STUDIA UNIV. BABEŞ–BOLYAI, INFORMATICA, Volume **LXXI**, Number 1-2, 2026
DOI: 10.24193/subbi.2026.02

THE RISK OF POLITICAL QUISHING

ALEXIA MARIA GOIA AND IMRE ZSIGMOND

Abstract. This study examines the risk of QR code phishing — which we will be referring to as quishing from this point forward — in the context of political elections in Romania. Through a field experiment, we deployed posters featuring both political and social content, each framed in either a neutral or clickbait style, to evaluate how different social engineering techniques influence interaction outcomes. Our results indicate that politically framed clickbait posters generated substantially higher scan rates, while conversion patterns varied across conditions. These findings highlight the viability of QR codes as a powerful attack vector in politically charged environments, and the need for awareness campaigns, as subjects were not only interested in scanning them, but also in submitting their email addresses.

1. Introduction

In today's world, information is one of the most valuable resources we possess. It is essential not only for our societal development, but also as a potent weapon with immense harm capabilities. With vast access to information, malicious actors can influence public opinion or deceive users into disclosing sensitive data [1]. One of the most prevalent methods through which such manipulation occurs is social engineering, a form of psychological manipulation that exploits trust, curiosity, or emotion to elicit unintended actions.

The rapid growth of online media consumption has further increased society's exposure to manipulative information. An increasing number of people

Received by the editors: 13 November 2025.

2010 *Mathematics Subject Classification.* 68M99.

1998 *CR Categories and Descriptors.* D.4.6 [**Operating Systems**]: Subtopic – *Information flow controls*; K.4.1 [**Public Policy Issues**]: Subtopic – *Abuse and crime involving computers*.

Key words and phrases. quishing, clickbait, social engineering.

© Studia UBB Informatica. Published by Babeş-Bolyai University

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Licence.

are choosing to rely on social media to stay informed during election campaigns and other major events, with over 62% of adults getting their news online [2], where content is often optimized for engagement rather than accuracy or safety. This environment has proven ideal for the proliferation of clickbait, which is represented by emotionally charged or deceptive headlines designed to attract attention and provoke interaction.

At the same time, phishing remains one of the most persistent cyber-security threats worldwide. Traditionally associated with fraudulent emails or fake websites, phishing has been diversified through the use of new delivery mechanisms, with quishing rapidly gaining popularity since the pandemic [3]. These matrices offer convenience but conceal risk: in some QR scanning applications, such as Google Lens, their encoded destinations are shortened for the user prior to scanning. In addition, attackers can use URL shorteners to make links seem more trustworthy [4]. This, combined with the fact that in a previous study, users were questioned whether they were aware of the fact that malicious QR codes exist, and 67.5% of the subjects were unaware of the fact [5], makes them ideal tools for attackers.

In Romania, these digital and psychological vulnerabilities intersect with a complex political landscape. The country's presidential elections have been marked by sharp divisions and widespread online misinformation [6]. Political actors and supporters frequently employ emotionally manipulative or outrage-driven messages to mobilize voters, especially in the context of lackluster platform moderation [7]. This environment provides fertile ground for exploring how political and emotional framing affect individuals' willingness to engage with unfamiliar digital content, particularly when mediated through an already established, growingly popular and easily distributable medium such as a QR code [8].

The present study investigates whether users exposed to politically framed clickbait are more likely to engage with potentially risky content compared to those exposed to neutral or non-political material. Specifically, it examines how the combination of political context and emotional tone influences the rate at which individuals scan QR codes and proceed to submit personal information — in our case, email addresses. To test this, a field experiment was conducted in Cluj-Napoca during the 2025 Romanian presidential elections campaign, involving the public display of posters containing both political and social messages in either clickbait or neutral form.

By conducting the experiment in a real electoral context, the study aims to bridge the gap between theory and practice when it comes to the hypothetical potential of social engineering in the context of politics. The findings provide insights into how certain cues influence users' decisions and how easily one

can be deceived based on the appearing trustworthiness and contents of a QR code poster. Furthermore, the results contribute to understanding people's susceptibility to manipulation and emphasize the need for increased public awareness and education on more uncommon cyber-security threat topics, such as quishing.

2. Previous work

Earlier work on quishing, clickbait and political persuasion has investigated these elements individually, but little to no research has studied them in tandem. This section reviews the main contributions from related domains, outlining how the current paper builds upon and extends existing literature.

2.1. **QR codes and public interaction.** The usage of QR codes in public environments has been extensively studied since their introduction as marketing and informational tools. Relevant to our experiment is a previous study on the effectiveness of QR codes in political marketing, where it was remarked that most respondents were using at least a form of social media to stay informed on politics, and 44.9% of respondents are likely to scan QR codes to keep up with political campaigns [9].

Early experiments regarding the usage of this medium in phishing demonstrated that curiosity and convenience are the primary motivations for scanning QR codes, rather than a conscious evaluation of safety. Vidas et al. conducted one of the first large-scale field studies on QR code interaction, deploying 139 posters across public spaces and observing 225 scans over four weeks [4]. Their findings revealed that the vast majority of users did not inspect URLs or verify authenticity before visiting the linked websites, confirming a strong element of blind trust in the medium and the previously proven inability of distinguishing between legitimate and fraudulent domains. Recent studies also show that not only users' perception of phishing threat directly drives protective behaviors [10], but also that people who believe to be good at detecting phishing are more susceptible to it [11].

2.2. **Clickbait and persuasion principles.** Persuasion has long been recognized as a fundamental component of social engineering attacks. Ferreira et al. identified six key principles — authority, reciprocity, commitment, scarcity, liking, and social proof — that are frequently used in phishing messages to manipulate user perception and decision-making [1]. These principles, originally articulated by Cialdini [12], have since been applied in diverse contexts such as other types of phishing and malicious advertising.

Design cues and emotional manipulation also play an essential role in user engagement. A recent study compared two types of QR code posters: one plain, and one visually enhanced with color, branding, and reward messaging. They found that the persuasive design significantly increased interaction rates [13]. Similarly, studies in campus environments demonstrated that posters containing institutional cues such as university logos or formal typography produced higher engagement than anonymous designs [14]. These findings illustrate that visual trust markers and emotional appeal strongly influence whether a user perceives a QR code as credible and worth scanning.

In parallel to research on QR interaction, a growing body of literature examines clickbait and its psychological mechanisms. Clickbait headlines exploit users' cognitive biases by invoking curiosity, surprise, or outrage. Blom and Hansen distinguish between curiosity-based clickbait, which withholds key information to prompt engagement, and ragebait, which provokes strong negative emotion to elicit sharing or reacting [15]. Studies consistently show that emotionally charged messages—especially those involving political or moral outrage—generate higher engagement metrics than neutral, informational content [16].

From a behavioral security perspective, this effect is directly relevant to social engineering. Users displaying strong emotional responses are less likely to engage in critical thought, making them more vulnerable to phishing or misinformation.

2.3. **Political disinformation and Romanian context.** Disinformation campaigns during election periods prove opportune for studying susceptibility to manipulative content. Previous analyses of Romanian elections have documented extensive use of emotionally driven and divisive narratives, often spread through social media platforms and online influencers [6]. During the 2024 Romanian presidential elections, allegations of electoral fraud and polarized rhetoric between major candidates created an atmosphere of distrust and emotional volatility. Reports indicated that politically charged content—particularly when framed in simple, provocative language—achieved far greater reach than factual or neutral communication [17].

In such contexts, individuals' trust in familiar symbols, such as party logos or slogans, can be easily exploited. The emotional charge surrounding political identity reduces skepticism, mirroring the same mechanisms that make users susceptible to online phishing. This environment therefore provides an ideal setting for examining how political framing interacts with social engineering cues to influence user behavior.

Despite the abundance of literature on phishing, QR code interactions, and clickbait, no prior study has empirically combined these factors within a real-world electoral context, and there has been no quishing study conducted in Romania. The present research addresses these gaps by testing how emotional and political framing affect user engagement with QR codes in the public spaces of Cluj-Napoca. By merging insights from persuasion theory, design psychology, and field-based cyber-security research, this study contributes new evidence on how social engineering strategies manifest beyond digital-only environments and into the outside world.

3. Methodology and Implementation

3.1. **Poster Design and Persuasive Principles.** We conducted a QR-based phishing experiment to evaluate the effect of poster content and tone on email capture. When choosing the types of posters, we have considered two dimensions regarding content and framing, resulting in four types of posters:

- **Political-Clickbait**: Inflammatory headlines, candidate-specific posters. We created two posters of this kind to also factor in whether a certain candidate attracts more scans.
- **Political-Neutral**: Informative campaign-style poster, depicting both candidates and their opinions.
- **Social-Clickbait**: Invitation to take part in a giveaway.
- **Social-Neutral**: Typical social awareness campaign poster.

The experiment was conducted during an active election period, making political content highly relevant and engaging for participants. Social-themed posters were included as a comparison to observe baseline engagement with less trending content that would normally be observed in urban areas. The tones were chosen based on psychological principles of curiosity, which suggest that individuals are more likely to engage with stimuli that are surprising, provocative, or emotionally charged [18]. Accordingly, clickbait phrased with a negative tone was expected to evoke greater curiosity than neutral wording.

As seen in Figure 1, each variant consisted of a visually prominent QR code, notable visual cues, and a short call-to-action. For political posters, the layouts were intentionally modeled after existing political campaign posters of the two presidential candidates commonly found in public spaces, including the voted sigil of a voting stamp. All three variants of the political posters featured stock images of individuals with intentionally blurred faces, designed to evoke the impression that they represented the recognizable political figures. To be in accordance with laws regarding political materials, no direct mention of any party or candidate has been made. Trust cues such as small logos

or authoritative phrasing were selectively added to those designs, following studies showing that contextual legitimacy increases scanning rates [13].

The clickbait variants used inflammatory, sensational language, similar to news headlines of the 2010s and online articles, that can pique a person's interest by withholding key information [16]. For the neutral-clickbait variant, we chose a giveaway poster as the attractiveness of giveaways lies in their promise of free rewards combined with the chance-based prospect of winning. In contrast, neutral posters were modeled after conventional public notices, using standard language that invites people to become informed, similar to social awareness materials.

FIGURE 1. Poster designs ordered by tone: political (first row), social (second row)

3.2. **Deployment Procedure.** Seven high-traffic urban locations were chosen for poster placement, near points of interest such as university campuses and high-mobility areas. The posters were attached to various surfaces, such

as street poles and walls where other public announcements, advertisements or media was frequently installed.

Each location was revisited daily to document the condition of the 35 posters and replace any that had been torn or damaged. Due to the politically charged timing of the experiment, some posters were frequently vandalized or removed. Weather conditions also affected visibility and QR code quality during the week of deployment, with rain occasionally damaging exposed posters. These incidents were logged and are addressed as limitations in Section 3.7.

3.3. **Website and Backend Implementation.** Each QR code directed users to a custom-built website that simulated a phishing scenario. The landing page was created using React for the frontend and was connected to an Express.js server. Each link could be uniquely identified by three obfuscated URL parameters encoding the poster type, content and location, thus allowing us to distinguish between experimental conditions while ensuring no unnecessary information was distributed to the users.

Upon scanning, users are presented with a short themed message consistent with the poster type they encountered and are prompted to enter an email address to obtain more information regarding the topic presented in the scannable poster. When the website was loaded, we stored the scan event, along with the timestamp, poster information, location and a randomly generated visitor UUID. Once the user submitted their email address, it was validated by the server, hashed using SHA-256, and this hash, the timestamp and validation response were stored in a database hosted on the cloud.

Immediately after submission, participants are redirected to a debriefing page explaining the study's purpose, providing cyber-security education, and confirming that no personal data was retained, as seen in Figure 2.

3.4. **Data Cleaning and Validation.** After the deployment period, the data was exported to a local machine and manually cleaned up. We retained initial scans, email address inputs, and invalid inputs in three different tables. The invalid inputs table automatically filtered certain entries that had incorrect URL parameters, that we assume to be a result of curious third-parties studying the access links.

To clean up the first table, we started by addressing duplicates created due to a bug in the logic of the UUID generation. A single device accessing the site could generate multiple entries in the scans table, corresponding to different UUIDs. Such duplicate entries were identified through matching timestamps and locations, then collapsed into single records. If one of the duplicate entries had a corresponding record in the mail input table, the associated UUID was retained. For the second stage of the cleanup, we excluded email address inputs

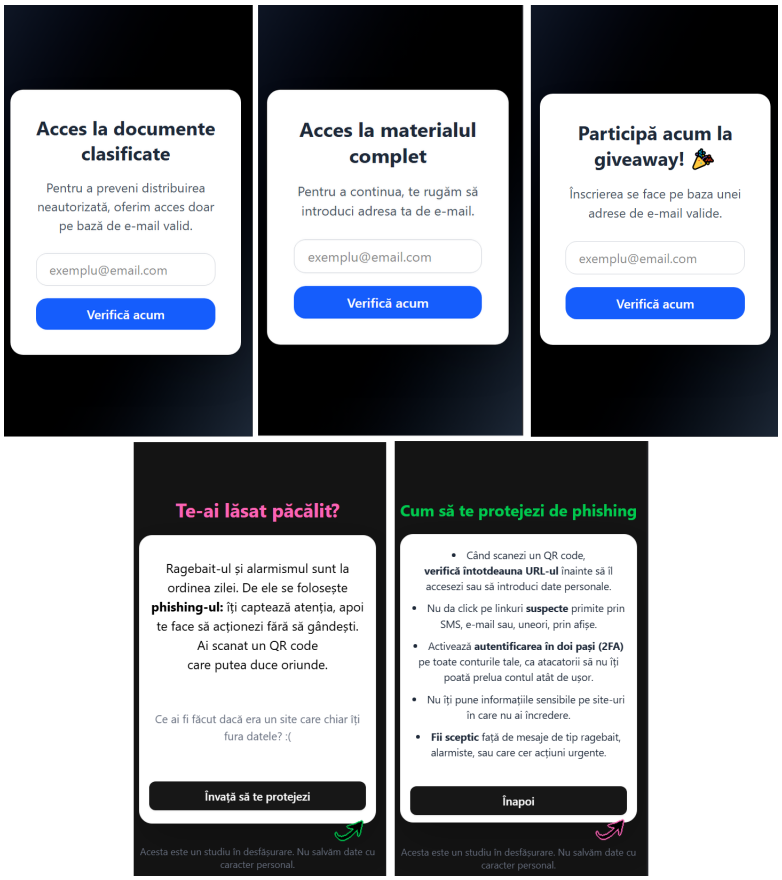

FIGURE 2. Landing page variants and post-submission page

failing the API validation check, and those that did not have a corresponding UUID in the initial scan table, as that meant that the data was inconsistent and potentially tampered with outside of the intended scan environment. In the end, we removed 26 duplicate scan events, 11 invalid email inputs and 7 inconsistent email inputs.

3.5. **Ethical Considerations.** From an ethical standpoint, there are a few points to address. Firstly, the study involved mild deception, as participants were unaware that the posters were part of a controlled experiment until after inputting their email address. However, ethical safeguards were implemented throughout the process. Only minimal, anonymized data was collected, and all participants were debriefed immediately after the interaction. The experiment

adhered to ethical guidelines for field research in cyber security, emphasizing informed post-participation consent and data minimization.

Secondly, permission for public posting was not formally obtained; however, no property was damaged, as posters were only placed in locations already used for similar materials.

3.6. **Data Analysis.** The collected data was analyzed to evaluate the relationship between poster type and user engagement. Two dependent variables were measured: the number of unique QR scans and the rate of email submissions. Scan counts provided a measure of initial curiosity or engagement, while submissions reflected a potential successful simulated phishing attempt.

3.7. **Limitations.** Several limitations affected the interpretation of the results. The consistent damaging and removal of posters reduced exposure time unevenly across locations. As the posters within a given location were not all affixed to the same surface, variations in pedestrian flow may have affected their visibility, and, subsequently, the number of scans. Limited manpower prevented immediate replacement after damage, and adverse weather occasionally rendered certain QR codes unscannable. Additionally, the low-cost validation API used for email verification may have allowed invalid or disposable addresses to pass initial checks, or, on the contrary, yielded a false-negative for standard addresses.

Another aspect to consider is the fact that we have no information on the demographics of the population, as we have not conducted any post-scan survey. Finally, because the study was conducted within an electoral context, with specific cultural factors, and only in the city of Cluj-Napoca, its findings may not generalize to other populations or time periods.

4. Results and Discussion

4.1. **Engagement and Conversion Rates.** As shown in Table 1, politically framed posters generated substantially higher engagement than social ones. Each of the three political variants received approximately 50 to 51 scans per poster, while the social versions received only 11 to 13 scans, showing that the political topic was 4-4.5 times more efficient than the social topic. This indicates that political content acted as a strong attractor of attention, likely due to its contextual relevance during the election period.

While political posters dominated in visibility, the conversion rate — defined as the percentage of scans that led to email submission — reveals a more complex behavioral pattern. Although the political clickbait variants produced moderate conversion rates (20–29%), the highest rate was observed in the

Content Type	Tone	Scans	Emails	Conversion (%)
Political (Blue)	Clickbait	50	10	20.0
Political (Yellow)	Clickbait	51	15	29.4
Political (Neutral)	Neutral	51	11	21.6
Social	Clickbait	11	2	18.2
Social	Neutral	13	5	38.5

TABLE 1. Summary of engagement and compliance results by poster category

social neutral condition, where 38.5% of scanners provided an email address.

This finding suggests that emotional activation may generate attention but not necessarily trust. The social neutral poster, while hardly giving any information about its contents, can be perceived as more curious, but also harmless in comparison to the others. One might be more inclined to submit an email address (potentially a burner address) on the basis that the outcome may fulfill their curiosity. This interaction feels low-risk, and any potential malicious outcome can be dismissed as a simple nuisance and promptly ignored.

In comparison, given the tense climate at the time of the experiment, it can be fair to assume users' skepticism when it comes to the political posters. While the act of scanning the QR code might have a higher perceived value than in the case of a neutral tone poster, requesting an email address is what tips the scale in favor of users abandoning the website.

This leads us to believe that part of the initial hypothesis may be factual, that users are more inclined to interact with political content. An interpretation of this is the fact that the environmental and social context can greatly influence the visibility and thus success of phishing campaigns. However, given the modest number of total scans, the results should be interpreted as indicative rather than definitive; still, the consistency of behavioral differences across conditions lends credibility to the observed patterns.

4.2. **Clickbait Versus Neutral Tone.** Our initial assumption was that inflammatory content would lead to higher scan and phishing rates. However, our findings disprove this theory. In the case of the political posters, tone does not seem to cause any significant difference in interactions. In the social condition, however, an interesting trend emerged: the neutral version produced a conversion rate more than double that of the clickbait version (38.5% vs. 18.2%).

This reversal illustrates an interesting psychological mechanism discussed in persuasion research—the *attention–trust trade-off*. Emotionally charged or sensational messages draw attention but also increase skepticism. Users may perceive emotionally manipulative content as less credible or as an attempt to provoke them, leading to reduced willingness to share information. The initial cost of scanning the QR code was already high due to the tone of the poster, so a reluctance in complying with the demands of the website follows. While the social neutral poster might appear curious and harmless, the social clickbait one can be seen as posing a higher risk. At the same time, it is possible that due to its execution, the clickbait poster can potentially blend into its surroundings, as a simple giveaway announcement among a multitude of advertisements. These results echo Cialdini's principle that persuasion relies on subtle, contextually appropriate cues, and that excessive emotional intensity can undermine compliance [12].

4.3. **Political Context and Behavioral Observations.** Political framing consistently outperformed social framing in attracting engagement, yet its impact on compliance remains limited. Given Romania's highly polarized political climate during the experiment, it is plausible that users were drawn to the posters out of curiosity or familiarity but refrained from entering personal data due to suspicion.

Content Type	**Tone**	**Emails**	**Capture rate (%)**
Political (Blue)	Clickbait	10	22.2
Political (Yellow)	Clickbait	15	33.3
Political (Neutral)	Neutral	11	24.4
Social	Clickbait	2	4.4
Social	Neutral	5	11.1

TABLE 2. Effectiveness of poster types in email collection

As can be seen in table Table 2, the political yellow posters are the most successful when it comes to email collection, with a 33.3% rate (N = 43) which may be correlated to the amount of information and controversial events related to the corresponding candidate happening that week. During field deployment, user interactions reflected real-world unpredictability. Political posters were more frequently damaged or removed — likely a consequence of their controversial nature — whereas social posters were less often tampered with. This behavioral difference further demonstrates the polarizing effect of political material in public spaces. One of the blue posters, particularly near

a university campus was constantly vandalized, often being torn in half the morning after it was replaced.

One possible explanation for this trend is the attempt to combat possible misinformation. To an outside view, the posters can appear at first glance as a last-ditch effort to bias people's votes. An unplanned interaction with a person who was trying to damage one of the posters after initially scanning it supports this theory, as they mentioned assuming it was put up by malicious individuals.

Together, the results reveal that emotional intensity and contextual familiarity play complementary but opposing roles. While emotion increases visibility, familiarity increases trust. Educators designing awareness campaigns should, therefore, recognize that the most effective manipulation may stem not from provocative design, but from inconspicuousity.

5. Conclusions and future work

In summary, the experiment demonstrated an interesting contrast between getting attention and collecting information. While political clickbait posters showed the highest email capture and scan rates in this experiment, neutral social posters inspired trust and higher conversion rates despite lower visibility. It is worth mentioning that the research is not intended to endorse attack methods. Instead, it reveals an environment where users may be more vulnerable to QR-based phishing and inflammatory content, informing the necessity for future awareness campaigns and quishing mitigation.

These insights reinforce the importance of context, subtlety, and credibility in shaping real-world user behavior toward phishing stimuli. Future iterations of this experiment could incorporate a short questionnaire to better capture demographic characteristics and find out which cues were most impactful in the decision-making of the participants. Ultimately, the experiment illustrates the threat posed by this method, the need for awareness regarding quishing amongst the general populace, and, last but not least, the fact that in social engineering, the most successful deception may not be the one that shouts the loudest, but the one that blends in more.

6. Acknowledgements

We are extremely grateful and would like to thank all the individuals that were involved in supporting the completion of this paper.

Firstly, we would like to thank the friends that have helped with the poster distribution, including Alex Poenaru, Victor Unguroiu and Tudor Murariu, as this paper would not have been possible without their help.

We would also like to extend our gratitude to Levin Tschuertz for providing us with some of the cited articles, and to Daniel Gulei for proofreading the chapters.

References

[1] Ana Ferreira, Lynne Coventry, and Gabriele Lenzini. Principles of persuasion in social engineering and their use in phishing. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 36–47. Springer, 2015.

[2] Antino Kim and Alan R Dennis. Says who? the effects of presentation format and source rating on fake news in social media. *Mis quarterly*, 43(3):1025–1040, 2019.

[3] Filipo Sharevski, Amy Devine, Emma Pieroni, and Peter Jachim. Phishing with malicious qr codes. In *Proceedings of the 2022 European Symposium on Usable Security*, pages 160–171, 2022.

[4] Timothy Vidas, Emmanuel Owusu, Shuai Wang, Cheng Zeng, Lorrie Faith Cranor, and Nicolas Christin. Qrishing: The susceptibility of smartphone users to qr code phishing attacks. In *International conference on financial cryptography and data security*, pages 52–69. Springer, 2013.

[5] Dongwan Shin and Huiping Yao. A user study of security warnings for detecting qr code based attacks on android phone. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 4(4):49–64, 2013.

[6] Mihai VACARIU. Alegerile prezidențiale din românia 2024: dezinformare și manipulare în campania lui georgescu. *ELITELE POLITICE LA ROTATIVA ISTORIEI. ALEGERILE DIN 2024*, page 115, 2024.

[7] Premier Ministre-SGDSN. Manipularea algoritmilor și instrumentalizarea influencerilor. concluzii desprinse din alegerile prezidențiale din românia & riscuri pentru franța, 2025.

[8] Pavlo Burda, Luca Allodi, and Nicola Zannone. Cognition in social engineering empirical research: a systematic literature review. *ACM Transactions on Computer-Human Interaction*, 31(2):1–55, 2024.

[9] Leonardo Ballesteros-López, Carlos Mejía-Vayas, Sonia Armas-Arias, and Carla-S Castro-Altamirano. Qr codes as a strategy in political marketing 2.0. In *International Conference on Computer Science, Electronics and Industrial Engineering (CSEI)*, pages 3–13. Springer, 2022.

[10] F Ley Sylvester. Mobile device users' susceptibility to phishing attacks. *arXiv preprint arXiv:2203.01823*, 2022.

[11] Liliana Ribeiro, Inês Sousa Guedes, and Carla Sofia Cardoso. Which factors predict susceptibility to phishing? an empirical study. *Computers & Security*, 136:103558, 2024.

[12] Aya Muhanad, Israa Abuelezz, Khaled Khan, and Raian Ali. On how cialdini's persuasion principles influence individuals in the context of social engineering: a qualitative study. In *International Conference on Web Information Systems Engineering*, pages 373–388. Springer, 2024.

[13] Marvin Geisler and Daniela Pöhn. Hooked: A real-world study on qr code phishing. *arXiv preprint arXiv:2407.16230*, 2024.

[14] Jeremiah D Still, Thomas Morris, and Morgan Edwards. Investigating university qr code interactions. In *International Conference on Human-Computer Interaction*, pages 204–214. Springer, 2024.
[15] Jonas Nygaard Blom and Kenneth Reinecke Hansen. Click bait: Forward-reference as lure in online news headlines. *Journal of pragmatics*, 76:87–100, 2015.
[16] Jieun Shin, Chris DeFelice, and Soojong Kim. Emotion sells: Rage bait vs. information bait in clickbait news headlines on social media. *Digital Journalism*, pages 1–20, 2025.
[17] Mihai Vacariu. Manipulation and disinformation in the 2024 romanian presidential elfections. *Redefining Community in Intercultural Context*, 12(1):81–88, 2025.
[18] Esther Niehoff and Suzanne Oosterwijk. To know, to feel, to share? exploring the motives that drive curiosity for negative content. *Current Opinion in Behavioral Sciences*, 35:56–61, 2020.

Department of Computer Science, Babeş-Bolyai University, Cluj-Napoca, Romania

Email address: goiaalexia@proton.me and imre.zsigmond@cs.ubbcluj.ro