Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 3830 – 3843
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.6226

Cross-Sectional Analysis to Discover Phishing Cyberattack Trends in Saudi Arabia

Suaad Alarifi[1], Dania Aljeaid[2]

Abstract

Phishing attacks exploit social engineering to deceive users, potentially leading to data breaches, financial losses, or, worse, identity theft. To counter these threats, Saudi Arabia has recently implemented robust initiatives, including awareness campaigns, regulatory measures, and new legislation aimed at phishing prevention. This cross-sectional study, as part of an ongoing longitudinal series, assesses the effectiveness of these efforts by comparing data from phishing identification surveys conducted in 2018 and 2022. The findings indicate a 632% increase in phishing attempts reported by Saudi users, accompanied by notable gains in user awareness and skepticism. However, the success rates of these attacks remain unclear, highlighting the need for continued assessment of user resilience. The study also identifies evolving phishing tactics, offering strategic insights to strengthen anti-phishing measures in Saudi Arabia and guide global efforts against similar threats.

Keywords: *Phishing, Cybersecurity, Social Engineering, Security Awareness.*

Introduction

Phishing attacks have become increasingly prevalent worldwide, with many households in Saudi Arabia falling victim to such attempts. Using social engineering, attackers fraudulently extract sensitive information, such as credit card details or passwords, through increasingly convincing emails and websites (Benavides et al., 2020), (Hadnagy, 2018) and (Maurer et al., 2012). Indicators like spelling errors or odd URLs may hint at a scam, yet attackers increasingly craft convincing emails and websites to evade detection and deceive users (Maurer et al., 2012). Stolen data can be used for financial fraud or worse, identity theft (Mugarura, 2020). Recovering stolen money is often impossible.

Governments and the private sector work to educate individuals and counter phishing attacks through regulations and security frameworks. The National Cybersecurity Authority (NCA) in Saudi Arabia has introduced several initiatives since its establishment in 2017 to promote digital transformation (NCA, 2025). The question remains: have these efforts reduced phishing risks for Saudi users?

This study examines phishing awareness among Saudis from 2018 to 2022. It examines changes in user knowledge, skepticism, and engagement rates to evaluate awareness efforts. The study also analyzes phishing tactics and their effectiveness, offering recommendations to enhance resilience, using Saudi users as the sample.

In this Study

- User skepticism gauges the level of caution users exhibit when evaluating messages for potential phishing, often reflected by responses like "maybe" when uncertain about a message's legitimacy.

- User knowledge assesses users' ability to recognize phishing cues, such as poor grammar and unusual requests, reflecting their understanding of phishing tactics and awareness of potential

[1] Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia, Email: salarifi@kau.edu.sa, (Corresponding Author)

[2] Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia, Email: daljeaid@kau.edu.sa

scam indicators.

The main contributions include:

- A comparative analysis of Saudi user awareness and susceptibility to phishing from 2018 to 2022.
- An evaluation of trends and shifts in attackers' techniques over time.
- Recommendations for improved phishing prevention, focusing on tailored awareness and technical measures.

The 2018 study by (Aljeaid et al., 2020) established a baseline understanding of Saudi users' knowledge and awareness of phishing, marking the first study in this longitudinal series. This study builds upon those findings by re-evaluating user awareness and susceptibility in 2022, highlighting trends in phishing tactics and user responses. This study hypothesizes that ongoing Saudi initiatives have reduced successful phishing attacks and enhanced user awareness, improving phishing detection.

Hypothesis: Phishing awareness initiatives have significantly increased user awareness and skepticism toward phishing attacks among Saudis between 2018 and 2022.

Research Questions to Support the Hypothesis:

- RQ1: How has user knowledge and skepticism toward phishing attacks evolved from 2018 to 2022?
- RQ2: What trends in phishing techniques have emerged, and how do users respond?
- RQ3: What gaps remain in user behavior, indicating areas for improvement in anti-phishing strategies?

The rest of the paper is organized as follows. Section 2 provides the background and theoretical context. Section 3 reviews related work and the previous assessment on which this research is built. Section 4 covers the methodology and experiment used to test the hypothesis. Section 5 includes discussion and security analysis. The final section presents the conclusion and future work.

Background and Theoretical Context

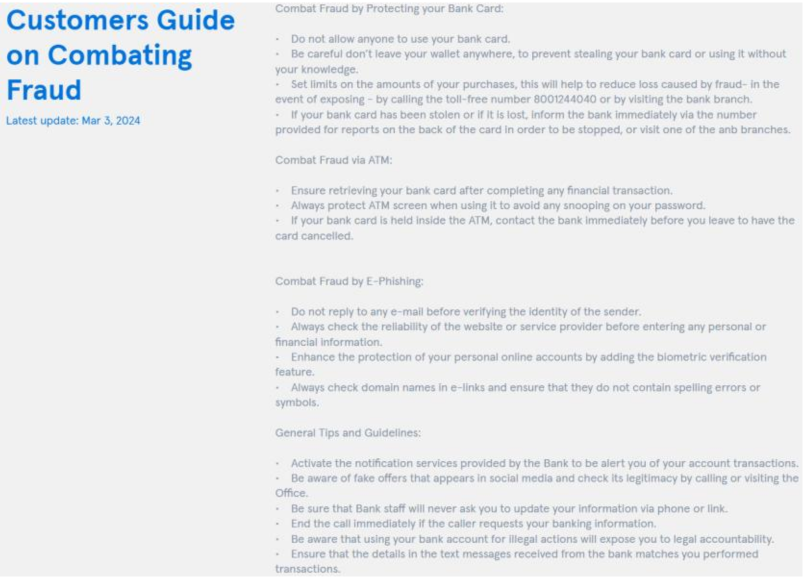
Governments and the private sector protect citizens and customers from phishing attacks through regulations, awareness campaigns, and technical solutions. Regulations enhance accountability in the banking sector by controlling money transfers to prevent crimes such as money laundering (Swift, 2023). Awareness campaigns and user training help mitigate phishing risks (Swift, 2023), while technical defenses such as multi-factor authentication, URL filtering, and machine learning improve protection (Maurer et al., 2012) and (Abusaimeh et al., 2021).

Technical solutions are crucial for defending against phishing, as users often fail to detect attacks due to a lack of focus on security (Maurer et al., 2012). Anti-phishing tools, such as Barracuda Sentinel, leverage AI to scan links and emails, blocking suspicious content (Barracuda, 2025). Additionally, governance, policies, and procedures strengthen security by addressing vulnerabilities that phishing attacks frequently exploit (Hadnagy, 2018).

With the rise in phishing threats, organizations are continuously updating policies to mitigate attacks and enhance awareness. For example, Saudi banks such as the Arab National Bank (ANB) enforce strict anti-phishing measures. Figure 1 illustrates ANB's security awareness page, which emphasizes its policy of never

ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.6226

requesting personal data via email, helping customers identify and ignore phishing attempts (A. N. Bank, 2025).



Customers Guide on Combating Fraud

Latest update: Mar 3, 2024

Combat Fraud by Protecting your Bank Card:

- Do not allow anyone to use your bank card.
- Be careful don't leave your wallet anywhere, to prevent stealing your bank card or using it without your knowledge.
- Set limits on the amounts of your purchases, this will help to reduce loss caused by fraud- in the event of exposing - by calling the toll-free number 8001244040 or by visiting the bank branch.
- If your bank card has been stolen or if it is lost, inform the bank immediately via the number provided for reports on the back of the card in order to be stopped, or visit one of the anb branches.

Combat Fraud via ATM:

- Ensure retrieving your bank card after completing any financial transaction.
- Always protect ATM screen when using it to avoid any snooping on your password.
- If your bank card is held inside the ATM, contact the bank immediately before you leave to have the card cancelled.

Combat Fraud by E-Phishing:

- Do not reply to any e-mail before verifying the identity of the sender.
- Always check the reliability of the website or service provider before entering any personal or financial information.
- Enhance the protection of your personal online accounts by adding the biometric verification feature.
- Always check domain names in e-links and ensure that they do not contain spelling errors or symbols.

General Tips and Guidelines:

- Activate the notification services provided by the Bank to be alert you of your account transactions.
- Be aware of fake offers that appears in social media and check its legitimacy by calling or visiting the Office.
- Be sure that Bank staff will never ask you to update your information via phone or link.
- End the call immediately if the caller requests your banking information.
- Be aware that using your bank account for illegal actions will expose you to legal accountability.
- Ensure that the details in the text messages received from the bank matches you performed transactions.

Figure 1. Security Awareness Page (A. N. Bank, 2025).

Phishing Cyberattack Statistics

The Anti-Phishing Working Group (APWG, 2022) reports a significant rise in phishing activity from 2018 to 2022. In Q3 2018, 151,014 phishing websites were detected (APWG, 2018). By Q2 2022, phishing websites had exceeded one million (APWG 2nd, 2022), marking a 627% increase over the four-year period under review.

In Q2 2020, Kaspersky's (Kaspersky, 2020) spam and phishing report revealed that Saudi Arabia faced nearly one million phishing attacks in just three months, closely aligning with the global average reported by the (APWG 2nd, 2022).

The APWG 2022 report revealed a rise in wire transfer BEC attacks, with average losses reaching $109,467 (APWG 2nd, 2022). Healthcare and transportation were among the most targeted industries for ransomware attacks via phishing. In Q2 2022, the financial sector was the most targeted (27.6%), followed by webmail and SaaS providers. Phishing against social media companies rose from 8.5% in Q4 2021 to 15.5%, while e-commerce attacks dropped to 5.6% (APWG 2nd, 2022).

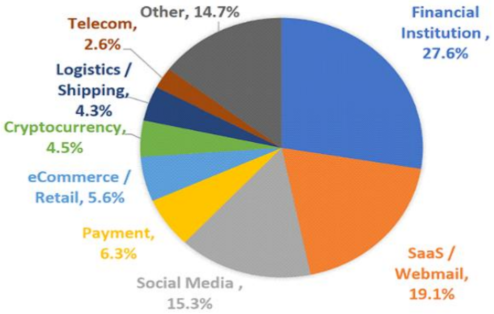


Figure 2. Most Targeted Industries 2nd Q, 2022 by (APWG 2nd, 2022).

Phishing activity trend reports highlight that phishing cyberattacks have become a serious and increasingly sophisticated threat over time.

Principles of Persuasion in Phishing Attacks

Dr. Robert Cialdini's six principles of persuasion explain how people are influenced, offering insights into phishing tactics (Cialdini, 1984). These principles, widely applicable in cybersecurity, marketing, and behavioral analysis, help explain why individuals may be vulnerable to phishing and other social engineering tactics.

- Reciprocity: Attackers frame messages as favors or offers to trigger a sense of obligation.
- Commitment and Consistency: People act on requests that align with prior commitments.
- Social Proof: Fake reviews or popular links exploit people's tendency to follow others.
- Authority: Phishing emails mimic trusted institutions like banks to pressure recipients into compliance.
- Liking: Relatable or familiar personas increase influence.
- Scarcity: Urgent or limited-time messages create a sense of urgency.

These principles reveal how phishing campaigns manipulate psychological responses to deceive users.

Related Work

The first wave of fieldwork was conducted in October 2018, with the report published on November 25, 2019 (Aljeaid et al., 2020). This study evaluated Saudi users' knowledge and awareness of cybersecurity through a phishing attack identification assessment. It was one of the few experiments conducted exclusively on Saudi society. The researchers in (Aljeaid et al., 2020) collected data using two methods: a survey and an attack identification assessment, to test the following hypotheses:

Are end users in Saudi Arabia insufficiently knowledgeable regarding cyberattacks?

Do they lack the ability to protect themselves against various types of phishing attacks?

The survey examined users' experiences with phishing attacks and measured their knowledge, while the attack simulations assessed users' responsiveness and behavior toward different phishing attacks. The study demonstrated that users easily fall victim to phishing attacks because (1) they lack cybersecurity knowledge and awareness; (2) they rely solely on technical safeguards; and (3) cybercriminals are adept at manipulating users' intuition by combining persuasion principles with new malicious techniques (Aljeaid et al., 2020).

The second wave of fieldwork was conducted in October 2022. The results will help reassess the same factors identified in (Aljeaid et al., 2020) and re-evaluate the maturity level of Saudi users after a four-year span. Since phishing attacks are categorized as social engineering attacks, the strategies used to design such attacks can be analyzed using persuasion principles (Cialdini, 1984).

Other Studies

In 2017, the Potomac Institute for Policy Studies assessed Saudi Arabia's cybersecurity profile using the Cyber Readiness Index 2.0 (CRI) (P. Institute, 2017) and (Hathaway et al., 2017). The report highlighted gaps in legal infrastructure, such as insufficiently trained court judges and a lack of data breach notification regulations. Despite these challenges, Saudi Arabia has made significant progress, driven by frequent

ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.6226

cyberattacks (P. Institute, 2017) and (Hathaway et al., 2017). In response, the government established the National Cybersecurity Authority (NCA) in 2017 to implement the National Information Security Strategy (NCA, 2025). By 2020, Saudi Arabia ranked second globally in the Global Cybersecurity Index, rising 12 places since 2018, alongside the United States and the United Kingdom (Table 1).

Table 1. A Snapshot of GCI Results: Global Score and Rank (P. Institute, 2017).

Country Name	Score	Rank
United State of America** 1	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5

(Wilhelms et al., 2014) analyzed users' decisions when encountering phishing attacks. They studied users' initial actions when receiving a phishing email, including whether they would click on the link, delete the email, copy and paste the URL, or perform other actions. They then examined behavioral responses to the attacks and discovered interdependencies between different factors such as awareness, knowledge, susceptibility to risk, and cost. The researchers considered intentions alongside users' behaviors. They found that procedural knowledge, such as determining URL legitimacy, helped users adjust their risk decisions.

Research in measuring users' susceptibility and analyzing their decisions and responses to attacks is considered socio-technical research, which combines information security with social science. (Ferreira et al., 2014) developed a framework for the social and technical analysis of security. It aimed to analyze technical weaknesses in addition to social vulnerabilities to achieve effective security. The framework, called STEAL (Socio-Technical Attack Analysis), was one of the first socio-technical evaluations of security. Although this area of research is expanding rapidly in understanding phishing attacks, knowledge gaps remain. A more focused study approach to delineate the boundaries and challenges would help investigate these specific attacks moving forward.

While previous research has made important strides in understanding users' vulnerability to phishing attacks in Saudi Arabia, several key areas remain underexplored. The 2018 study (Aljeaid et al., 2020) provided insights into user awareness and responsiveness but did not explore how this awareness has evolved over time with increasing phishing threats. Additionally, the socio-technical frameworks, such as STEAL (Ferreira et al., 2014), have highlighted both social and technical vulnerabilities, but they fall short in examining the specific role of national cybersecurity initiatives, like those by the National Cybersecurity Authority (NCA), in shaping user behavior over a multi-year span. This research seeks to fill these gaps by analyzing the changes in phishing awareness among Saudi users from 2018 to 2022, while also examining the impact of national initiatives in strengthening resilience against phishing attacks.

Methodology and Experiment

This study employs a cross-sectional analysis to compare data from two specific time points: 2018 and 2022. The initial dataset was collected in 2018 by (Aljeaid et al., 2020), establishing a baseline for user awareness and behavior regarding phishing in Saudi Arabia. Four years later, a second data collection was conducted with a comparable sample population to ensure consistency in results. This methodological approach allows for an effective assessment of changes in user behavior and awareness over time (Edgar et al., 2014).

Cross-sectional studies are commonly used in social sciences to analyze user behavior and evaluate levels of knowledge and awareness (Majumder et al., 2020). By comparing data from these two time points, this study identifies trends and changes in user susceptibility to phishing attacks. Recollecting data from a similar population enhances the accuracy of the comparison and provides insights into the effectiveness of awareness campaigns and other preventive measures implemented over the years.

Data was gathered through surveys and a phishing identification assessment. The surveys measured participants' general knowledge and awareness of cybersecurity threats, while the phishing identification assessment evaluated their ability to identify phishing attacks in simulated scenarios. This dual approach provides a comprehensive understanding of both theoretical knowledge and practical responses to phishing threats.

The collected data were analyzed using statistical methods to determine the significance of any observed changes. The analysis focused on identifying trends and examining variations in user awareness, skepticism, and engagement with phishing attempts over time. Key metrics included changes in the accuracy of identifying phishing threats, shifts in reported confidence and knowledge levels, and variations in responses to phishing cues between 2018 and 2022. These indicators enable a detailed evaluation of the impact of phishing awareness initiatives on user susceptibility.

The study was conducted among members of Saudi society. We adapted the original survey created by (Aljeaid et al., 2020) with minor modifications to improve clarity. The survey was developed in both English and Arabic and included eight multiple-choice questions. It was divided into two parts: the first part collected demographic information such as gender and age, while the second part focused on specific phishing-related questions.

A total of 203 participants took part in the study, with respondents ranging in age from 13 years and older. Although all respondents were proficient in Arabic, English translations were provided to clarify technical terms. The survey was created using Google Forms and distributed online via WhatsApp, targeting groups of Saudi users with a message specifying that the study was intended for members of Saudi society.

To ensure the validity of the results, we took measures to minimize external influences on participants. They were informed that the survey was part of a research study on phishing attacks. An ethical approval form was included to confirm compliance with ethical standards.

The study was conducted in three stages:

- Stage One: Participant recruitment. Individuals residing outside Saudi Arabia were excluded to focus on the target population.

- Stage Two: Experiment design with minimal influence. In socio-technical studies, external influences can impact data reliability. For example, if par- ticipants perceive a risk, their responses may differ from typical behavior (Aljeaid et al., 2019).

- Stage Three: Data collection and analysis, including prevalence estimation and trend detection.

Survey Questions

After gathering background information on residency, nationality, age, and gender, participants answered the following survey questions, with specified response options:

How well do you know phishing attacks?

Knowledge Level: No knowledge, Little knowledge, Moderate knowledge, High

knowledge.

Have you experienced a phishing attack?

Frequency: Frequently, Sometimes, Rarely.

What types of phishing attacks have you encountered?

Type of Phishing Attack: Social media, Personal contact, Phone call, SMS, Email,

None.

Do you usually share your personal information with strangers online?

Response: Yes, No

Have you received any of the following types of messages through email, text message, or any other platform?

Type of Case

Link claiming that your ATM card is blocked, requiring action such as updating your information and inviting you to contact suspicious numbers.

Link claiming that you won a prize or money.

Link soliciting donations from an unknown party.

Message claiming to be from Apple support, requesting login with your username and password on a fake site.

Other

Do you agree or disagree that the following image is a scam?

Response: Yes, No, Maybe.

Image Description: A screenshot of a phishing email in Arabic. Below is the translation:

Ministry of Interior

Dear Ahmed, We would like to inform you that the Visa under your name with number 1191*** dated 28-12-2022 will expire soon. If this Visa is not under your name, please visit our online service from this link to review the visas of all workers under your name.

Greetings,

Absher support team

Note: Absher is the government online system providing services to Saudi citizens and residents. The original screenshot will be included in the analysis section.

Do you think the image shown is a scam?

Response: Yes, No, Maybe.

Image Description: A screenshot of a phishing email in English, resembling an official message from Instagram requesting email confirmation. The original screenshot will be included in the results section.

Results and Analysis

The data collected was analyzed using Microsoft Excel to compute various statistical measures. Chi-square tests were conducted to assess whether there were statistically significant differences between the years 2018 and 2022. In this study, p-values smaller than 0.05 and 0.01 were considered statistically significant.

For general demographic questions, both the 2018 and 2022 surveys showed that approximately 80% of respondents were female. In the 2018 survey, most respondents were between 19 and 23 years old (about 52%), whereas in the 2022 survey, the majority shifted to those over 23 years old (about 61%).

The detailed results and analysis of the main survey questions are presented below.

Question 1: How well do you know phishing attacks?

Knowledge levels and their percentages in 2018 and 2022

Knowledge Level	2018	2022
No knowledge	12%	12%
Little knowledge	42%	29%
Moderate	37%	37.5%
High knowledge	9%	21.5%

In 2018, a chi-square goodness-of-fit test ($\chi^2_{2018} = 68.64$ critical value = 7.815, df = 3, α = 0.05) revealed a statistically significant uneven distribution in phishing knowledge levels, with 42% reporting "little knowledge," indicating low awareness. By 2022, the test ($X^2_{2022} = 28.28$) remained significant but showed higher proportions of "moderate" and "high knowledge," reflecting improved awareness. A chi-square test for independence confirmed a significant difference between the years, with" high knowledge" responses rising from 9% in 2018 to 21.5% in 2022, suggesting increased phishing awareness and reduced vulnerability within Saudi society.

Question 2: Have you been attacked with a phishing attack?

Frequency of Phishing Attacks in 2018 and 2022

Frequency	2018	2022
Frequently	7.1%	52%
Sometimes	28.1%	25%
Rarely	64.8%	23%

In 2018, a chi-square test ($\chi^2_{2018} = 103.46$, critical value = 5.991) showed a statistically significant uneven distribution, with "rarely" being the most frequent response (64.8%), indicating low phishing exposure. By 2022, the test ($\chi^2_{2022} = 31.48$) remained significant, with "frequently" becoming the dominant response (52%), reflecting increased phishing exposure. A chi-square test for independence

(χ^2 = 109.08, df = 2, critical value = 5.991) confirmed this change, showing a 632% rise in frequent phishing encounters, from 7.1% in 2018 to 52% in 2022, highlighting growing phishing risks in Saudi society.

Question 3: What types of phishing attacks have you en- countered?

Types of Phishing Attacks Encountered in 2018 and 2022

Type of Phishing Attack	2018	2022
Social media	19%	20.5%
Personal contact	7%	2.2%
Phone call	19%	21.3%
SMS	38%	30.9%
Email	17%	21.9%
None	0%	3.2%

In 2018, a chi-square test ($\chi^2_{2018} = 50.27$, critical value = 11.07, df = 5, α = 0.05) revealed a statistically significant uneven distribution of phishing attack types, with SMS phishing being the most common at 38%. By 2022, the chi-square test ($\chi^2_{2022} = 100.47$) confirmed a continued uneven distribution, though SMS phishing declined to 30.9%, reflecting a shift in attack strategies.

A chi-square test for independence (χ^2 = 14.484, df = 5, critical value = 11.07) confirmed a significant change in phishing methods between the two years. While SMS phishing remained dominant, its decline was accompanied by reduced use of personal contacts (from 7% in 2018 to 2% in 2022), likely due to attackers minimizing direct contact to avoid detection. Meanwhile, phishing via social media, email, and phone calls increased slightly, suggesting evolving attacker strategies while maintaining SMS as the primary method.

Question 4: Do you usually share your personal information with strangers online?

Do you usually share your personal information with strangers online?

Year	Yes	No
2018	20%	80%
2022	16%	84%

In 2018, a chi-square test ($\chi^2_{2018} = 72$, critical value = 3.841, df = 1, α = 0.05) revealed a significant reluctance to share personal information with strangers, as most respondents answered "No." This trend persisted in 2022 ($\chi^2_{2022} = 92.48$) reflecting continued privacy awareness.

A chi-square test for independence (χ^2 = 0.7507, df = 1, critical value = 3.841) indicated no major behavioral changes between the two years, though respondents in 2022 showed slightly heightened privacy consciousness. Notably, gender differences emerged in 2022, with 75% of females reporting sharing personal data compared to 25% of males. However, given that females made up 80% of the sample, these results should be interpreted cautiously due to potential sample size imbalances.

Question 5: Have you received any of these cases by email, text message, or any other platform?

Cases received by email, text message, or any other platform in 2018 and 2022

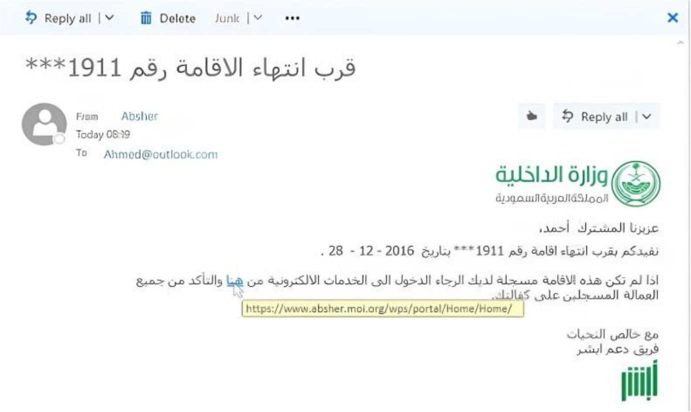
Type of Case	2018	2022

Link claiming that your ATM card is blocked, requiring action such as updating your information and inviting you to contact suspicious numbers.	27%	39.4 %
Link claiming that you won a prize or money.	16%	41%
Link soliciting donations from an unknown party.	45.6%	12%
Message claiming to be from Apple support, requesting login with your username and password on a fake site.	9.5%	7.5%
Other	1.9%	0%

In 2018, a chi-square test ($\chi^2_{2018} = 59.051$, critical value = 9.488, df = 4, α = 0.05) showed significant variability in reported phishing case types, with donation-based scams dominating at 46%. By 2022, the test ($\chi^2_{2022} = 72.61$) indicated continued variability, though donation scams dropped to 12%, likely due to the establishment of **Ehsan**, a Saudi government-regulated donation platform aimed at ensuring secure and transparent charitable contributions while reducing risks of fraud and terrorism financing (Ehsan, 2025).

A chi-square test for independence ($\chi^2 = 35.13$, df = 4, critical value = 9.488) confirmed a shift in phishing tactics over time. Prize-based scams rose from 16% in 2018 to 41% in 2022, exploiting the reciprocity principle (Cialdini, 1984). Bank-related threats also increased from 27% to 39%, leveraging authority-based persuasion. Apple impersonation scams remained below 10% both years, possibly due to survey wording constraints (Aljeaid et al., 2019).

Question 6: Do you think the image shown is a scam?



قرب انتهاء الاقامة رقم 1911***

From Absher
Today 08:19
To Ahmed@outlook.com

وزارة الداخلية
المملكة العربية السعودية

عزيزنا المشترك أحمد،

نفيدكم بقرب انتهاء اقامة رقم 1911*** بتاريخ 2016 - 12 - 28 .

اذا لم تكن هذه الاقامة مسجلة لديك الرجاء الدخول الى الخدمات الالكترونية من هنا والتأكد من جميع
العمالة المسجلين على كفالتك.

https://www.absher.moi.org/wps/portal/Home/Home/

مع خالص التحيات
فريق دعم ابشر

ابشر

Figure 3. Screenshot of a Phishing Email

The English translation of the Arabic text in the picture is as follows: Ministry of Interior

Dear Ahmed, We would like to inform you that the Visa under your name with number 1191*** date 28-12-2022 will expire soon. If this Visa is not under your name please visit our online service from *this link* to review the visas of all workers under your name. Greetings Absher support team

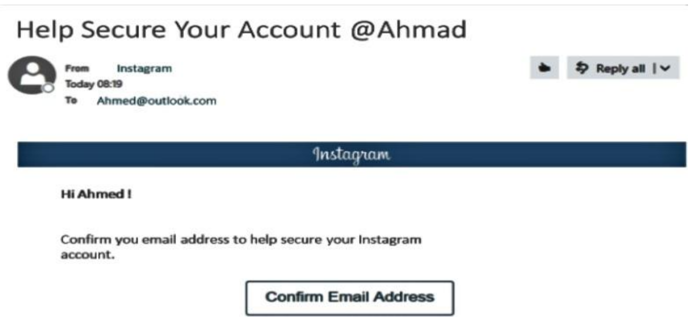
Do you think the image shown is a scam?

Response	2018	2022
Yes	47.3%	50%
No	52.7%	27%
Maybe	0.0%	23%

In 2018, a chi-square test ($\chi^2_{2018} = 100.46$, critical value = 5.991, df = 2, α = 0.05) indicated a statistically significant response distribution, with "Yes" and "No" responses dominating over "Maybe," suggesting distinct participant opinions. By 2022, the chi-square test ($\chi^2_{2022} = 25.46$) showed continued significance, with an increased frequency of "Yes" responses, reflecting improved recognition of phishing scams.

A chi-square test for independence (χ^2 = 62.16, df = 2, critical value = 5.991) confirmed a significant shift in responses between 2018 and 2022. The correct answer was "Yes," as the email was a scam due to its ".org" domain instead of the expected ".gov." In 2018, nearly half of participants missed this, though "Maybe" responses increased in 2022, reflecting greater caution. Anomalously, the 2018 survey showed no "Maybe" responses, possibly due to survey design flaws, highlighting the need for improved future survey designs.

Question 7: Do you think the image shown is a scam?



Help Secure Your Account @Ahmad

From Instagram
Today 08:19
To Ahmed@outlook.com

Instagram

Hi Ahmed !

Confirm you email address to help secure your Instagram account.

Figure 4. Screenshot of a Phishing Email.

Do you think the image shown is a scam?

Response	2018	2022
Yes	35.8%	32%
No	64.2%	33.5%
Maybe	0.0%	34.5%

In 2018, a chi-square test ($\chi^2_{2018} = 123.396$, critical value = 5.991, df = 2, α = 0.05) revealed a statistically significant response distribution, with "No" responses dominating despite being incorrect. This indicates a common susceptibility among respondents to deceptive tactics. By 2022, the chi-square test ($\chi^2_{2022} = 0.191$) showed no significant difference, with responses more evenly distributed across "Yes," "No," and "Maybe," though ideally, "Yes" should have been the majority as the correct answer.

A chi-square test for independence (χ^2 = 88.67, df = 2, critical value = 5.991) confirmed a significant shift in response distribution between 2018 and 2022. The correct answer was "Yes," as the email contained a noticeable spelling error ("you" instead of "your"), indicating a phishing scam. The percentage of incorrect "No" responses decreased from 64.2% in 2018 to 33.5% in 2022, while "Maybe" responses increased, reflecting improved skepticism toward phishing scams among Saudi users.

Discussion

The findings from this study support the Primary Hypothesis: that phishing awareness initiatives in Saudi Arabia have contributed to an increase in user awareness and skepticism and a potential decrease in successful phishing attacks between 2018 and 2022. The results suggest a positive trajectory, but there remain areas that require ongoing focus to bolster resilience against evolving phishing tactics.

To address RQ1 ("How has user knowledge and skepticism toward phishing attacks evolved from 2018 to 2022?"), the data demonstrates a significant increase in phishing awareness, with the proportion of users reporting ’high knowledge’ rising from 9% to 21.5%. Moreover, users displayed heightened skepticism, with more respondents in 2022 selecting ’Maybe’ instead of ’No’ when evaluating potential phishing messages. This shift in responses suggests a more cautious approach among Saudi users, likely influenced by awareness campaigns, media coverage, and increased exposure to cyber threats. These findings indicate an encouraging trend toward improved knowledge and critical judgment, supporting the hypothesis that awareness initiatives are enhancing user behavior.

In response to RQ2 ("What trends in phishing techniques have emerged in recent years, and how do users respond?"), the analysis reveals a diversification in phishing techniques. While SMS remained the primary phishing medium, there was a notable increase in prize-based scams, which leverage the reciprocity principle to entice users. In contrast, donation-based phishing tactics, which were prevalent in 2018, decreased significantly due to the introduction of government-regulated donation platforms. These shifts suggest that attackers are adapting their methods to target users through channels they deem credible, and users’ responses reflect varied levels of susceptibility depending on the method used. This adaptation in phishing tactics highlights the need for awareness campaigns to continue evolving in response to emerging techniques.

Finally, RQ3 ("What gaps remain in user behavior, indicating areas for improvement in anti-phishing strategies?") is addressed by observing certain behavioral gaps that persist. While awareness has improved, a segment of the population still engages in risky data-sharing behaviors, with female respondents showing a higher tendency to share personal information online. Privacy awareness is increasing, but at a gradual rate, indicating a need for focused educational efforts on data privacy and protection. Addressing these gaps through targeted campaigns could further enhance users’ resilience and reduce susceptibility.

Overall, the findings lend support to the hypothesis, with evidence of increased awareness and skepticism over the years. However, the substantial rise in phishing attacks from 2018 to 2022 underscores the importance of continuous monitoring and updating of anti-phishing strategies. The ongoing evolution of phishing tactics requires both users and regulatory bodies to remain vigilant, suggesting that future studies should re-evaluate these trends periodically to maintain and improve cyber resilience in Saudi society.

Conclusion and Future Work

This study offers valuable insights for the research community and decision-makers regarding the resilience of Saudi society to phishing attacks and how this resilience has evolved from 2018 to 2022. Findings indicate that Saudi users have become increasingly skeptical of phishing tactics, likely contributing to improved resistance against such attacks. Additionally, user knowledge about phishing has grown, further enhancing digital security. Although phishing attacks have risen by approximately 632%, the actual success rates of these attacks remain unknown, highlighting a critical area for further investigation.

Awareness campaigns should continue to address the various channels through which phishing occurs—such as emails, phone calls, social media, and especially SMS. Regulators may consider restricting the collection of sensitive information via these means to reduce phishing risks, like how banks restrict data collection through email. Technical solutions, like URL filtering, are also essential to controlling phishing risks. Relying solely on users to detect phishing remains risky, necessitating integrated technical protection.

This study has certain limitations. The focus on Saudi users may limit the generalizability of the findings to other regions, as cultural and technological factors can shape phishing awareness and responses. Additionally, relying on self-reported data introduces potential bias, and the timeframe (2018-2022) may not capture the latest phishing tactics. Furthermore, this research primarily examines awareness campaigns and user behaviors, leaving technical aspects of phishing detection and prevention relatively unexplored.

Key Research Gaps in Phishing Prevention

Addressing the following gaps could lead to a more comprehensive understanding of phishing attacks and inform better protective measures:

- Investigate whether increased user skepticism toward phishing is reflected in other security behaviors.
- Examine the correlation between the rising number of phishing attempts and the success rates of these attacks.
- Explore potential feedback channels within phishing communities to understand attackers' tactics and adaptations.
- Determine the geographical origins of phishing attacks to assess whether attackers are predominantly based abroad or domestically.
- Investigate privacy perceptions among Saudi users to design more effective privacy solutions and awareness initiatives, potentially guiding future regulations.
- Conduct an in-depth study of SMS as a phishing medium to identify intervention points and disrupt common attack methods. Conversely, personal contact scams may require less focus, as this approach has shown a decline.
- Test the influence of authority and reciprocity tactics (e.g., "winning a prize" or "blocking a bank card") on phishing susceptibility and exploring additional social engineering methods for further insights.

Addressing these gaps can build a more robust understanding of phishing dynamics and enhance the effectiveness of preventive strategies.

Future research will include another cross-sectional study in 2026 to monitor progress, identify emerging trends, and validate our 2022 findings. This ongoing research aims to provide a deeper understanding of the evolving phishing landscape and assess the effectiveness of countermeasures within Saudi Arabia. Through this continuous effort, we aspire to support a safer digital environment for users by staying ahead of phishing trends.

References

A. Ferreira, J.-L. Huynen, V. Koenig, and G. Lenzini, "A conceptual framework to study socio-technical security," in Human aspects of information security, privacy, and trust, T. Tryfonas and I. Askoxylakis, Eds., Cham: Springer International Publishing, 2014, pp. 318–329.

A. N. Bank, "Security awareness." 2025. Available: https://anb.com.sa/en/web/anb/customers-guide-on-combating-fraud

Barracuda, 2025. Available: https://sentinel.barracudanetworks.com/

C. Hadnagy, Social engineering: The science of human hacking, 2nd ed. Wiley Publishing, 2018.

D. Aljeaid, A. Alzhrani, M. Alrougi, and O. Almalki, "An exploratory study: Assessing user security awareness of cybercrimes in Saudi Arabia," King Abdulaziz University, Computer; Information Technology College, 2019.

D. Aljeaid, A. Alzhrani, M. Alrougi, and O. Almalki, "Assessment of end-user susceptibility to cybersecurity threats in Saudi Arabia by simulating phishing attacks," Information, vol. 11, no. 12, p. 547, 2020, doi: 10.3390/info11120547.

E. A. Wilhelms and V. F. Reyna, "Predictors of risky decisions: Improving judgment and decision making based on evidence from phishing attacks," in Neuroeconomics, judgment, and decision making, Psychology Press, 2014, pp. 257–271.

E. Benavides, W. Fuertes, S. Sanchez-Gordon, and M. Sanchez, "Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review." Springer Singapore, pp. 51–64, Jan. 2020. doi: 10.1007/978-981-13-9155-2_5.

H. Abusaimeh and Y. Alshareef, "Detecting the phishing website with the highest accuracy," TEM Journal, vol. 10, no. 2, pp. 947–953, 2021, doi: 10.18421/TEM102-58.

J. Majumder, D. S. Gangopadhyay, and S. Biswas, "A cross sectional study on knowledge of cyber security among urban and semi urban college goers of east midnapore district," International Journal of Scientific and Technology Research, vol. 9, 2020.

M. Hathaway and F. Spidalieri, "Kingdom of Saudi Arabia cyber readiness at a glance," Potomac Institute for Policy Studies, 2017. Available: https://potomacinstitute.org/images/CRI/CRI2_0_SaudiArabiaPofile.pdf

M.-E. Maurer and L. Höfer, "Sophisticated phishers make more spelling mistakes: Using URL similarity against phishing," in Cyberspace safety and security, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 414–426.

N. Mugarura and E. Ssali, "Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system," Journal of Money Laundering Control, vol. ahead–of–print, pp. 10–28, Apr. 2020, doi: 10.1108/JMLC-11-2019-0092.

P. Institute, "Cyber readiness index (CRI)." 2017. Available: https://www.potomacinstitute.org/images/CRI/CRI2_0_SaudiArabiaPofile.pdf

R. B. Cialdini, Influence: The psychology of persuasion. Business Library, 1984. Available: https://books.google.com.sa/books?id=mJidPwAACAAJ

S. A. for Data and A. Intelligence, "Ehsan platform." 2025. Available: https://ehsan.sa/

S. A. led GCC in number of phishing attacks in Q2: Kaspersky report, "Gulf business." 2020. Available: https://gulfbusiness.com/saudi-arabia-led-gcc-in-number-of-phishing-attacks-in-q2-kaspersky-report/

S. A. National Cybersecurity Authority, "National cybersecurity authority." 2025. Available: https://nca.gov.sa/en

T. A.-P. W. Group, "Phishing activity trends report (2nd quarter 2022)," Docs.Apwg.Org, 2022. Available: https://docs.apwg.org/reports/apwg_trends_report_q2_2022.pdf

T. A.-P. W. Group, "Phishing activity trends report (3rd quarter 2018)," Docs.Apwg.Org, 2018. Available: https://docs.apwg.org/reports/apwg_trends_report_q2_2018.pdf

T. A.-P. W. Group, "Phishing activity trends reports," APWG, 2022. Available: https://apwg.org/trendsreports/

T. S. for Worldwide Interbank Financial Telecommunications, "How to spot, stop and defend against cyber-attacks," Swift, 2023. Available: https://www.swift.com/your-needs/financial-crime-cyber-security/financial-fraud/how-defend-against-cyber-attacks

T. W. Edgar and D. O. Manz, Research methods for cyber security. Syngress Publishing, 2017, pp. 1–404.