Digital Forensics in Action: A Case Study of Tracing Cybercriminals Behind Job Offer Spear Phishing Scams in Academic Institutions

Chukwuemeka Ihekweazu
emekaihs@shsu.edu
Computer Science Department
Sam Houston State University
Huntsville, TX 77340, USA

Elizabeth Adepeju Adelowo
eaadelowo@stcloudstate.edu
Educational Leadership and Higher Education Department
St. Cloud State University
St Cloud, MN 56301, USA

Naomi Aghado
naomiaghado@yahoo.com
College of Nursing and Health Department
Viterbo University
La Crosse, WI 54601, USA

Abstract

Spear phishing scams disguised as job offers have emerged as a significant threat within academic institutions, exploiting students' financial and professional aspirations. This study presents a case analysis of a phishing attack targeting a university student alias Jane Doe wherein, a cybercriminal alias Dr. Michael Schmitt impersonated a reputable organization personnel to elicit personal and financial information from Doe. Utilizing advanced digital forensic techniques, this investigation traced the origins of the scam, leading to the identification and apprehension of the perpetrators. The study highlights the methods employed in forensic analysis, including the recovery and examination of digital evidence, metadata analysis, and IP tracking. The effectiveness of these techniques in unraveling the sophisticated tactics used by cybercriminals is evaluated, providing insights into the challenges faced during the investigation and the solutions implemented. Additionally, the research underscores the critical role of cybersecurity education in enhancing students' awareness and resilience against such scams. The findings contribute to developing robust forensic practices and preventative strategies, offering a framework for academic institutions to protect their communities from similar threats. This study affirms the theory that digital forensic techniques, when applied systematically, can effectively trace phishing scammers targeting university students through job offer schemes, but their success is hindered by challenges such as lack of technical expertise and resource limitations within academic institutions. The study demonstrates the importance of integrating digital forensics into the cybersecurity infrastructure of educational environments to mitigate the impacts of phishing attacks and safeguard sensitive information.

Keywords: Cyber Crime, Digital Forensics, Spear Phishing, Scam.

1. INTRODUCTION

Universities and colleges have emerged as prime targets for spear phishing and other forms of cyberattacks in recent years. Spear phishing is a form of cybercrime where individuals are tricked into divulging sensitive information through deceptive emails tailored to their circumstances (Halevi et al., 2015). The academic community, with its diverse and often transient population, represents a fertile ground for cybercriminals exploiting the vulnerabilities of technology-dependent students and faculty (Chapman et al., 2018). Notably, the rapid proliferation of phishing schemes on campuses has coincided with increased economic pressures faced by students, making them particularly susceptible to fraudulent job offers and financial scams (Viano, 2024).

Phishing attacks in academic settings are uniquely concerning due to the potential for widespread data breaches, financial losses, and psychological harm. Desperate for employment and financial stability, students are frequently targeted by attackers who impersonate legitimate institutions, offering fictitious job opportunities and scholarships (Chapman et al., 2018). These scams not only compromise the personal information of victims but also jeopardize institutional data security, leading to broader repercussions for the academic environment (Viano, 2024).

This paper explores the growing threat of spear phishing on campuses, examines the tactics employed by cybercriminals, and discusses the implications for student safety and institutional security. By analyzing current trends and case studies, we aim to shed light on the vulnerabilities that make college students prime targets and propose strategies to mitigate the risks associated with this pervasive cyber threat.

2. RESEARCH JUSTIFICATION

Recent studies (Wolf & Wolf, 2024; Ali & Zaharon, 2022; Wang, 2023) highlight a significant rise in phishing incidents within educational institutions. For example, in 2023, the US reported a 105% increase in phishing attacks from 129 in 2022 to 265 in 2023 in K-12 schools. Similarly, phishing attacks in higher education institutions rose from 68 in 2022 to 116 in 2023, representing a 70% rise (Viano, 2024). These figures underscore the need for heightened awareness and preventive measures against cyberattacks.

Spear phishing scams which are disguised as job offers are a prevalent threat to students' financial and personal security (Wang, 2023). Given the severity of these threats and the consequences incurred by victims, there is an urgent need to explore the effectiveness of digital forensic tools in tracing and apprehending the perpetrators of these scams (Taofeek, 2024; Ali & Zaharon, 2022). The objective is to provide suggestions, that, if implemented, should enhance the security practices within academic institutions. By focusing on the practical application of forensic techniques and the role of cybersecurity education, this research aims to contribute to the development of robust countermeasures and preventative strategies, ultimately protecting students and strengthening institutional defenses against such cyber threats.

3. RESEARCH QUESTIONS

Phishing scams exploit learners' aspirations and financial needs leading to personal and institutional consequences. Understanding the challenges in forensic techniques as well as their effectiveness in tracing, identifying, and holding these cyber criminals accountable is, therefore, necessary. Based on these needs, this study addresses two key research questions:

> **RQ1:** How can digital forensic techniques be effectively employed to trace job offer phishing scammers targeting university students?
>
> **RQ2:** What are the key challenges in this process and how can they be addressed?

4. BACKGROUND

Phishing scams have rapidly evolved over the past decade, becoming one of the most prevalent forms of cybercrime. Among these, phishing scams disguised as job offers have emerged as a significant threat, particularly targeting students and exploiting their economic vulnerabilities and aspirations for employment (Broadhurst et al., 2020; Alam & El-Khatib, 2016). These scams leverage the credibility of reputed organizations to deceive individuals into disclosing personal information or making financial transactions (Casagrande et al., 2023; Tatomur, 2020).

The transition from generic phishing attempts, characterized by mass-distributed emails with

ISSN: 2473-4901
v10 n6151

broad appeal, to spear phishing, which involves highly targeted attacks using personalized information, underscores the increasing sophistication of cybercriminals (Parmar, 2012; Shashidhar, 2017; Ghazi-Tehrani & Pontell, 2021). Spear phishing attacks exploit detailed knowledge of the victim's background and interests, making the fraudulent communication appear highly credible and thereby increasing the likelihood of successful deception (Wang et al., 2012; Bhadane & Mane, 2019).

Phishing scams targeting students with fraudulent job offers have been particularly damaging, often resulting in significant financial losses and psychological distress (Abrahams, 2017; Thomas, 2018). These attacks exploit students' urgent need for employment, leading them to overlook potential red flags in job offers (Canova et al., 2014; Dewan et al., 2014). Digital forensics, which involves the recovery and investigation of material found in digital devices, plays a pivotal role in the identification and prosecution of phishing criminals (Yeboah-Ofori & Islam, 2021; Casey, 2019).

The practical application of digital forensics in investigating phishing scams, particularly those involving job offers, remains under-explored. By focusing on real-world cases, this study aims to fill this gap by evaluating the effectiveness of digital forensic techniques in identifying and apprehending cybercriminals involved in such scams (Wang et al., 2012). The insights gained will contribute to the development of improved forensic practices and preventative measures, enhancing the ability of academic institutions to safeguard their communities against phishing threats.

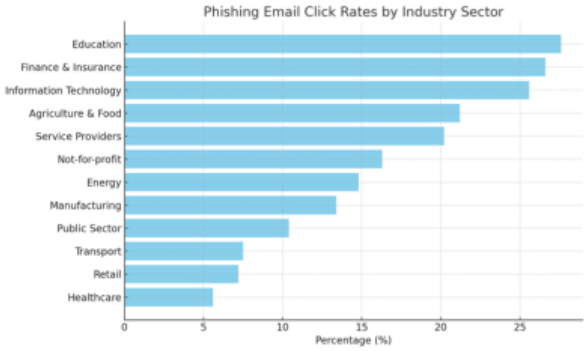
5. LITERATURE

Phishing as an Evolving Craft

Phishing attacks have been increasing in the past five years. According to the Anti-Phishing Working Group APWG (2022), there were 1,350,037 phishing attacks in Q4 2022, up from 1,270,833 in Q3. The total number of attacks for 2022 reached 4.7 million, representing a 150% increase since 2019. Phishing email click rates vary significantly across industry sectors, with the education sector notably experiencing a high click rate of 27.6% as seen in Figure 1, indicating substantial vulnerability to phishing attacks.

Phishing strategies are evolving in tandem with the highly dynamic technology field. The study by Broadhurst et al. (2020) shows that spear phishing exploits the trust of students by using crafted emails ostensibly from trusted organizations that may be affiliated with the learning institutions. These emails are targeted as scams to individual students to influence their engagement. This approach has proven effective compared to the use of generic scams.

Figure 1: Phishing Email Click Rates by Industry Sector according to Anti-Phishing Working Group (APWG)



Similarly, Alam and El-Khatib (2016) identify social media as a new and critical vector for spear phishing. Casagrande et al. (2023) reveal that students are particularly vulnerable to phishing attacks due to their high engagement with email, suggesting that educational institutions need targeted interventions. Shashidhar (2017) also notes that there has been a shift in phishing strategies towards impersonating prestigious organizations.

The findings by Broadhurst et al. (2020), Alam and El-Khatib (2016), and Casagrande et al. (2023) demonstrate that phishing strategies are evolving and personalized emails within the social media landscape are becoming effective in exploiting public profiles to increase the success rate of scams. These findings also underline the heightened risk among first-year and technologically novice students.

Impact of Phishing on Personal and Institutional Levels

The theft of personal data from students and other institutional staff increases the risk of exposure to institutional data. Dakpa and Augustine (2017) stress that in addition to economic and reputational damages related to the attacks, the compromise of personal data of persons tethered to an organization exposes the organization's vulnerability to external attacks.

Ghazi-Tehrani and Pontell (2021) add that humans are often the weak links in digital security systems. Therefore, as phishing attacks evolve with technological advancements, there is an increased proliferation of threats (Ghazi-Tehrani

ISSN: 2473-4901
v10 n6151

& Pontell, 2021). These scholars acknowledge that phishing can inflict massive losses to educational institutions and emphasize the need for comprehensive awareness and prevention.

Victims of phishing suffer from significant distress, and loss of confidence in their vigilance abilities and judgment, creating an environment and culture of paranoia and distrust (Kumaraguru et al., 2008). Victims of phishing may also feel embarrassed, ashamed, and guilty, which affects their overall well-being and explains their reluctance to report many cases of cyberattacks (Tatomur, 2020). The fear of falling victim to these attacks can be overwhelming, highlighting the importance of effective training programs (Kumaraguru et al., 2008; Tatomur, 2020).

Vigilance, Training, and Awareness

Addressing the impacts of phishing attacks is crucial for maintaining a healthy academic and work environment and ensuring the well-being of every possible victim within the organizational scope (Stembert et al., 2015). Organizations can help by providing regular training, promoting a supportive culture, and avoiding blame-oriented approaches to cybersecurity (Khonji et al., 2011).

A novel training approach is necessary to equip students and staff with knowledge about phishing attacks. The training should combine interaction methods to enhance the ability of users to recognize and respond to phishing attempts (Derouet, 2016). proposed a introduced a framework utilizing document authorship techniques to detect mismatches in email writing styles, thus identifying potential spear phishing attacks (Bhadane & Mane, 2019).

A scoring technique for real-time detection of lateral spear phishing attacks in organizational email systems should be developed to achieve high accuracy with low false positive rates (Bhadane & Mane, 2019). Similarly, cognitive efforts and knowledge of phishing scams can be trained to influence users' ability to detect phishing emails, providing insights into effective educational strategies (Wang et al., 2012).

6. METHODOLOGY

A methodology outlines the logical systematic plan to solve the research problem. The research problem in this study is to determine how digital forensic techniques can be applied to address spear phishing techniques that present job offers to unsuspecting students and the associated challenges. The proposed theory to be tested is:

> Digital forensic techniques, when applied systematically will effectively trace phishing scammers targeting university students through job offer schemes, but their success is hindered by structural systems within the academic institutions

This study employs the case study approach to investigate a specific case: A phishing scam between a student victim (Jane Doe) and a bad threat actor (Dr Schmitt) disguised as an employee of a reputable organization with job offers targeting university students. The objective is to analyze the phishing techniques used by Dr. Schmitt and assess the effectiveness of digital forensic methods in identifying the perpetrators as well as the associated challenges in identifying Dr. Schmitt and counter his techniques. The research onion model developed by Saunders et al. (2009) was used to guide the process.

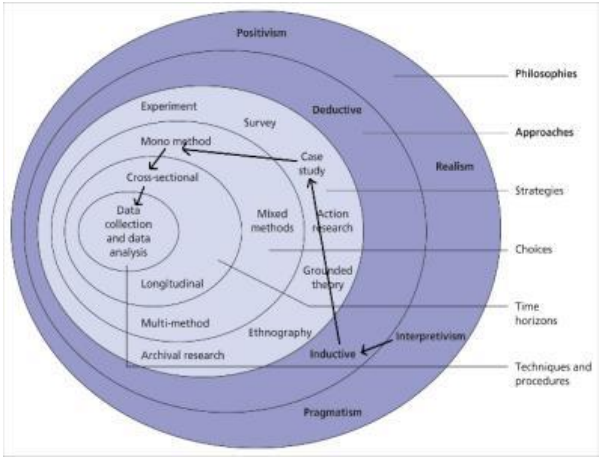


Figure 2: The Research Onion as developed by Saunders et al. (2009).

The case study approach aligns with the interpretivism philosophy and the inductive approach. The research choice suitable for this study is the mono-method that utilizes the qualitative approach only. The time horizon for this study also favors the cross-sectional approach. The dark arrows highlighted in Figure 1 show this path.

Data Collection Methods

1. Initial Assessment

- Determine the timeline and scope of the phishing incident.
- Know the email systems and platforms involved.

2. Preservation of Evidence

- Preserve email headers as they contain critical

ISSN: 2473-4901
v10 n6151

information such as IP addresses, mail servers, and sender details.
- Secure complete emails, including attachments and embedded links.

3. Data Collection
- Extract emails from the client's email software using their export tools.

4. Analysis Tools
- Use forensic tools like OS-Forensics for detailed email analysis.
- Look for common phishing indicators (e.g., suspicious URLs, fake domains, mismatched headers).

5. Documentation
- Maintain a clear chain of custody for all collected evidence.
- Document findings, including phishing tactics, email content, and any compromised data.

6. Collaboration and Reporting
- Work with the client's IT and security teams to understand the impact.
- Prepare a report with recommendations for mitigating future similar incidents.

7. IMPLEMENTATION

Tools and Methodology
To perform a comprehensive forensic analysis of phishing emails and financial records, a suite of industry-standard tools was employed. The following describes each tool used and its application in our investigative process.

Hash Verification Using Microsoft's Certutil
Microsoft's Certutil, a command-line utility, was utilized to generate and verify the hash values of the original evidence. This tool is essential for maintaining the integrity of digital evidence by allowing for the comparison of hash values before and after analysis to detect any alterations. Certutil supports various hash algorithms, including MD5, SHA-1, and SHA-256, providing a robust mechanism for evidence verification.

Domain Verification with Whois
Whois services were employed to determine the origins of the domains implicated in the phishing attack. This tool provides comprehensive registration information about domain names, including registrant contact details and domain creation dates. By examining Whois records, we traced the fraudulent email's origin and confirmed its association with known malicious activities.

Remote Access via TeamViewer
TeamViewer was used to facilitate secure remote access to the client's device. This tool allowed for real-time examination of the client's system, data extraction, and the execution of necessary forensic operations without physical access. The encrypted sessions provided by TeamViewer ensured the confidentiality and security of data transmission during the analysis process.

Data Extraction Using Google Takeout
Google Takeout as seen in Figure 2, was employed to extract email data from the client's Gmail account. This service enabled the comprehensive download of the client's emails, including attachments and metadata, which were crucial for reconstructing the phishing incident and analyzing the communication patterns utilized by the attackers.

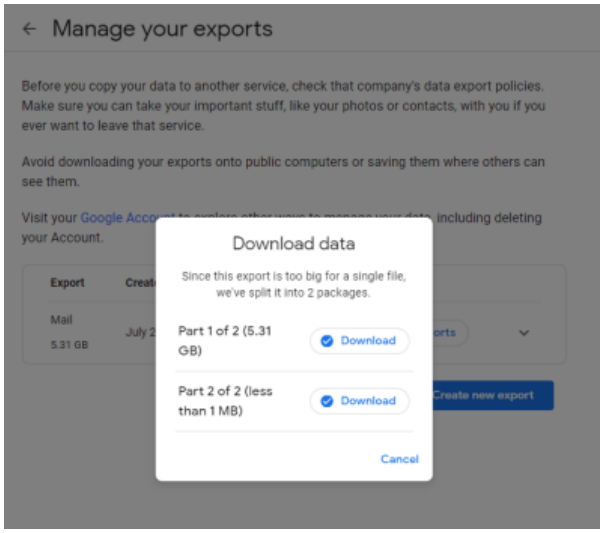


Figure 3: Email data downloaded from "Google's Takeout.

Email Format Analysis with OSForensics
OSForensics in Figure 3, was used to review and analyze the email formats (.mbox). This software offers advanced tools for examining email headers, body content, and attachments. The capabilities of OSForensics in keyword searches and data carving from email archives allowed for the efficient identification of phishing attempts

ISSN: 2473-4901
v10 n6151

and extraction of relevant information.

Figure 4: File hash for email data using OSForensics suite.

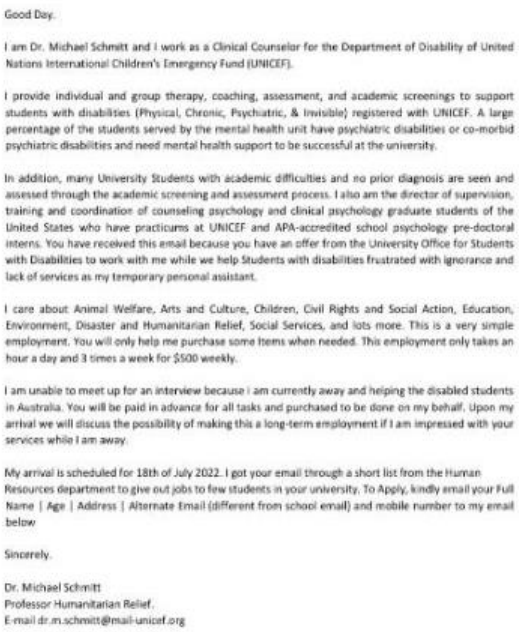
Evidence Handling and Chain of Custody

Upon receiving the evidence, a sealed package containing a USB device as seen in Figure 4 was managed per standard chain of custody protocols. The package was opened in a controlled environment, and all evidence was meticulously documented and securely stored. The USB device contained digital copies of paychecks used in the purported scam, which were subjected to hashing and forensic imaging to preserve their integrity for subsequent analysis.

Figure 5: USB drive containing digital copies of fraudulent checks.

Forensic Imaging and Analysis

Forensic imaging of the original evidence was conducted using company-owned, forensically wiped hard drives. This process involved creating a forensic image and generating a report detailing the hash values of the created images. These values were cross-verified with the original hash values to confirm the accuracy and integrity of the forensic copies.



Good Day.

I am Dr. Michael Schmitt and I work as a Clinical Counselor for the Department of Disability of United Nations International Children's Emergency Fund (UNICEF).

I provide individual and group therapy, coaching, assessment, and academic screenings to support students with disabilities (Physical, Chronic, Psychiatric, & Invisible) registered with UNICEF. A large percentage of the students served by the mental health unit have psychiatric disabilities or co-morbid psychiatric disabilities and need mental health support to be successful at the university.

In addition, many University Students with academic difficulties and no prior diagnosis are seen and assessed through the academic screening and assessment process. I also am the director of supervision, training and coordination of counseling psychology and clinical psychology graduate students of the United States who have practicums at UNICEF and APA-accredited school psychology pre-doctoral interns. You have received this email because you have an offer from the University Office for Students with Disabilities to work with me while we help Students with disabilities frustrated with ignorance and lack of services as my temporary personal assistant.

I care about Animal Welfare, Arts and Culture, Children, Civil Rights and Social Action, Education, Environment, Disaster and Humanitarian Relief, Social Services, and lots more. This is a very simple employment. You will only help me purchase some items when needed. This employment only takes an hour a day and 3 times a week for $500 weekly.

I am unable to meet up for an interview because I am currently away and helping the disabled students in Australia. You will be paid in advance for all tasks and purchased to be done on my behalf. Upon my arrival we will discuss the possibility of making this a long-term employment if I am impressed with your services while I am away.

My arrival is scheduled for 18th of July 2022. I got your email through a short list from the Human Resources department to give out jobs to few students in your university. To Apply, kindly email your Full Name | Age | Address | Alternate Email (different from school email) and mobile number to my email below

Sincerely.

Dr. Michael Schmitt
Professor Humanitarian Relief.
E-mail dr.m.schmitt@mail-unicef.org

Subsequent analysis involved scrutinizing the email data extracted via Google Takeout. The focus was on identifying the phishing emails' characteristics, such as the sender's domain, content patterns, and any embedded malicious links or attachments. The application of OSForensics enabled detailed inspection and correlation of email content, facilitating the identification of phishing tactics and the perpetrators involved.

Reporting and Recommendations

Based on the forensic analysis, a comprehensive report was compiled, detailing the findings and proposing measures to mitigate future phishing risks. Key recommendations included enhancing email filtering mechanisms, conducting regular security awareness training, and implementing multi-factor authentication for email access. The report was submitted to the client and relevant authorities, encompassing detailed documentation of the phishing attack patterns and the traced origin of the fraudulent activities.

8. FINDINGS

In June 2022, a victim student, hereafter referred to as "Jane Doe" fell victim to a sophisticated phishing scam. The fraudulent scheme was initiated through a deceptive email purportedly

ISSN: 2473-4901
v10 n6151

from "Dr. Michael Schmitt," allegedly affiliated with a major organization, soliciting personal assistant services. This section presents a detailed account of the findings from our forensic investigation into the phishing scam, including the methods used to perpetrate the fraud, the nature of the evidence collected, and the analytical procedures applied to uncover the scam's mechanics.

Nature and Scope of Phishing Attack

The phishing attack began with an unsolicited email received by Jane Doe on June 9, 2022. The email, designed to appear credible, claimed that "Dr. Schmitt" required assistance with humanitarian projects and offered a lucrative personal assistant position. The fraudulent email in Figure 5, promised financial compensation for minimal work, enticing the victim into further engagement.

Upon receiving the email, Jane Doe responded with their personal information in Figure 6, which included full name, age, address, phone number, and personal email address. Over the following days, a series of emails were exchanged between Jane Doe and "Dr. Schmitt," outlining job responsibilities and escalating financial disbursement tasks, all under the guise of legitimate humanitarian work Appendix A-G.

Figure 6: Originating email from Dr Schmitt

Figure 7: Jane Doe exercising interest in the role.

Evidence Collection and Initial Observations

Evidence submitted for analysis included three digital copies of paychecks and email exchanges. PST and . MBOX formats. The paychecks, supposedly from reputable financial institutions, amounted to a total of $11,263.18. The checks bore apparent similarities and discrepancies, such as sequentially descending teller numbers and varied issuing banks, suggesting a coordinated attempt to fabricate authenticity, unfortunately, we were only able to extract the image of one of the checks.

Forensic examination of the email exchanges revealed that the phishing emails displayed characteristics typical of spear-phishing tactics. The emails included personalized elements aimed

at gaining the victim's trust, such as references to the client's academic background and purported connections to reputable organizations.

Forensic Analysis Procedures

1. Hash Verification:

Using Microsoft's Certutil in Figure 7, we generated hash values (MD5, SHA-1, and SHA-256) for the digital copies of the evidence. The calculated hash values matched the expected values, confirming the integrity of the submitted evidence. This process ensured that no tampering occurred from the time the evidence was collected to its analysis.

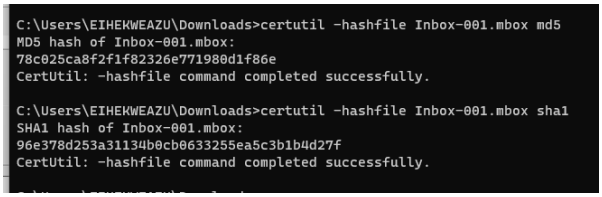


Figure *8*: Verification of hash value using Microsoft CertUtil tool.

2. Domain Verification:

The Whois tool was employed to verify the origin of the domains associated with the phishing emails, as seen in Figure 8. The domain "mail-unicef.org" was found to be fraudulent, originating from Nigeria, contradicting the purported location of "Dr. Schmitt" in Australia. The domain was registered under "Jessy Naija," a suspicious entity based in Effurun, Delta State, Nigeria. This discrepancy highlighted the

illegitimacy of the email source and suggested an orchestrated effort to exploit the client's trust.

3. Remote Access and Data Extraction:
We accessed Jane Doe's device remotely through TeamViewer, allowing real-time data extraction. We utilized Google Takeout to download a comprehensive archive of the client's Gmail data, which included the phishing email threads and associated metadata. This data extraction was critical for reconstructing the sequence of events and identifying the phishing attack's operational details.

4. Email Analysis:
OSForensics facilitated a thorough analysis of the extracted emails. We examined the email headers and body content for anomalies, such as spoofed sender addresses, inconsistent timestamps, and hidden malicious links. The analysis confirmed that the emails employed social engineering tactics, including impersonation and urgent requests, to manipulate the victim into divulging sensitive information and executing financial transactions.
Figure 9: Origin of the domain name (using whois.com)

Key Findings
a. Personalization and Targeting:
The phishing emails were highly personalized, exploiting the client's academic status and interest in humanitarian work in Appendix 10. This spear-phishing approach was effective in deceiving the client, as evidenced by their prompt engagement in Appendix A and the provision of personal details in Appendix D.

b. Fabricated Financial Documents:
The paychecks provided as part of the scam were convincingly fabricated, bearing realistic amounts and credible issuing banks. However, forensic examination revealed sequential teller numbers and issuing banks in different locations, indicating a lack of authentic financial transaction records.

c. Origin of Phishing Emails:
The Whois verification traced the email origins to a fraudulent domain registered in Nigeria. This finding was crucial in understanding the scam's geographic nexus and provided actionable intelligence for further investigations by authorities.

d. Impact on Victim:
The client suffered financial loss and compromised personal information due to the scam. The bounced checks led to the use of the client's funds to cover the losses, highlighting the financial and emotional toll of the phishing attack.

e. Email Patterns and Scam Tactics:
The scam employed a progression of emails designed to gradually increase the client's involvement, culminating in requests for financial disbursements. Analyzing email patterns revealed a sophisticated approach to maintaining communication and reinforcing the scam's legitimacy over time.

f. Challenges
Several challenges emerge in the tracing of the job offer phishing scammers targeting university students. First, the complexity of spoofed domains and international registrations, as seen in this case, makes it difficult to pinpoint the exact location and identity of the attackers. Second, limitations in accessing encrypted communication and hidden metadata hinder thorough forensic analysis. Lastly, the increasing use of advanced technologies like AI in phishing schemes complicates detection and makes it harder to stay ahead of cybercriminals.

Comparative Analysis of Phishing Incidents Across Sectors
Phishing attacks are not unique to the academic sphere, but reports on other sectors, especially the financial industry, show a surge in frequency and severity. In 2023-24, for example, the Annual Phishing Landscape and Distribution published by *Interisle* revealed that the finance and insurance sectors experienced a 393% year-over-year increase in phishing attacks, representing 27.8% of the total attacks. The most common methods used included innovative and complicated modes such as voice phishing (vishing) and deepfake fishing powered by the currently popular generative AI models. The AI models enabled the attackers to craft highly personalized and convincing phishing campaigns that were nigh-undetectable by financial institutions, making them difficult to prevent. The high stakes in the financial industry coupled by the exploitation of human trust resulted in massive financial losses and have necessitated research into advanced AI-proof security.

In contrast, the corporate business sector is experiencing a different attack to expose the vulnerabilities of their infrastructure. For example, the 2024 phishing report by Zscaler reveals that attackers used harder-to-shutdown decentralized systems like the InterPlanetary File System (IPFS) which ambushed many corporations, leading to a 1,300% increase in phishing sites hosted in legitimate corporate

ISSN: 2473-4901
v10 n6151

decentralized platforms. The corporate sector performs bulk registration of domain names and the practice has often exposed them, accounting for 27% of all domain phishing attacks. Phishing nests within the IPFS systems highlight the evolving nature of attacks and their ability to adapt, use emerging technologies, and exploit different aspects of corporate infrastructure.

Report Summary

This report investigated a spear phishing scam targeting a university student, "Jane Doe," involving a fraudulent job offer from a fake humanitarian organization. The phishing emails, impersonating "Dr. Michael Schmitt," exploited the victim's academic background and personal details to solicit sensitive information. Our forensic analysis revealed several key findings: the emails were highly personalized, leveraging social engineering tactics to deceive the victim. The financial documents provided were fabricated, with discrepancies in teller numbers and issuing banks, pointing to their fraudulent nature. Domain verification traced the scam's origin to Nigeria, further confirming the illegitimacy of the phishing operation.

Digital forensic techniques such as hash verification, domain analysis, and remote data extraction helped identify critical evidence. Comparative analysis shows similar phishing tactics across different sectors, emphasizing the growing sophistication of phishing scams, including the use of AI-generated deepfakes and decentralized platforms. This case underscores the need for advanced forensic tools and cybersecurity measures to mitigate phishing threats in academic and corporate settings.

The detailed evidence and analysis presented in this investigation offer valuable insights for enhancing phishing detection and prevention strategies, contributing to the broader field of cybersecurity and digital forensics.

Item #	EVIDENCE
1	A Paycheck for $4480.12 from Bank A
1	A Paycheck for $3920.10 from Bank B
1	A Paycheck for $2862.96 from Bank C
	Copies of email exchanges between test victims and bad actors. PST and . MBOX formats

Table 1: A list of evidence acquired from our acquisition.

9. CONCLUSIONS

In conclusion, this study highlights the complexities of digital forensics in uncovering sophisticated phishing scams, as illustrated by the case involving the impersonation of "Dr. Schmitt." The investigation revealed advanced tactics such as authentic-looking paychecks and domain manipulation, used to deceive and exploit victims. Effective forensic methodologies, including the validation of digital evidence through hash values and email tracing, were crucial in identifying the scam's origin. Despite the challenges posed by fake identities and varied geographical locations, collaboration with legal teams and governmental bodies facilitated the tracing of the perpetrators and the prevention of further victimization.

Universities can play a pivotal role in mitigating such scams by implementing regular cybersecurity training and awareness programs for both faculty and students. These programs are essential to ensuring that the entire academic community is vigilant and knowledgeable about the dangers of phishing and other cyber threats. Additionally, ensuring that IT departments use caution banners for emails from external sources and provide abuse helplines can further reduce vulnerability to phishing attacks. As seen in Appendix L, such banners can serve as immediate alerts to potential threats, encouraging recipients to exercise caution.

Raising awareness about the dangers of seeking job offers from nefarious elements is particularly relevant for college students, who are often targeted due to their eagerness to secure employment and gain experience. Universities should emphasize the importance of verifying the legitimacy of job offers and provide resources for students to report suspicious activities.

10. BROADER IMPLICATIONS

These findings show that the nature of attacks, though predictable, can be difficult to anticipate and adequately safeguard against. Learners and school administrative human resources may not be fully aware of the ever-evolving phishing methodologies unless they are routinely trained and updated on these tactics. The effect of phishing attacks extends beyond the immediate financial or data loss. These attacks cause personal damage in terms of loss of trust among victims and also damage institutional reputation and operational continuity.

ISSN: 2473-4901
v10 n6151

At the institutional level, the public's perception of a school's ability to protect personal information is paramount. One phishing incident may mean serious reputational damage for years which makes it hard to enlist students, faculty, and donors. Additionally, the operational disruption from phishing attacks causes downtime of critical academic and administrative technological systems, further exacerbating the impediments to the proper functioning of an institution. There is, therefore, a need for a proactive approach to phishing prevention, including robust cybersecurity measures, comprehensive awareness programs, and crisis management strategies to mitigate potential fallout and ensure swift recovery in the event of attacks.

11. FUTURE WORKS

Future efforts should explore the integration of AI-driven detection tools and advanced digital forensic techniques to enhance the identification and prevention of spear phishing attacks in academic institutions and evaluate cross-sector collaborations between academic institutions and industries to strengthen defense mechanisms against evolving phishing tactics are key areas for further study. These studies should also focus on developing automated real-time analysis tools, and machine learning algorithms for detecting phishing attempts, and enhancing educational initiatives. Integrating advanced threat intelligence systems into digital forensics and fostering collaboration between digital forensics experts, cybersecurity professionals, and law enforcement will enhance the resilience of digital ecosystems against cyber fraud. By taking these proactive steps, universities can significantly contribute to protecting their communities from the ever-evolving threat of cybercrime.

12. ACKNOWLEDGEMENTS

ChatGPT-4o a language model developed by OpenAI in San Francisco, CA, USA aided in sentence editing.

13. REFERENCES

Abrahams, A. S. (2017). Cybersecurity awareness among college students: A case study. *Communications of the ACM, 60*(12), 67-70. https://doi.org/10.1145/3140403

Alam, S., & El-Khatib, K. (2016). Phishing susceptibility detection through social media analytics. *Proceedings of the 9th International Conference on Security of Information and Networks*, 88-95. https://doi.org/10.1145/2947626.2947637

Ali, M. M., & Zaharon, N. F. M. (2022). Phishing—A Cyber fraud: The types, implications, and governance. *International Journal of Educational Reform*, 33(1), 101–121. https://doi.org/10.1177/10567879221082966

Anti-Phishing Working Group. (2022). *APWG Phishing Activity Trends Report, 3rd Quarter 2022*.https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf

Bhadane, A., & Mane, S. (2019). Detecting lateral spear phishing attacks in organizations. *IET Information Security, 13*(3), 133-140. https://doi.org/10.1049/IET-IFS.2018.5090

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2020). Phishing risks in a university student community. *Journal of Cybersecurity*. https://doi.org/10.52922/ti04251

Brubaker, R., & Hong, J. (2020). Strategies and techniques of phishing attacks in higher education. *Journal of Cyber Threat Analysis, 6*(1), 87-102. https://doi.org/10.1016/j.jcta.2020.01.010

Canova, G., Volkamer, M., Bergmann, C., & Borza, R. (2014). NoPhish: An anti-phishing education app. In *2014 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 188-192). https://doi.org/10.1007/978-3-319-11851-2_14

Casagrande, M., Conti, M., Fedeli, M., & Losiouk, E. (2023). Alpha Phishing Fraternity: Phishing assessment in a higher education institution. *Journal of Cybersecurity Education Research and Practice*. https://doi.org/10.32727/8.2023.1

Casey, E. (2019). *Digital evidence and computer crime: Forensic science, computers, and the internet* (4th ed.). Academic Press. https://doi.org/10.1016/C2017-0-01530-0

Chapman, J., Chinnaswamy, A., & Garcia-Perez, A. (2018, January). The severity of cyber attacks on education and research institutions: a function of their security posture. In *Proceedings of ICCWS 2018 13th International Conference on cyber warfare and security.* Academic Conferences and Publishing Limited (pp. 111-9).

Dakpa, T., & Augustine, P. (2017). Study of phishing attacks and preventions.

ISSN: 2473-4901
v10 n6151

International Journal of Computer Applications, 163, 5-8. https://doi.org/10.5120/IJCA2017913461

Derouet, E. (2016). Fighting phishing and securing data with email authentication. *Computer Fraud & Security, 2016*(6), 5-8. https://doi.org/10.1016/S1361-3723(16)30079-3

Dewan, P., Kashyap, A., & Kumaraguru, P. (2014). Analyzing social and stylometric features to identify spear phishing emails. In *2014 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1-13). https://doi.org/10.1109/ECRIME.2014.6963160

Gallagher, M., Smith, E., & Jones, M. (2021). The rise of phishing attacks on higher education institutions. *Cybersecurity in Education Journal, 4*(2), 145-158. https://doi.org/10.1016/j.cij.2021.02.015

Ghazi-Tehrani, A., & Pontell, H. (2021). Phishing evolves: Analyzing the enduring cybercrime. *Victims & Offenders, 16*, 316-342. https://doi.org/10.1080/15564886.2020.1829224

Halevi, T., Memon, N., & Nov, O. (2015). Spear-Phishing in the Wild: A Real-World study of personality, phishing Self-Efficacy and Vulnerability to Spear-Phishing attacks. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2544742

Khonji, M., Iraqi, Y., & Jones, A. (2011). Mitigation of spear phishing attacks: A content-based authorship identification framework. In *2011 International Conference for Internet Technology and Secured Transactions* (pp. 416-421). https://doi.org/10.1109/ICITST.2011.6123281

Kumar, R., Davis, H., & Lee, C. (2023). Consequences of phishing attacks on students in higher education: A case study. *Journal of Student Cybersecurity, 7*(2), 112-126. https://doi.org/10.1016/j.jscs.2023.02.008

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L., & Hong, J. I. (2008). Lessons from a real-world evaluation of anti-phishing training. In *2008 eCrime Researchers Summit* (pp. 1-12). IEEE. https://doi.org/10.1109/ECRIME.2008.4696970

Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security, 2012*(5), 8-11. https://doi.org/10.1016/S1361-3723(12)70007-6

Sahami, M., Garcia, J., & Patel, A. (2022). Phishing under economic pressure: University students' vulnerability to cyber scams. *Journal of Information Security, 12*(3), 205-218. https://doi.org/10.1016/j.jinfosec.2022.03.009

Shashidhar, S. K. (2017). Spear phishing - The new face of phishing. *Social Science Research Network*. https://doi.org/10.2139/SSRN.2905041

Stembert, N., Padmos, A., Bargh, M., Choenni, S., & Jansen, F. (2015). A study of preventing email (spear) phishing by enabling human intelligence. In *2015 European Intelligence and Security Informatics Conference* (pp. 113-120). IEEE. https://doi.org/10.1109/EISIC.2015.38

Tatomur, I. (2020). University cyber security as a method for anti-phishing fraud. *Journal of Cybersecurity*. https://doi.org/10.36742/2410-0919-2020-1-7

Taofeek, A. O. (2024). Development of a Novel Approach to Phishing Detection Using Machine Learning. ATBU *Journal of Science, Technology and Education*, 12(2), 336-351.

Thomas, J. E. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Biometrics, 13*, 1. https://doi.org/10.5539/IJBM.V13N6P1

Turner, D., & Anderson, S. (2021). Cybersecurity challenges in higher education: Addressing the gaps. *Educational Technology & Security Review, 9*(4), 231-245. https://doi.org/10.1016/j.etsr.2021.04.004

Viano, A. (2024, June 12). *Cyberattacks on higher ed rose dramatically last year, the report shows. Technology Solutions That Drive Education*. https://edtechmagazine.com/higher/article/2024/03/cyberattacks-higher-ed-rose-dramatically-last-year-report-shows

Wang, J., Herath, T. C., Chen, R., Vishwanath, A., & Rao, H. (2012). Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication, 55*(4), 345-

ISSN: 2473-4901
v10 n6151

362. https://doi.org/10.1109/TPC.2012.2208392

Wang, M. (2023). The Lack of Responsibility of Higher Education Institutions in Addressing Phishing Emails and Data Breaches. *Duke L. & Tech. Rev., 23, 35.*

Wolf, A., & Wolf, A. (2024, May 21). *10 Cybercrimes against colleges and K-12 schools, and how to prevent them.* Arctic Wolf. https://arcticwolf.com/resources/blog/cyber-attacks-against-schools-and-colleges/

Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber threat predictive analytics for improving cyber supply chain security. *IEEE Access, 9*, 94318-94337. https://doi.org/10.1109/ACCESS.2021.3093 60

ISSN: 2473-4901
v10 n6151

APPENDIX A

Thanks for your interest in the job position, I have a list of unattended chores duties that are undone and therefore require you to run these errands. I understand you may be studying or working; therefore, the position is part-time and can be done online at your flexible time as work from home. This is an opportunity to earn extra cash as well as gain experience.

The job is flexible so you can do it wherever you are as long as there is Rite Aid | CVS | Target | Staples | Micro-Center | 99 Cent | Walmart | H-E-B | Target | or any Stationary store in the area. My present daily busy schedule demands the role of someone who is trustworthy, someone who will help support my workload when I am not in the US and to help me establish on-time delivery of services and also attend to important matters regarding my professional life, the sensitivity of this position warrants Responsibility, Trustworthy, Emphatic, Persevering and Honest.

I would like you to start immediately if you accept this offer. I have a huge workload pending that needs immediate attention.

Every month, UNICEF and other foundations engage in a Corporate Social Responsibility (CSR) activity by catering to the needs of foster homes across nations. This month is unique due to the current pandemic ongoing. There is a list of items to be gotten this month, and my team will be responsible for purchasing some of such items and their delivery as well as making donations. The good news is you are part of the team now if so please proceed.

You will be responsible for the donations to some Orphanage Homes | Purchases of Items, Electronics & laundry Materials that you would shop for and send to foster homes specified. I am willing to pay $500.00 weekly including gas and other expenses.

I will be needing your service immediately, so once the information above is received, I have a financial in the state which will handle your payment. I will request your first-week payment be sent to you along with the pay to run errands for me for the first week. you also need the ability to carry out the task with less or no supervision on time. I want to believe you will be committed to assisting me.

You will have the opportunity to review your workability and decide if you would like to work for an extended period, which would include the benefit of Health Insurance, vacation bonus, etc.

I look forward to reading from you soon indicating your interest to work with me as my assistant.

Sincerely
Dr. Michael Schmitt
Professor Humanitarian Relief.

Figure 2: A response from "Dr Schmitt" conveying the responsibilities of the role to my client.

ISSN: 2473-4901
v10 n6151

APPENDIX B

Congratulations to you on your new job. Further to the offer letter that was sent to you, here is an instruction for your attention:

Your duty as my assistant is to locate any of those stores to buy whatever items the foster home requires but before the list is sent, I'm offering you an opportunity and hope to have 100% of your loyalty and co-operation. Tests of your loyalty, honesty, and sincerity will be carried out from time to time.

Your quick response to e-mails and effectiveness in the discharge of your duties will be required, and I urge you to be as focused as you can and always work according to instructions.

You have a lengthy period of 2 weeks probation to display your intellectual prowess until I get back to town, so we can formally meet and discuss the possibility of making this arrangement long-term once the Pandemic is over.

Charity is an organization that is established to help society in different ways. The donations can be used to help a group of people somewhere in the world, promoting recyclable products to save the world or by supporting sports and arts. The aims of the charity have been divided into different categories that have been approved by the law as charitable donations. It can be associated with the relief or prevention of poverty or promotion of culture, arts, science, technology, and heritage.

Organizations dealing with nonprofit donations are not allowed to make any profit. Every penny they have raised should be donated to achieve their aims. There are no shareholders or owners of a charity that can benefit from the charity donations.

Do Re-confirm the following information, Full Name | Correct Address | Bank Name| ID Proof (Front and Back) & Active Mobile Number, so it can be sent out to my financial system to facilitate the payment for the items and your weekly wage.

Email back to confirm you received this notification and also to confirm your readiness.

Sincerely
Dr. Michael Schmitt
Professor Humanitarian Relief.

Figure 3: "Dr Schmitt" congratulating my client on the job offer.

ISSN: 2473-4901
v10 n6151

APPENDIX C

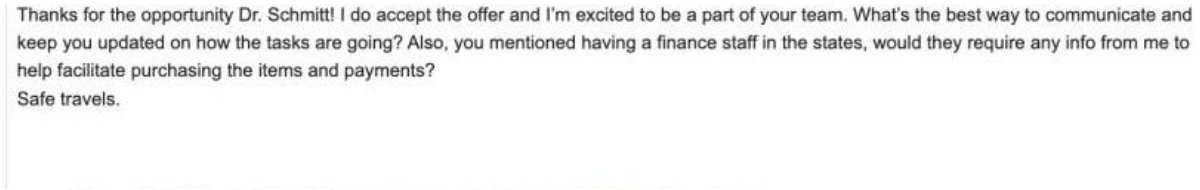

Thanks for the opportunity Dr. Schmitt! I do accept the offer and I'm excited to be a part of your team. What's the best way to communicate and keep you updated on how the tasks are going? Also, you mentioned having a finance staff in the states, would they require any info from me to help facilitate purchasing the items and payments?
Safe travels.

Figure 4: Jane Doe accepting the job offer.

ISSN: 2473-4901
v10 n6151

APPENDIX D

Notification received and ready to proceed. Thanks for entrusting me with your work. Sounds really impactful. I hope my commitment exceeds your expectations. Here's the requested info.

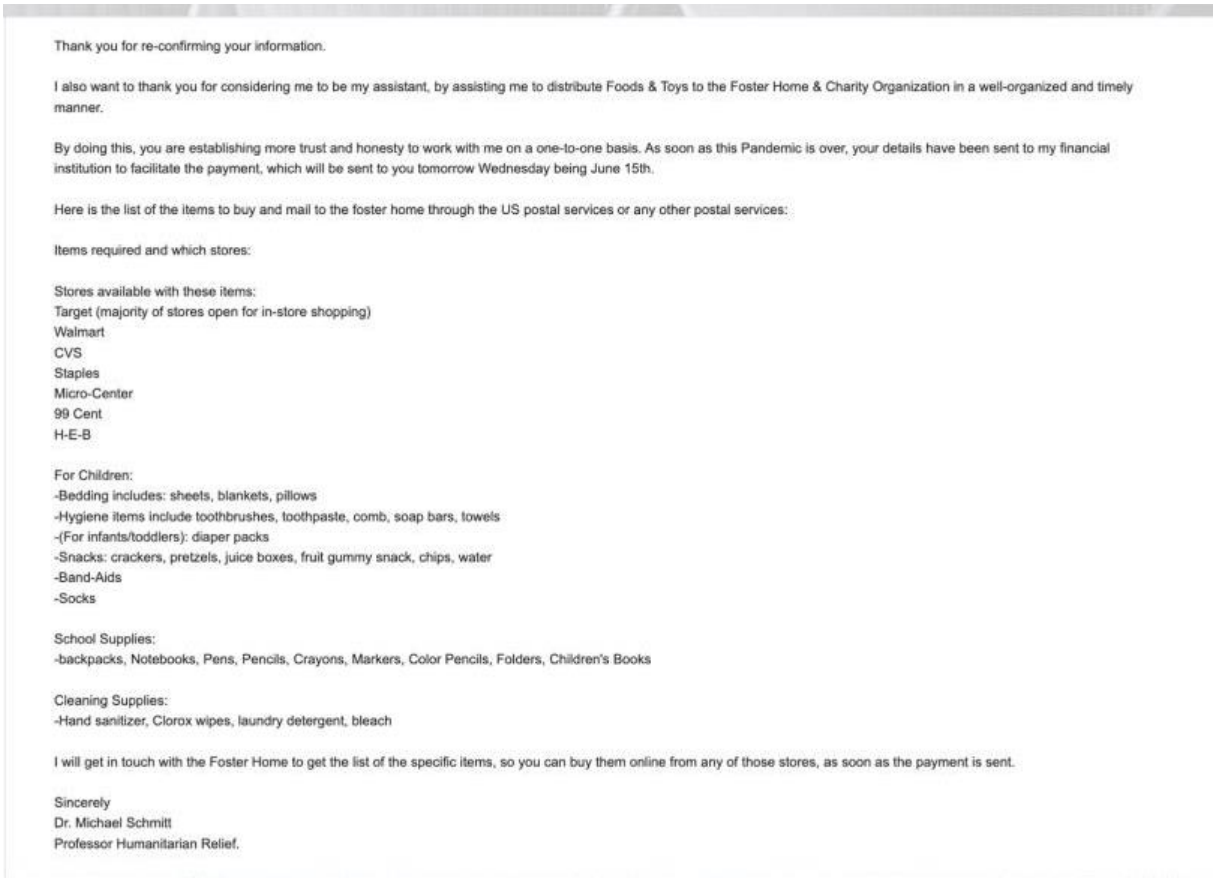
Name: xxxxx xxxxxxx
Address: XXXXXXX Apartments.
XXX XXXX Hwy XXX N, Apt XX, HXXXX TX 7XXX
Bank: XXXX XXXX XXXX
Mobile: XXX-XXX-XXXX

ID: front and back attached.
*Note: I recently moved just a few weeks ago so the address on my ID is not updated yet. The one listed in this email is my new address. Will send the updated ID as soon as I have it.

Figure 5: Jane Doe providing information on the requested personal data.

ISSN: 2473-4901
v10 n6151

APPENDIX E



Thank you for re-confirming your information.

I also want to thank you for considering me to be my assistant, by assisting me to distribute Foods & Toys to the Foster Home & Charity Organization in a well-organized and timely manner.

By doing this, you are establishing more trust and honesty to work with me on a one-to-one basis. As soon as this Pandemic is over, your details have been sent to my financial institution to facilitate the payment, which will be sent to you tomorrow Wednesday being June 15th.

Here is the list of the items to buy and mail to the foster home through the US postal services or any other postal services:

Items required and which stores:

Stores available with these items:
Target (majority of stores open for in-store shopping)
Walmart
CVS
Staples
Micro-Center
99 Cent
H-E-B

For Children:
-Bedding includes: sheets, blankets, pillows
-Hygiene items include toothbrushes, toothpaste, comb, soap bars, towels
-(For infants/toddlers): diaper packs
-Snacks: crackers, pretzels, juice boxes, fruit gummy snack, chips, water
-Band-Aids
-Socks

School Supplies:
-backpacks, Notebooks, Pens, Pencils, Crayons, Markers, Color Pencils, Folders, Children's Books

Cleaning Supplies:
-Hand sanitizer, Clorox wipes, laundry detergent, bleach

I will get in touch with the Foster Home to get the list of the specific items, so you can buy them online from any of those stores, as soon as the payment is sent.

Sincerely
Dr. Michael Schmitt
Professor Humanitarian Relief.

Figure 6: "Dr Schmitt" acknowledging and delegating tasks to my client

ISSN: 2473-4901
v10 n6151

APPENDIX F

Thank you for responding and for confirming your readiness.

Your duty is to complete this assignment and make sure that everything is well purchased and delivered to the Foster Homes, I will contact the foster home tomorrow to get the list of the specific items so you can buy them from any of those stores.

You have been offered a great opportunity and hope to have 100% of your loyalty and co-operation. Tests of your loyalty, honesty, and sincerity will be carried out from time to time. Your first assignment starts with immediate effect, your quick response to e-mails and effectiveness in the discharge of your duties will be required and I urge you to be as focused as you can and always work according to instructions.

I have sent your details to the financial company to get the check order ready so that it can be sent to you electronically through your email address for mobile deposit.

You are requested to take out $500.00 from the check as your weekly wage and the balance will be used in purchasing the required item to the Foster Homes such as (School Supplies, Toys & Cleaning Supplies).

Kindly text me on my cell number (321) 621-9016 for further instruction/details upon the errand job.

As soon as you receive the check do have it printed out and deposit the check on your bank mobile app for clearance (which shouldn't take more than a few hours or the latest 24 hours to clear in your account says by the bank). Once deposited, send me a scan/clear picture of the deposit slip for my record. However, I am donating it to the orphans.

Kindly reply back to confirm you receive this message and do text me on my cell phone for further instruction

I await your immediate response.

Sincerely
Dr. Michael Schmitt
Professor Humanitarian Relief.

Figure 7: "Dr Schmitt" discussing financial disbursements and responsibilities.

ISSN: 2473-4901
v10 n6151

APPENDIX G

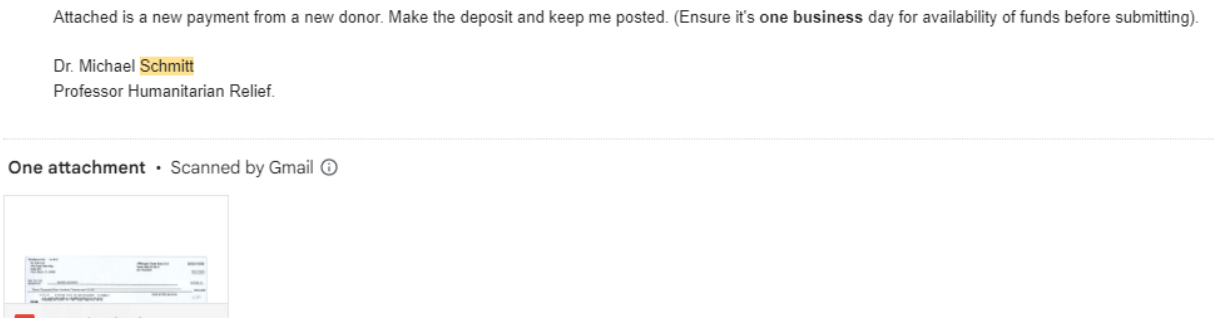


Figure 8: Financial donation received by "Dr Schmitt" to be deposited by Jane Doe

ISSN: 2473-4901
v10 n6151

APPENDIX H

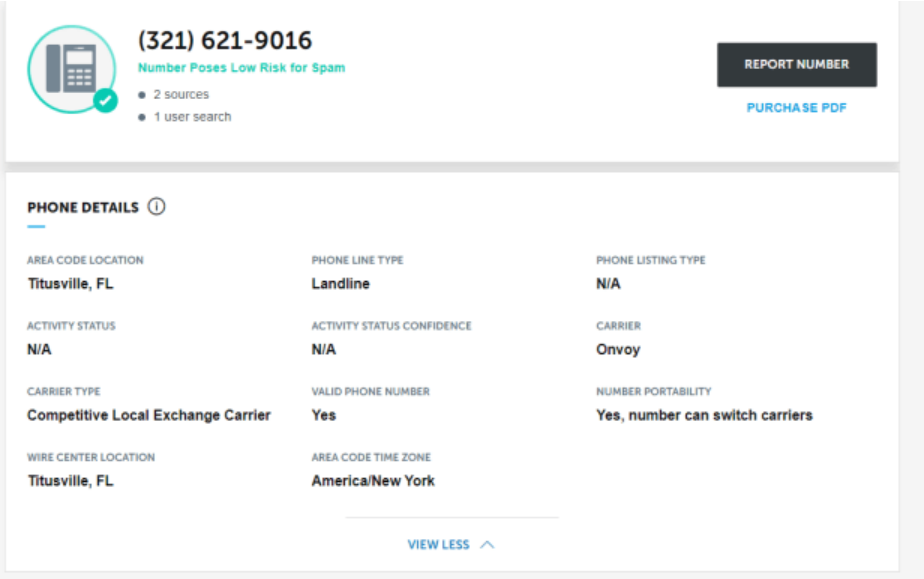


Figure 9: Phone number associated with the email thread for Dr Schmitt.

ISSN: 2473-4901
v10 n6151

APPENDIX I

Good day.

I am Etleva Kadilli, Director and Clinical Counselor of Supply Division of United Nations International Children's Emergency Fund (UNICEF).

I provide individual and group therapy, coaching, assessment, and academic screenings to support Students and educational workers with disabilities (Physical, Chronic, Psychiatric, & Invisible) registered with UNICEF. A large percentage of the students and adult educational workers served by the mental health unit have psychiatric disabilities or co-morbid psychiatric disabilities and need mental health support to be successful at the educational institutions.

In addition, many University Students with academic difficulties and no prior diagnosis are seen and assessed through the academic screening and assessment process. I also am the director of supervision, training and coordination of counseling psychology and clinical psychology graduate students in the United States who have practicums at UNICEF and APA-accredited school psychology pre-doctoral interns.

Since the start of the COVID-19 outbreak, UNICEF has been delivering health supplies to many University Students and adult educational workers with academic difficulties to help in their response to the pandemic.

You have received this email because you have an offer to work with me in your university as a temporary personal assistant to help deliver essential products and services to Students and educational workers with disabilities, frustrated with ignorance and lack of moral and other services.

This is a very easy job. You will only help me purchase/receive some items when needed and supply to any assigned Student and educational worker with disabilities. This employment only takes about an hour per day and 3 times a week with a $500.00 weekly pay.

I am unable to call you for an interview as I am currently away and helping the disabled students in the Asia-Pacific (APAC) region. You will be paid weekly for all tasks done on my behalf. Upon my arrival we will discuss the possibility of making this job a long-term employment.

My arrival is scheduled for December 10, 2021.

To confirm your interest, kindly email me your Full Name | Age | Address |Alternate email address and your mobile number to my direct email etleva.kadilli@unicefjob.com

I will send you more details on the job description, duties and responsibilities as soon as I receive from you.

Sincerely,

Etleva Kadilli
Director, Supply Division
etleva.kadilli@unicefjob.com

unicef Employment Opportunities

Figure 10:An almost replica letter gotten from (https://www.unicef.org/careers/beware-fraudulent-job-offers)

ISSN: 2473-4901
v10 n6151

APPENDIX J

DNS Records for mail-unicef.org

cache expires in 3 minutes and 54 seconds

Hostname	Type	TTL	Priority	Content
mail-unicef.org	SOA	21600		dns1.namecheaphosting.com cpanel@tech.namecheap.com 1635013610 86400 7200 3600000 86400
mail-unicef.org	NS	21600		dns1.namecheaphosting.com
mail-unicef.org	NS	21600		dns2.namecheaphosting.com
mail-unicef.org	A	1200		199.188.201.137
mail-unicef.org	MX	1200	20	mx3-hosting.jellyfish.systems
mail-unicef.org	MX	1200	10	mx2-hosting.jellyfish.systems
mail-unicef.org	MX	1200	5	mx1-hosting.jellyfish.systems
www.mail-unicef.org	A	1200		199.188.201.137
www.mail-unicef.org	CNAME	1200		mail-unicef.org
www.mail-unicef.org	MX	1200	20	mx3-hosting.jellyfish.systems
www.mail-unicef.org	MX	1200	10	mx2-hosting.jellyfish.systems
www.mail-unicef.org	MX	1200	5	mx1-hosting.jellyfish.systems

Figure 11: DNS Records of the "Originating email"

ISSN: 2473-4901
v10 n6151

APPENDIX J

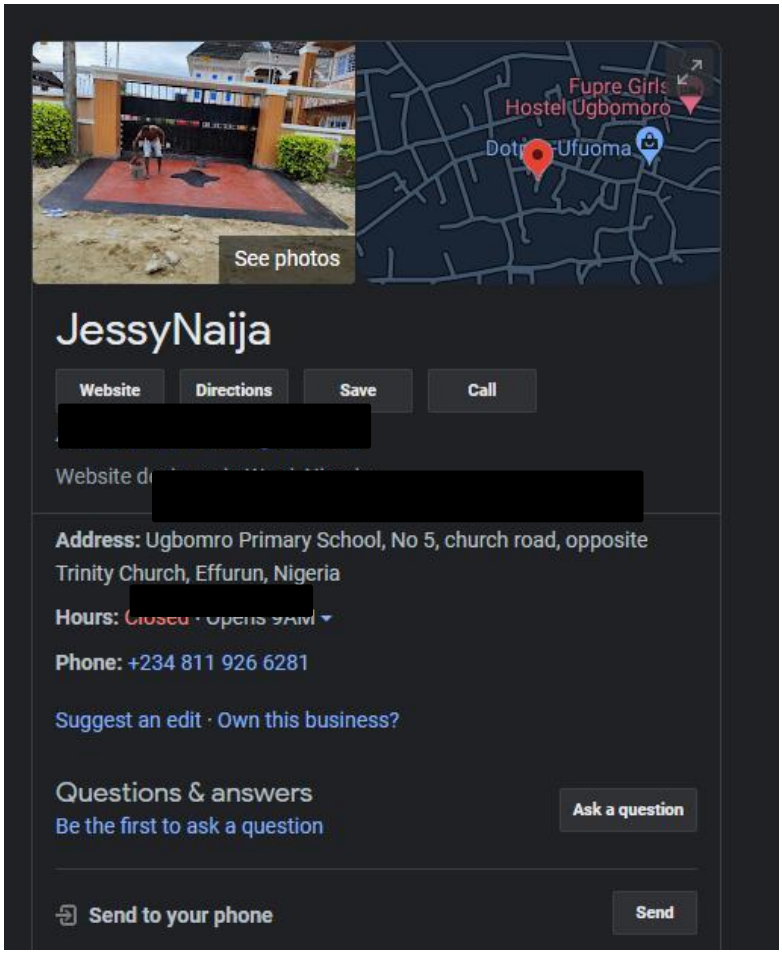


Figure 12: Google search on the location of the originating email.

ISSN: 2473-4901
v10 n6151

APPENDIX K

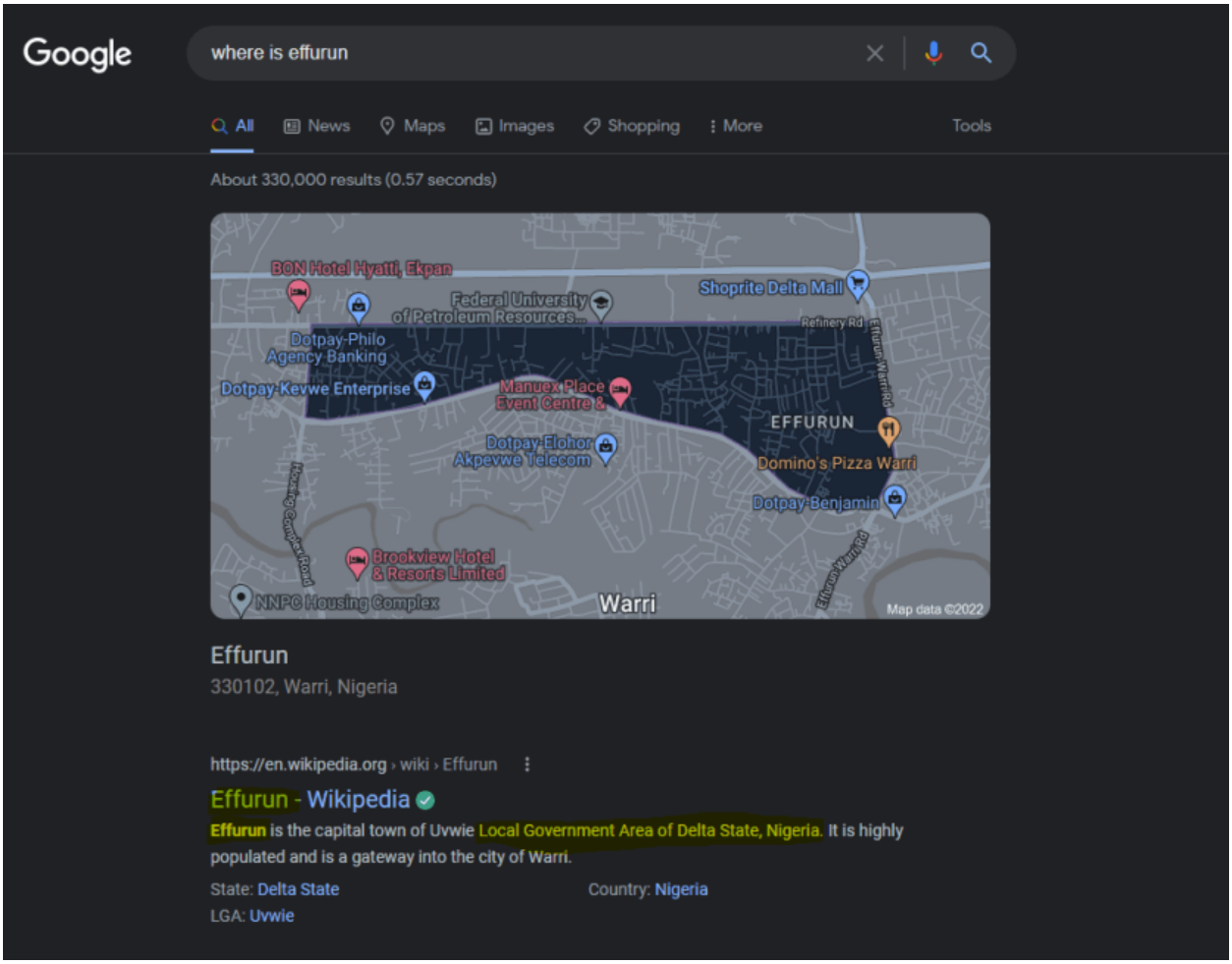


Figure 13: More information on the location of the Registrar Data.

ISSN: 2473-4901
v10 n6151

APPENDIX L

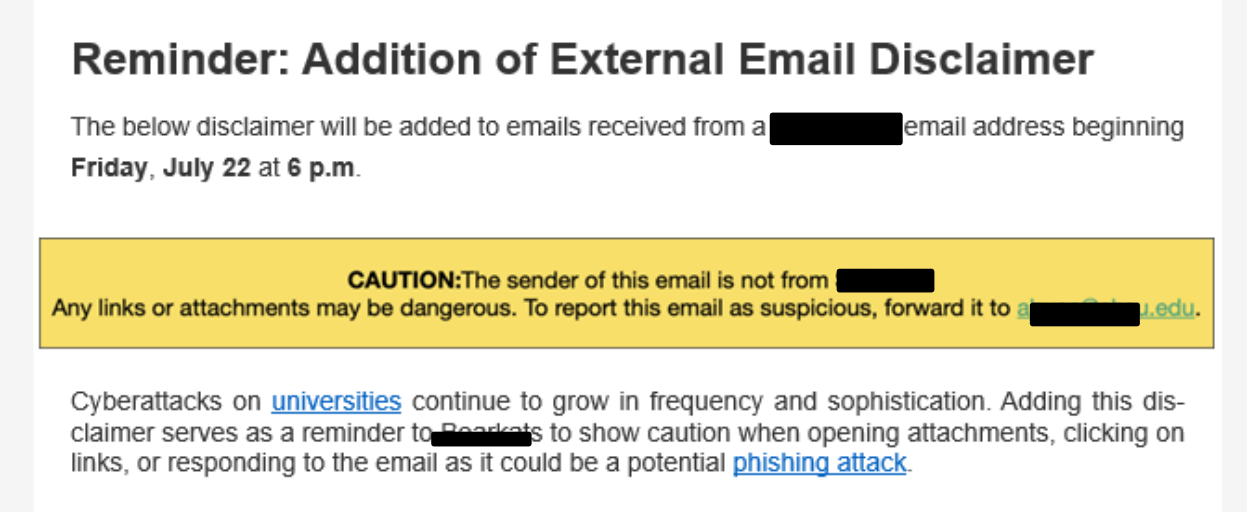


Figure 14: Caution Banner put up by university's IT Team