Designing Against Employment Smishing: Interface Affordances, Cue Use, and Trust Miscalibration

Angela Tran
University of Guelph
Guelph, Ontario, Canada
atran13@uoguelph.ca

Yaa Nuamah Kusi-Fordjour
University of Guelph
Guelph, Ontario, Canada
ykusifor@uoguelph.ca

Haroun Al Tabishi
University of Guelph
Guelph, Ontario, Canada
haltabis@uoguelph.ca

Dylan Gaspar
University of Guelph
Guelph, Ontario, Canada
dgaspar@uoguelph.ca

Hedyeh Nazari
University of Guelph
Guelph, Ontario, Canada
hnazari@uoguelph.ca

Zhao Zhao
University of Guelph
Guelph, Ontario, Canada
zzhao24@uoguelph.ca

Abstract

Employment-related SMS phishing ("smishing") is increasing, yet users must judge message legitimacy through the limited cues provided by messaging interfaces. We conducted a screenshot-based study in which participants evaluated job-related messages across multiple messaging platforms, judged legitimacy, and reported the cues informing their decisions. Across platforms, participants relied on similar heuristic cues regardless of judgment correctness, suggesting challenges in cue interpretation rather than cue availability. We identify a pattern of interface-driven trust miscalibration, where platform-level trust perceptions shape message-level judgments, and implications for messaging and job-search systems.

CCS Concepts

• **Human-centered computing** → **User studies**; *Empirical studies in HCI*; Mobile phones; Smartphones; • **Security and privacy** → *Phishing*; Usability in security and privacy; • **Information systems** → *Texting*.

Keywords

SMS phishing, smishing, user behaviour, mobile security, employment scams, platform trust

ACM Reference Format:
Angela Tran, Yaa Nuamah Kusi-Fordjour, Haroun Al Tabishi, Dylan Gaspar, Hedyeh Nazari, and Zhao Zhao. 2026. Designing Against Employment Smishing: Interface Affordances, Cue Use, and Trust Miscalibration. In *Proceedings of Poster at Graphics Interface 2026 (GI '26).* ACM, New York, NY, USA, 3 pages.

1 Introduction

Employment scams have risen to become one of the riskiest scam categories in 2024 [20] and often exploit hope, opportunity, and trust among individuals actively seeking work on legitimate platforms [19]. Focusing on SMS phishing ("smishing") in employment contexts, we conducted a screenshot-based study in which participants assessed job-related messages presented across iMessage, Android SMS, and WhatsApp.

Our research aims to answer the following research questions:

- **RQ1:** What cues do users rely on when judging the legitimacy of employment-related messages in mobile messaging interfaces?
- **RQ2:** How do users interpret these cues across different messaging platforms?
- **RQ3:** What do users believe platform security features indicate, and where do misconceptions arise?

Our findings reveal three key patterns: participants demonstrated limited discrimination ability, participants relied on similar heuristic cues (e.g., message content, typos, and area codes) regardless of judgment correctness, and participants' judgments were shaped by perceptions of platform trust, often leading to overgeneralization of platform-level properties as indicators of message legitimacy. We synthesize these patterns as *interface-driven trust miscalibration.*

2 Related Work

2.1 Job Phishing

When employers recruit potential employees, they commonly post job listings on platforms such as LinkedIn and Indeed [27], but their legitimacy can also be exploited by attackers who create fraudulent listings to lure victims [15]. Employment scams also disproportionately affect young adults, particularly individuals aged 18–24, such as students and recent graduates [2]. Beyond demographic targeting, employment scams differ from many other phishing scenarios in their psychological framing. Rather than relying primarily on urgency or threat, these scams often leverage opportunity, legitimacy, and trust. This creates conditions in which users may rely on surface-level cues and platform familiarity when evaluating legitimacy, making employment smishing particularly difficult to detect.

2.2 Phishing on Mobile Platforms

Mobile interfaces often lack structural elements such as message headers, provide limited text visibility, and reduce the availability of contextual features that users can draw upon when evaluating legitimacy [3, 4, 14]. These constraints are further compounded by interface design and device limitations. Due to smaller screen sizes and reduced contextual information, users are less likely to scrutinize sender details or fully inspect message content [6, 7, 11–13, 16, 17, 22]. Prior work shows that cues such as message content, sender information, urgency, typographical or grammatical errors,

Poster at Graphics Interface 2026 (GI '26), Waterloo, ON, Canada
2026.

links, and suspicious company names are commonly used to judge legitimacy [9, 10, 13, 23, 24].

Behavioural factors further contribute to users' vulnerability on mobile platforms. Compared to email, text messages are more likely to be read and responded to quickly [4, 21]. The "always-on" nature of mobile devices also increases immediacy, encouraging rapid, low-effort decision-making [1]. These factors create conditions in which users may rely on surface-level cues and make judgments without thorough evaluation.

2.3 User Perception of Different Platforms

Messaging platforms differ not only in technical features but also in how they are perceived by users. Prior work suggests that security features, such as end-to-end encryption, can create a false sense of safety, leading users to trust the messages they receive on these platforms [8]. Trust in messaging platforms is also shaped by familiarity and social context. While reliance on familiarity can support efficient communication, it can also be exploited by attackers through impersonation and social engineering tactics [5].

In addition to social context, platform design differences can influence how risk is communicated to users. For example, Tabassum et al. [23] observed differences in spam detection between Android and iOS messaging systems, with Android providing more visible warning indicators while iOS offered fewer explicit cues. These variations in how warnings and sender information are presented may shape how users interpret message legitimacy.

3 Study Design

Messages were collected from Smishtank [25, 26] and the first author's personal device, with employment-based smishing programmatically filtered from the dataset. We constructed a balanced dataset consisting of four legitimate and four smishing messages, with legitimate messages derived from real job-related communications (e.g., interview invitations, verification codes) and edited for anonymity. Standardized screenshots were created to simulate iMessage, Android SMS, and WhatsApp interfaces while preserving platform-specific visual characteristics. All identifying information was removed or anonymized, and area codes were retained to preserve realism. To examine platform-level effects, warning indicators were systematically varied and randomly assigned across messages, and message order within each platform was randomized.

Participants were recruited via Amazon Mechanical Turk (MTurk) through a two-stage process using unique completion codes to ensure data integrity. A screening survey collected demographic information and measures of technical and cybersecurity experience, adapted from prior work [13, 18]. Participants aged 18–34 were selected for the main task, resulting in 554 qualified participants. In the classification task, participants evaluated message screenshots across three platforms (iMessage, Android SMS, and WhatsApp) over 72 trials (24 per platform), with one attention check embedded in each block. At the end of the task, participants answered an open-ended question indicating which platform they found most trustworthy and explained their reasoning. Measures included: binary legitimacy judgment (where participants classified each message as "Legitimate" or "Scam"), multi-select cue identification (participants selected cues influencing their judgment, such as area code, message content, typos/grammar, warning messages, other), and open-ended rationale (participants provided explanations when selecting "Other" and for the final trusted-platform question). To ensure data quality, we excluded uniform response patterns, irrelevant or low-quality open-ended responses, failed attention checks, and invalid or duplicate completion codes.

4 Results

Participants showed chance-level discrimination between legitimate and fraudulent messages (A'=0.50-0.57), consistently across platforms, indicating a general difficulty in detecting employment-related smishing. Across platforms, they frequently cited message-level heuristics such as message content, typos and grammatical errors, and area code. Open-ended responses highlighted factors including generic or vague phrasing, the presence of a link (fraudulent), and two-factor authentication codes, message tone, and inclusion of specific job-related detail (legitimate), but they did not improve accuracy, suggesting that errors are not primarily driven by the absence of relevant cues, but rather by how those cues are interpreted.

These patterns were consistent across all three platforms, and warning messages had minimal impact on performance, suggesting limited influence from platform-specific affordances. Participants also frequently attributed trust to platform-level security features such as "verified" indicators and end-to-end encryption as signals of authenticity, revealing a trust-calibration gap between perceived and actual security.

Overall, these findings suggest users rely on fragile cues and platform-level beliefs rather than reliable legitimacy indicators. Design implications include: (1) shifting attention toward higher-signal cues and provenance, (2) clarifying what security indicators do *and do not* mean, and (3) supporting cross-channel verification flows.

5 Conclusion

This work examined how people judge the legitimacy of employment-related messages in mobile messaging interfaces and how platform trust shapes those judgments. Participants frequently relied on manipulable, surface-level cues, revealing a trust-calibration gap that may increase vulnerability to increasingly sophisticated employment-related smishing. These findings are limited by the small sample size, controlled screenshot-based design, and reliance on MTurk participants, which may not fully reflect real-world contexts and broader populations. Future work can build on these findings by conducting deeper qualitative investigations and evaluating interface interventions to better support users in assessing message authenticity across communication channels.

References

[1] 2022. https://www.lookout.com/documents/reports/Global-State-of-Mobile-Phishing-Report.pdf

[2] 2023. https://bbbmarketplacetrust.org/wp-content/uploads/2024/02/Targeting-our-youth-full-report.pdf

[3] Eric Blancaflor, Mariah Anne Romero, Irish Nacu, and Denver Ryan Golosinda. 2023. A Case Study on Smishing: An Assessment of Threats against Mobile Devices. In *Proceedings of the 2023 9th International Conference on Computer Technology Applications* (Vienna, Austria) *(ICCTA '23)*. Association for Computing Machinery, New York, NY, USA, 172–178. doi:10.1145/3605423.3605446

[4] Jessica Childres. 2024. Smishing vs. phishing vs. Vishing: Protect yourself from cyber scams. https://www.hp.com/us-en/shop/tech-takes/smishing-vs-phishing-vs-vishing

[5] Kyle Chin. 2025. What is an impersonation attack?: Upguard. https://www.upguard.com/blog/impersonation-attack

[6] Neelam Choudhary and Ankit Kumar Jain. 2018. Comparative Analysis of Mobile Phishing Detection and Prevention Approaches. In *Information and Communication Technology for Intelligent Systems (ICTIS 2017) - Volume 1*, Suresh Chandra Satapathy and Amit Joshi (Eds.). Springer International Publishing, Cham, 349–356.

[7] Matt Dixon, James Nicholson, Dawn Branley-Bell, Pam Briggs, and Lynne Coventry. 2022. Holding Your Hand on the Danger Button: Observing User Phish Detection Strategies Across Mobile and Desktop. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 195 (Sept. 2022), 22 pages. doi:10.1145/3546730

[8] Yaron Dror. 2024. Top WhatsApp scams in 2024 and how to avoid them. https://ironvest.com/blog/whatsapp-scams/

[9] Morgan Edwards, Thomas Morris, Jing Chen, and Jeremiah Still. 2023. SMiShing Attack Vector: Surveying End-User Behavior, Experience, and Knowledge. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 67, 1 (2023), 1911–1915. arXiv:https://doi.org/10.1177/21695067231192193 doi:10.1177/21695067231192193

[10] Morgan E. Edwards and Jeremiah D. Still. 2026. Cyber hygiene of SMiShing: What they know and where they look. *Computer Standards & Interfaces* 95 (2026), 104048. doi:10.1016/j.csi.2025.104048

[11] Cori Faklaris. 2024. Mitigating smishing: Challenges and future work. https://arxiv.org/abs/2401.14520

[12] Diksha Goel and Ankit Kumar Jain. 2018. Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security* 73 (2018), 519–544. doi:10.1016/j.cose.2017.12.006

[13] Eleni Alexandra Katsarakes, Morgan Edwards, and Jeremiah D. Still. 2024. Where do users look when deciding if a text message is safe or malicious? *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 68, 1 (Aug 2024), 221–225. doi:10.1177/10711813241264204

[14] Mingxuan Liu, Yiming Zhang, Baojun Liu, Zhou Li, Haixin Duan, and Donghong Sun. 2021. Detecting and Characterizing SMS Spearphishing Attacks. In *Proceedings of the 37th Annual Computer Security Applications Conference* (Virtual Event, USA) *(ACSAC '21)*. Association for Computing Machinery, New York, NY, USA, 930–943. doi:10.1145/3485832.3488012

[15] Jennifer Maki. 2025. Protect yourself from fake job postings: Your guide. https://www.andersoncollege.com/protect-yourself-from-fake-job-postings-your-guide/

[16] Sandhya Mishra and Devpriya Soni. 2019. SMS Phishing and Mitigation Approaches. In *2019 Twelfth International Conference on Contemporary Computing (IC3)*. 1–5. doi:10.1109/IC3.2019.8844920

[17] Sandhya Mishra and Devpriya Soni. 2023. DSmishSMS-A System to Detect Smishing SMS. *Neural Computing and Applications* 35, 7 (01 Mar 2023), 4975–4992. doi:10.1007/s00521-021-06305-y

[18] Md Lutfor Rahman, Daniel Timko, Hamid Wali, and Ajaya Neupane. 2023. Users Really Do Respond To Smishing. In *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy* (Charlotte, NC, USA) *(CODASPY '23)*. Association for Computing Machinery, New York, NY, USA, 49–60. doi:10.1145/3577923.3583640

[19] Andrew Ramspacher. 2025. Q&A: Why are "recruiters" blowing up my phone with job opportunities? https://news.virginia.edu/content/qa-why-are-recruiters-blowing-my-phone-job-opportunities

[20] Hannah Rudderham. 2025. Employment scams on the rise, experts warn young people at particular risk | CBC news. https://www.cbc.ca/news/canada/new-brunswick/employment-scams-money-1.7553192

[21] Mahdi Shadkam. 2017. Consumer's attitude to receive and response to SMS advertising. *International Journal of Business Information Systems* 24, 1 (2017), 69–90. arXiv:https://www.inderscienceonline.com/doi/pdf/10.1504/IJBIS.2017.080946 doi:10.1504/IJBIS.2017.080946

[22] Ho Sung Shim, Hyoungjun Park, Kyuhan Lee, Jang-Sun Park, and Seonhye Kang. 2024. A persuasion-based prompt learning approach to improve Smishing detection through data augmentation. https://arxiv.org/abs/2411.02403

[23] Sarah Tabassum, Cori Faklaris, and Heather Richter Lipford. 2024. What drives SMiShing susceptibility? a U.S. interview study of how and why mobile phone users judge text messages to be real or fake. In *Proceedings of the Twentieth USENIX Conference on Usable Privacy and Security* (Philadelphia, PA, USA) *(SOUPS '24)*. USENIX Association, USA, Article 21, 19 pages.

[24] Daniel Timko, Daniel Hernandez Castillo, and Muhammad Lutfor Rahman. 2025. Understanding Influences on SMS Phishing Detection: User Behavior, Demographics, and Message Attributes. In *Symposium on Usable Security and Privacy (USEC) 2025* (San Diego, CA, USA) *(USEC '25)*. USA.

[25] Daniel Timko and Muhammad Lutfor Rahman. 2023. Commercial Anti-Smishing Tools and Their Comparative Effectiveness Against Modern Threats. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 1–12.

[26] Daniel Timko and Muhammad Lutfor Rahman. 2024. Smishing Dataset I: Phishing SMS Dataset from Smishtank.com. (2024), 289–294.

[27] Sokratis Vidros, Constantinos Kolias, Georgios Kambourakis, and Leman Akoglu. 2017. Automatic Detection of Online Recruitment Frauds: Characteristics, Methods, and a Public Dataset. *Future Internet* 9, 1 (2017). doi:10.3390/fi9010006