CYBERSECURITY, SOCIAL ENGINEERING ATTACKS

Weaponizing the Birthday: An Experimental Study of Social Media Profiling and Event-Triggered Phishing Susceptibility among Nigerian Social Media Users

Adam Folohunsho Zubair[1*], Micheal Tokunbo Adenibuyan[2], Ezekiel Charles Ochojila[1], Chidera Madu[1], Fawazat Bashir[1], Israel Temitope Opaaje[1]

[1]Department of Computer Science, Faculty of Computing and Information Technology, Lagos State University, Lagos, Nigeria
[2]Department of Computer Science, Bells University of Technology, Ota, Ogun State, Nigeria

Published November 2026

Abstract

Widespread disclosure of personal information on social media has made ordinary life events usable as attack surfaces. This study investigates how one such event, the birthday, can be used to increase susceptibility to personalised phishing among Nigerian social media users, with particular reference to students and staff of the Faculty of Computing and Information Technology at Lagos State University. Adopting a quantitative, experimental design, the research designed, implemented and deployed a controlled birthday-triggered phishing honeypot: a PHP and MariaDB web application that ingests consensually provided participant profiles, automatically generates personalised birthday-reward lures, dispatches them via simulated email and SMS on the eve of each participant's birthday, and records behavioural responses through a decoy reward-wheel landing page. A final valid sample of 190 participants received the simulation via either email (n = 110) or SMS (n = 80). The experiment recorded a high level of susceptibility: 77.9% of participants opened the message, 53.7% clicked the embedded link and 34.2% proceeded to the simulated compromise stage. These figures are far above the sub-10% click-through rates typical of generic phishing. A chi-square test of independence found a statistically significant association between delivery channel and click behaviour ($\chi^2 = 4.34$, df = 1, p = .037), with SMS (62.5% CTR) outperforming email (47.3% CTR). The findings confirm that publicly available birthday data can substantially increase the success of social-engineering attacks, especially over mobile channels, and that human-centric defences in the Nigerian digital environment remain inadequate against personalised attacks. The study recommends data-hygiene practices, greater caution during personal milestones, and the adoption of ethical, personalised phishing simulations in security-awareness programmes.

Keywords: phishing; social engineering; honeypot; social media profiling; birthday-triggered attack; smishing; cybersecurity awareness; Nigeria

1 Introduction

The adoption of social media has changed how people communicate and share personal information. Platforms such as Facebook, Instagram, X (formerly Twitter) and LinkedIn let users disclose names, birthdays, contact details, employment history and social relationships. While these platforms support connectivity and commerce, they also introduce cybersecurity risk because of the volume and sensitivity of user-generated information that is often publicly accessible (Parker and Flowerday, 2020).

Phishing is a common form of cybercrime that exploits human vulnerability rather than technical weakness. It manipulates users into disclosing sensitive information or performing actions that compromise security, usually by impersonating trusted organisations. Although phishing originally relied on email, attackers now use social media to conduct targeted, personalised attacks known as spear phishing (Frauenstein and Flowerday, 2020). Personalised messages that include identifiable user attributes achieve higher success rates than generic attacks because they exploit trust, familiarity and perceived legitimacy (Purkait et al., 2022).

In Nigeria these risks are heightened by rapid growth in internet penetration and social media use, together with uneven digital literacy. Social media serves not only as a communication medium but as a marketplace, identity repository and channel for financial engagement. Phishing remains a significant challenge, and social platforms are increasingly used as vectors for fraud (Adeyemo et al., 2025). The close linkage of phone numbers to digital financial services adds to concerns about identity exposure, since phone numbers act as primary identifiers for banking, mobile payments and account recovery.

One emerging tactic is the exploitation of personal life events such as birthdays, anniversaries and achievements to prompt emotional responses and lower a user's guard. Birthday information is frequently disclosed on social media alongside public posts and congratulatory messages. Event-triggered phishing is particularly effective because it aligns with a user's expectations and emotional state, which raises perceived authenticity (Purkait et al., 2022). Even so, there is limited empirical research on birthday-triggered phishing within a controlled experimental framework, particularly in developing economies such as Nigeria.

Against this background, the study adopts a controlled, ethical experimental approach to evaluate the cybersecurity risks associated with social media profiling and birthday-triggered phishing. By simulating phishing within a honeypot framework and analysing user responses, it provides empirical evidence on how personal data disclosure influences phishing susceptibility.

1.1 Aim and objectives

The aim is to experimentally evaluate the cybersecurity risks associated with social media profiling and birthday-triggered phishing in Nigeria, and to propose effective mitigation strategies. The specific objectives are to: (1) review the literature on social media profiling, phishing and personalised social engineering; (2) design a conceptual and system model for a controlled birthday-triggered phishing honeypot that meets ethical and legal standards; (3) develop and run a controlled experimental prototype that simulates birthday-themed phishing from participant-provided data; (4) deploy the simulation and collect user interaction data; and (5) evaluate the outcomes statistically to determine the influence of profiling and personalisation on susceptibility.

1.2 Research questions

1. What birthday- and identity-related information is commonly disclosed by Nigerian users on social media?
2. To what extent does social media profiling influence susceptibility to phishing in the Nigerian context?
3. How does birthday-triggered personalisation affect the likelihood of engaging with simulated phishing messages?

4. What behavioural and demographic factors significantly influence susceptibility during birthday-themed simulations?
5. How effective is a controlled honeypot-based framework for evaluating personalised phishing risk?

1.3 Scope

The study is limited to an experimental investigation of phishing susceptibility within the context of social media profiling and birthday-triggered personalisation among Nigerian users. It uses only simulated phishing scenarios in a controlled environment; no real financial institutions, banking systems or live phishing attacks are involved. It does not identify individuals, access private social media content, or collect sensitive credentials such as passwords, PINs or one-time passwords, and it focuses instead on user interaction behaviour.

2 Literature Review

2.1 Conceptual review

This review examines the core constructs that underpin the study: social media profiling, personal data disclosure, phishing and social engineering, event-triggered attacks, honeypot systems, and the Nigerian digital environment.

2.1.1 Social media profiling

Social media profiling is the systematic collection, aggregation and analysis of information users disclose online to infer personal characteristics, behaviours and relationships. Advances in analytics and automation have deepened profiling, which lets both legitimate and malicious actors build detailed digital representations of individuals (Kosinski et al., 2015). From a security perspective, profiling enables targeted social engineering: attackers use public data to personalise deceptive messages, and effectiveness increases when multiple data points such as names, affiliations and life events are correlated across platforms (Albladi and Weir, 2020).

2.1.2 Personal data disclosure

Personal data disclosure may be intentional (profile fields) or unintentional (posts, images, comments). Many users underestimate the misuse of information that appears trivial or socially expected, a tendency described as the privacy paradox (Barth and de Jong, 2017). Birthday disclosure is especially significant because it acts as both an identity attribute, used in authentication and account recovery, and a temporal trigger that enables time-specific attacks exploiting positive emotional states.

2.1.3 Phishing and social engineering

Phishing and social engineering rely on psychological manipulation such as trust, authority, urgency and familiarity rather than purely technical exploits (Hadnagy, 2018). Contemporary phishing has shifted from generic, high-volume campaigns toward targeted, spear-phishing approaches that incorporate profiled information, and these consistently outperform generic attacks (Frauenstein and Flowerday, 2020).

2.1.4 Event-triggered and context-aware phishing

Event-triggered and context-aware phishing exploits temporal or situational events such as birthdays, anniversaries, emergencies and deadlines to raise credibility and emotional impact. Birthday-based attacks are effective because they use positive emotions, reward expectations and routine celebratory communication, and because emotionally salient events reduce cognitive vigilance (Parsons et al., 2019; Vishwanath et al., 2020).

2.1.5 Honeypot systems

Honeypot systems are decoy environments designed to attract and observe activity. Originally used to study technical intrusions, honeypots have been adapted for human-centred research, which lets researchers deploy simulated phishing and monitor behavioural responses without exposing participants to real harm (Spitzner, 2003). This captures actual behaviour rather than self-reported susceptibility, provided that ethical safeguards such as informed consent and anonymisation are maintained.

2.1.6 Cybercrime in the Nigerian digital environment

The Nigerian digital environment is characterised by rapid mobile connectivity and deep integration of phone numbers across social media, messaging and banking. This linkage increases exposure to identity-based cybercrime, and variation in digital literacy makes personalised, event-triggered phishing particularly effective (Olayemi, 2023).

2.2 Theoretical review

Because phishing exploits human cognition rather than technical flaws, behavioural and psychological theories provide the interpretive lens for this study. Four theories are particularly relevant.

2.2.1 Social Engineering Theory

Social Engineering Theory explains how attackers exploit cognitive biases, trust and emotion rather than technical weaknesses. Referencing a victim's name or birthday aligns a message with their lived reality and raises its perceived authenticity, which is one reason personalised lures outperform generic ones (Hadnagy, 2018).

2.2.2 Protection Motivation Theory

Protection Motivation Theory holds that protective behaviour depends on threat appraisal, namely perceived severity and vulnerability, and on coping appraisal, namely the perceived ability to respond. A birthday framing lowers threat appraisal by presenting the message as celebratory rather than risky, which weakens the motivation to act defensively (Rogers, 1983).

2.2.3 Theory of Planned Behaviour

The Theory of Planned Behaviour attributes behaviour to intentions shaped by attitudes, subjective norms and perceived behavioural control. Because birthday messages are socially normative and expected, they strengthen the intention to engage and increase compliance (Ajzen, 1991).

2.2.4 Elaboration Likelihood Model

The Elaboration Likelihood Model distinguishes central, rational processing from peripheral, cue-based processing. Emotionally salient birthday cues encourage peripheral processing, so users

respond to surface signals of legitimacy rather than scrutinising the message, which raises susceptibility (Petty and Cacioppo, 1986).

2.2.5 Relevance to the present study

Taken together, these theories explain why personalised, event-triggered attacks outperform generic ones. Social Engineering Theory accounts for the manipulation strategy, Protection Motivation Theory and the Theory of Planned Behaviour for individual differences in risk perception and intention, and the Elaboration Likelihood Model for the shift toward impulsive, cue-driven decisions. They frame the interpretation of the experimental results reported in later sections.

2.3 Empirical review

Empirical work consistently shows that personalised phishing is more successful than generic phishing because personal relevance raises perceived legitimacy (Albladi and Weir, 2020; Frauenstein and Flowerday, 2020). Simulated-phishing studies show that users frequently fail to identify phishing even with basic awareness, as emotional cues and perceived authority override rational assessment (Vishwanath et al., 2020). Research on context-aware personalisation finds tailored messages more persuasive, but most studies examine personalisation broadly rather than isolating specific life events such as birthdays (Purkait et al., 2022). Honeypot methods remain underused for human-centred phishing research, and within African and Nigerian contexts empirical work is sparse and largely descriptive, relying on surveys rather than behavioural simulation (Olayemi, 2023).

2.4 Related systems and research gaps

Existing defences prioritise technical safeguards such as email filtering, malware detection and URL analysis over human-centric solutions, and existing phishing simulations tend to use generic scenarios rather than event-triggered personalisation derived from profiling. A systematic review of related literature (including Kosinski et al., 2015; Acquisti et al., 2015; Albladi and Weir, 2020; Vishwanath et al., 2020; Purkait et al., 2022; Parsons et al., 2019; Olayemi, 2023) confirms three gaps this study addresses: a scarcity of experiment-based research within the Nigerian context; limited isolation of birthday-triggered attacks as a specific variable; and a lack of ethical experimental frameworks for testing these vectors without causing harm.

2.5 Coverage of the phishing attack lifecycle

Table 1 maps the reviewed studies against the five stages of a personalised phishing attack. Prior work clusters around profiling, lure design and the click decision, while the delivery channel and the final compromise stage, together with their combination within a single event-triggered experiment, remain largely unaddressed. That combination is the gap this study fills.

Table 1. Coverage of the phishing attack lifecycle across prior studies.

Study	Profiling	Lure personalisation	Delivery channel	Engagement / click	Compromise
Kosinski et al. (2015)	✓	✗	✗	✗	✗
Acquisti et al. (2015)	✓	✗	✗	✗	✗
Albladi & Weir (2020)	✓	✓	✗	✓	✗
Vishwanath et al. (2020)	✗	✓	✗	✓	✗

Study	Profil-ing	Lure personalisa-tion	Delivery chan-nel	Engagement / click	Comprom-ise
Frauenstein & Flowerday (2020)	✓	✓	✗	✓	✗
Purkait et al. (2022)	✗	✓	✓	✓	✗
Parsons et al. (2019)	✗	✗	✗	✓	✗
Olayemi (2023)	✗	✗	✗	✗	✗
This study	✓	✓	✓	✓	✓

Note. ✓ = stage addressed; ✗ = not addressed.

3 Methodology

3.1 Research design

The study adopts a quantitative, experimental design to evaluate the cybersecurity risks of social media profiling and birthday-triggered phishing. Rather than relying on perception-based surveys, it uses a controlled, ethical experiment to capture actual decision-making when users face personalised threats. Central to the design is a controlled birthday-triggered phishing honeypot, a prototype that generates and delivers simulated phishing based on participant-provided exposure data and serves as a decoy environment that runs social engineering without exposing participants to real financial or reputational harm.

3.2 Population and sampling

The target population comprises students and teaching staff of the Faculty of Computing and Information Technology, Lagos State University, made up of Diploma programme students together with faculty lecturers. This is an active group of Nigerian social-media users for whom these platforms serve as repositories for identity, social interaction and everyday communication. Given the ethical constraints of a controlled cybersecurity experiment, the study uses non-probability, voluntary sampling: participants are recruited on the basis of informed consent, and the data source is restricted to information a real-world attacker could access without compromising platform controls. Private messages, restricted profiles and encrypted communications are excluded. Because the sample is drawn from a single faculty, it is not fully representative of the wider Nigerian population, since digital literacy, socio-economic background and geography vary, but it is well suited to examining the mechanics of birthday-triggered phishing among digitally active members of a university faculty.

3.3 System model and instrumentation

The primary instrument is a custom, high-interaction honeypot built to measure behavioural responses to personalised threats. Its conceptual architecture (Figure 1) comprises a Controlled Input Module that ingests consensually provided data points (first name, birth month and day, and a preferred contact of email address or phone number); a Dynamic Attack Generator that populates social-engineering templates and includes a Temporal Logic component to schedule delivery to coincide with each participant's birthday; a User Interaction Interface that presents the simulated message and a decoy landing page; and a Behavioural Data Capture Module that records a set of susceptibility indicators, namely whether the message was opened, whether the link was clicked, and

whether data submission was attempted. All interaction logs are pseudonymised and stored in a secure, encrypted datastore.

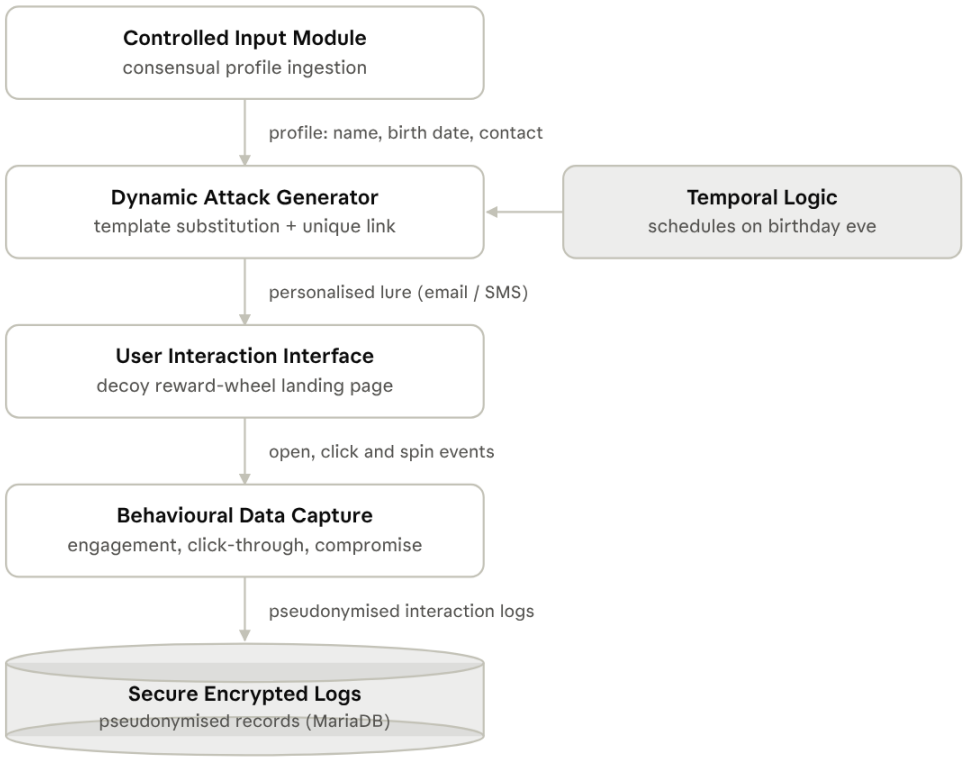

Figure 1. Architecture of the birthday-triggered phishing honeypot.

The prototype was implemented as a server-side web application using PHP 8.2 on an Apache/XAMPP (LAMP) stack, chosen for open-source accessibility and reproducibility within the Nigerian shared-hosting ecosystem. Participant profiles and behavioural logs were stored in a MariaDB/MySQL database accessed through PDO with prepared statements. The Dynamic Attack Generator was realised as a template-substitution engine in which researcher-defined email and SMS templates carry name and link placeholders that are populated at dispatch with each participant's name and a unique, single-use link. The Temporal Logic was implemented as a scheduled task that each day identifies participants whose birthday falls the following day. The decoy interface, an animated reward wheel, captured the behavioural act of engagement rather than live credentials: a token lookup registered the click-through and the spin registered the compromise-equivalent action. To preserve ethical containment, message delivery used a mock dispatch layer that wrote each rendered message, with timestamp, recipient, subject and link, to append-only server-side logs inspected through an administrative dashboard. This reproduced a campaign's full workflow and audit trail without routing traffic through live carrier networks.

The relational schema comprised four normalised tables: a users table holding pseudonymised participant profiles, access tokens and spin outcomes; a gifts table defining the reward inventory and its win-probability weights; a settings table storing the editable message templates; and an admins table for authenticated researcher accounts. Figure 2 shows the schema and the link between a participant's recorded spin outcome and the reward inventory.

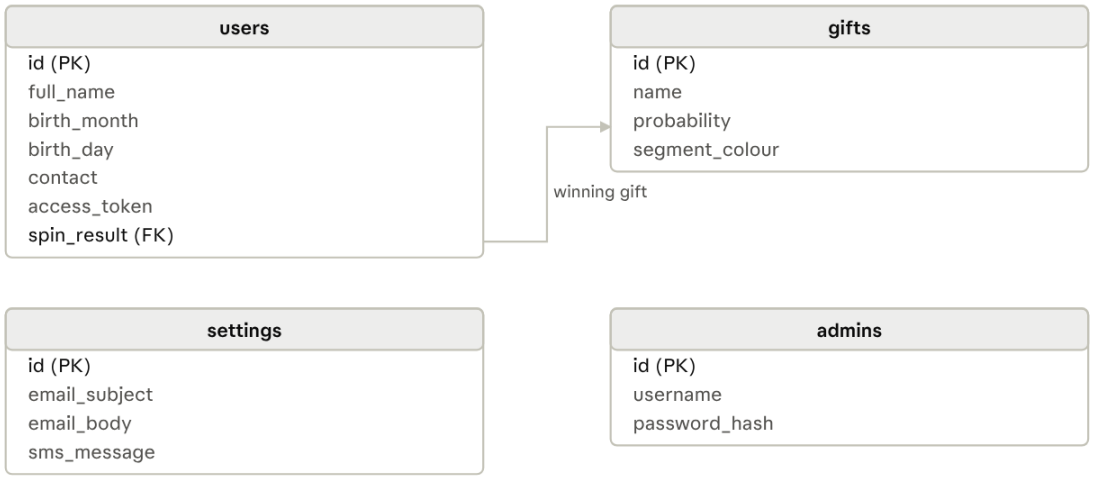

Figure 2. Database schema of the honeypot.

3.4 Data collection procedure

Data collection followed four phases. In Phase 1 (onboarding and base profiling), participants gave informed consent and provided non-sensitive data points, while the specific birthday-trigger methodology was blinded to prevent response bias. In Phase 2 (automated deployment), the generator crafted personalised narratives and the temporal engine scheduled delivery to coincide with the participant's birthday via the designated channel. In Phase 3 (real-time monitoring), the capture module logged three metrics over a defined window: engagement (message opened), click-through (link clicked) and compromise attempt (data submitted on the decoy page). In Phase 4 (debriefing), participants were informed that the message was a simulation, both to ensure no real risk and to provide immediate education on how the lure was constructed from their profile. Figure 3 summarises the four phases.

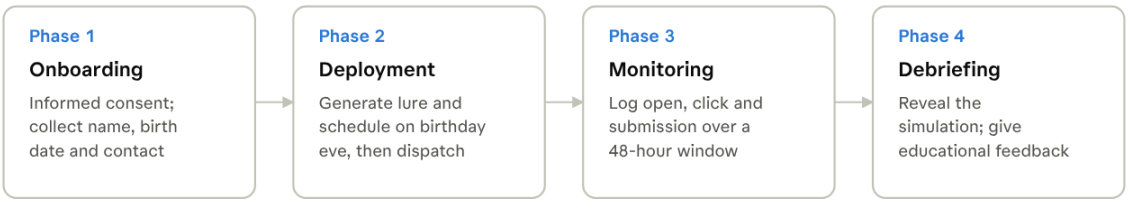

Figure 3. Four-phase data collection procedure.

3.5 Method of data analysis

Descriptive statistics (frequencies and percentages) summarised the three susceptibility metrics and characterised the success funnel. Inferential analysis used a chi-square test of independence to assess the association between communication channel and link-click behaviour, with significance evaluated at $\alpha = .05$.

3.6 Validity, reliability and ethics

Content validity of the simulated messages was established through expert review and comparison with documented real-world templates, and construct validity by measuring actual behaviour (clicks, submissions) rather than reported intention. Reliability was supported by pre-testing the generator and capture modules and by automated, standardised logging that minimised recording error. Ethically, the study used a two-stage consent process (broad consent to a cybersecurity-awareness and digital-behaviour study, with full disclosure at debriefing), contained no malware or real banking systems, impersonated no real institution, and collected no passwords, PINs or one-time passwords. Any data entered on decoy pages was immediately hashed or discarded once the behavioural action was logged, and every participant was debriefed.

4 Results

4.1 System implementation and deployment

The honeypot was deployed as a working web application operated through a single administrative portal. Access was protected by a session-based login (Figure 4). From the dashboard (Figure 5), the researcher managed the participant directory, monitored upcoming birthdays and triggered the automated alert dispatch. The reward wheel was configured through a prize-inventory screen whose win probabilities always summed to 100% (Figure 6). Email and SMS templates, together with the live dispatch logs, were managed from a single communication panel (Figure 7). On the participant side, the personalised link opened a birthday landing page built around an animated reward wheel (Figure 8); completing a spin produced a prize-claim screen that recorded the behavioural equivalent of a compromise (Figure 9).

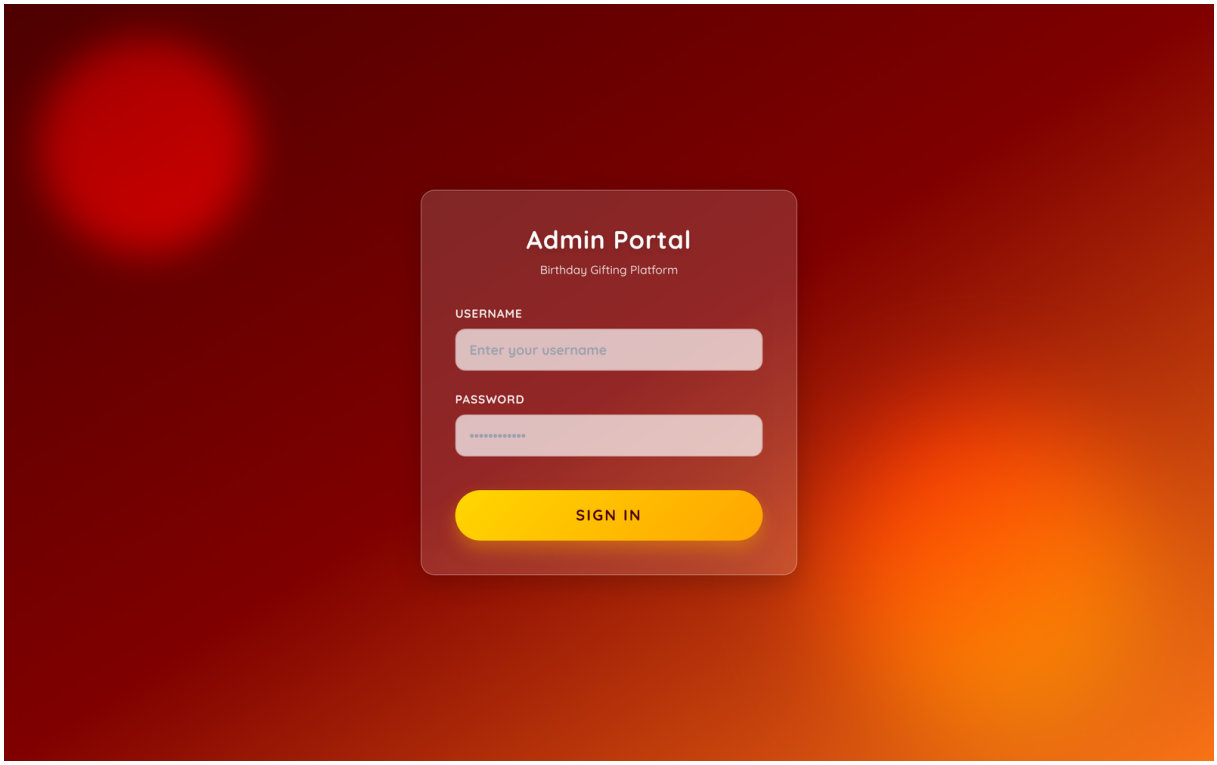

Figure 4. Administrative authentication portal (login).

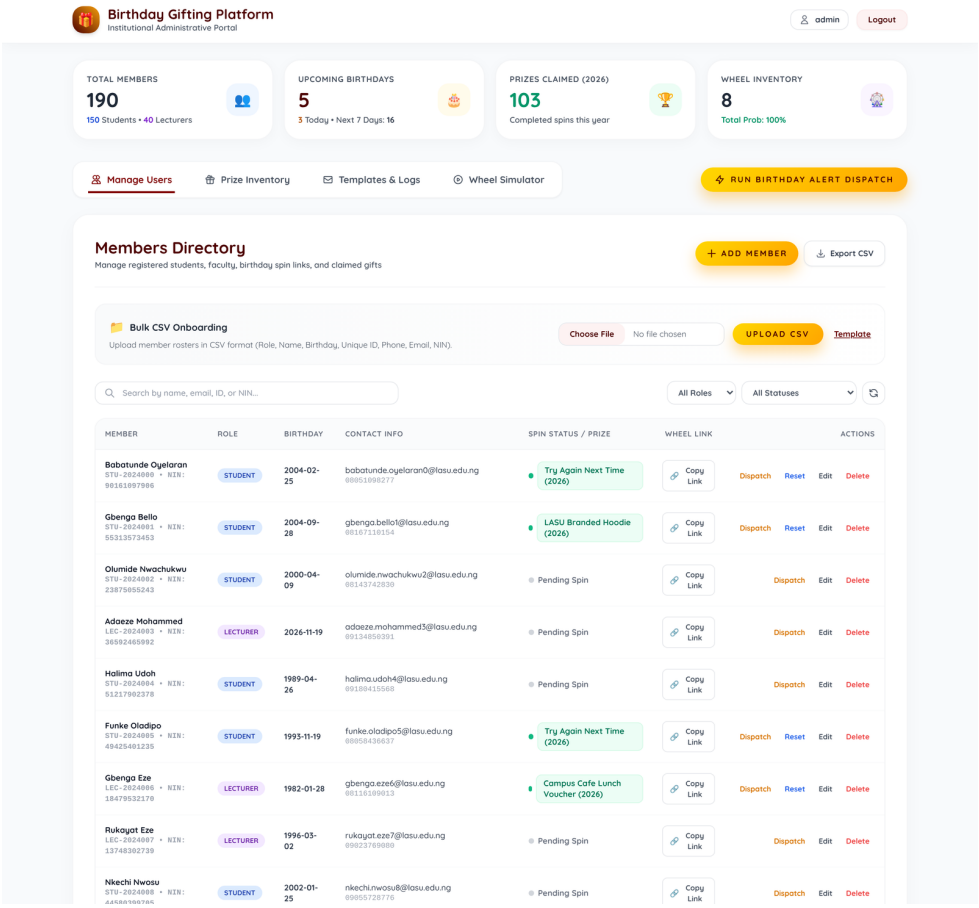

Figure 5. Administrative dashboard: participant directory and study analytics.

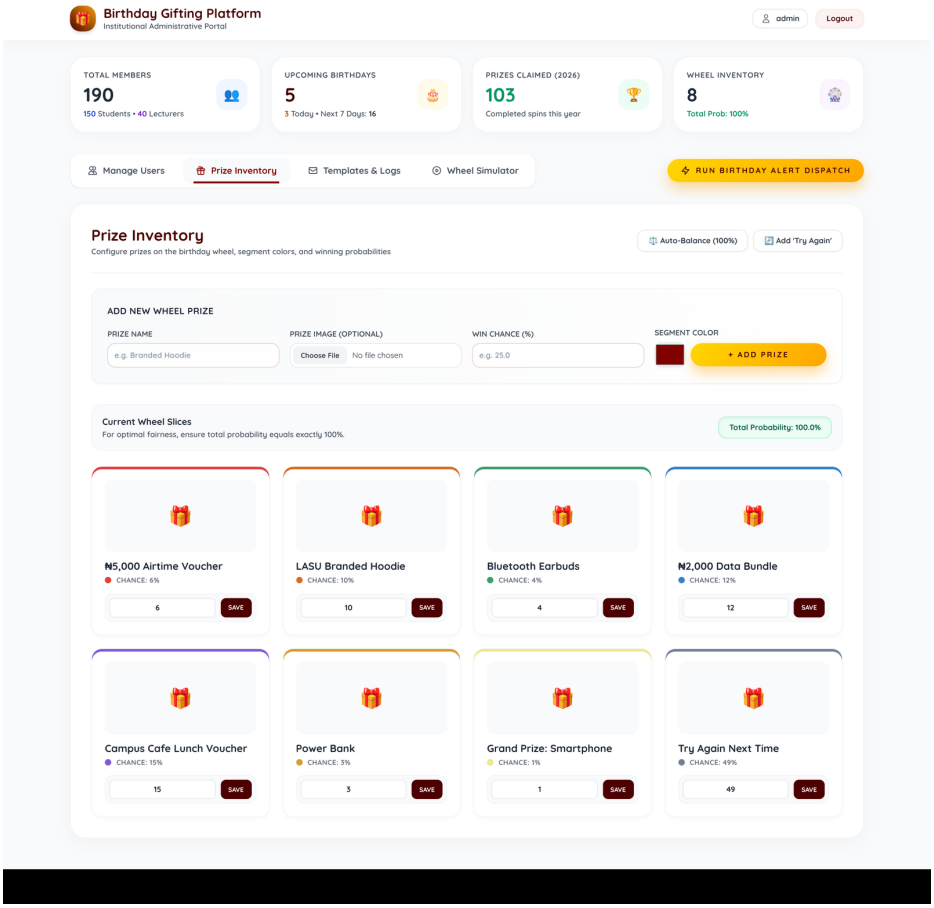

Figure 6. Prize inventory and wheel probability configuration.

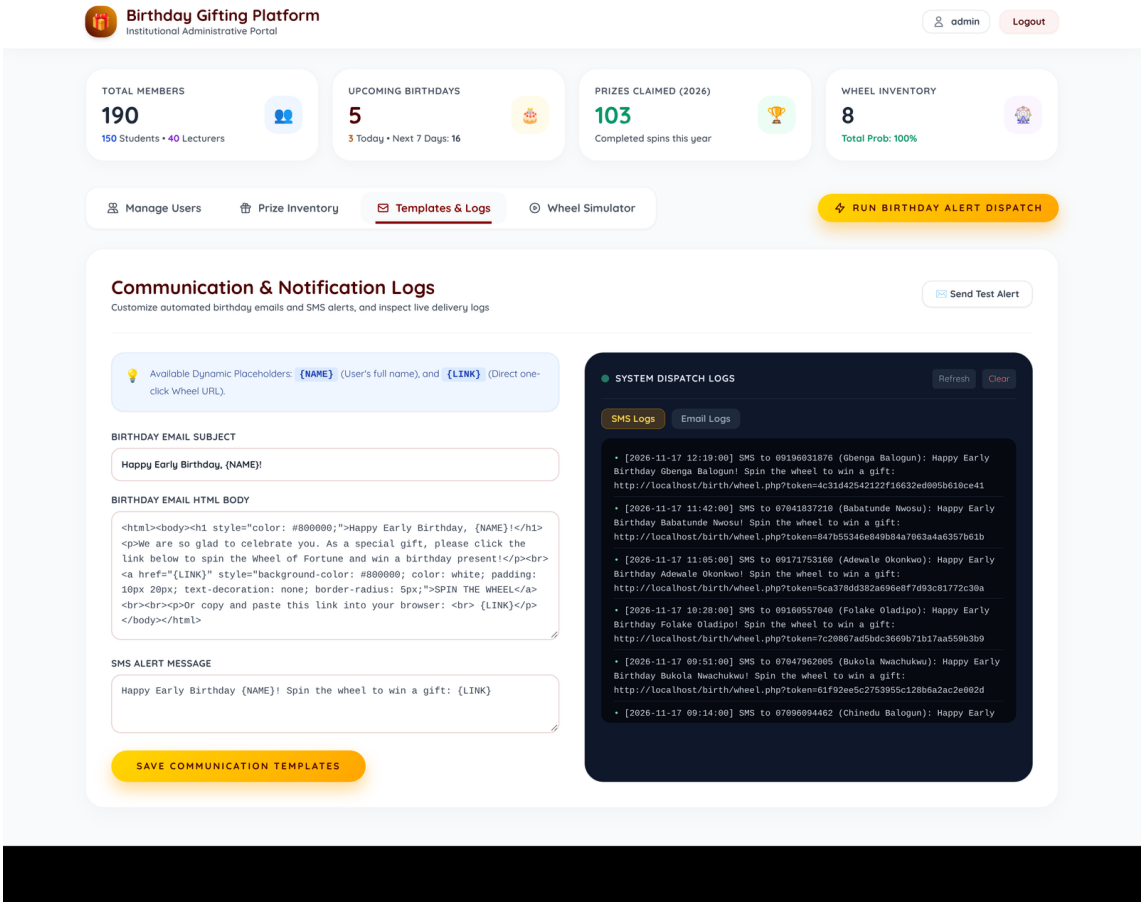

Figure 7. Communication template management and live dispatch logs.

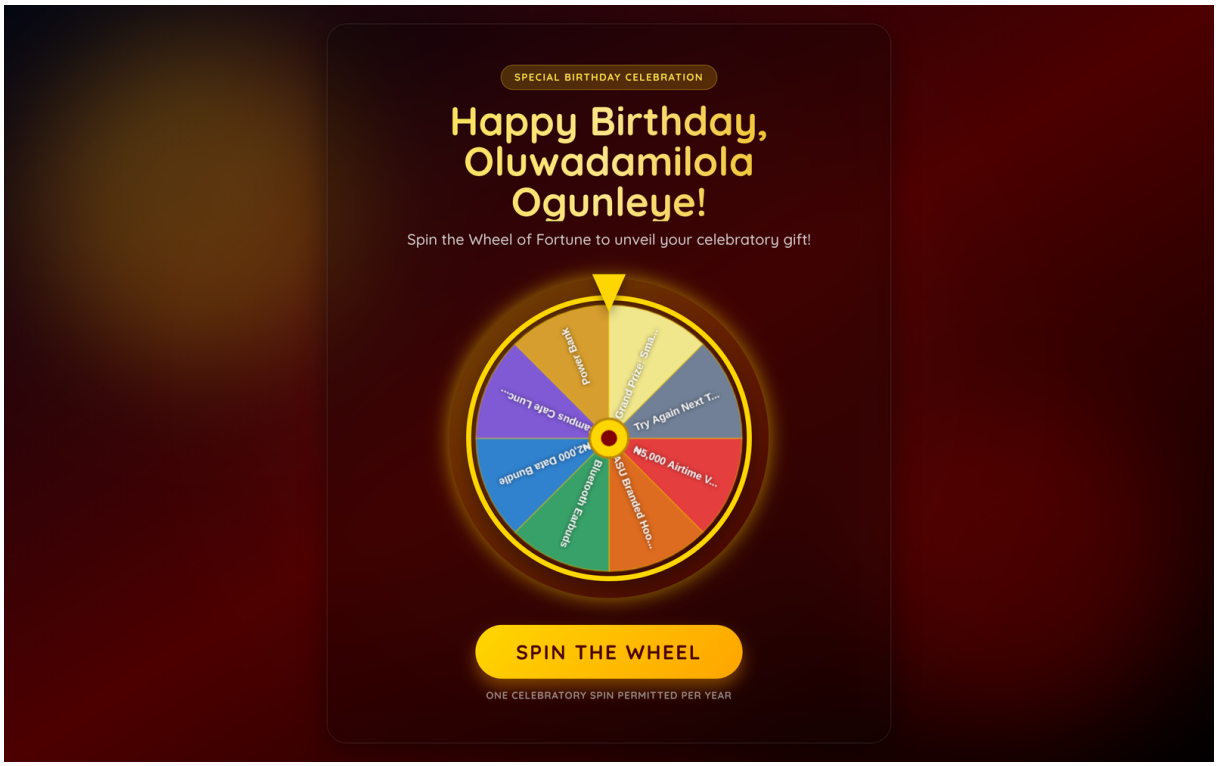

Figure 8. Decoy birthday landing page (the reward wheel).

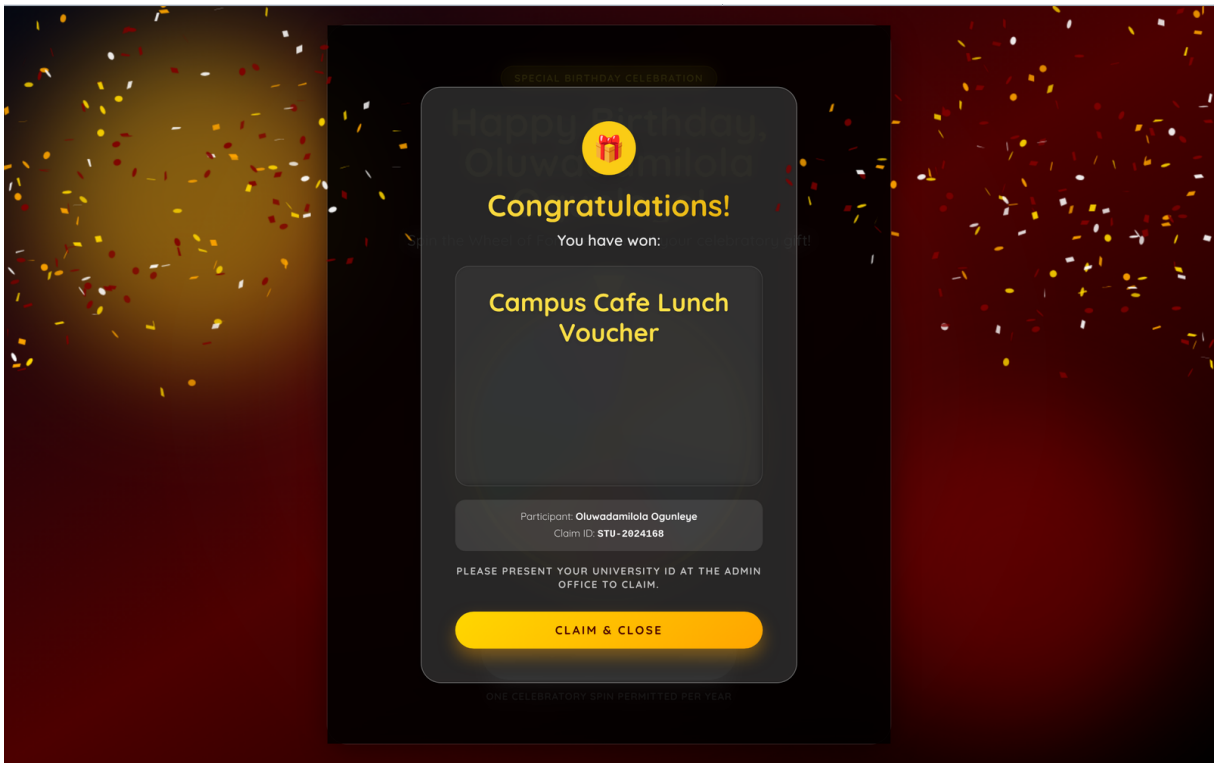

Figure 9. Simulated prize-claim (compromise) capture screen.

4.2 Sample characteristics

During cleaning, 15 records were removed for incomplete profile information that prevented a valid personalised vector, and 10 for verified technical delivery failures (bounced email or undelivered SMS), so that non-behavioural factors did not skew the metrics. The final valid dataset was N = 190 active Nigerian social media users who successfully received the birthday-triggered simulation. For comparative analysis the sample was stratified by channel: 110 participants (57.9%) received the vector via email and 80 (42.1%) via SMS.

4.3 Overall behavioural results

The simulation produced a steep success funnel (Table 2, Figure 10). Of 190 delivered simulations, 77.9% (n = 148) engaged with the message, which indicates that personalised subject lines and sender identities were effective at capturing attention. More than half of the full pool, 53.7% (n = 102), clicked the embedded link, which shows that the birthday-framed narratives were convincing enough to bypass most users' caution. At the highest-risk stage, 34.2% (n = 65) attempted to submit data on the decoy page. Among those who clicked, nearly two-thirds (63.7%) went on to attempt submission. This indicates that once the trigger breaches a user's primary defensive barrier, completion of the fraudulent action is highly likely.

Table 2. Behavioural success funnel (N = 190).

Behavioural stage	Frequency (n)	% of total sample	Conversion from previous stage
Stage 1: Simulation delivered	190	100.0%	n/a
Stage 2: Message engaged (opened)	148	77.9%	77.9%
Stage 3: Link clicked (CTR)	102	53.7%	68.9%

Behavioural stage	Frequency (n)	% of total sample	Conversion from previous stage
Stage 4: Compromise attempted (data submitted)	65	34.2%	63.7%

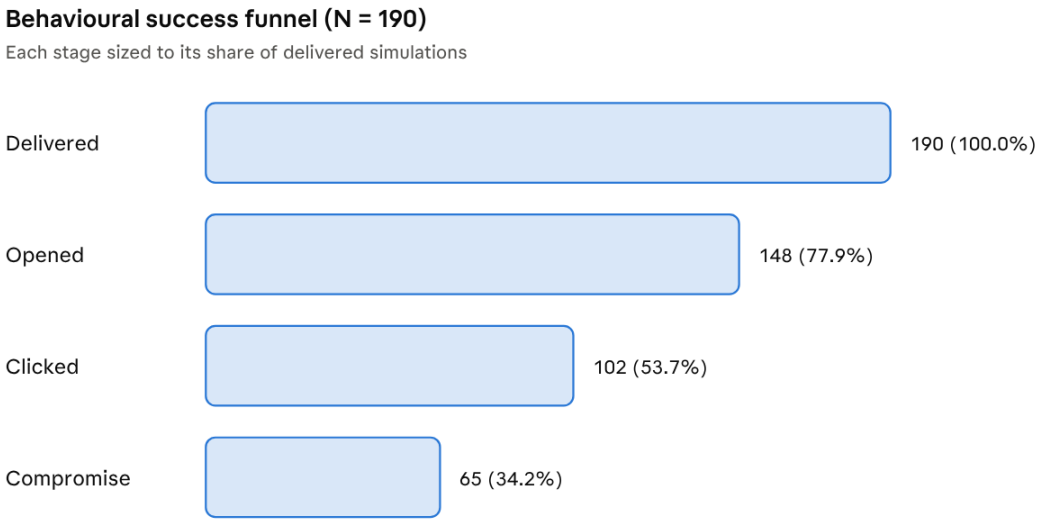

Figure 10. Behavioural success funnel of the simulation.

Figure 11 places these results in context. The click-through rate of 53.7% and the compromise-attempt rate of 34.2% are several times the sub-10% click-through typically reported for generic, untargeted phishing, which shows how much personalisation raises the effectiveness of the attack.

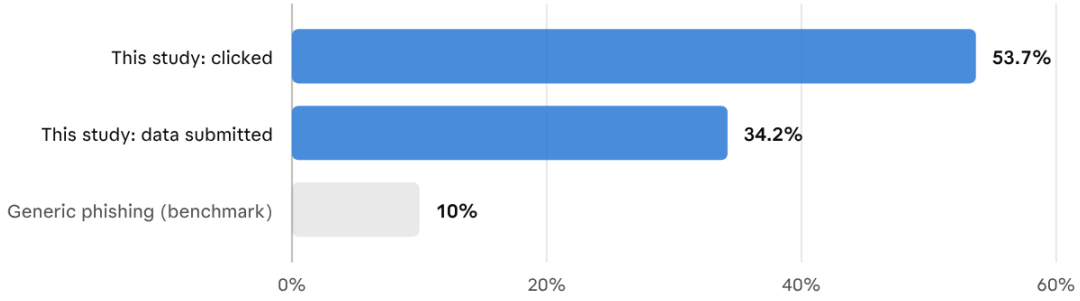

Figure 11. Overall susceptibility compared with the generic-phishing benchmark.

4.4 Susceptibility by communication channel

To test whether the delivery medium influenced susceptibility, a chi-square test of independence compared link-click behaviour across the email (n = 110) and SMS (n = 80) groups (Table 3 and Figure 12). SMS participants clicked at a higher rate (62.5%) than email participants (47.3%). The test was statistically significant, $\chi^2(1) = 4.34$, $p = .037$; because $p < .05$, the null hypothesis that click behaviour is independent of channel is rejected. Mobile-centric SMS delivery therefore produced significantly more impulsive clicking than email in this experimental context, consistent with the view that the immediacy and personal nature of text messaging lowers cognitive vigilance.

Table 3. Communication channel vs. link-click behaviour.

Channel	Did not click	Clicked	Total	Click-through rate
Email	58	52	110	47.3%
SMS	30	50	80	62.5%
Total	**88**	**102**	**190**	**53.7%**

Note. $\chi^2 = 4.34$, df = 1, p = .037.

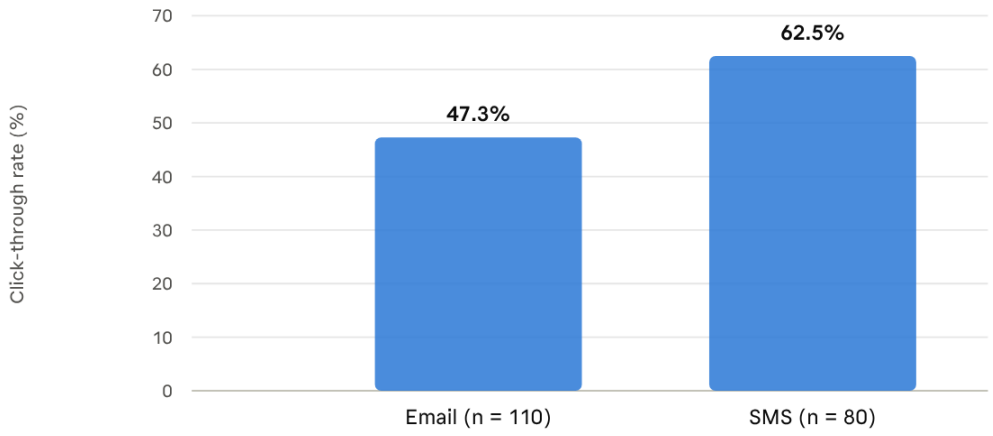

Figure 12. Click-through rate by communication channel.

5 Discussion

5.1 The birthday effect and high overall susceptibility

The most significant finding is the high rate of susceptibility to personalised, event-triggered attacks: an overall click-through rate of 53.7% and a compromise-attempt rate of 34.2%, far above the sub-10% click rates often reported for generic phishing. This supports the premise that publicly available social media data, specifically birthdays, can be used to substantially increase the success of social-engineering attacks. The Elaboration Likelihood Model offers an explanation: a message timed to a birthday acts as a strong peripheral cue, and the positive emotional state and social expectation of well-wishes reduce cognitive vigilance. Rather than evaluating the sender's legitimacy or the URL through the central route, users default to the peripheral route and make an impulsive decision on the emotional hook, while personalisation creates an impression of familiarity that bypasses standard suspicion filters.

5.2 The success funnel: from click to compromise

A key insight is the high conversion between stages: of those who clicked, nearly two-thirds (63.7%) went on to attempt data submission. The primary defensive barrier is therefore the initial decision to click; once the trigger persuades the user to take that first action, subsequent resistance drops sharply. Protection Motivation Theory accounts for this: on a benign-looking reward page, threat appraisal stays low while coping appraisal (the ease of entering a few details) stays high, and the discomfort of backing out after clicking is too great for many users. Security-awareness training

should therefore focus on the pre-click moment of hesitation, since recovery after the click is statistically unlikely in a highly personalised scenario.

5.3 Channel effect: SMS versus email

The significant association between channel and susceptibility ($\chi^2 = 4.34$, $p = .037$), with SMS clicking (62.5%) exceeding email (47.3%), has clear implications for the mobile-centric Nigerian landscape. Several factors likely contribute. Mobile devices are used in distracted, always-on contexts that prompt quicker, less considered reactions. The SMS interface is less informative than an email client, and it often obscures full URLs and lacks robust sender-verification cues. SMS is also perceived as a more personal, immediate and urgent channel, which compresses decision time and increases impulsive clicks. These factors make smishing a significant vector in Nigeria.

6 Conclusion and Recommendations

6.1 Conclusion

Through the design and deployment of a controlled, birthday-triggered phishing honeypot, this study quantified a threat that prior Nigerian research had largely left to survey and anecdote. The findings support a clear conclusion: the public availability of personal identifiers, particularly the combination of name, birthday and phone number, is a critical cybersecurity vulnerability for Nigerian digital users. Attackers need no sophisticated technical exploit, only enough contextual data to craft a believable narrative. By using a universal human milestone, the simulated attacks exploited cognitive biases and left a large share of the sample vulnerable to compromise. Current human-centric defences are insufficient against highly personalised social engineering, especially on mobile platforms, and technical controls alone cannot compensate when users unwittingly supply the context that bypasses their own judgement.

6.2 Recommendations

At the level of individual behaviour, the most effective response is to reduce the personal data available to attackers. Hiding the birth year, and ideally the birth day and month, on platforms such as Facebook and LinkedIn removes the specific attribute this study found to be exploitable. Users should also treat moments of personal significance as periods of heightened risk, since an unexpected gift or reward message that arrives around a birthday and asks for a click is a common lure. Verifying any such message through a separate channel before acting is a simple and reliable safeguard. Because SMS produced higher susceptibility than email in this experiment, text messages deserve at least the same suspicion as email, and shortened links from unverified senders should not be opened.

Institutions and employers, for their part, can no longer rely on generic phishing tests, which rarely reflect the personalised attacks that users actually encounter. Security-awareness programmes should incorporate ethical, personalised simulations of the kind used in this study, and training should address smishing directly, including the way mobile interfaces conceal the cues people rely on to judge a message. Organisations would also benefit from auditing the public social-media footprints of high-value staff, since the aggregate exposure of a workforce is often considerably larger than any individual member appreciates.

6.3 Limitations

The study relies on a simulated environment, which may not fully capture the scale and adaptive strategies of real attacks. Profiling was limited to publicly available, voluntarily provided data. The voluntary sample, drawn from a single university faculty, is not fully representative of the wider Nigerian population, and the design isolates birthday-themed triggers rather than the full range of event-based lures such as emergencies, promotions and regulatory alerts.

6.4 Suggestions for further research

Future work could test other profile-based triggers such as job changes, travel and hobbies; conduct longitudinal studies measuring whether just-in-time debriefing improves resistance in later tests; and examine correlations between susceptibility and demographic factors such as age, digital literacy and professional background within the Nigerian context.

References

[1] Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514.

[2] Adeyemo, O., Babalola, O., & Ojo, T. (2025). Cybersecurity threats in Nigeria: Evaluating phishing trends and user vulnerabilities. *African Journal of Information Systems*, 17(1), 45-62.

[3] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

[4] Albladi, S. M., & Weir, G. R. (2020). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, 10(1), 1-24.

[5] Barth, S., & de Jong, M. D. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior. *A systematic literature review*. Telematics and Informatics, 34(7), 1038-1058.

[6] Frauenstein, E. D., & Flowerday, S. V. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security*, 94, 101862.

[7] Hadnagy, C. (2018). Social engineering: The science of human hacking (2nd ed.). *John Wiley & Sons*.

[8] Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. *Keele University and Lincoln University Technical Report*.

[9] Kosinski, M., Matz, S. C., Gosling, S. D., Popov, V., & Stillwell, D. (2015). Facebook as a research tool for the social sciences: Opportunities, challenges, best practices, and new directions. *American Psychologist*, 70(6), 543-556.

[10] Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & The PRISMA Group. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Medicine*, 6(7), e1000097.

[11] Olayemi, O. J. (2023). Cybercrime in Nigeria: Trends, challenges and the way forward. *International Journal of Cyber Criminology*, 17(2), 112-128.

[12] Parker, F., & Flowerday, S. (2020). Information security and social media: A systematic literature review. *Journal of Information Security and Applications*, 54, 102544.

[13] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2019). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165-176.

[14] Petticrew, M., & Roberts, H. (2006). Systematic reviews in the social sciences: A practical guide. *Blackwell Publishing*.

[15] Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. *Advances in Experimental Social Psychology*, 19, 123-205.

[16] Purkait, S., Dehghantanha, A., & Smith, S. (2022). A systematic review of context-aware phishing attacks. *Journal of Information Security and Applications*, 66, 103135.

[17] Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *J. Cacioppo & R*. Petty (Eds.), Social psychophysiology: A sourcebook (pp. 153-176). Guilford Press.

[18] Spitzner, L. (2003). Honeypots: Tracking hackers. *Addison-Wesley Professional*.

[19] Vishwanath, A., Harrison, B., & Ng, Y. J. (2020). Suspicion, cognition, and automaticity: A model of phishing susceptibility. *Communication Research*, 47(8), 1146-1166.

[20] Yoro, D. I., Musa, A., & Ibrahim, K. (2023). Demographic characteristics and social engineering susceptibility among social media users in Nigeria. *Journal of Cybersecurity and Privacy*, 3(4), 812-825.