Understanding Behavioral and Psychological Aspects of Employment and Tax Scams via a Social Engineering Competition

Hwanhee Park, Rachel Bleiman, and Aunshul Rege
Temple University, hwanhee.park, rachel.bleiman, rege@temple.edu

Abstract - **Employment scams have skyrocketed over the past few years. Employment scams have skyrocketed over the past few years, given the challenging economy, high inflation, ever-increasing cost of living, and change of careers. Unsuspecting job seekers are duped into fake job postings and work-from-home scams by mimicking legitimate companies. The financial losses experienced by victims are further compounded by intangible costs, such as emotional setbacks, stress, and embarrassment, or by offshoot crimes from disclosing their sensitive information, such as identity fraud or tax fraud. This paper shares findings from a 2024 Employment and Tax Scam and Social Engineering Competition that introduced students to the behavioral and psychological aspects of employment and tax scams. The paper details the competition design, structure, and logistics, which were based on a real-life employment and tax scam case study. It also shares findings about students' experiences across various aspects of the competition, including their use of the MITRE ATT&CK framework and the NIST Phish Scale. Further, it discusses findings about students' understanding of the use of psychological persuasion across the modus operandi of the employment and tax scam and their recommendations pre- and post-victimization. The competition gave students the opportunity to treat scam victims with dignity by employing tactical empathy. In the context of understanding scams, students reported identifying red flags (58%), developing the employer/scammer profile (44%), and creating victim checklists (30%) to be among the easiest components, while 65% ranked the ATT&CK mappings and 44% felt that classifying the persuasion techniques across the scam timeline were among the hardest components.**

Index Terms – Cybercrime victimization, Cybercriminal behavior and psychology, Cybersecurity competitions, Employment scams, Experiential learning, MITRE ATT&CK, Social engineering, Tax scams.

INTRODUCTION

Employment scams have skyrocketed over the past few years, given the challenging economy, high inflation, ever-increasing cost of living, and change of careers. Unsuspecting job seekers are duped into fake job postings and work-from-home scams by mimicking legitimate companies, offering high-paying salaries and great benefits, and then the victim's stealing personal information or money [1;2]. These scams heavily employ social engineering (SE), which is the psychological manipulation of human behavior to convince individuals to perform an action (divulge sensitive information, give up money, etc.) that they otherwise would not do. While estimating the financial losses stemming from these scams is difficult to estimate, the Better Business Bureau approximates that Americans experienced USD 2 billion in direct losses every year while the Federal Trade Commission places this number at USD 68 million; either estimate clearly indicates the jarring monetary costs of these scams [1]. These financial losses are further compounded by intangible costs, such as emotional setbacks, stress, and embarrassment, or by offshoot crimes, such as identity fraud where scammers used sensitive information that victims provided during the application or interview for the bogus job to commit other crimes, such as tax fraud. Employment scams have risen 54.2% from 2022 to 2023 and are particularly problematic for ages 18-44 [3].

Given the recent sharp increase in bogus jobs and the susceptibility of desperate job seekers, the authors implemented an employment and tax scams and social engineering competition (ETSSEC). The next section offers an overview of literature in the area of SE and psychological persuasion, employment scams and their modus operandi, and tax scams. The following section describes the competition structure, logistics, and participants in the event. It also reports the ETSSEC's impact on students' views of social engineering's relevance to cybersecurity and their confidence in social engineering skills. Additionally, it shares findings on students' understanding of using the MITRE ATT&CK framework to analyze cyberadversarial behaviors and the NIST Phish Scale to rate email phishing, as well as their ability to identify red flags in scam modus operandi and provide recommendations for pre- and post-victimization. The paper concludes with the relevance of the employment and tax scams, particularly to the demographic of the competition participants, and the exposure to useful frameworks (NISH Phish Scale, ATT&CK) and cybersecurity consulting experiences.

LITERATURE REVIEW

I. Social engineering and psychological persuasion

Several SE techniques have been identified in the literature: (i) phishing, where personal or sensitive information is obtained when victims click on malicious links or attachments. The goals of phishing can also be carried out via phone (vishing) or short messaging service (smishing), (ii) baiting, where victims are lured through enticement strategies by exploiting human curiosity, fear, trust, or impatience (iii) quid pro quo, where services or assistance is offered in exchange for information or access, (iv) pretexting, where attackers create a credible story to build a sense of trust with victims to confirm or obtain information, and (v) tailgating or piggybacking, where unauthorized individuals are given entry to restricted areas by those who have permission and access [4].

SE techniques rely on psychological persuasion principles, such as authority, commitment, consistency, reciprocity, likeness or commonality, scarcity, urgency, social proof, tactical empathy, and a natural inclination to help [5]. The authority principle leverages an individual's readiness to comply with requests from those in positions of power (lawyers, doctors, supervisors, law enforcement officers, etc.). The commitment principle targets an individual's beliefs and mores, while consistency is based on the fact that individuals are likely to behave in ways that are consistent with their value systems. Reciprocity rests on the fact that people are obliged to return favors in exchange for one that they may have received before. Likeness or commonality is used when perceived similarities between individuals enhances the likelihood of compliance and agreement. Scarcity persuades individuals by providing opportunities or objects that are perceived as highly valuable but have limited availability; scarcity is often used to generate a sense of urgency, where not acting quickly may result in the loss of that opportunity or object. Social proof exploits the tendency that people are more likely to perform an action if others, especially those that they know personally or look up to, have already done the same. Tactical empathy involves understanding or recognizing another person's emotions, perspectives, and mindset, and making that person feel understood by vocalizing that recognition [6]. This principle involves developing trust, rapport, and likeability with the person. Lastly, the natural inclination to help principle rests on the fact that human beings are wired to help those who are in need [5].

II. Employment scams

According to the Federal Trade Commission, scammers use an assortment of employment offerings to dupe their victims into divulging sensitive information and sending money. The work-from-home job scams attract hopeful employees who wish to work from home (WFH), but end up paying for training, certifications, and startup equipment [7;8]. WFH scams could include reshipping scams, where victims receive packages, repackage them, and then reship them to an address provided by the scammer [7]. Caregiver or virtual assistant scams occur when victims are 'hired' and are sent a check that they are told to deposit in their accounts; victims are then instructed to keep a portion of these funds and send the rest to someone else. Unfortunately, the original check is fake, but the money victims have sent out is real. The bank then expects victims to repay the full amount of the fake check that bounces. Thus, victims not only send their own money to the scammer, but also have to cover the full amount of the bogus check [7]. Employment placement scams operate under the guise of staffing agencies that 'connect' victims to businesses; however, victims need to pay 'fees' to process applications and obtain training [7;8]. Individuals have not only suffered financially by losing their savings, pensions, and investments, but have also experienced shame, stress, loss of trust, and (on occasion) loss of life via suicide.

III. The modus operandi of employment scams

Employment and tax scams unfold as a process, with recruitment, interview, and extraction stages. In the recruitment phase, scammers, like legitimate businesses, use traditional online employment platforms for advertising job opportunities and receiving applications [7; 9]. They also use social media platforms, such as Facebook, Instagram, Snapchat, Kik, Telegram, and WhatsApp to post phony jobs and recruit victims [1]. They may pose as human resource managers or recruiting agents and either approach potential victims or target those that have applied to the nonexistent positions. Next, victims enter the interview phase, where they often engage in online or chat-based interviews where HR representatives or managers [10]. Victims are almost always contacted immediately after with an acceptance offer, fantastic benefits, and administrative paperwork to complete [10]. This stage often involves the extraction of sensitive information via the official forms sent by the bogus employer. Some of this information could include full name, contact information, date of birth, social security numbers, and tax id numbers [10]. This extraction stage often provides enough information to initiate identity impersonations that would allow scammers to get jobs, wages, and/or file taxes [8].

IV. Tax scams

The Internal Revenue Service releases an annual "dirty dozen" common scams that taxpayers may experience, particularly during filing season [11]. In 2024, the top scams included fake charities, bogus donation deductions, spearphishing attacks against businesses, inaccurate or misleading tax advice and tax avoidance strategies, ghost tax preparers, fake tax debt resolution, false tax credit and employee retention credit claims, and scammers assisting with setting up online accounts [11]. Additionally, the organization warned about the usual ph/sm/vishing campaigns.

There are three instances where employment and tax scams are connected. First, is the illegitimate unemployment

benefit scam, where fraudsters acquire enough sensitive information (social security number) via phishing emails or data breaches to then submit fraudulent unemployment claims under unsuspecting victims' identities [12]. Second, is the employee retention credit scam where fraudsters charge fees upfront to claim credits on the victim's behalf [12]. The W-2 form phishing scam is when scammers try to obtain an individual's W-2 form from an organization's human resources or finance department [12].

Employment and tax scams come with a myriad of harms that can be avoided with proper education, awareness, and training. Thus, the following section describes the authors' efforts to train the next generation on recognizing and preventing victimization to these scams via the Employment and Tax Scam Social Engineering Competition (ETSSEC).

COMPETITION STRUCTURE, LOGISTICS, AND PARTICIPANTS

The authors have hosted several social engineering competitions (SEC) that are open to high school, undergraduate, and graduate students from all over the world. These SECs, which focus on careers and are inspired by real-world events, are rehashed to create virtual real-time simulated settings that provide a safe, fun, and ethical space for students to try SE and understand the relevance of the human factor in cyberattacks and cybersecurity. Students have taken the role of penetration testers to test the susceptibility of the authors' lab to SE attacks [13], negotiators when the authors' lab was 'hit' with ransomware [14], and fraud fighters to help a romance scam victim [15].

In June 2024, the authors hosted an employment and tax scams social engineering competition (ETSSEC), which took place virtually over a three-day period. Eighteen teams competed in the event, including three high school teams, five graduate teams, and ten undergraduate teams. Teams consisted of two to four members.

Most students came from a disciplinary background in the hard sciences (86%), with few from the social sciences (8%) or other backgrounds such as communications, Japanese language, and cybersecurity leadership. Females made up the majority of competitors (59%). Most students were white (37%) or Asian (29%), while 10% were African American, 5% were mixed-race/multiracial, and 20% preferred not to say. The majority of competitors were not Hispanic or Latino (59%); however, 32% preferred not to say.

The premise of the competition was that student teams had to represent the authors' cybersecurity lab as 'fraud fighters', engaging with a young adult client who was in the midst of being victimized in an employment and tax scam. The roles of the client, client's friends, and scammer were played by the authors as well as government and non-profit sector representatives from the Cybersecurity Infrastructure Security Agency (CISA), the MITRE Corporation, and the Internal Revenue Service (IRS). Students were required to assess whether the client was a victim of a scam and illustrate their comprehension of how psychological persuasion tactics were employed in different exchanges between the client and the scammer.

Two weeks before the event, the authors hosted an orientation session. In addition to the event logistics, rules, and instructions, students learned from government and non-profit representatives on the competition-relevant topics of social engineering, employment scams, IRS CI's role in handling tax fraud, an overview of the ATT&CK framework, and an overview of NIST's phish scale.

I. Case study

The simulated scam was based on a real case study experienced by a student from the authors' university. The platform where they posted their resume, the time between posting their resume and receiving initial contact from the scammer, the job position being remote, and all communication between the victim and the scammer was replicated from the case study to the competition. This ensured the competition offered students a realistic experience of how an employment and tax scam unfolds.

Students were introduced to several different characters throughout the simulated event (portrayed by the authors/external representatives). First was Sam, their client, whom the authors created to resemble an undergraduate student with little experience with the job search process, making them a prime target for an employment and tax scam. Throughout the event, students witnessed interactions between Sam and several additional characters, including the recruiter who sent an initial job invitation email as well as a chat-based interviewer whose name differed from the display name on the interview platform. The display name appeared throughout the emails from the recruiter, yet Sam never engaged with that character. Furthermore, the names of two unrelated companies were used interchangeably by the scammers throughout the event.

II. Live competition

Teams met with the client's friends on Day 1 of the competition, oversaw interactions between the client and the scammer on Day 2, and presented their evidence and conclusions on Day 3. During each day, students had to use tactical empathy while completing a set of objectives and deliverables, which are detailed below across the three days of the competition.

Instructions were communicated, and deliverables were submitted virtually through One Drive, while all meetings occurred virtually on Zoom.

IIa. Day 1: Client meetings

Teams had a 10-minute meeting with the client's friends (portrayed by the authors and external representatives) to gain an initial understanding of the situation and why they were concerned. Students learned that their client, Sam, had a job interview scheduled for the following day with a company that they never applied to.

Teams had to ask relevant questions during this meeting to guide them in their OSINT and identification of red flags. For instance, teams asked what platform Sam posted their resume on and when, or about Sam's educational background.

IIb. Day 2: Scammer exchange

On the second day of the competition, Sam agreed to let the CARE Lab sit in on the virtual chat-based interview, despite Sam's firm belief that the job was legitimate. During the two scammer interactions, teams sat in on the chat-based communications, acting as consultants for the client and providing identification of red flags signifying a potential scam. Sam first shared the initial contact they received from the scammer, which was an email inviting Sam to interview for a job. When the interview started, teams pointed out anything suspicious about the scammer's messages that might indicate a scam. Teams had to use psychological persuasion and tactical empathy during this process, as Sam was uncooperative with their suggestions. Later in the day, the teams again sat in on the communication between the client and scammer as Sam received an email with their offer letter and employment forms to fill in and return (including a W-4).

In addition to providing live advisement for Sam, students could use evidence from the exchanges to conduct additional OSINT and gather more evidence in the form of red flags. Teams also had to complete ATT&CK mappings for the chat communication playbook, emails, and their OSINT and red flags. Further, students scored each email using the NIST Phish Scale.

At the end of day 2, students submitted final reports, which included finalized versions of their OSINT findings, red flags, pre- and post-checklists for victims of job scams, ATT&CK mappings, and NIST phish scale scores.

IIc. Day 3: Formal debrief

On the final day of the event, teams engaged in a 10-minute meeting to provide a formal debrief and presentation to the client, Sam. Teams presented their evidence and conclusion about the legitimacy of the job offer in a persuasive and tactically empathic way. Teams had to choose their most convincing evidence to present, make recommendations for next steps, and answer questions from the client or their friends.

STUDENT EXPERIENCES

I. Pre/post surveys

Students reported that the ETSSEC increased their perceptions of SE's relevance to a career in cybersecurity, with those thinking it is 'completely relevant' growing from 37% to 54%. It also increased their confidence in being an effective social engineer, with those reporting feeling 'extremely confident' from 7% to 25% and 'somewhat confident' from 38% to 49%. Overall, students reported that the event provided them with practical experience in applying concepts they may or may not have learned before. For instance, one person noted "I had not tried something like this before, and actually being able to do it made me feel more confident."

About 48% of competitors ranked their favorite or second favorite component of the competition to be presenting evidence in the formal debrief. The most frequent least favorite or second-to-least favorite component of the competition, according to students, was the report writing deliverable (58%). In terms of difficulty, students found the easiest components of the event to be demonstrating tactical empathy in the client meetings (48%), asking the right questions during client meetings (38%), and the live identification of red flags they had to do while guiding their client through the interview exchange (38%). The most difficult components were the report/deliverable writing (48%), convincing the client using tactical empathy during the formal debrief (42%), and convincing the client using tactical empathy during the interview exchange (36%).

Regarding the report, students thought the easiest components were listing the red flags (58%), developing the employer/scammer profile (44%), and victim checklist (30%). Students struggled the most with the application of their findings, with 65% ranking the hardest or second-hardest component to be the ATT&CK mappings and 44% to be mapping the persuasion techniques across the timeline.

II. MITRE ATT&CK

The MITRE ATT&CK framework helps organize and analyze cyberadversarial behaviors, such as tactics (why the behavior was performed), techniques (how the tactical goal was achieved), and procedures (what the adversary did specifically to implement the technique) (TTPs) [16]. This framework provides practitioners with a consistent and structured process to track, model, and understand cyberadversarial behaviors [16].

Most student teams consistently identified the use of open-source intelligence (OSINT) techniques to gather information about potential victims from public job-seeking sites such as ZipRecruiter and social media platforms. These teams found that scammers actively scan hiring websites to seek new potential targets, focusing on collecting information such as email addresses. The tactical goal of these scammers involves gathering comprehensive information about the victim's identity, employing techniques associated with Reconnaissance (TA0043). Specifically, they use OSINT to search open websites/domains (T1593), social media (T1593.001), and search engines (T1593.002) to gather victim identity information (T1589.003). For instance, one graduate team highlighted the technique of gathering victim host information (T1529), which includes administrative data such as assigned IP, operating system specifics, and configuration details.

The majority of student teams discovered that initial access to victims is often achieved through phishing (T1566), particularly spearphishing via services

(T1566.003). For example, scammers crafted a fake job offer using Sam's (victim's) resume and sent it via email. This suspicious email contained a malicious link (T1204.001) & (T1566.002) and an offer letter as lures (T1566.001), prompting Sam to engage further exploitation and potentially granting access to the scammer. Another critical method identified by most teams was impersonation (T1656), where scammers pose as recruiters or company executives to gain the victim's trust. All high school team was successful in pointing out impersonation.

This deception enabled the scammers to obtain personal information by soliciting banking and personal details, extending to requesting personal documents via email – such as passport photo, signed employment letter, driver's license, and an employment application – from Sam. Following instructions from the phishing email, which included tasks like contacting the hire manager or purchasing specific office items (T1204.002), Sam provided sensitive information (T1114). Teams highlighted techniques for exfiltration, where the job offer sent via email required Sam to fill out forms and provide both personally identifiable and financial information over a web service (T1567).

Additionally, there are methods and techniques uniquely mentioned by a few teams. One undergraduate team noted the tactic of exploiting trusted relationships (T1199). Sam's legitimate text exchange with the interviewer built trust, leading her to disclose personal information under the guise of a job opportunity. Another undergraduate team mentioned the technique of acquiring valid accounts (T1078), in which the scammers simulated an onboarding process to request personal identification and to acquire legitimate account credentials. Furthermore, a high school team pointed out the use of automated collection (T1119), employing automated chat interviews were used to systematically gather information about Sam.

III. NIST Phish Scale

The National Institute of Standards and Technology developed the Phish Scale to help individuals rate a human's ability to detect whether an email is a phish, by using email cues and premise alignment [17]. Phish email cues include errors (grammar, typos), technical indicators (email addresses, hyperlinks, attachments), visual presentation indicators (logos, design, formatting), language and content (generic openings), and persuasion principles (urgency, authority, natural inclination to help) [17]. Premise alignment encompasses the relevance of the email's content (premise) to the target audience and its corresponding context (roles, responsibilities, cultures) [17].

The Phish scale cues classify emails based on the number of cues: few, some, and many. Emails with few cues offer fewer chances to identify phishing, while those with some cues offer a moderate number. Emails with many cues provide the most opportunities for detection. Premise alignment is categorized into three levels: strong (high alignment with the target audience, making the email difficult to detect), medium (moderate alignment), and weak (low alignment, making the email easier to detect). After evaluating cues and premise alignments, the categories of cues and premise alignments are analyzed collectively to determine the phishing email's overall detection difficulty. A sample team's phish scale worksheet is shown in Figure 1.

Out of the 10 teams, eight identified many cues, indicating that the emails were generally less difficult to detect as phishing attempts. The remaining teams identified some cues, suggesting a moderate detection difficulty. In terms of premise alignment, four teams demonstrated strong alignment, indicating that phishing emails are more challenging to detect. Two teams showed medium alignment, while four teams displayed weak alignment, indicating that the emails were easier to identify as phishing. Overall, six teams rated the phishing emails as moderately difficult to detect, while four teams found them to be least difficult. Students found this portion of the event beneficial, as it introduced them to a phishing classification system: "I learned more about the importance of […] the Phish Scale, which is great for developing/judging a phishing email."

How many times does the email express time pressure, including implied?	1
How many threats are included in the message, including implied threats?	0
How many appeals does the email make to help others?	0
How many times does the email offer something that is too good to be true, such as having won a contest, lottery, free vacation, and so on?	0
Does the email offer anything personalized and unexpected just for you?	0
How many times does the email offer something for a limited time?	0

Total Cue Count = Sum of Tallies (14) + "Yes" responses (5) = 19

Total Cue Count	Cue Category
1 – 8 cues	Few (more difficult)
9 – 14 cues	Some
15 or more cues	Many (less difficult)

Difficulty: Many Cues (less difficult)

Premise Alignment	Applicability (0-8)
Mimics a workplace process or practice	8
Has workplace relevance	8
Aligns with other situations or events, including external to the workplace	8
Engenders concern over consequences for NOT clicking	4
Has been the subject of targeted training, specific warnings, or other exposure	0

Premise Alignment Rating = SUM(first four) – five = 28

Premise Alignment Rating	Premise Alignment Category
10 and below	Weak
11 – 17	Medium
18 and higher	Strong

Premise Alignment Category: Strong

IV. Red flags across the scam modus operandi as identified by student teams

Several common red flags were identified across the student teams in initial recruitment email, during interviews, and from extraction stage.

The initial recruitment emails often contained unsolicited interview requests with generic greetings like "Dear Candidate," lacking personalization. They did not specify particular job positions or responsibilities, offering varied positions that did not align with the candidates' qualifications. The hourly pay rate mentioned was unusually high compared to the candidate's level of education and

experience, making it appear too good to be true. Additionally, there were inconsistencies between the company name mentioned in the emails and the email domains used. The company name appeared outdated, and there were discrepancies between the provided website domain and official sources. The legitimate position of the supposed interview manager did not involve recruitment, suggesting impersonation. Like this, there were inconsistencies in the provided information, including the names of the director, interviewer, and company positions.

During the interview process, the interviewer introduced themselves as a different person than expected, and the name on the chat with the Microsoft Teams link was misspelled. Similarly, the employer claimed to represent a different company than the one mentioned in the initial email and later switched back. The employer pressured the candidate to make quick decisions and share sensitive information, including personal and financial questions irrelevant to the job position, such as inquiries about the candidate's mobile network provider. Furthermore, the interview contained unnatural conversation flows, such as asking the candidate to outline the duties of an administrative assistant instead of providing the information directly – a response pattern typical of generative AI. The fact that the interviews were conducted via chat rather than video call further contributed to the unusual nature of the process.

The majority of student teams found red flags from the extraction stage as well. The interviewer's immediate job offer and the rapid timeline of the hiring process were suspicious. The interviewer employed multiple benefit opportunities to persuade the candidate to accept the offer using scarcity as a technique. The interviewer requested sensitive personal information, including a W4 tax document, a photo of the passport, social security number, and banking institution details early in the onboarding process by employing the sense of urgency. These issues not only highlight suspicious hiring practices but also pivot to concerns about tax scams. Lastly, teams also found that the offer letter stated the candidate would have to purchase their own office equipment from a supplied vendor and would be reimbursed, a common scam tactic.

Overall, throughout the whole process, the communications were unprofessional, with emails and interview messages full of grammatical errors, capitalization issues, poor punctuation, and inconsistent formatting. The recruiter's email address did not match the expected professional format. There was a vague and inconsistent email signature, with title positions changing between communications. There was a lack of branding throughout all contact, as most companies usually include a header, footer, and logo in their emails.

While the common red flags highlighted pervasive issues, a few teams also identified unique aspects of the scam. A few undergraduate teams and one graduate team noted the absence of standard pre-employment procedures; the employer did not require background or work history checks before offering the role to the candidate. Two undergraduate teams and one graduate team highlighted the reversed application process, where the candidate was asked to complete an employee application after receiving a job offer. One high school team pointed out that the scammer sent a check to the candidate instead of directly sending materials and equipment. This is a common tactic known as the caregiver or virtual assistant scam mentioned in the literature review, where the fake check eventually bounces, and the bank holds the victim responsible for the amount.

Moreover, the scammer employed several persuasion techniques in their initial email. They established a sense of authority by arranging a meeting with a high-ranking employee to exploit the candidate. They also invoked scarcity by offering a high-paying remote position, a rarity for someone with limited professional experience. Furthermore, the scammers used reciprocity and flattery, praising the applicant's commitment and charisma to gain their trust.

The student teams were able to identify these red flags throughout the scam's modus operandi. By examining the recruitment emails, interview processes, and extraction stages, they uncovered a pattern of suspicious behaviors such as inconsistencies, the use of persuasion techniques, and atypical hiring practices, and tactics employed by the scammers.

V. Pre-victimization checklist

In exploring various pre-victimization checklists developed by student teams, a common thread emerges in their approach to identifying potential scams in both employment and tax-related contexts. Based on the findings from most student teams, the following checklist summarizes the commonly identified indicators to help individuals recognize and avoid potential scams.

First, scammers often use personal email addresses instead of official company domains. Teams emphasize the danger of unsolicited job offers that promise high pay for minimal work. Another important aspect identified is the upfront request for personal information such as bank account details and social security number, even before a formal offer is made. As mentioned in the literature review, this tactic is called the illegitimate unemployment benefit scam, often under the guise of administrative processes or preparatory steps for employment. As mentioned in the literature view, this tactic is called the illegitimate unemployment benefit scam. Additionally, teams noted inconsistencies in emails and job descriptions where job postings or communications contained grammatical errors, capitalization issues, incorrect punctuation, lacked specific details about job responsibilities or shifted between different company names or job roles during the recruitment process.

Furthermore, the pressure to act quickly emerges as a prevalent tactic employed by scammers. A few social engineering techniques mentioned in the literature review such as urgency in decision-making, coupled with scarcity of threating missed opportunities, push individuals to bypass

thorough verification processes. The majority of teams also underscore the importance of verifying company credentials and conducting thorough online research. Legitimate companies typically have a robust online presence with verifiable contact information, including physical addresses and official websites. On the contrary, scams may present themselves with generic or inconsistent information, making it important to cross-reference details and seek reviews or complaints from other users online.

In the context of tax fraud, several teams highlighted distinctive warning signs. These include unexpected demands for payment or refunds from tax authorities without prior communication, especially when done through unconventional methods like gift cards or cryptocurrency. Moreover, fraudulent tax schemes often involve suspicious links or attachments in emails, posing as official communications from tax agencies.

These are some of the unique checklists that were mentioned by one or a few teams. A few undergraduate teams recommended getting in touch with real employees at the company, possibly through LinkedIn, to confirm their work status and validate the job offer. During interviews, they suggested asking about the goals of the company, the reasons for the many job openings, and requesting detailed information about the job or tax service, including contracts, job descriptions, or tax forms to ensure transparency. Furthermore, two undergraduate teams listed to discuss any suspicious offers or documents with someone you trust. They advised being wary of requests for payment or sending money for certifications, training, equipment or other expenses necessary to accept the job. To further protect yourself, one team mentioned checking scam tracking databases, such as the Better Business Bureau scam tracker, for any similar scams.

When dealing with tax matters, it is crucial to never interact with IRS impersonators over the phone, email, or social media. The IRS will never call to demand immediate payment. One undergraduate team discussed the importance of ensuring you file your taxes on secure, legitimate websites that use the HTTPS protocol or through official tax filing software. Furthermore, one team mentioned tax fraud often involves stealing someone's social security number and filing their tax return on their behalf. To prevent this, never send social security numbers via insecure or unencrypted channels.

VI. Post-victimization checklist

Most teams emphasize several key steps for victims to take immediately after identifying they have fallen prey to a scam. First, it is critical to cease all communication with the scammer to prevent further exploitation. Victims should block the scammer's contact information and report the scam to relevant authorities such as the Federal Trade Commission (FTC), the Internal Revenue Service (IRS) by filing Form 14039, Identity Theft Affidavit, and local law enforcement. Some teams also recommend informing any companies that were impersonated during the scam to help prevent further victimization.

After reporting the scam, changing passwords for all potentially compromised accounts and enabling two-factor authentication are essential steps. It is also advised to document all interactions with the scammer, including emails, text messages, and any financial transactions, as this documentation can be important for reporting and investigating the incident. Victims are encouraged to contact their financial institutions immediately to report any unauthorized transactions and to monitor their accounts and credit cards closely for suspicious activity. Additionally, freezing credit with major bureaus can help prevent identity theft.

Here are unique checklists that were mentioned by a few teams. A couple teams suggest adjusting privacy settings on social media and job platforms to limit exposure. A few teams suggest adjusting privacy settings on social media and job platforms to limit exposure. Some teams highlighted the importance of educating oneself about common scams and staying vigilant for any future fraudulent activity. They also advise seeking support from friends, family, or a professional counselor to handle the emotional toll scams can take on individuals.

Additionally, one undergraduate team suggested steps to take if the scammer has made you run an application granting them remote access to your computer or installed malware. The team recommended uninstalling any such applications and running a scan with a reliable antivirus program. If issues persist, the team advises making a fresh installation of the operating system after backing up any important files.

This section reviewed student experiences and their analysis of scams using various frameworks. The ETSSEC enhanced students' understanding of social engineering and overall increased their confidence in detecting scams. Analysis using the MITRE ATT&CK framework and NIST's Phish Scale revealed common scam tactics such as phishing techniques, impersonation, and methods for evaluating phishing detection difficulty. Students successfully identified key red flags and unique elements of scams. Pre- and post-victimization checklists provided practical advice for recognizing and responding to employment and tax scams.

NEXT STEPS/CONCLUSION

This paper provided a social engineering cybersecurity competition case study that focused on employment and tax scams. As noted in Section 3, the material used for this event was based on the experience of an undergraduate student at the authors' home institution, which echoes the findings from Section 1, that these scams are problematic for ages 18-44. The employment and tax scams theme was thus particularly relevant for high school and college students as they embark on their work trajectories, some potentially for the first time. As such, many of the red flags and recommendations are beneficial for personal use.

Students were also exposed to useful frameworks and taxonomies such as the NIST Phish Scale and the ATT&CK framework, both of which can be used in their future careers. The Phish Scale can be used as part of cybersecurity awareness and phishing training programs. The ATT&CK framework can be used to identify where adversaries are in the intrusion chain, provide insights into the tactics and techniques used by bad actors, and corresponding defense measures that inform security operations.

Many students also stated that they got a feel for cybersecurity consulting, by assessing vulnerabilities, implementing security measures, developing guidance on best practices and protective measures, and fostering a culture of security awareness. In addition to developing a working knowledge of social engineering, students also learned how to develop strong verbal and written communication skills, which are crucial in most work sectors. They interfaced with clients by actively listening, building trust, and developing the art of negotiation to convince them of the scam and take the appropriate next steps and security measures.

Understanding scam strategies and psychological persuasion is critical as fake job listings on career and networking sites like LinkedIn and Indeed increased by 118% in 2023 [18]. This steep rise can be attributed to artificial intelligence (AI) as job seekers will find it increasingly difficult to distinguish between real and fake: "The rapid improvement in the look, feel and messaging of identity scams is almost certainly the result of the introduction of AI-driven tools [that] refine the 'pitch' to make it more believable as well as compensate for cultural and grammar differences in language usage" [18]. To keep pace with these developing trends in real-world SE, the authors plan to use AI in future competitions to not only design the backend, but also during the live event to educate students on how AI can change the SE playing field (e.g., voice cloning in vishing). Efforts from the authors to use AI in future events include using it to create virtual sandboxes to allow students to practice SE in a safe and ethical environment. Efforts also include students using AI in pretext/persona creation, generation or enhancement of phishing emails and vishing scripts, and developing their skills in prompt engineering to incorporate OSINT findings and persuasion principles into their strategies. Doing so will ensure that the next generation workforce is exposed to, and is trained about, the ever-changing deployment of AI and SE in cyberattacks.

ACKNOWLEDGMENT

This work was supported by the National Science Foundation Award # 2032292. The authors thank representatives from Cybersecurity Infrastructure Security Agency (CISA), MITRE ATT&CK, the National Initiative for Cybersecurity Education (NICE), and the Internal Revenue Services (IRS) who served on the competition's advisory board and engaged with students during the competition. The authors also thank the undergraduate student at their home institution who was brave and willing to share correspondence with the scammers in their personal experience with employment and tax scams.

REFERENCES

[1] Kelly, J. (2023). Fake Job Scams Are Becoming More Common – Here's How to Protect Yourself. https://www.forbes.com/sites/jackkelly/2023/06/01/fake-job-scams-are-becoming-more-common-heres-how-to-protect-yourself/

[2] Robinson, C. 2024. How To Avoid Job Scams While Changing Careers. https://www.forbes.com/sites/cherylrobinson/2024/05/02/how-to-avoid-job-scams-while-changing-careers/

[3] BBB. 2023. BBB Scam Tracker Risk Report. https://bbbmarketplacetrust.org/riskreport/

[4] Rege, A., Williams, K., & Mendlein, A. (2019, June). A social engineering course project for undergraduate students across multiple disciplines. In 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-8). IEEE. Anonymize for review

[5] Uebelacker, S. & Quiel, S. 2014. The Social Engineering Personality Framework, In 2014 Workshop on Socio-Technical Aspects in Security and Trust (pp. 24-30). IEEE.

[6] Voss, C., & Raz, T. (2016). Never split the difference: Negotiating as if your life depended on it. Random House.

[7] FTC. 2023. Job Scams. https://consumer.ftc.gov/articles/job-scams. July 2, 2024.

[8] FTC. 2024. Consumer Sentinel Network. https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf. June 29, 2024.

[9] Cole, T. (2022). Exploring Fraudsters Strategies to Defraud Users on Online Employment Databases. International Journal of Cyber Criminology, 16(2), 61-83.

[10] Better Business Bureau (BBB). 2024. BBB Scam Alert: How to spot a job scam – no matter how sophisticated. https://www.bbb.org/article/scams/28372-bbb-scam-alert-how-to-spot-a-job-scam-no-matterhow-sophisticated. June 29, 2024.

[11] IRS. 2024. The Dirty Dozen represents the worst of the worst tax scams. https://www.irs.gov/newsroom/dirty-dozen. July 2, 2024.

[12] Cleary, B. 2024. Tax scams: 15 IRS scams and tips for how to avoid them. https://lifelock.norton.com/learn/identity-theft-resources/irs-tax-scams-to-watch-out-for. July 2, 2024.

[13] Rege, A., Bleiman, R., Williams, K. (2023a). "The Relevance of Social Engineering Competitions in Cybersecurity Education". Proceedings from the IEEE Cyber Science Conference. Anonymize for review

[14] Rege, A., Bleiman, R. (forthcoming). "A Case Study of a Ransomware and Social Engineering Competition." Proceedings from the IEEE Cyber Science Conference. Anonymize for review

[15] TBD

[16] Rege, A., Williams, J., Bleiman, R., & Williams, K. (2023b, June). Students' Application of the MITRE ATT&CK® Framework via a real-time Cybersecurity Exercise. In European Conference on Cyber Warfare and Security (Vol. 22, No. 1, pp. 384-394). Anonymize for review

[17] Dawkins, S., & Jacobs, J. (2023). NIST Phish Scale User Guide. National Institute of Standards and Technology, Gaithersburg, MD, NIST TN, 2276.

[18] Identity Theft Resource Center (ITRC). 2024. 2023 Trends in Identity Report. https://www.idtheftcenter.org/publication/itrc-trends-in-identity-report-2023/