but emerging research and sensitive work as well. The tendency by HEIs to outsource information security to a third party creates a sense of complacency amongst the organization. This creates the illusions that the burden of information security has been shifted from the HEI to the third party, and thus the responsibility to ensure proper data security is no

longer theirs. This puts them at one of the most crowded intersections of information security, controlling some of the most important personal information in an environment that loosely handles tons of data every day.

Concurrently, phishing scams have been evolving at an alarming rate in the wake of the COVID-19 pandemic. In the 2022 article *How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society*, Carrol et al. notes that "Phishing email attacks are one of the top cybercrime occurrences and top cyber security threats. Phishing attacks have been the most common crime from 2020, with phishing incidents nearly doubled in regularity". Much of our lives have moved online since 2020, and thus our exposure to online scams has increased concomitantly. While attacks are growing in frequency, they are also evolving in complexity. A 2018 article titled *Phishing – challenges and solutions* illustrates how scammers have revolutionized their social engineering and targeting tactics to pin down potential victims:

> "There are dangerous new advanced phishing methods that utilize personal information that is easily available to the public in order to produce plausible and believable attacks that directly target victims. Methods such as social phishing and context aware phishing are perfect examples of attacks utilizing the massive amount of public information to increase the effectiveness of their scams. One study shows that victims are 4.5 times more likely to fall for a phishing attempt if it is from a personal contact or personally relates to them. Phishers have become more skilled at forging websites to appear identical to the expected location, even including logos and graphics in the phishing emails to make them more convincing.

The increase in frequency and complexity of phishing emails coupled with the complacency of HEI's to effectively address cybersecurity policies leaves a gap between the intersection of university anti-phishing policies and the evolving nature of phishing scams as it concerns all university stakeholders. This research is concerned with discovering if said gap exists at HEI's, the extent to which the gap endangers university stakeholders and leaves them exposed to phishing scams, and how HEI's have addressed the problem in the wake of the increase in phishing attacks since 2020. This research is a case study into cybersecurity and anti-phishing policies and practices at the University of Wisconsin-La Crosse to discover the extent of which university policies and practices have kept up with and continue to monitor current phishing threats as they concern all university stakeholders, including faculty, staff, and students. This study will outline a framework to assess the efficacy of a university's cybersecurity policies and practices and identify the gaps that exist in a university's response to evolving cyber threats.

Commented [AR1]: Could add a section about recommended policies/practices?

METHODS

Policy Analysis Methodology

The sampling method used for the policy analysis section was purposive sampling of all UW System information security policies, UWL-specific phishing policies and guidance issued in the past 10 years, and UW system internal employee memos. This method allowed for an exhaustive search to be conducted into all controlling policies and influencing guidance that shape UWL's overall phishing mitigation strategy. The purpose of the policy analysis section is to identify the university's obligation to protect students from phishing messages and what their specific responsibilities are as outlined in the UW System's Information Security policies. The purpose of analyzing non-policy, UWL-specific phishing guidance is to assess the quality of said guidance and its relevance to the scams facing students today. These articles were chosen based on their frequency of use by the University as current and relevant guidance; many of the selected articles/videos are linked on the university's website as the definitive and exhaustive source of phishing mitigation guidance. However, a few articles were chosen that were not available to students directly but were used in internal employee communications on the UW system employee intranet. The purpose of looking at both student-directed and employee-directed phishing guidance is to determine the gaps in guidance given to both parties to gain a better understanding of the cybersecurity landscape as it applies to all university stakeholders.

Each article/policy will be described objectively, pulling quotes directly from the source material whenever possible, as well as being read plainly and deferring to UW system definitions when defining key terms. This is to ensure that no subjective bias will be allowed to influence the reading of the text. Though all UW System Information Security policies were analyzed during the research process, only those most relevant to phishing

mitigation strategy were included in the analysis section. The goal of this section is to identify the phishing-specific information security policies that control local university practice and discover the parameters and most popular guidance issued by the university as to recommended phishing mitigation strategies. These will then be compared with real phishing messages received by a UWL student in the past 6 months to determine the efficacy of said policies and practices, and highlight discrepancies, if any.

Message Analysis Methodology

The sampling method employed for the message analysis section was purposive sampling, or intentional selection from a pool based on specific characteristics. This method allows for the selection of specific emails from a set of samples that are relatively homogenous to analyze specific rhetoric and characteristics of unique and usual examples. Though there is room for selection bias by the researcher, the emails selected were from a sample set that are homogenous, in other words, the selected phishing emails are representative of those that were not selected. There is little variation in the set, and the overall selection criteria is laid out below. Additionally, the emails selected for analysis were received by the same account. If this experiment were to be replicated in the future, one could obtain emails from multiple students. However, one recipient was chosen for convenience and feasibility of completion within the timeline and resources. This does not contribute to selection bias, as the scams received by the researcher were in relation to their role as "student" within the organization, meaning other similarly situated individuals (students) would receive the same emails as well. There were no other studies or sources influencing the selection of emails for analysis.

The content of the sample emails is specifically directed at internship scams, as that type makes up most of phishing emails received by the researcher in that time frame, however date sent was not a relevant factor in email selection. Emails that included IT notifications of account termination, system maintenance, and other subject lines not including internship scams were excluded from consideration, as those represent a small fraction of scams received. Emails with the subject line including the words or phrases "Part-time, personal assistant, student employment, student job, career opportunity, administrative assistant", and similar were taken into consideration. Emails with both non-university and university-affiliated domain names were considered, as well as those emails that included links and those that did not. Emails that included reputable non-profit organizations, such as UNICEF or the Red Cross, were given special consideration, as those represent the more effective, persuasive scams. The emails chosen are representative of the sample set based on their content; as internship scams, there is little variability in the format. Though the sender, organization, pay, and contact methods may vary slightly, factors like the stated qualifications of the job, job requirements, and structure of the interaction are the same. The latter are essential for the scam to be initiated, as the remote flexibility of the position guarantees only telecommunications and garners the trust of the victim to carry out tasks like purchasing supplies without meeting the employer face-to-face.

Five emails were selected for analysis based on the stated criteria. These emails will be analyzed and coded based on:

- Sender's email domain (non-university or university-spoofed)
- Mailbox received (focused/other/junk)
- Organizational affiliation (private/public/non-profit, department)
- Inclusion of logos/other official demarcation
- Job description/requirements (remote vs. in person)
- Time requirements (flexibility)
- Pay rate
- Contact method (email/phone/link, preferred method of communication)
- Signature block
- Grammar/formatting (general appearance)

These elements represent typical phishing awareness guidance, such as sender domain, inclusion of official logos, signature block, and grammar and/or formatting inconsistencies. They also account for elements unique to internship scams, such as organizational affiliation, job description/location, time requirements, pay rate, and contact method. The mailbox that received the message indicates where in the student's Outlook inbox the message was

initially sent; the "focused" inbox receives the highest priority messages, with messages filtered to "other" and then "junk" based on Outlook's algorithmic categorization of the message based on content, sender, and frequency of interaction from the student. Messages that come from UWL-domain accounts will automatically be sent to a student's focused inbox.

RESULTS

Policy Analysis Results

UW System Information Security Awareness Policies. UW System Policy 1032 (2021) titled "Information Security: Awareness" details the various levels of security awareness training all "authorized users who are issued digital credentials to access non-public IT resources … including but not limited to: currently enrolled students, employees, authorized contractors, vendors, volunteers, and other authorized users as determined by UW institutions (SYS 1032, 2021) are required to receive.

Annually, employees must:

a. Upon hire and annually thereafter, review Regent Policy Document 25-3, Acceptable Use of Information Technology Resources and any supplemental institution acceptable use policies, if applicable.
b. Complete information security awareness training, as assigned, that provides information security best practices and explains the individual's role in protecting the university's systems and data. Employees shall be assigned security awareness training on an annual basis. Security awareness training must be completed within the timeframe prescribed (SYS 1032, 2021).

The policy describes penalties for employee's who do not complete information security awareness training, including:

> Institutions are responsible for ensuring that employees have access to, and have completed, information security training as prescribed. For any employee who fails to take security awareness training within the timeframe prescribed, the university may take steps to reduce the risk associated with the employee's continued access to university resources, up to and including the suspension of the employee's network account (SYS 1032, 2021).

Systemwide, the policy also outlines role-based training supplemental to the required awareness training:

> "When appropriate, institutions should supplement the systemwide information security awareness training with role-based training commensurate with an employee's roles within the organization. Institutions may also foster additional broad-based information security awareness activities as they deem necessary through methods such as:
>
> - Websites
> - Email
> - Social media
> - In-person or online training sessions
> - Conferences or events
> - New employee or student orientations
> - Social engineering campaigns (SYS 1032, 2021)

Conversely, students must annually:

a. Receive notification of Regent Policy Document 25-3, Acceptable Use of Information Technology Resources.
b. Be provided access to information security awareness training that includes information security best practices and their role in protecting the university's systems and data (SYS 1032, 2021)

Vendors, authorized contractors, and other UW approved authorized users "whose employees will directly access UW System data and resources, [contract] language such that employees will complete security awareness training by their employer, prior to accessing UW System data and resources" (SYS 1032, 2021). Protocols for volunteers are not mentioned, but it can be assumed they would be incorporated into this third-party clause should their work directly access UW system data.

Phishing Simulations. Beginning in 2017, the UW system implemented a phishing awareness program to test employees' digital literacy when it comes to online scams (UWSA, 2017). UW System Policy 1032 sets the framework for phishing simulations supplemental to the security awareness training to be conducted at various points throughout the year. These consist of bait emails designed to look like real phishing emails to test employees on their abilities to identify scam emails. Should they "fall" for three of these campaign scams by clicking on the link provided in the email, they will be enrolled in supplemental phishing training and must complete it within 30 days of assignment.

Though this program is required of employees, the policy does not indicate if the same is true of students. Section A of UW SYS Policy 1032 titled "Security Awareness Training*"* indicates that "social engineering campaigns" may be included in "additional broad-based information security awareness activities" conducted by the University supplemental to their required training (2021). Social engineering campaigns are defined by cybersecurity company Proofpoint as "the set of tactics used to manipulate, influence, or deceive a victim into divulging sensitive information or performing ill-advised actions to release personal and financial information or hand control over to a computer system" (Proofpoint, 2023). This includes phishing, voice phishing (vishing), SMS phishing (smishing), CEO/executive fraud (spear phishing), and other forms of fraud.

The policy does not define "social engineering campaign", what it would look like on campus, or the scope of those involved, however it could be inferred that phishing simulations fall under their umbrella of "social engineering" based on all available definitions of the term. "Broad-based information security awareness activities" does not define the scope of said activities, but based on the included examples, such as websites, email, conferences, and student/employee orientations, it can be implied that the scope would include all those with UW system credentials, meaning both staff and students. Regardless, any supplemental campaigns targeted towards students, nor any subsequent training, are not required, nor are they conducted by the university.

UW System Administration Employee Intranet. In a December 2017 article titled "UW System Phishing Awareness Program to Begin in December", a background is given on phishing to prepare employees for the upcoming phishing campaigns. It defines phishing as "…[A]n online scam, usually leveraging email, involving carefully crafted messages with a link that appears to be from a trusted source, but is not (UWSA, 2017)" It also outlines the purpose of phishing emails, as well as offering tips to avoid them:

> Phishing messages may ask for you to respond with your information by email, phone, or most commonly, by clicking upon an embedded browser link within the email message you have received. To be safe, do not click on links in the email; instead, visit websites by typing the web address directly into your browser's address bar. If a message sounds suspicious or too good to be true, it is most likely an attack. Simply delete the message. To protect yourself, keep the following in mind:
>
> - If you are suspicious about a message from someone you know, call the person to verify it was actually sent by them.

- Be suspicious of any email directed to “Dear Customer” or some other generic salutation.
- Be skeptical of any message that requires “immediate action.”
- Be suspicious of messages that have grammar or spelling mistakes.
- Before you click on a link, “hover” your mouse over it. This will display the true destination. Do not click on the link if it looks to be an illegitimate website (UWSA, 2017).

The article does not define what makes an email “suspicious” or “too good to be true” but leaves the definition up to the employee’s best judgement. Additionally, it emphasizes the importance of avoiding suspicious links and the risks involved with exposing the system to malicious actors. It mentions taking caution with emails that are overly generic, pressuring, or that have grammar/spelling errors, however, it does not mention checking if the email sender’s domain is legitimate or spoofed.

Knowledge Base. The UWL internal general knowledge board for technologies and teaching tools included an 2018 article titled “Phishing-How to Spot a Phishing Email”. This was one of three articles on phishing offered by Knowledge Base and is the only one to contain a comprehensive definition of the topic. It is also regarded as the definitive anti-phishing guide from UWL for students, as this is the source identified on the UWL Help Desk webpage. It defines phishing as:

> …[W]hen someone is trying to obtain your confidential or financial information. It may be an email from someone claiming to be a friend asking you to wire money to a far-off country or someone claiming you won money, but they need your financial account information to deposit it (UWL, 2018).

The mention of asking one to wire money to a far-off country is in reference to an infamous phishing campaign from the early 90’s dubbed the “Nigerian Prince Scam.” In the email, the sender would pose as a Nigerian Prince or high-ranking official from different foreign country requesting your assistance in closing a business deal with the government of that country and a legitimate business. The victim would be asked to deposit a large sum of money-often tens to hundreds of thousands of dollars, in a foreign bank account-and in return, they would receive a large share of the deal price. In 2018, Americans lost an estimated $703,000 to this type of scams (Leonhardt, 2019), however they represent a small fraction of social engineering scams that exist today.

The Knowledge Base article then outlines various strategies for identifying and protecting oneself from phishing scam attempts, including:

- Phishing emails will usually have bad grammar, poor spelling or even odd formatting. They often contain links, images, and attached files that they tell you to click on. Or, the phishing emails may try to engage in a conversation with you in order to get you to take an action, like buy gift cards for you to share with them or sharing personal information with them.
- UWL emails will usually contain official logos and signatures, so be careful of any suspicious logos and signatures within these emails.
    - Note: Phishing emails are becoming much more sophisticated. An official logo does not guarantee the e-mail is valid.
- Phishing emails will most likely have been sent from non-university email accounts, so always double check the sender of the suspicious email, even if the email signature looks legit.
- Don't fall for threats and be cautious of emails stressing urgency which appears unfounded
- Look at inconsistencies in email addresses, incorrect order of characters, or URLs which have added characters or numbers. For example. www.uw1ax.edu or uwlax.@edu (UWL, 2018)

This article further lays out the foundation for what phishing emails are more so than the 2017 UWSA article. They echo some of the same points as the UWSA article, namely how phishing emails will have bad grammar and spelling, skepticism at emails urging immediate action, and suspicion of foreign links. It goes on to

elaborate about email domain spoofing; often, phishing attempts will either have domains that imitate legitimate ones while varying one element, such as uwlax.@edu vs. uwlax@edu, or come from a non-university affiliated email to begin with. It also mentions how most university affiliated communications will contain an official seal or logo, however modern scams may render this hallmark useless, as they too use official seals to feign legitimacy.

Educational Videos. UWL has released two educational videos about the dangers of phishing and how to protect oneself. The first video, titled *Cyber Security-Don't Click on the Link!* was presented at Cybersecurity Keynote for the UW system ITMC Joint Conference held at UWL in 2017. The purpose of this video was to explain the importance of online safety, as well as offer other UW system universities strategies to keep students and staff informed about phishing attacks.

The video does not define what a phishing attack is, but they offer some reasons why phishing attacks are targeted at universities and when they are most effective. Director of IT Client Services James Jorstad asserts there are two major reasons: first, attackers will target students at the beginning of a school semester because new freshman are not part of the "culture of cyber security"; second, the rise of smartphones makes it difficult for mobile users to differentiate between real and scam emails, leading users to click on suspicious links at a higher rate. Because they cannot hover over these links on a mobile device like they can on a computer, he claims smartphone users are more likely to click on dangerous links and subject the university to risk (UWL, 2017).

Jorstad then puts forth five strategies to increase phishing awareness and security online and on campus. First, students and staff should regularly change their passwords and use multifactor authentication services. If one believes their information has been compromised, they should change all affected passwords immediately. Second, the university should have a "good communications team" that includes one person or a group of people "vetting your messages to make sure they're clear, short, and brief". It is unclear what this is in relation to. Third, universities should use analytical, digital, and analog tools to track email usage and plan for better email communications in the future. Fourth, target and time messages to maximize outreach. Fifth, and most importantly, universities should create a "culture of cyber security". This means identifying student and faculty advocates of cybersecurity to help spot and report phishing attacks, as well as educating the university population on how to spot and report attacks themselves (UWL, 2017).

This video offers the most comprehensive explanation of phishing attacks and the importance of protecting oneself, however it lacks a proper definition of the term itself. Additionally, many of the strategies for universities seem attenuated from the issue itself; having a good communications team, timing emails to maximize visibility, and varying communication mediums are all strategies that could further proper communications about phishing but do nothing to address the problem itself. The video does offer one unique strategy, by introducing the idea of creating a campus culture of cyber security. While other methods of phishing prevention may be costly and difficult to implement, creating a culture of cyber security is one of the most effective methods of phishing prevention. By educating students and faculty on what phishing emails look like, ways to identify a scam, and how to report them, campuses can better fight scams without spending money on anti-phishing software. The video does not elaborate on ways to create a stronger culture of cyber security.

The second video, titled *The CyberZone: The Link to Disaster*, is from February 2020. This video was posted by the university as an update to the original video from 2017. The video does not define phishing but claims that human error is the largest cause of cyber security breaches and offers a few strategies for individuals to protect themselves and their universities. First, don't click suspicious links or use your mobile device to access suspicious links. Though an email may have official-looking signage or logos, does not mean it is coming from that organization. Second, all passwords should be strong, containing a combination of uppercase and lowercase letters, special symbols, and numbers. Third, all accounts should have different passwords to limit the damage should a data breach occur. If the same password is used for multiple accounts, then a hacker could easily access other accounts as well. If an account has been breached, one should change their password immediately (UWL, 2020).

This video only offers three strategies to keep individuals safe from phishing attacks but offers no solutions for the greater university. The strategies offered in the video are echoed in other anti-phishing messaging disseminated by the university but does not address how to identify phishing attacks in the first place. Though it touches on being wary of official-looking logos, it does not offer any other tips for identifying phishing attacks.

Message Analysis Results

Message One. The message comes from a university affiliated email, meaning it is likely spoofed. The sender is reaching out to the recipient on behalf of UWL sharing job information about a part-time job opportunity for UNICEF. The position would net $450 weekly. There is no job description, however the sender notes at the bottom that the position is "strictly work from home", in all caps. The recipient is asked to contact Dr. Peter Harrison at harrisonpeter842@gmail.com, a non-university affiliated account, and asks the recipient to respond with a non-university affiliated account. The message ends with "Regards" without a comma, and a large official UWL logo.

This email was selected because it is representative of the majority of the sample set: a. it includes a university spoofed account that is indistinguishable from a non-spoofed account; b. it includes an official university logo; c. the position is at a well-known non-profit organization; d. the grammar of the message is nearly flawless. First, from all appearances, the message is from a university-affiliated account, as it appears identical to all other student accounts with the student's last name followed by 4 numbers and @uwlax.edu. Additionally, the message was sent to the student's main mailbox, and the university logo is displayed very large at the bottom of the message, making the message seem as though it were sent through a job outreach program at the school. UNICEF is a well-known organization and would likely elicit a response from a student looking to gain experience with such a renowned organization.

The message includes no links and encourages the recipient to reach out to the provided email directly to enquire about the position. The message contains no syntactical or spelling errors, however it does contain a few punctuation errors: there is a space between the slash separating "students" and "staff", and the message chooses to use a backslash instead of the typical forward slash. There is also a space between the curly braces on either side of the non-university email, and the braces are inconsistent with the rest of the message, which uses brackets. The phrase "Paid UNICEF Part-Time Job" capitalizes the first letter of each word, as well as "Weekly" at the end of the sentence. The signature block does not contain a comma after "Regards" and does not include a name.

Message Two. This message comes from a university affiliated account. The sender is reaching out on behalf of the American Red Cross about a part-time, remote distribution assistant position. The assistant would "work in the procurement and distribution of essential products… to individuals with disabilities, students, and foster homes in your local community. The position description states that the role would require students "purchase items online and drop-ship them to individuals with disabilities, students, and foster homes in your local community". The job description states that the position is flexible, part-time, and remote, all qualities busy college students would likely find attractive in a school-year job. The recipient is asked to contact Michael Lander at micheal.lander@hotmail.com with their frequently used personal email. The signature block contains the name of the sender, Noah Van Asten, as well as their position on the mass care team at the American Red Cross.

This message was chosen for its strong ties to a legitimate organization and stylistic choices throughout. The message establishes its ties to the American Red Cross, a notable non-profit organization, within the first few words. It furthers its legitimacy by listing the affected groups as "individuals with disabilities, students, and foster homes in your local community", all typical vulnerable groups served by the Red Cross. It repeats the same phrase in the job description, word for word, in the following paragraph, which is an odd stylistic choice.

This message does not explicitly ask recipients to respond with a non-university email, but rather to "use your frequently used personal email for regular communication", implying they should use a personal, rather than school-related, email account. The message signs off by thanking the recipient for their interest in working with them, and a signature block which includes the sender's name, Noah Van Asten, as well as his position on the "mass care team", and the organizations name. Notably, Michael Lander is not mentioned again, and his position in the American Red Crosse is never mentioned. It is also not explained why applicants would message Mr. Lander rather than Noah Van Asten, nor how the "mass care team" relates to Van Asten's perceived role as an outreach and recruitment

coordinator. Though the subject of the email is “UWL Job Posting”, it does not appear that Van Asten works for the university, as his name appears in the signature block connected to the American Red Cross.

The message is written in a uniquely formal style. In the initial job listing, the position’s function is described as “the procurement and distribution of essential products”. The term “procurement” is unusual in this context, as it denotes the formal process of obtaining goods rather than the informal nature of the position. A remote drop-shipping assistant position would likely not be establishing official channels of distribution but ordering supplies from online retailers and sending them to the appropriate parties. Additionally, the message does not contain any grammatical errors, and only one spelling error; Michael Lander’s email address is Micheal.Lander@hotmail.com, which is a different, and generally incorrect, spelling of the name “Michael”. This is the only grammar or spelling mistake in the entire message, which is notable because a typical “tell” of a phishing email is frequent grammar or spelling mistakes. The absence of grammatical mistakes, coupled with the uniquely formal style, lends to the theory that this message was AI-generated, though this cannot be independently verified.

Message Three. This message comes from a university-affiliated account. The sender is reaching out on behalf of Association and Community Management, an HOA management company, about an administrative assistant position. The duties and responsibilities are listed in bullet form, and resemble duties and tasks typically required of an administrative assistant: reply to email, telephone, and face-to-face inquiries, manage paperwork and filing, follow up on requests for vendor proposals and prepare bid summaries, and assist homeowners with problem resolution. Notably, the job duties do not mention purchasing or drop shipping, nor does the message assert that the position is part-time, flexible, or remote. Association and Community Management is a legitimate organization based in Colorado, and one can infer that the scam solicitation would necessarily mean the position is remote, as it has been sent to students in Wisconsin. However, the job requirements do not imply this position would be remote, as one of the responsibilities entails “reply[ing] to email, telephone, and face-to-face inquiries.

This message was chosen for a few of its unique qualities. First, it is not explicitly an internship scam in the way many others are: first, applicants are asked to copy and paste a link to fill out a form to be considered for the position. Upon following the link, a page appears saying “the website’s trial period has ended”, and there is no place to enter information. This leads to a few inferences: had the link been clicked when the message was sent, it can be presumed that a website was created to mimic the real ACM website to further lure applicants into divulging personal information. Second, it is impossible to know what the intentions of the scammer was. Often, when scammers use fake websites to trick users, it is to gain access to their accounts, passwords, or financial information. However, it is unclear how the scammer would have obtained this information during the onboarding process. One is not typically asked to divulge user names, passwords, or sensitive banking information like a routing and account number during their onboarding at a new company, so it is unlikely this was the goal. It is more likely that the website would have gotten the applicant’s personal email and initiated a conversation from there, however since the website is not live, it is impossible to know.

The second reason this message was chosen was because it was sent multiple times by multiple different accounts. The first time it was sent was 7/18/2023 from [redacted]8957@uwlax.edu. The second time was a day later on 7/19/2023 and was sent by [redacted]2025@uwlax.edu. These emails are identical to each other, including the link. The third message was sent on 7/22/2023 from [redacted]6812@uwlax.edu. The content of this message is the same, but the link is different. When the link was followed, it resulted in the same “trial period” message.

The message contains a few grammatical, spelling, and formatting errors. The first line contains a formatting error, placing a space before the first word to indent it slightly, and drops the plural suffix in United States, making it United State. In the first two iterations of the message, it does not add a space between company background and Job Duties and Responsibilities line In the last line, whereas in the message sent to [redacted]6812@uwlax.edu, it was. Finally, it capitalizes the word Below in the middle of the final sentence, and includes the line “NB (Makes sure you copy the url to apply), which uses the improper form of “make”, and uses spaces before and after open brackets. The message does not contain any UWL affiliated logos or signage, and the signature block is empty after “regards,”. In the message sent to [redacted]6812@uwlax.edu, there is an unidentified picture that appears to be an unrendered logo or signature block.

This message was sent from a university-affiliated account. This email is unique in that it is split into two parts: the message and a google form. These will be analyzed separately and compared for stylistic and content differences. The main message does not indicate if the sender is affiliated with the university, however the UWL logo is featured prominently at the bottom. The position is listed as “Personal Assistant/Bookkeeper”, though there is no stated company or organization tied to the position. There is no job description that states the roles and responsibility of the

position, rather the message emphasizes the remote, flexible, and part-time nature of the job and how applicants must be "organized and attentive to details". In the paragraph long email, it uses the word "flexible" and "part-time job" three times respectively and claims that "all the tasks are work from home/on campus job, you don't need to travel somewhere and also you don't need to have a car to get started", thus indicating the remote nature of the position. The position would pay $450 and require 5-7 hours weekly, though it does not explain how many days a week the job would be.

Message Four. This message was chosen for multiple reasons: first, it has a grammatical, syntactical, and form style most similar to a stereotypical phishing email, as well as including a link to initiate the recruitment process. Second, it has a two-step process with the Google form and continues its unique style throughout both documents. Third, while it collects information from applicants similar to other internship scams, it also collects information for an unspecified use. The goal of internship scams is not to obtain any kind of credentials, so it is unclear what will be done with that information.

The message has a uniquely unconventional style and formatting characteristic of a stereotypical phishing email. The tone is informal, illustrated by the phrase "you don't need to travel somewhere and also you don't need to have a car to get started". This phrase feels like a stream-of-consciousness sentence, with details strung together like an afterthought. The word "somewhere" is vague and is an unconventional fit for that phrase, and the detail about the car seems irrelevant; since it was already established that one doesn't have to go anywhere for the job, it would follow they would not need a car.

The following line directs the applicant to look below for more information, however the information is listed in the paragraph itself rather than bulleted below. After the message lists the job hours, it adds no punctuation before beginning the next sentence, which again tells the applicant to look below for information that is included in line with the paragraph. The link is attached to the phrase "APPLY NOW" which was inserted in the middle of the sentence "Don't miss this APPLY NOW for further details", creating two sentences in one; "Don't miss this APPLY NOW" and "APPLY NOW for further details" are themselves complete phrases, however the message strings them together. The message concludes by reminding the applicant that the position is "a Flexible part-time job" and repeats the phrase "FLEXIBLE HOURS" again below.

The tone and appearance of the message itself appears to be a stereotypical phishing email: odd formatting and capitalizations, unconventional syntax, and users must click on a link to proceed with the application process. One feature unique to this message was the image used as the profile picture. The picture is of a young man, 20-35, dressed in a tan suit from the neck up, with fair skin and dark hair. None of the other phishing emails received by the researcher included an image in the profile picture. It could not be determined the identity of the person in the picture, nor whether the image was taken of a real person or computer generated.

If the applicant clicks the "APPLY NOW" link, they are taken to a Google Form titled "Job Placement and Student Welfare". The form includes an "about me" section, job responsibilities, benefits, and form questions. The form appears to be more credible than the message, as it offers more details about job responsibilities, benefits, and schedules, however it was written in a similar style. The "about me" section includes information about the employer, their background, and values:

> I'm an International Businessman / Consultant with high moral and ethical values who is also a Philanthropist, entrepreneur that is involved in many different projects from real estate to retail businesses, Real estate investor and Investment trader. I have been successful in a handful of ventures and also got involved in investment Networks in both Canada and the United States to various welfare and community service programs, I love to work and enjoy challenges. This job is a great opportunity to learn business skills they don't teach you in school. But presently in Australia running some network programs, will be back to the States by 28th of next month.

There are several similarities between this paragraph and the original message, specifically in the long, stream-of-consciousness like phrases. Adding the phrase "who is also" after mentioning high moral and ethical values seems to indicate the following labels are additional to the original label of "international businessman / consultant", which itself is two labels. By adding so many high-profile job titles to the nameless employer, it widens the net of interest from college students; international businessman, consultant, philanthropist, entrepreneur, real estate investor,

and investment trader are all positions within the field of business and stand to make the credibility of the employer and potential for growth by working with this person appear greater. The employer illustrates this point, saying “this job is a great opportunity to learn business skills they don’t teach you in school”, indicating to the applicant that they will have the opportunity to be under the wing of a person with advanced knowledge in many areas of business and finance.

The form outlines the job responsibilities in greater detail than the original message, and includes a section on benefits, which is unique to this message; no other internship offering has mentioned benefits. The benefits would include $450 weekly, AD and D insurance, and a 401k. It is wholly unclear why the internship would offer that kind of insurance, as AD & D insurance covers “accidental death and dismemberment”, and this position does not imply any danger inherent in the position. The job responsibilities include “assisting with errands such as will be assigned", “schedule, bookings and payment for reservations for events on behalf of my clients”, and “purchase and deliveries of Gift Items, Groceries, Stamps, and Stationary”. Aside from the odd grammatical choices, these responsibilities prepare the applicant for what the employer will ask of them as part of the scam: making purchases on their behalf. This section takes a formal tone compared to the rest of the form, which is generally informal.

The message concludes by asking the applicant a series of questions: Full name, email, alternative email (non school), phone number, current occupation, bank name, school name, age, sex, and available time. Some of this information is relevant to the scam, like your name and non-school email used for communication, and phone number and bank name used to send the initial Zelle payment. It is unclear why the form asks for a school name, current occupation, age, sex, or available time.

Message Five. This message was sent from a non-university affiliated email with a @gmail.com domain. It was sent on behalf of Professor Elliot Forbes, an assistant professor of computer science at UWL, looking for a virtual student assistant to support him within the department. The job tasks include “managing my calendar, email sorting and correspondence, and assisting with data collection”, and would be paid $350 weekly. The position is remote to “[allow] you to balance your academic commitments while gaining valuable experience in a professional setting”. Additionally, the job is open to students of any department in the university, greatly expanding the net of prospective students eligible for the position.

The message includes key qualities applicants should have, like strong organizational skills, ability to work independently, communication skills, and basic proficiency in “relevant software and online tools”, which are unspecified. In return, the opportunity will afford applicants “valuable networking opportunities, hands-on experience in cutting edge research, mentorship and flexible hours to accommodate your class schedule”. These qualities make the position incredibly attractive, as students are keen to gain experience that will serve them well outside of the institution. Applications should be sent directly to the sender’s email rather than an outside email, and they offer a phone number “for more information on the position”. This maximizes the messages legitimacy, as no other internship scam solicitation has included a phone number one can call for more information. The area code is (669), which serves San Jose, CA, and the surrounding area. The message concludes with a signature block, which includes Elliot Forbes and his position as assistant professor in the department of science and engineering at UWL.

This message was chosen for many reasons: first, it is the first in the sample set not to be sent from a university affiliated account. As such, it is also the only message without a link that invites applicants to respond directly to that account. Second, this message is highly personalized and directly targeted at college students who attend this specific university. Elliot Forbes is a real professor at UWL who holds this exact title and department. The message is written from perspective directly to the student. Often, these scams use an intermediary, or a university-affiliated account to speak on behalf of individuals looking to solicit interns and assistants. It is more feasible for a UWL professor to solicit interns by directly reaching out to students, thus making the position seem more credible.

There are a few small grammar mistakes that, when considered with the entire tone of the message, go unnoticed. This is because the message makes bold the important information, drawing your eye away from the imperfections. First, there is a word missing in the phrase “Department of Computer Science and Engineering, University of Wisconsin-La Crosse”. The word “at” would fit more naturally in that space than a comma. Additionally, there is an added comma in the phrase “You will take on administrative tasks like, managing my calendar…”. These are the only notable mistakes, and they are buried under the strong ethos established by the message.

DISCUSSION

The results from the textual analysis will now be compiled based on each analysis criteria outlined in the methodology. The purpose of this is to compare the similarities and differences of the messages and come away with qualities unique to UWL-specific internship phishing scams. Once these features have been identified, they will be compared with UWL guidance regarding phishing email prevention to see whether the guidelines are adequate to protect students from cyber scams.

Sender domain

Out of the five analyzed emails, four of them came from university affiliated accounts. This means they either spoofed or created specifically to mimic real UWL domains. According to cybersecurity company Proofpoint, email spoofing is "technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they know or trust" (Proofpoint 2023). When you send an email, clients like Outlook for Microsoft automatically insert the sender's address on the "from" line. Using basic code, that name can be changed to come from any account, regardless of it exists. Outgoing servers cannot determine whether the accounts are legitimate or not, and thus, scammers can easily spoof one's domain to make recipients believe the message is coming from a legitimate source.

This is important because it goes against guidance given by UWL; the 2018 article from Knowledge Base advises users that "[p]hishing emails will most likely have been sent from non-university email accounts, so always double check the sender of the suspicious email, even if the email signature looks legit". Additionally, they advise to "[l]ook at inconsistencies in email addresses, incorrect order of characters, or URLs which have added characters or numbers. For example. www.uw1ax.edu or uwlax.@edu" (KB, 2018). None of the university-affiliated email senders contained obvious differences in this way but had an @uwlax.edu domain. This makes it impossible for students to tell an email phishing based off the domain alone which is one of the key ways experts advise to assess the legitimacy of an email (Irwin, 2022) This also highlights an issue of information security: scammers are figuring out ways to access student emails so they can spoof them.

Delivery Location of Message Received.

All of the analyzed messages, as well as all phishing messages received by the researcher, were received in the "focused" mailbox in Outlook. Microsoft's Outlook has two primary mailboxes: focused and other. The only secondary inbox that receives messages directly is junk. The focused tab uses machine learning to analyze what messages you receive, their content, and users you communicate with most to determine which emails you are most likely to read and respond to (Najimy, 2023). This system ensures members of an organization can maintain an efficient mailbox and see the most pertinent messages. This cannot be influenced by the sender, as it is Microsoft's algorithm that sorts the messages. This is significant because it places scam emails in student's most important mailbox alongside legitimate communications, further increasing the scammer's credibility. Currently, the "report phishing" function is not available on the Outlook app, however it is active on the web browser version. Regardless, nowhere does UWL guidance instruct individuals to use this function to report phishing.

Subject line.

The messages contain a different subject line, each with increasing specificity. Messages one and three have simplistic, non-specific subject lines: Student job advising and Administrative Assistant respectively. They are general, non-specific, and versatile, meaning they could be sent to any school. Message one includes a large UWL logo, which ties the subject line "student job advising" to the message, making the email as a whole seem as though it were part of university correspondence. Message three does not include any logos or other university-related signage, nor anything directing the position to students.

Message two has the subject line "UWL job posting". This is generally vague; however it does have a direct tie to the university. The subject line does not disclose any of the contents of the message, nor does it follow typical grammatical conventions of capitalization. Though the message itself does not contain any direct ties to UWL, the subject line makes it seem as though it is coming from a member of the UWL community on behalf of the Red Cross as part of a university-sponsored job initiative or program. Messages four and five have the most descriptive subject lines. Message five includes the subject line "Part-Time Student Assistant Needed". It does not have any direct ties to the university, but the content of the message is highly specific to UWL, rendering it redundant. The subject line is

precise; it includes the time-commitment of the position, as well as the educational setting in which the job will be held.

Message four includes the subject line "UWL Work Study Employment Opportunity", which is the most specific of the messages analyzed. Not only does it include a direct tie to the university in the subject line, but it describes the unique work-study nature of the position; work study positions are tied to financial aid considerations and assistance, as well as guaranteeing a flexible work schedule to work with student's school commitments. Because of this, work study programs can be preferable to some students over on/off campus jobs. The term "opportunity" has positive connotations, making the position seem attractive and in-demand. When coupled with the content of message four, which had the most phishing-like characteristics, the subject line carries much of the weight of persuasion. UWL does not give specific guidance regarding subject lines of phishing emails, however in the 2017 UWSA article, they advise to "be suspicious of any email directed to "Dear Customer" or some other generic salutation". Subject lines that explicitly contain the acronym "UWL" or contain verbiage specific to the position, are specific, rather than generic, subject lines (UWSA, 2017).

Organizational Affiliation

All but one of the messages include ties to a legitimate organization or individual; messages one and two offer positions at reputable non-profits, message three offers a position at a private company, and message five offers a direct assistant position under a current UWL professor. Message four does not mention a specific individual or organization with which the position would be held but eludes that the position would serve "an International Businessman / Consultant with high moral and ethical values who is also a Philanthropist, entrepreneur that is involved in many different projects from real estate to retail businesses, Real estate investor and Investment trader."

In their definition of phishing, the 2017 UWSA article states that phishing is "…[A]n online scam, usually leveraging email, involving carefully crafted messages with a link that appears to be from a trusted source, but is not." Though these messages may come from unfamiliar UWL email accounts, or non-university accounts, they purport to be on behalf of a legitimate organization soliciting their vacant position. The UWSA offers fair advice for exercising caution around unknown messages from reputable sources. In the same article, they warn users, "[i]f a message sounds suspicious or too good to be true, it is most likely an attack" (UWSA, 2017). Message one offers a position at UNICEF, an international organization part of the United Nations. Internships/assistantships at this organization are incredibly competitive, so being contacted directly by someone from the organization about a position can be a student's dream come true. Though the article did not define nor provide examples of "too-good-to-be-true" offers, the UNICEF offer would fall under that umbrella. It is important to note that students do not ordinarily have access to UWSA articles. Since it is part of the employee/administrative database, students must have valid credentials to access internal communications and the UWSA platform does not appear in routine Google searches.

Message five is unique because it does not offer an opportunity that is "too-good-to-be-true", but rather one that could be commonplace on a college campus. It is not unheard of for professors to have close working relationships with students or have students as aids for research projects. Professor Elliot Forbes is a real UWL professor, and thus it could be possible he is reaching out to students directly for this position. It is understandable why he would reach out to students outside his discipline, as he states in the message that students from any department can apply. He also offers students the opportunity to work with new technologies on a research project, two aspects of the position appealing to college students as well as within the realm of a professor's position.

Inclusion of logos

Messages one and four are the only emails that include logos. Both are featured prominently at the bottom of the message and occupy roughly 1/3rd of the entire message. The logo is one of the most commonly used UWL logos; the phrase "University of Wisconsin LA CROSSE" is displayed in grey lettering under a maroon lettered UWL with the L spirit mark. This logo is one of the four main full color logos included on the "Logos" page on the UWL website. UWL personnel, or individuals with UWL online credentials, can download the logos for free from the website, however one could obtain a picture of the logo in other ways as well, such as screenshots or Google image searches.

The 2018 KB article mentions logos and phishing. It warns that one should be wary of suspicious logos or signatures, as UWL correspondence often contains official UWL logos and signatures. However, it adds a note: "Phishing emails are becoming much more sophisticated. An official logo does not guarantee the e-mail is valid" (KB, 2018). This guidance seems to directly contradict what came before; it does not offer additional guidance or factors to

consider when receiving a suspicious email that includes logos. It also does not give a definitive or clear answer on whether logos are signs of phishing or not, but rather claims that both are simultaneously true. While this sentiment itself is not incorrect, as logo usage is not mutually exclusive, it is not helpful guidance.

Time Requirements

Except for message three, all messages assert that their positions are part-time, flexible, and remote, all with varying degrees of emphasis. Message one does not explicitly state their position is part-time nor does it mention it is flexible, however it claims the position is strictly work from home. This is stated in a note at the bottom of the message in all-caps, illustrating the importance of getting this point across. Additionally, there is not a statement of hourly or weekly commitment. The message mentions an employment schedule, however there is not one attached.

Message two states that "the position offers flexibility, with part-time, remote work,". The position would only require students to work three days a week for three hours at a time. Message five states "the position has flexible hours…It is remote and available to students of every department of the university". It states that the position is part-time in the subject line, however it does not include this in the body of the message. It also does not state an hourly/weekly time commitment.

Message four states the time commitment of the position the most out of the set. The message states that the position averages 5-7 hours weekly, however it does not say how many days a week the position requires. The message is emphatic about the flexible, part-time nature of the position. It asserts in three separate places that the position is flexible and part time; once in the second sentence as a standalone phrase, once in the last sentence as part of a larger phrase, and once again the phrase "FLEXIBLE HOURS" is capitalized at the bottom. Though the message does not explicitly state that this is a remote position, it does explain that "All the tasks are work from home/on campus job, you don't need to travel somewhere and also you don't need to have a car to get started", which implies the position is remote.

Message three is the only email that does not state the position is part-time, flexible, or remote. Additionally, it does not include an hourly/weekly time commitment. Since one of the job duties for the position is "reply to email, telephone, and face-to-face inquiries", it can be inferred this position would not be remote. It is unclear if Association and Community Management has locations nationwide as they are based in Colorado. This would complicate the in-person nature of the position should a UWL student get the job. The message did include a link to a website that is no longer in service, so it is unclear if that information would have been included there.

Job Description

Each message offers a different position title and job requirements. The position in message four has the job title "Personal Assistant/Bookkeeper" and does not include any further details in the message itself. In the attached Google form however, the job responsibilities are listed as "assisting with errands…", "purchase and deliveries of Gift items, groceries, stamps, and stationary", and "schedule, bookings, and payment for reservations and events on behalf of my clients". This description adequately primes students for what the scammer will ask them to do should they accept the job; they will be required to purchase gift cards and other items for the scammer and never receive reimbursement.

Message two has a similar description. The position title is "distribution assistant", which describes the position's functions in more detail than simply "administrative assistant". The job responsibilities will "require you to purchase items online and drop-ship them to individuals…". This job description is untrue as the assistant will not be drop-shipping items from their home but sending them to the location specified by the scammer directly; Drop-shipping involves bulk purchasing items and sending them to clients from your personal store. This means one must physically come into contact with the supplies they're sending out and typical internship scams work because assistants never come into contact with their goods; these scams work best on an accelerated timeline where the assistant does not have time to contemplate the tasks they are asked to fulfil, and direct shipments are the best way to ensure this process is completed fast. The term "drop-shipping" is a popular buzzword to indicate to readers the modern and independent nature of the position which can be attractive to college students looking to break into newer industries.

Message five does not have a job description specific to the tasks required to complete the scam, but rather includes responsibilities that would be expected for an assistant to a university professor. This includes "managing my calendar, email sorting and correspondence, and assisting with data collection" This message also includes qualifications for the role, including "strong organizational skills, an ability to work independently, proper

communication skills, and basic proficiency in relevant software and online tools". Requirement of these soft skills prepares the assistant to fulfill the tasks asked of the scammer; the independent nature of the job requires the assistant to complete tasks without assistance from the scammer, but the requirement of communication skills means the assistant must consistently respond.

Message three has the longest list of job responsibilities; the message lists nine responsibilities for the position, all of which would be typical of an administrative assistant for an HOA management company. This list looks identical to one that would be included on a real job solicitation, as it is the most in depth and job-and-company specific of the set. It does not indicate if purchasing and sending materials would be required of the position, however the attached website cannot be accessed which may have included additional information about the position. On the other hand, message one does not include any job description nor position title. All that is known about the position is that it is a "paid UNICEF Part-time job".

UWL does not address supplementary information used in social engineering. The purpose including high levels of detail in these descriptions is that it enhances the legitimacy of the solicitation; though college students may have never applied for an internship or assistantship, they likely have encountered a job ad which lists the job title, responsibilities, and qualifications. The closer the scam message comes to appearing like a legitimate job solicitation, the more likely they are to elicit a response, and thus catch a new victim.

One common tactic from social engineers generally is fabricating urgency and stress to cause the victim to react in ways they likely would not if they took the time to assess their situation. The 2018 KB article reinforces this, saying "[d]on't fall for threats and be cautious of emails stressing urgency which appears unfounded". However, this tactic is not commonly found in internship scams, nor were they used in any of the analyzed messages. This is because this kind of scam uses "pretexting", or creating a fake scenario to increase the chances the victim engages with the scammer. After they have created rapport and a relationship with the victim, such as recruiting them for a job, they begin to engage in emotional manipulation to pressure victims into beginning the job as soon as possible. Since the victim has already corresponded with someone they believe to be offering them a legitimate position, they will likely not register that their new employer is using a scam tactic on them, pressuring them to complete tasks without adequate time to assess their legitimacy. This model goes against UWL's guidance, which asserts that scammers will use pressuring language within the message itself, rather than as part of regular correspondence (KB, 2018).

Pay Rate

Messages one, two, and four have the same pay rate at $450 a week, message five promises $350 a week and message three does not include a pay rate. If a student were to work this assistantship for an entire year at a $450/week rate, they would make $23,400 minus taxes and deductions. It is important to note the importance of pay rate in luring students into falling for these scams; many college students are not able to work during school or have jobs that adequately provide for them. According to job recruitment site ZipRecruiter, as of December 1st, 2023, college student made $2,872 a month, with the lowest salary being $1,250. For the 2024-25 school year, UWL predicts that a Wisconsin resident will pay $17, 511 a year for tuition, housing, food, and personal expenses (ZipRecruiter, 2018). Though off-campus residents would likely pay less for food and housing overall, the payments for those amenities, including utilities, water, and Wi-Fi, are recurring. This requires students to budget year-round rather than paying a lump sum up front, and likely means they will have to find employment to support themselves.

Application Method

Though each message has varying application methods, they share a key similarity in that they require correspondence with an individual outside UWL. Messages one and two both originate from @uwlax.edu accounts and ask applicants to contact email addresses with non-university affiliated accounts. Additionally, these accounts are not affiliated with the organizations they appear to represent and have domains of @gmail.com and @hotmail.com respectively. Message five originates from a non-university affiliated Gmail account and is the only message that encourages applicants to reply directly to the message itself. Messages three and four both include external links for application. While message three's link is inactive, message four's Google Form asks applicants for their email as well as an alternative, non-school email. They do not explain what is meant by "email" compared to "alternative email", however it can be inferred this would mean an applicant's school email would be their "email" when juxtaposed with their "non-school, alternative" email.

UWL does not offer guidance for responding to non-university emails within university-related correspondence, however the 2018 Knowledge Base article says this about non-university emails: "Phishing emails will most likely have been sent from non-university email accounts, so always double check the sender of the suspicious email, even if the email signature looks legit" (KB, 2018). They have given guidance in the past regarding contact with outside UWL emails, however they do not acknowledge situations in which students are receiving messages from UWL accounts and asked to respond to non-university accounts. Though students may be wary to avoid messages from non-UWL accounts, it is not uncommon for one to correspond with a non-UWL account about a non-UWL affiliated employment opportunity. The outlier is message five, which solicits a university assistantship and was sent from a non-university account with an email that did not resemble the name of the sender.

Signature Block

Only messages two and five include a complete signature block, while messages one, three, and four include incomplete signature blocks or only a logo in place of one. Messages one and four have large UWL logos in place of a signature block. This can be inferred because the logo comes after the message's farewell; in message one, the logo is inserted under the phrase "regards," with the clause remaining unfinished. In message four, the logo is inserted under the phrase "Thank you.", with a completed clause. Message three has a similar farewell to message one, as it finishes with the phrase "regards," and does not complete the clause.

Message two's signature block matches the name of the sender; however, it does not match the name of the employer the applicants are asked to contact. The signature block also includes the sender's position at the Red Cross on the Mass Care Team, as well as listing their organization. The "mass care team" at the American Red Cross is not responsible for recruiting; their responsibilities include "provides activities and services on a congregate basis to the community as a whole including feeding, sheltering, reunification, and distribution of emergency supplies" (American Red Cross, 2023). The position is flexible and need-based; it also does not mention individuals with disabilities, students, and/or foster homes, as serving these populations would be a longer-term time commitment and require establishing rapport, rather than serving in disaster situation. Although the position description is vague, one might view the sender's position on the "mass care team" establishing their ethos. Message five's signature block is the most sophisticated; not only does it include Professor Elliot Forbes' name, but it also includes his real position, department, and place of employment at UWL. As mentioned above, message five is unique in that it uses the name of a legitimate UWL professor to create a position that originates from the school, which is an especially deceptive tactic.

UWL offers guidance for signature blocks in their 2018 article: "UWL emails will usually contain official logos and signatures, so be careful of any suspicious logos and signatures within these emails" (KB 2018). This guidance is sufficient, as many of the emails do not contain typical UWL signatures. Message five is the exception, as it offers the professor's name, position, department, and place of employment. Though the article does not define what makes an email signature "suspicious", emails one-four each contain out-of-the-ordinary signature blocks; message one and three leave room for a signature block and do not use one, message four uses the logo in place of a signature block and does not use a grammatical structure that would imply there should be something in its place, and message two uses a signature block with a vague job title.

General Appearance (grammar/formatting)

The messages vary most in their grammar, style, level of formality, and formatting. Appearance and readability are the most important factors in determining a message's effectiveness and overall ability to fool readers into believing it is legitimate. Each message will be analyzed from worst overall appearance to best.

Message four has the worst overall appearance; the entire message is contained within a paragraph and offers an extremely vague description of the position. The tone is informal at times, as evidenced by the phrase "…you don't need to travel somewhere and also you don't need to have a car to get started". Then in the following phrase, it reverts to formality: "Please find the position and some basic information below". It features inconsistent spacing, sentence length, and places the "APPLY NOW" link directly in the middle of a phrase that, without the break, still would not make sense. The Google form does not incur as many grammatical violations; however, it still carries odd formatting and sentence lengths. This email reads and is formatted consistent with stereotypical phishing. Message one does not contain as many grammatical or formatting errors as message four, however the message feels incomplete due to the lack of aforementioned "employment schedule"; the message begins with the writer asking the student a rhetorical question on behalf of the school regarding the UNICEF position and does not elaborate on the job responsibilities

further. It can be implied that the responsibilities, along with other information, would have been included in the attached employment schedule. Without this, the message feels incomplete and does not resemble a typical job ad.

Message three does not contain any glaring grammatical or formatting errors, however it feels the most informal of all the messages. It does not include a greeting and instead launches directly into the organizational background and responsibilities of the job. The job duties and responsibilities section most closely resembles that of a job ad, however its inclusion is unexpected as the position is not introduced at any time before this. At the end, it includes the phrase "NB", which translates to "nota bene", or "note well" in Latin. This phrase is most used in formal settings, which is out of place in a message that did not use high levels of formality throughout. Messages two and five are the most cohesive of the set and contain the fewest formatting and grammatical errors. They both use a heightened plain language style, which incorporates higher level vocabulary in relatively simple sentences. Both explain the purpose of the message well, as well as properly introducing the position and its responsibilities. Message five uses bolded text on the most important points of the email, including the mention of the position's availability to any student at the university and the application method. Rather than appearing as job ads like message three, they read like correspondences sent from an individual which further enhances their appearances as job solicitations and makes them appear more legitimate.

UWL gives the most consistent guidance on grammar and formatting inconsistencies. Both the 2017 and 2018 articles mention poor grammar and odd formatting as a tell-tale sign a message is phishing; the 2017 article advises to "[b]e suspicious of messages that have grammar or spelling mistakes", and the 2018 article asserts that "[p]hishing emails will usually have bad grammar, poor spelling or even odd formatting" (UWSA, 2017). It is important to note that while the 2017 article does not state that grammar errors are inherent to phishing emails, the 2018 article affirms that phishing emails will "usually" contain these things (KB, 2018). This is true of messages like one and four that contain many obvious grammatical and formatting errors, however, does not ring as true for messages two and five that on their face do not appear to contain significant errors. On the contrary, these mistakes may be invisible to the reader who believes that phishing emails are most distinguishable based on their formatting and grammar. Though errors do exist, they appear in ways that one would likely miss their first few times reading the message.

CONCLUSION

Cybersecurity policy at UWL is insufficient to address phishing scams targeted at students, as evidenced by a lack of information security awareness training for students, a weak reporting system, and outdated guidance that does not address current threats. It is widely agreed that information security awareness training is one of the best ways to limit engaging with scam messages and protecting stakeholders. Though there is not a policy from the UW system mandating that UWL must provide this training, the university should require bi-annual training for students as well as phishing simulations. This is significant, as students are all-but required to use a university email to receive benefits as a student, and thus are involuntarily subjected to scams in their student inbox. Along with a mandatory training course, students should also be made aware of phishing reporting protocol, and such protocol should be strengthened and given specific attention. Currently, students are advised to send all phishing emails to the Eagle Help Desk, which deals with all student and faculty technology issues. However, since students are generally unaware of anti-phishing resources on campus, this reporting system is mainly utilized by faculty and staff. The ITS department should create a designated email account for phishing emails so that the general help desk is not overwhelmed with phishing reports and ITS employees can track trends and patterns in current phishing threats. Most importantly, UWL must update it's phishing guidance and commit to publishing semi-annual updates and additional guidance. Scams have increased in sophistication since 2020, therefore adhering to guidance from 2018 is unacceptable. As shown by the message analysis, current phishing messages do not match the outdated guidance, and in many ways go directly against what the university labels as "phishing". It is imperative that the university update its guidance to best reflect the current trends in phishing so university stakeholders are properly informed.

When it comes to cyber security, higher education institutions must balance the demands of all stakeholders to ensure the protection of important data. Historically, those with the keys to the data castle-i.e. faculty and staff-were given extensive trainings and guidance regarding online phishing scams so that the university could minimize exposing stakeholder data or falling victim to financial scams. Since the pandemic, students have been increasingly targeted by financial scams, with many HEI's slow to respond. The purpose of this study was to analyze the efficacy of anti-phishing policy and practice as it pertains to students and how universities can begin to address the specific issues facing their campuses. The framework set forth by this research will lay the foundation for another small-mid sized university to analyze the phishing threats facing their students and how they can best address them.

LIMITATIONS

Sample size and demographic considerations are two important limitations for the message analysis portion of the study. The emails were selected only from one student's inbox, meaning the sample could be unrepresentative of phishing emails received by the entire student body. Though there is no evidence that scammers targeting UWL students did so based on an individual's identity insofar as their role as "student", more work should be done in this area to confirm. Future research should expand the sample size to include emails from multiple students to ensure fair representation of emails selected for the study.

Demographic considerations were not considered for this study but may be useful to future researchers in analyzing the degree of specificity in message targeting. This may be significant, as the increasingly targeted nature of phishing scams leads to higher variability in messages received by students based on major, club affiliations, and other distinguishing factors. Future research should note the demographics of the students who received the scam message-including but not limited to-major(s), minor(s), clubs, sports, career interests, and year in school. These identities branch off the greater "student" identity and would allow future researchers to determine if identity-based targeting is occurring.

ACKNOWLEDGEMENTS

Special thanks to the UWL Student Research, Creativity, and Experiential Learning department for providing the funding for this project as well as the Research in the Rotunda presentation at the Wisconsin Capitol. I would also like to extend my deepest gratitude to my advisor Dr. Bryan Kopp for supporting my vision for the project even when I myself had lost it, and for always pushing me to think critically.

REFERENCES

Carruthers, S. (2023, October 24). *Ai vs. human Deceit: Unravelling the new age of phishing tactics*. Security Intelligence. https://securityintelligence.com/x-force/ai-vs-human-deceit-unravelling-new-age-phishing-tactics/

Information security: Awareness. UW Policies. (2022, May 24). https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-awareness/

Irwin, L. (2022, March 22). *5 ways to detect a phishing email: With examples*. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email

Leonhardt, M. (2019, April 18). *"Nigerian prince" email scams still rake in over $700,000 a year-here's how to protect yourself*. CNBC. https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html

Najimy, A. (2023, October 30). *Understanding the focused inbox*. Boston HelpDesk. https://www.bostonhelpdesk.com/understanding-the-focused-inbox/#:~:text=Focused%20Inbox%20studies%20the%20history,them%20on%20a%20centralized%20list.

Phishing- How to spot a phishing email. Knowledge Base. (2018, August 13). https://kb.uwlax.edu/page.php?id=84838

Student salary: Hourly Rate November 2023 United States . ZipRecruiter. (2023, December 7). https://www.ziprecruiter.com/Salaries/Student-Salary

Students: Beware of employment scams via email. Students: Beware of employment scams via email | Information Security Office. (2023, December 7). https://security.berkeley.edu/news/students-beware-employment-scams-email

UW System Phishing Awareness Program to Begin in December. UWSA Employee Resources. (2017, December 6). https://www.wisconsin.edu/uwsa/employees/archive/uw-system-phishing-awareness-program-to-begin-in-december/

Volunteer opportunities. American Red Cross. (2023). https://volunteerconnection.redcross.org/?nd=rco_opportunity_detail&opportunity_id=131217&postal_code=75235&return_nd=rco_opportunity_browse_list

What is email spoofing? definition & examples: Proofpoint us. Proofpoint. (2023a, November 4). https://www.proofpoint.com/us/threat-reference/email-spoofing

What is social engineering? - definition, types & more: Proofpoint us. Proofpoint. (2023b, November 17). https://www.proofpoint.com/us/threat-reference/social-engineering

What is spear phishing? - definition, examples, prevention: Proofpoint us. Proofpoint. (2023c, October 12). https://www.proofpoint.com/us/threat-reference/spear-phishing#:~:text=For%20example%2C%20an%20attacker%20might,from%20a%20legitimate%20PayPal%20employee.